

2

Analyse und Entwicklung
von Netzwerken

Teil 2 der Abschlussprüfung

Allgemeine Korrekturhinweise

Die Lösungs- und Bewertungshinweise zu den einzelnen Handlungsschritten sind als Korrekturhilfen zu verstehen und erheben nicht in jedem Fall Anspruch auf Vollständigkeit und Ausschließlichkeit. Neben hier beispielhaft angeführten Lösungsmöglichkeiten sind auch andere sach- und fachgerechte Lösungsalternativen bzw. Darstellungsformen mit der vorgesehenen Punktzahl zu bewerten. Der Bewertungsspielraum des Korrektors (z. B. hinsichtlich der Berücksichtigung regionaler oder branchenspezifischer Gegebenheiten) bleibt unberührt.

Zu beachten ist die unterschiedliche Dimension der Aufgabenstellung (nennen – erklären – beschreiben – erläutern usw.).

Für die Bewertung gilt folgender Punkte-Noten-Schlüssel:

Note 1 =	100 – 92 Punkte	Note 2 =	unter	92 – 81 Punkte	
Note 3 =	unter	81 – 67 Punkte	Note 4 =	unter	67 – 50 Punkte
Note 5 =	unter	50 – 30 Punkte	Note 6 =	unter	30 – 0 Punkte

1. Aufgabe (24 Punkte)

aa) 2 Punkte

Router, Schnittstelle	IP-Adresse
R-Rusticus-ext, ETH	203.0.113.65
R-Rusticus-int, ETH0	203.0.113.70

ab) 8 Punkte

Netzwerk-ID	Subnetzmaske	Schnittstelle oder Next-Hop
203.0.113.64	255.255.255.248	ETH
198.51.100.0	255.255.255.252	LWL
10.0.0.0	255.0.0.0	203.0.113.70
0.0.0.0	0.0.0.0	198.51.100.1

b) 4 Punkte

SPI sorgt dafür, dass Antworten für erlaubten Traffic für einen bestimmten Zeitraum automatisch ebenfalls die Firewall passieren dürfen, ohne dass der Admin dafür manuell Regeln aufstellen muss.

Andere Formulierungen möglich.

c) 10 Punkte (2 Punkte pro korrekter Regel)

Aktion	Protokoll	Quelle	Ziel	Quellport	Zielpport	Von Interface	Nach Interface
Permit	TCP	any	203.0.113.67/32	any	80	LWL	ETH
Permit	TCP	any	203.0.113.67/32	any	443	LWL	ETH
Permit	TCP	any	203.0.113.68/32	any	25	LWL	ETH
Permit	TCP	any	203.0.113.68/32	any	143	LWL	ETH
Deny	IP	any	any				

2. Aufgabe (23 Punkte)

a) 3 Punkte

Der Client hat keine IP-Adresse für `www.google.de` zwischengespeichert, darum muss erst die IP-Adresse für `www.google.de` abgefragt werden.

Andere Antworten sind möglich.

b) 4 Punkte

(In Zeile 126 wird ein **A** Eintrag (**IPv4**) über einen IPv6-DNS-Server abgefragt. Die Antwort kommt mit Frame No. 132. Der relevante Rückgabewert ist in INFO enthalten:)

..... **A www.google.de A 142.250.184.227**

c) 4 Punkte

IPv4: **10.0.0.101** (2 Punkte)

IPv6: **2001:db8:3726:1a00:70cd:9f70:a8a8:4627** (2 Punkte)

d) 3 Punkte

fd00::7642:7fff:fe0c:62f7 (Die einzige neben der des Clients genutzten lokalen Adresse (8.8.4.4) ist öffentlich und nicht lokal.)

e) 3 Punkte

Die Antwort mit der Adresse `2a00:1450:4016:809::2003` ist erst nach dem abgesendeten ICMPv6-request eingetroffen. Der Zeitstempel (Time) ist höher, also später in der Zeit angesiedelt.

f) 3 Punkte

128 – 118 = 10

(Hinweis: Gesendet werden icmp Nachrichten i. d. R. mit einem hop limit von 128. Beim Durchlaufen des Pakets in einem Router wird das hop limit um 1 erniedrigt.

In der ping-Antwort (Echo reply Paket 135) ist das hop limit mit 118 angegeben.

Die Differenz beträgt 10.)

g) 3 Punkte

- Lastverteilung über DNS
- Es wurden unterschiedliche DNS-Server angefragt (IPv4 und IPv6).
- Der lokale IPv6-DNS-Server (Forwarder) hat andere (ältere) DNS-Einträge zwischengespeichert.
- Der öffentliche IPv4-DNS-Server (8.8.4.4) hat andere (neuere) DNS-Einträge.
- Der lokale DNS-Server nutzt weitere DNS-Forwarder (z. B. beim Provider) für DNS-Abfragen.

Weitere Antworten sind möglich.

3. Aufgabe (27 Punkte)

a) 4 Punkte

- Authentifizierung des Servers beim Client
- Vertraulichkeit der übertragenen Daten
- Schutz der übertragenen Daten vor Manipulation

b) 9 Punkte

Nachteile von TLS 1.2:

- TLS1.2 lässt Schlüsseltausch ohne PFS zu
- TLS1.2 enthält veraltete kryptografische Bibliotheken
- TLS1.2 lässt Teile des Handshakes unverschlüsselt
- TLS1.2 ermöglicht Angriffe durch „session resumption“

Andere Antworten sind möglich, auch möglich: Vorteile von TLS 1.3 nennen.

c) 6 Punkte

Intern:

- Eigene Kontrolle über Root-Keys
- Kontrolle des Verfahrens
- Ausstellen von neuen Zertifikaten sofort möglich

Weitere Antworten sind möglich.

Extern:

- Wahrscheinlich mehr Erfahrung bei externem Anbieter
- Keine eigene Infrastruktur notwendig
- Hinterlegen der public-keys der CA erfolgt über SW-Updates

Weitere Antworten sind möglich.

d) 8 Punkte

1. einfach zu implementieren; Anmeldung ist von beliebigen Endgeräten aus möglich
2. 2FA; Anmeldung lediglich an Geräten möglich, die über die Zertifikatsdatei verfügen
3. 2FA; 2ter Faktor an Hardware (= Besitz) gebunden
4. 2FA, keine Anschaffungskosten für zweiten Faktor, einfacher zu implementieren, da jeder User die App selbst installieren kann

Andere Antworten sind möglich.

4. Aufgabe (26 Punkte)

a) 5 Punkte

Berechnung:

Fünf Gespräche intern = 10 Teilnehmer * 64 kBit/s = 640 kBit/s (2 Punkte)

Fünfzehn Gespräche Extern = 15 Teilnehmer * 64 kBit/s = 960 kBit/s (2 Punkte)

Zusammen 1.600 kBit/s * 1,1 (Overhead) = 1.760 kBit/s (1 Punkt)

Folgefehler berücksichtigen, andere Rechenwege sind möglich.

ba) 3 Punkte

Das bedeutet, wenn die Bandbreite unzureichend ist, priorisiert die Software Audio-Qualität höher als Video-Qualität.

bb) 3 Punkte

Video-Layout, Video-Auflösung, und Video frames per second (fps)

c) 2 Punkte

10 * 2.500 kbit/s upload = 25.000 kbit/s

10 * 4.000 kbit/s download = 40.000 kbit/s

d) 4 Punkte

Maßgeblich ist das Download-Limit des ADSL-Anschlusses.

$$34 \text{ MiB/min} * 5 \text{ min} = 170 \text{ MiB}$$

$$170 \text{ MiB} * 1.024 \text{ (KB pro MB)} = 174.080 \text{ KiB} * 1.024 \text{ (Byte pro KB)} = 178.257.920 \text{ Byte} * 8 \text{ Bit pro Byte} = 1.426.063.360 \text{ Bit}$$

$$1.426.063.360 \text{ Bit} / 16.000.000 \text{ Bit/s} = 89,12896 \text{ Sek.} = 90 \text{ Sek.}$$

Berechnung und Ergebnis 90 Sek.

e) 4 Punkte

Quality of Service priorisiert die Daten von Echtzeitanwendungen. Auswirkungen: weniger Störungen, weniger Aussetzer, andere Antworten möglich.

f) 5 Punkte

VoIP ist auf Sprachübertragung optimiert, nicht auf Datenübertragung. Ein Sprach-Codec muss ggf. Datenverlust ausgleichen können, was bei Sprache ungehört bleibt, bei Fax aber zum Abbruch der Übertragung führen kann.

Weitere Lösungen sind möglich.