Level 3 Technical Level

IT: NETWORKING

A/507/6495

Unit 6: Network security management

Mark scheme

January 2019

Version: 1.0 Final

Mark schemes are prepared by the Lead Assessment Writer and considered, together with the relevant questions, by a panel of subject teachers. This mark scheme includes any amendments made at the standardisation events which all associates participate in and is the scheme which was used by them in this examination. The standardisation process ensures that the mark scheme covers the students' responses to questions and that every associate understands and applies it in the same correct way. As preparation for standardisation each associate analyses a number of students' scripts. Alternative answers not already covered by the mark scheme are discussed and legislated for. If, after the standardisation process, associates encounter unusual answers which have not been raised they are required to refer these to the Lead Assessment Writer.

It must be stressed that a mark scheme is a working document, in many cases further developed and expanded on the basis of students' reactions to a particular paper. Assumptions about future mark schemes on the basis of one year's document should be avoided; whilst the guiding principles of assessment remain constant, details will change, depending on the content of a particular examination paper.

Further copies of this mark scheme are available from aqa.org.uk

Copyright information

For confidentiality purposes acknowledgements of third-party copyright material are published in a separate booklet which is available for free download from www.aqa.org.uk after the live examination series.

Level of response marking instructions

Level of response mark schemes are broken down into levels, each of which has a descriptor. The descriptor for the level shows the average performance for the level. There are marks in each level.

Before you apply the mark scheme to a student's answer read through the answer and annotate it (as instructed) to show the qualities that are being looked for. You can then apply the mark scheme.

Step 1 Determine a level

Start at the lowest level of the mark scheme and use it as a ladder to see whether the answer meets the descriptor for that level. The descriptor for the level indicates the different qualities that might be seen in the student's answer for that level. If it meets the lowest level then go to the next one and decide if it meets this level, and so on, until you have a match between the level descriptor and the answer. With practice and familiarity you will find that for better answers you will be able to quickly skip through the lower levels of the mark scheme.

When assigning a level you should look at the overall quality of the answer and not look to pick holes in small and specific parts of the answer where the student has not performed quite as well as the rest. If the answer covers different aspects of different levels of the mark scheme you should use a best fit approach for defining the level and then use the variability of the response to help decide the mark within the level, ie if the response is predominantly level 3 with a small amount of level 4 material it would be placed in level 3 but be awarded a mark near the top of the level because of the level 4 content.

Step 2 Determine a mark

Once you have assigned a level you need to decide on the mark. The descriptors on how to allocate marks can help with this. The exemplar materials used during standardisation will help. There will be an answer in the standardising materials which will correspond with each level of the mark scheme. This answer will have been awarded a mark by the Lead Examiner. You can compare the student's answer with the example to determine if it is the same standard, better or worse than the example. You can then use this to allocate a mark for the answer based on the Lead Examiner's mark on the example.

You may well need to read back through the answer as you apply the mark scheme to clarify points and assure yourself that the level and the mark are appropriate.

Indicative content in the mark scheme is provided as a guide for examiners. It is not intended to be exhaustive and you must credit other valid points. Students do not have to cover all of the points mentioned in the Indicative content to reach the highest level of the mark scheme.

An answer which contains nothing of relevance to the question must be awarded no marks.

The following annotation is used in the mark scheme:

;	- means a single mark
//	- means alternative response
/	- means an alternative word or sub-phrase
A	- means acceptable creditworthy answer
R	- means reject answer as not creditworthy
NE	- means not enough
I	- means ignore

DPT - in some questions a specific error made by a candidate, if repeated, could result in the candidate failing to gain more than one mark. The DPT label indicates that this mistake should only result in a candidate failing to gain one mark on the first occasion that the error is made. Provided that the answer remains understandable, subsequent marks should be awarded as if the error was not being repeated.

Question	Guidance	Mark
01 **Option C**	**Mark is for AO2** sender or origin of an email **R.** more than one box ticked	**1**
02 **Option C**	**Mark is for AO1** packet filtering **R.** more than one box ticked	**1**
03 **Option D**	**Mark is for AO1** redirect users to a different computer **R.** more than one box ticked	**1**
04 **Option A**	**Mark is for AO3** a network set up to invite attack **R.** more than one box ticked	**1**
05 **Option D**	**Mark is for AO4** the rules a user must accept before accessing a network **R.** more than one box ticked	**1**

Question	Guidance	Mark
06	**Mark is for AO1** Maximum of 1 from: • **constantly changing** (to avoid detection); • it can **change** ACCEPT "**morph**" (to avoid detection); • it can **evolve** in a variety of ways (to avoid detection); **A.** Different wording with similar meaning	**1**
07.1	**Mark is for AO2** Maximum of 1 from: • uses the same key for all messages; • uses the same key for both encryption and decryption; • all parties involved have to exchange / have access to / know the key used to encrypt data (before they can decrypt their data); **A.** Any other creditable answer	**1**
07.2	**Mark is for AO2** Maximum of 1 from: • uses two different keys; • for encryption and decryption; • requires both a public and a private / secret key; • the private key is kept secret / is known only to the receiver; **A.** Any other creditable answer	**1**

Question	Guidance	Mark
08.1	**4 marks for AO3** 1 mark for each correct point or expansion point, up to a maximum of 4 marks: • user access // user access rights // user access denied; • unauthorised access // attempted intrusions // attempted attacks; **A.** attack or virus (1 mark) • an event is a change in system state; • one (change of state) could be disk failure; • event messages stored in the event log; • provides the network manager real-time information about the network // traffic sent, eg amount / destination / origin; • event information could also be analysed retrospectively // audit trail // troubleshooting; • the severity of the event is stored in the log; • automated processes help NM decide what action to take; • **A.** abnormalities / problems; Any other creditable answer	4
08.2	**2 marks for AO3** Maximum of 2 (no repetition, see 8.1) from: who did what and how did the system behave . . . • devices connected; • resources accessed; • destination address; • source address; • time, chronology // audit trail;; • user login / failed logins // (failed) unauthorised access; **A.** Any other creditable answer	2

09.1	**Mark is for AO3** Maximum of 1 from: • analyses the bus/network packet /IP load; • captures / decodes packets; **A**. intercepts / logs network traffic **A.** Any other creditable answer	**1**

09.2	**Mark is for AO3** Maximum of 1 from: • telecom network protocol analyser; • bus analyser; **A.** “packet sniffer; **A.** IP load tester // any reference to monitoring the router log effectively, etc; **A**. commercial names, eg **Wireshark,** Ethereal, Optiview Protocol Expert, Netasyst Network Analyzer etc; **A.** Any other creditable answer	**1**

Question	**Guidance**	**Mark**
10.1	**Mark is for AO1** Maximum of 1 from: • finding / measuring the severity of vulnerabilities in a system; • producing lists of / prioritising vulnerabilities in a system; **A.** different wording with similar meaning, eg testing the network // finding a weakness in the network // assessing how secure a network is (from attack to its weak spots);	**1**
10.2	**4 marks for AO1** 1 mark for each correct threat or expansion point, up to a maximum of 4 marks: each correct threat;; each expansion point;; **Examples include:**	**4**

	• **unmanaged assets** / transient, changing assets (eg mobile phones, VPN) // BYOD; • **unknown applications**, services / assets not patched to resist intrusion • **lack of network visibility** eg missing encrypted data // difficult for any one tool to monitor all suspicious traffic, blind spots inevitable; • **employee action & inaction** // non-malicious opening of malware / software / attachments // malicious engagement // (internal) rogue attacks / exploits; • **A.** spyware; • **A.** adware; **A.** Any other creditable answer	

10.3	**3 marks for AO1** Maximum of 3 from: • simulating a (real) attack; • testing weaknesses // finding pathways a (real) attacker might exploit; • identifying how a (real) attacker might breach existing defences; • reporting vulnerabilities // providing feedback about vulnerabilities in the network; **A.** ethical hacker; **A.** Any other creditable answer	**3**

10.4	**2 marks for AO3** Maximum of 2 from: • continuous monitoring is part of a **process** / the same process of which static monitoring is a part / detects compliance and risk; • continuous monitoring **informs** better security / does not provide better security in itself / transforms process / makes process **dynamic, real time** / collecting the right data at the right time // continuous monitoring does not in itself resolve security issues; • continuous monitoring contributes to the **automation** of existing tools making them more cost-effective, consistent, efficient **A.** Any other creditable answer	**2**

Question	**Guidance**	**Mark**
11.1	**2 marks for AO1** Maximum of 2 from:	**2**

	• (network) / (host-based) firewall;
	• IDS // IPS;
	
	A. anti-virus;
	A. demilitarized zone (DMZ);
	A. user authentication;
	
	A. Any other creditable answer	

11.2	**4 marks for AO3** Maximum of 4 from: • reference to customer or supplier testing shared systems; as an ethical hacker (perhaps using pen test or similar); before allowing customer or supplier full access to shared system; • reference to customer-supplier having different hardware/software/ operational standards; • responsibility in the event of breach // can't 'outsource responsibility'; **Other examples include:** • supplier-customer links / shared gateways open / risks and vulnerabilities / exposure / common approach desirable / mitigates risk • sharing analytics / log data / best practice • exchanging information / identifying common threats / vulnerabilities / threat intelligence / end point data • compare what is happening in the network with what is happening elsewhere • more data sources / more data ingress and egress / challenges more complex and diverse /common approach, shared approach likely to be more effective	**4**

Question	Guidance	Mark
12.1	**2 marks for AO4** Maximum of 2 from: • protect resources (against intrusion / leakage) // ensure safety of sensitive data; • from anyone using wireless media (to penetrate network); • through unsecured or unapproved (wireless) communication methods; • because of the explosion in the use of wireless devices; • to **secure / protect** the information assets of an organisation; by ensuring all users and devices adhere to the **same rules**; **A.** Different wording with similar meaning	**2**
12.2	**2 marks for AO4** Maximum of 2 from: who / what can access data // action data transfer . . . • all permanent employees / contractors / vendors / agents / visitors / guests; • all organisation owned / personally or privately-owned computers / workstations / laptops / smartphones / other device capable of connecting remotely to the network • all remote access connections; used to work for or on behalf of the organisation (including email and intranet); how they connect to organisation's network; common, minimum standards for authenticated connection // security, anti-virus, anti-malware, etc; • it covers standards for connecting to the organisation's network; including requirements for remote user's systems // and how they connect to the organisation's network; **A.** Different wording with similar meaning	**2**

12.3	**2 marks for AO4** Maximum of 1 from: • **business email -** organisation has obligations, responsibilities to ensure integrity and accessibility (eg archiving) of all organisation records / security of (commercially) sensitive business information that may be sent or received via email / email is customer-facing and organisation needs to ensure any, all email not delivered is forwarded for an appropriate response and ensure the customer knows this has been done // requirement to use business email for business // requirement not to use personal email for business; Maximum of 1 from: • **personal email -** personal, external accounts should not be used for business purposes / organisation has, accepts no responsibility for personal, external accounts / failure to restrict company business to business email may put business at risk	**2**

Question	Guidance	Mark
13	**6 marks for AO4** Maximum of 6 from: **1** mark for each step;;; 1 mark for each expansion;;; **Examples include:** • **information gathering**, gather background information / review and clarify client needs / providers confirm what is being offered, level of service appropriate and achievable • ensure agreement, **achieve a consensus** / what does client and what does provider see as (most) important to the agreement / what is possible, impossible / unable to proceed until agreement, consensus on what SLA is and what it is for achieved • **document what's been agreed**, write down rules for working together / who and how will issues be escalated, dealt with / what time constraints, limits are appropriate / what penalties, incentives will apply for failure to supply, or for excellence of service // response times; • develop the agreement, **negotiate**, see SLA as an (ongoing) process not an end in itself / further input and discussion by both sides / increasing familiarity with what is required will modify and refine final agreement (to the benefit of both parties) • educate to encourage commitment, understanding, value, **buy-in** /moving from discussion and draft to final copy and sign-off / final chance to raise questions, offer suggestions / approve and finalise // key-player engagement, training, etc; • **implement and manage**, measure performance, quantify quality / unlikely to succeed if not (actively) managed / (named) points of contact / service reviews, focussed and scheduled / coordinating and modifying post-service review improvements / feedback loops for ongoing improvements, who and when and how often • **cost,** what's included // what's not included // exceptional items // additional costs; **A.** defining the service / establishing service ownership	6

Question	Guidance	Mark
14	**6 marks for AO4** Maximum of 6 marks overall. Clear reference to either SECTION (content list) or ITEM (section content) is sufficient for each mark, eg: security access and control; that section should include BYOD // guests and visitors user permissions; Maximum 2 marks per row. **A.** similarly worded or other reasonable section names **R.** repeated points	6

Indicative content	
SECTION (max 3 marks)	ITEM (max 3 marks)
Overview of organisation	mission statement / objectives / priorities
Management controls	team / operational and tactical planning
Goals	business objectives
Risk management	risk assessment / threats / vulnerabilities
Audit and compliance	audit & event logging
Incident management	non-compliance / breaches /data protection
Training, education and awareness	permanent staff / guests and visitors / access control / permissions
Security and access controls	permanent staff / guests and visitors user permissions / BYOD / CYOD
Monitoring, measurement and reporting	audit & event logging
Asset identification and classification **A.** software / hardware	permanent staff / guests and visitors / BYOD / CYOD
Employee and guest account management practices	permanent staff / guests and visitors / access control / user

	permissions / BYOD / CYOD / security breaches /
Review cycle / key dates	business critical reviews / who, when / timeline

Question	Guidance	Mark
15	**9 marks for AO2**	9

Level	Descriptor	Marks
3	Candidate clearly explains how both IPS and IDS contribute to a network security system using two or more appropriate examples	7-9
2	Candidate makes some appropriate comparison of both IPS and IDS, or clearly explains how one contributes to a network security system giving at least one appropriate example.	4-6
1	Candidate gives a general description of either IPS or IDS but not both.	1-3
No creditworthy content		0

Indicative content

IDS considered passive / monitors packets, port traffic v configured rules (anomaly based detection), approved traffic (signature-list based detection) / raises alarm as necessary; records incidents logged; documents existing threats; identifies problems with existing security policy and violations of existing security policy; shortcoming, needs to be regularly 'tuned' as new threats abound

IPS considered active, an improvement, a step beyond IDS / monitors a network for malicious activity and / or activity in violation of existing policy; it acts; can shutdown malicious activity, terminating a connection or user account or IP address; can block all access to targeted host, service, or application / can reconfigure other security controls (firewall, router) / can remove malicious content, eg removing an attachment before forwarding an email

IDS and IPS do different jobs and are active at different points of the network, both should therefore be used, and used concurrently / IDS could be used at the perimeter, more often sits inside the firewall / IDS and IPS often now

	supplied as one product, in one box	

Question	Guidance	Mark
16	**9 marks for AO2**	9

Level	Descriptor	Marks
3	Candidate clearly explains how effective NAC is and clearly explains how NAC secures access to a network and makes some effort to suggest how next generation NAC might protect the network more effectively.	7-9
2	Candidate makes some attempt to explain how effective NAC is and clearly explains how NAC secures access to a network.	4-6
1	Candidate gives a general description of how NAC secures access to a network	1-3
	No creditworthy content	0

Indicative content:

DEFINITION: restricts access to end-point devices to only those that comply with defined security policy

DISCUSSION:
without NAC, organisation dependent on the honesty of employees / guests in complying with BYOD policy; NAC can monitor BYOD devices, identifying those authorised for access and denying those coming from risky connection; with NAC, organisation has a comprehensive view of all devices connected to network / capability of discovering all devices connected to network / fingerprinting and profiling / authorising and excluding
Administrator is in control; defines access policies and determines users and devices connecting to network
NAC continuous monitoring / logs patterns of behaviour / detects malicious behaviour

NEXT GENERATION NAC
Policy enforcement, authenticate and authorise approved devices, users / dependent upon an inventory of authorised and unauthorised device / identification and management of end points / identifying devices connected to network / compliance and non-compliance
Device, user, requests access to a network, request approved or denied / works well with a fixed, static list
3.802.1X, IEEE standard, used to authenticate BYOD, CYOD, visitors, guest access, unknown hosts / next generation NAC is able to determine security standard of endpoint device to allow or deny access / real time discovery, classification, authentication BEFORE connection to network protects network, mitigates vulnerabilities

Question	Guidance	Mark
17.1	**6 marks for AO1** Maximum of 6 marks overall. Maximum of 3 from: **exposure:** • a mistake in code or configuration; • gives indirect access to a system or network; • could allow an attacker to (covertly) gather customer information that could be sold; • data / security leak; Maximum of 3 from: **exploit:** • attacker takes advantage of a **known** vulnerability, weakness; turning that vulnerability or weakness into a breach; • critics argue using CVE (eg known vulnerabilities); attackers often strike before deployment of available software patch or following a failure to install patch; • zero-day exploits are vulnerabilities about which vendors are unaware; • WannaCry successful because vulnerability (in MS version of SMB protocol) not highlighted / not patched; • other expansion point;; **R.** repeated points	**6**

17.2	**6 marks for AO1** Maximum of 6 from: Possible **high risk**; + 1 mark for any correct point • employee unlikely to have any loyalty to business; • little interest in continued success of current business; • may even feel grievance or malice towards business; • may be intent on causing harm before leaving eg knowingly clickiing on malicious email; **insider with ready, easy access**; + 1 mark for any correct point • has authenticated credentials; • has user account and authenticated access; **organisation risks loss of integrity/reputation/trust;** + 1 mark for any correct point (high profile) data breach might generate lots of adverse publicity; loss of (personal) data // data leak // expose data to the public, media, others (usernames, passwords, personal information, payroll, sales, commercial, strategic); might generate lots of adverse publicity AND legal action / GDPR 2018; **R.** repeated points	**6**

Assessment Outcomes					
Question	**AO1**	**AO2**	**AO3**	**AO4**	**Question Total**
SECTION A					
1		2e (1)			**1**
2	1b (1)				**1**
3	1c (1)				**1**
4			3c (1)		**1**
5				4a (1)	**1**
6	1c (1)				**1**
7.1		2b (1)			**1**
7.2		2b (1)			**1**
8.1			3b (4)		**4**
8.2			3b (2)		**2**
9.1			3c (1)		**1**
9.2			3c (1)		**1**
10.1	1b (1)				**1**
10.2	1b (3)				**3**
10.3	1b (4)				**4**
10.4			3a (2)		**2**
11.1	1b (2)				**2**
11.2			3a (4)		**4**
12.1				4a (2)	**2**
12.2				4a (2)	**2**
12.3				4a (2)	**2**
13				4b (6)	**6**
14				4b (6)	**6**
Total A	**13**	**3**	**15**	**19**	**50**
SECTION B					
15		2a (9)			**9**
16		2c (9)			**9**
17.1	1c (6)				**6**
17.2	1c (6)				**6**
Total B	**12**	**18**	**0**	**0**	**30**
Total A+B	**25**	**21**	**15**	**19**	**80**