

Familienname, Vorname (bitte durch eine Leerspalte trennen)

[illegible]

Fach		Berufsnummer				IHK-Nummer			Prüfungsnummer			
5	5	1	1	9	7							
Sp. 1-2		Sp. 3-6				Sp. 7-14						

IHK

1197

Punkte 1. Handlungsschritt Punkte 2. Handlungsschritt Punkte 3. Handlungsschritt Punkte 4. Handlungsschritt Punkte 5. Handlungsschritt

Spalte 1 - 14 s. o.	15 16	17 18	19 20	21 22	23 24
---------------------------	-------	-------	-------	-------	-------

Gesamtpunktzahl		
26	27	28

Prüfungszeit

25

Die entsprechende Ziffer (1, 2 oder 3) finden Sie in der Abfrage nach der Prüfungszeit im Anschluss an die letzte Aufgabe

Prüfungsort, Datum

Unterschrift

Ausschluss, der Entsprechung § 40 Berufsordnungsgesetz zusammengefasst ist, beschlossen.
Die Vervielfältigung, Verbreitung und öffentliche Wiedergabe der Prüfungsaufgaben und Lösungen ist nicht gestattet. Zuwiderhandlungen werden zivil- und strafrechtlich (§§ 97 ff., 106 ff. UrhG) verfolgt. – © ZPA Nord-West 2011 – Alle Rechte vorbehalten!

Die Handlungsschritte 1 bis 5 beziehen sich auf die folgende Ausgangssituation:

Sie sind Mitarbeiter/-in in der IT-Abteilung der Taliko AG, einem Zulieferer der Automobilbranche.

Die IT-Abteilung erhielt den Auftrag, die IT-Infrastruktur der Taliko AG zu reorganisieren.

Im Rahmen dieses Projekts sollen Sie folgende Aufgaben erledigen:

1. Zugangskonzept erstellen und erläutern
2. Firewall analysieren
3. Massenspeicher konfigurieren
4. IPv6-Fähigkeit prüfen
5. Sicherheitslücken im Netzwerk schließen

1. Handlungsschritt (25 Punkte)

Die Mitarbeiter/-innen der Taliko AG sollen sich von privaten Computern oder von Extranet-Client-PCs in das Intranet einwählen können.

- Die Anmeldung erfolgt über einen Zugangsserver (RAS).
- Die Benutzerverwaltung erfolgt mit einem RADIUS-Server (UNIX-Rechner), auf dem eine Datenbank mit Benutzerdaten installiert ist.
- Bei jedem Einwählversuch schickt der Zugangsserver eine RADIUS-Anfrage mit Username und Passwort (Check Items) zur Überprüfung an den RADIUS-Server. Stimmen die Angaben, wird der Zugang zum Netz gewährt. Andernfalls wird die Einwahl abgelehnt, und der Zugangsserver trennt die Verbindung.

a) Erstellen Sie einen vereinfachten Plan der Netzwerkstruktur mit allen genannten Komponenten.

(8 Punkte)

b) Der RADIUS-Server ist ein sogenannter AAA-Server.

Erläutern Sie, wofür AAA steht und was es bedeutet.

(6 Punkte)

c) Bei der Kommunikation zwischen Client und Server werden auf jeder Seite Sockets erzeugt.

ca) Nennen Sie die beiden Komponenten, die einen Socket eindeutig identifizieren.

(2 Punkte)

cb) Erläutern Sie kurz die Bedeutung von Sockets als Bestandteil der Client-Server-Kommunikation.

(4 Punkte)

cc) Beim Aufbau einer Kommunikation wenden Client und Server bestimmte Methoden an.

Markieren Sie mit X in folgender Tabelle, welche Methode vom Server und/oder Client angewendet wird.

(5 Punkte)

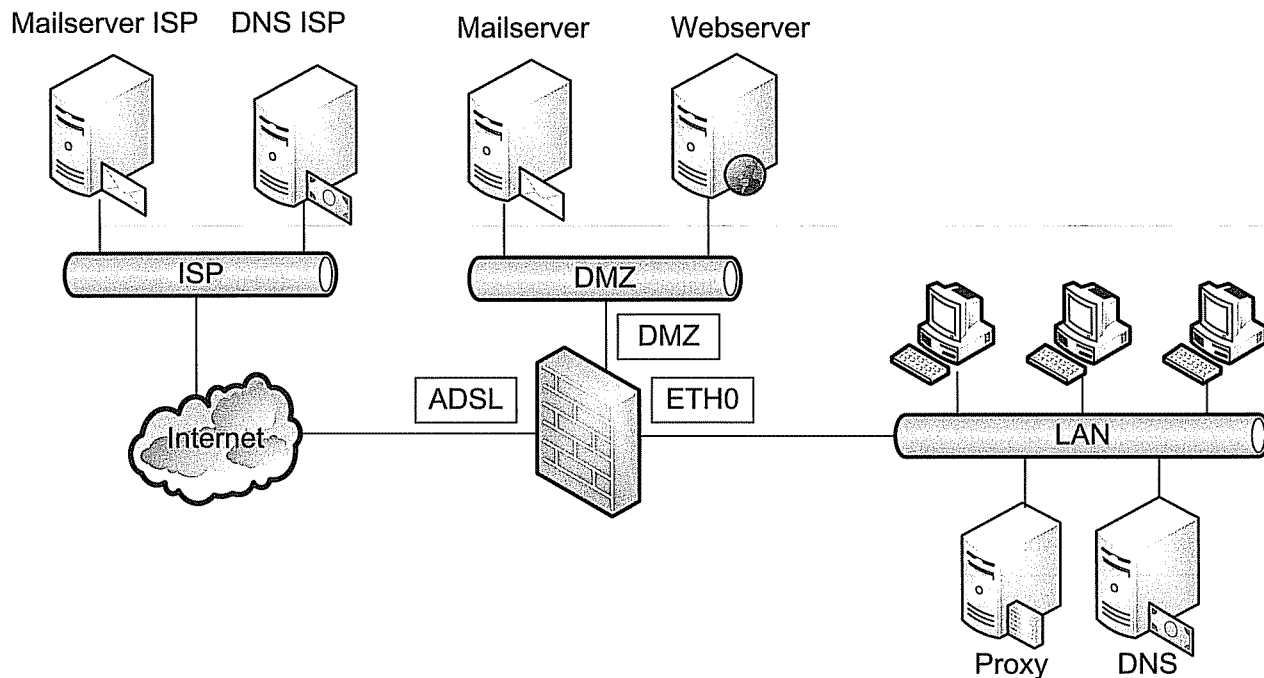
Methode	Server	Client
Bind	X	X
Listen		
Accept		
Connect		
Send		
Receive		
Close	X	X

2. Handlungsschritt (25 Punkte)

Korrekturrand

Im Rahmen der Reorganisation der IT-Infrastruktur der Taliko AG sollen Sie den Regelsatz der Firewall erläutern und erweitern.

Netzplan der Taliko AG



a) Die Firewall arbeitet nach dem Prinzip der Stateful Packet Inspection.

Erläutern Sie das Funktionsprinzip einer Stateful Packet Inspection Firewall.

(4 Punkte)

b) Nennen Sie die beiden Schichten (Name und Nummer) des OSI-Referenzmodells, auf denen eine SPI-Firewall arbeitet. (1 Punkt)

c) Auf der Firewall ist der folgende Regelsatz aufgestellt:

Nr.	Protokoll	Quell-IP	Ziel-IP	Quell-Port	Ziel-Port	Interface	Richtung	Aktion
1	TCP	Any	WebserverDMZ	> 1023	80	ADSL	IN	Accept
2	TCP	Any	WebserverDMZ	> 1023	443	ADSL	IN	Accept
3	TCP	MailserverISP	Mailserver	> 1023	25	ADSL	IN	Accept
4	TCP	Mailserver	MailserverISP	> 1023	25	DMZ	IN	Accept
5	TCP	Proxy	Any	> 1023	80	ETH0	IN	Accept
6	TCP	Proxy	Any	> 1023	443	ETH0	IN	Accept
7	IP	Any	Any	–	–	Any	Any	Deny

Formulieren Sie die Regeln 2 bis 7 (siehe Beispiel).

(6 Punkte)

Korrekturrand

Nr.	Regel
1	Beispiel: Verbindungsanfrage eines Internet-Clients zum Webserver für http weiterleiten
2	
3	
4	
5	
6	
7	

d) Der Regelsatz der Firewall soll erweitert werden:

- Die Clients im LAN sollen Mails zum internen Mailserver senden bzw. von ihm abrufen können.
- Die Namensauflösung durch den DNS soll möglich sein.

Ergänzen Sie die Regeln 7 bis 9.

(6 Punkte)

Nr.	Protokoll	Quell-IP	Ziel-IP	Quell-Port	Ziel-Port	Interface	Richtung	Aktion
1	TCP	Any	WebserverDMZ	> 1023	80	ADSL	IN	Accept
2	TCP	Any	WebserverDMZ	> 1023	443	ADSL	IN	Accept
3	TCP	MailserverISP	Mailserver	> 1023	25	ADSL	IN	Accept
4	TCP	Mailserver	MailserverISP	> 1023	25	DMZ	IN	Accept
5	TCP	Proxy	Any	> 1023	80	ETH0	IN	Accept
6	TCP	Proxy	Any	> 1023	443	ETH0	IN	Accept
7								
8								
9								
10	IP	Any	Any	–	–	Any	Any	Deny

Fortsetzung 2. Handlungsschritt →

ea) Erläutern Sie die Aufgabe des Splitters und des Modems bei einer ADSL-Anbindung. (4 Punkte)

eb) Ein Client verschickt eine E-Mail einschließlich Anhang mit der Größe von 3 MiB.
Berechnen Sie die Zeit, die für die Übertragung nötig ist. Der Rechenweg ist anzugeben. (4 Punkte)

[illegible]

Zur Datenspeicherung soll eine SAN-Box eingerichtet werden.

aa) Vervollständigen Sie nachfolgende Tabelle, indem Sie zu jedem Parameter eine entsprechende Maßeinheit angeben. (4 Punkte)

Parameter	Maßeinheit
Cache-Size	MiB
Rotational Speed	
Average Seek Time	
Form factors	
Mean time between failures	
Operating Temperature	
Interface Speed	
Limited Warranty	
Audible noise	

Dieses **Konzeptpapier** ist zur Eintragung von Nebenrechnungen und sonstigen Hilfsaufzeichnungen gedacht. Es muss vor Bearbeitung der Aufgaben dem Aufgabensatz entnommen werden. Bitte beachten Sie, dass Ihre Eintragungen **auf diesem Konzeptpapier** grundsätzlich nicht bewertet werden.



A series of horizontal lines for writing, spanning the width of the page below the header.

[illegible]

Handwriting practice lines consisting of 20 horizontal lines.

Handwriting practice lines consisting of 20 horizontal lines.

ab) In der Tabelle unter aa) sind neben der Bauform („Form factors“) vier weitere Parameter aufgeführt, die keinen Einfluss auf die Performance einer Festplatte haben.

Korrekturrand

Nennen Sie diese vier Parameter in Deutsch.

(4 Punkte)

ac) Zu einer Festplatte fehlt die Kapazitätsangabe. Gegeben ist jedoch die Angabe „*Guaranteed Sectors: 976,773,168*“.

Ermitteln Sie die Kapazität der Festplatte in GiB. Der Rechenweg ist anzugeben.

(3 Punkte)

[illegible]

b) Der RAID-Controller der SAN-Box unterstützt die RAID-Level: 0, 1, 5, 6, 10, 50, 60.

Die SAN-Box ist mit zehn identischen Festplatten ausgestattet. Die Kapazität jeder Festplatte beträgt 300 GiB.

ba) Nennen Sie den RAID-Level, der keine Redundanz unterstützt.

(1 Punkt)

bb) Ermitteln Sie rechnerisch die vom RAID-Controller unterstützten RAID-Level, mit denen sich ein redundantes Volumen von mindestens 2.300 GiB Netto-Speicherkapazität einrichten lässt.

Der Rechenweg ist anzugeben.

(6 Punkte)

[illegible]

bc) Während der Installation des Betriebssystems soll der Speicherort für die Auslagerungsdatei gewählt werden.

Erläutern Sie, warum es nicht sinnvoll ist, die Auslagerungsdatei im RAID-Volumen anzulegen.

(3 Punkte)

bd) Das RAID-System unterstützt „hotspare“ und „hotplug“.

Erläutern Sie die beiden Begriffe.

(4 Punkte)

hotspare

hotplug

4. Handlungsschritt (25 Punkte)

Die Taliko AG möchte ihr LAN für IPv6 vorbereiten. Sie sollen das bestehende LAN auf IPv6-Fähigkeit testen.

a) In einem englischen Handbuch zur IPv6 werden folgende Fachbegriffe erläutert.

Geben Sie die Erläuterungen jeweils sinngemäß in Deutsch wieder.

aa) Link local address (FE80/10): This address is found on each IPv6 interface after stateless auto-configuration.

Packets using link-local addressing will never pass a router.

(3 Punkte)

ab) Site local address (FEC0/10): An identifier for a network or host. Can be used to build a private network, like the private network address space (10.x.x.x) in Ipv4.

(3 Punkte)

ac) Global Unicast Address (2000/3): This address is the analogue of the normal IPv4 Addresses. Identified an Unique Interface.

(3 Punkte)

ad) 6to4 tunneling is a mechanism that allows IPv6-hosts, -sites or -networks to communicate across the IPv4 Internet. The local node encapsulates the IPv6 traffic with an IPv4 header and sends it to another 6to4 node over the IPv4 Internet. On this site the IPv4 header will be removed and the IPv6 traffic will be send to the destination node using the IPv6 network infrastructure.

(3 Punkte)

- b) In einem vorhanden Testnetz wurden zwei Systeme mit IPv6 konfiguriert. Mit einem Protokollanalyser wurden die folgenden zwei IP-Pakete aufgezeichnet.

Trace 1

```
60 00 00 00 00 40 3A 40 FE C0 01 01 00 00 00 00
00 00 AF C1 00 B8 00 51 FE C0 00 03 00 00 00 00
00 00 00 BE FE 30 01 F0 81 00 A4 6B 0C 1C 00 41
52 0F 36 47 9F 89 0C 00 08 09 0A 0B 0E 0F 10 11
...
```

Trace 2

```
45 00 00 54 A1 1B 00 00 41 01 55 52 C0 A8 01 02
C0 A8 01 E9 00 00 9B E3 3F 1C 00 09 24 13 36 47
D5 98 0D 00 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13
14 15 16 17 18 19 1A 1B 1C 1F 20 21 22 23 24 25
...
```

IPv6 – Header

Version (4bit)	Traffic Class (8bit)	Flow Label (20bit)			
Payload length (16bit)		Next Header (8bit)		Hop Limit (8bit)	
Source Address (128bit)					
Destination Address (128bit)					

- ba) Bestimmen Sie den Trace mit dem IPv6 Paket.

(1 Punkt)

- bb) Nennen Sie die IPv6 Senderadresse.

(2 Punkte)

- bc) Nennen Sie die IPv6 Empfängeradresse.

(2 Punkte)

Fortsetzung 4. Handlungsschritt →

-
- The screenshot shows the 'Eigenschaften von Internetprotokoll Version 6 (TCP/IPv6)' dialog box with the 'Allgemein' tab selected. The text explains that IPv6 settings can be automatically assigned if the network supports it, or manually configured by the network administrator. Two radio buttons are present: 'IPv6-Adresse automatisch beziehen' (unselected) and 'Folgende IPv6-Adresse verwenden:' (selected). The second option is followed by a group box containing three text input fields: 'IPv6-Adresse:', 'Subnetzpräfixlänge:', and 'Standardgateway:'. Below this, another set of radio buttons is shown: 'DNS-Serveradresse automatisch beziehen' (unselected) and 'Folgende DNS-Serveradressen verwenden:' (selected). This is followed by another group box with two text input fields: 'Bevorzugter DNS-Server:' and 'Alternativer DNS-Server:'. At the bottom left, there is a checkbox 'Einstellungen beim Beenden überprüfen' which is unchecked. At the bottom right, there is an 'Erweitert...' button. The very bottom of the window features 'OK' and 'Abbrechen' buttons.
- Eigenschaften von Internetprotokoll Version 6 (TCP/IPv6)**
- Allgemein**
- IPv6-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den Netzwerkadministrator, um die geeigneten IPv6-Einstellungen zu beziehen.
- ☐ IPv6-Adresse automatisch beziehen
- ☒ Folgende IPv6-Adresse verwenden:
- IPv6-Adresse:
- Subnetzpräfixlänge:
- Standardgateway:
- ☐ DNS-Serveradresse automatisch beziehen
- ☒ Folgende DNS-Serveradressen verwenden:
- Bevorzugter DNS-Server:
- Alternativer DNS-Server:
- ☐ Einstellungen beim Beenden überprüfen
- Erweitert...
- OK Abbrechen

[illegible]

5. Handlungsschritt (25 Punkte)

Korrekturrand

Obwohl die Firewall der Taliko AG erneuert wurde und ein Proxy mit Virenschanner zum Einsatz kommt, gelangen trotzdem Trojaner aus dem Internet in das LAN.

- a) Erläutern Sie zwei Aufgaben, die der Proxy im LAN der Taliko AG außer dem Virenschanner übernehmen kann. (4 Punkte)

- b) Bei einem der folgenden Ports kann der Inhalt der Daten weder durch eine Firewall noch durch einen Virenschanner überprüft werden.

Offener Port	Bedeutung
20	FTP
21	FTP
25	SMTP
53	DNS
80	http
110	POP3
143	IMAP
443	HTTPS

- ba) Erläutern Sie, warum eine Überprüfung der Daten mit Firewall oder Virenschanner an diesem Port nicht möglich ist. (3 Punkte)

- bb) Nennen Sie zwei typische Anwendungen, die diesen Port nutzen. (2 Punkte)

- c) Erläutern Sie zwei Maßnahmen, mit denen die Sicherheitslücke geschlossen werden kann. (6 Punkte)

Fortsetzung 5. Handlungsschritt →

Fortsetzung 5. Handlungsschritt

Korrekturrand

- d) Erläutern Sie das Handshake-Protokoll beim Verbindungsaufbau über HTTPS. Beginnen Sie mit „Der Client kontaktiert den Server und schickt ihm Verschlüsselungsparameter“.
- (10 Punkte)

PRÜFUNGSZEIT – NICHT BESTANDTEIL DER PRÜFUNG!

Wie beurteilen Sie nach der Bearbeitung der Aufgaben die zur Verfügung stehende Prüfungszeit?

- ☐ 1 Sie hätte kürzer sein können. ☐ 2 Sie war angemessen. ☐ 3 Sie hätte länger sein müssen.

☐