Abschlussprüfung Winter 2008/09

Lösungshinweise

1. Handlungsschritt (20 Punkte)

aa) 2 Punkte

- Bandbreite
- Verfügbarkeit
- Verzögerungszeit
- Fehlerrate
- Geräteinteroperabilität (z. B. VPN Gateways)
- u. a.

ab) 3 Punkte, 3 x 1 Punkt

A: end to site
B: end to end
C: site to site

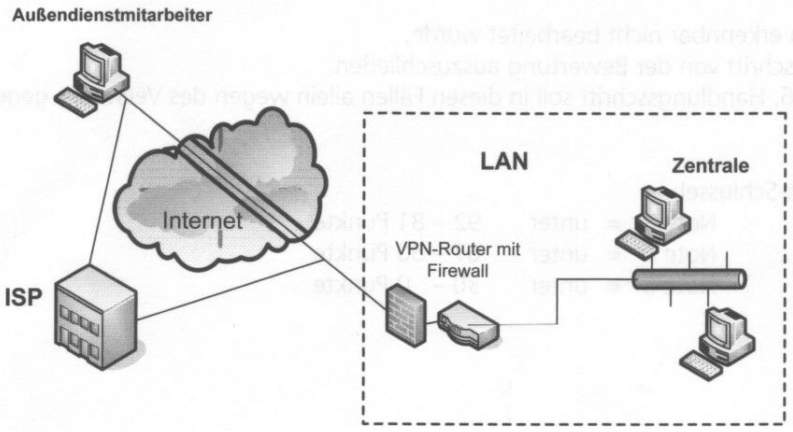
ac) 4 Punkte

end to site: Mobile Geräte der Außendienstmitarbeiter werden durch Remote Access VPN mit dem LAN der Zentrale verbunden.

b) 5 Punkte

- Anzahl der mobilen Anschlüsse (per UMTS u. a.)
- Anzahl der stationären Anschlüsse
- Art der VPN-Komponenten
- Art des VPN-Gateway
- Sicherheitsniveau der Übertragung
- VPN-Protokoll
- Art der Software für Remote PC
- Art der Authentifizierung gegenüber dem zentralen VPN-Gateway
- Endpoint Security
- Art und Weise der Aktualisierung der Personal Firewall
- u. a.

c) 4 Punkte



Auch andere Lösungen, z. B. mit RADIUS Server beim ISP oder im LAN, sind möglich.

d) 2 Punkte

Authentisierungsmöglichkeiten:

- Zertifikate (wie PKI, X.509v.3)
- Zertifikate auf Smartcards
- User-ID/Password (RADIUS)
- SecureID
- OTP (One Time Password)
- VPN-Client-Software mit Sicherheits-Policy

2. Handlungsschritt (20 Punkte)

aa) 5 Punkte

Der Konfigurationsassistent des IPSec VPN Client ermöglicht die Konfiguration in drei einfachen Schritten bei der Einrichtung des Remote Computers, der sich über ein VPN Gateway in ein Firmennetzwerk (LAN) verbinden soll.

ab) 2 Punkte

Hier wird der Typ des VPN Endpunktes angegeben.

ac) 3 Punkte

- Die externe IP- oder DNS-Namen des zu erreichenden VPN Gateways
- Der Preshared Key für diese Tunnelverbindung
- Die interne IP-Adresse des Netzwerks (LAN) hinter dem VPN Gateway (z. B. 192.168.1.0)

ba) 8 Punkte, 4 x 2 Punkte

192.168.1.0 - 192.168.1.63

192.168.1.64 - 192.168.1.127

192.168.1.128 - 192.168.1.191

192.168.1.192 - 192.168.1.255

bb) 2 Punkte

255.255.255.192 bzw. 192.168.1.0/26

3. Handlungsschritt (20 Punkte)

aa) 4 Punkte; 2 x 2 Punkte

- DoS (Denial of Service): Angriff auf einen Rechner in einem Datennetz mit dem Ziel, einen oder mehrere seiner Dienste arbeitsunfähig zu machen.
- DDoS (Distributed DoS): Der Angriff erfolgt koordiniert von einer größeren Anzahl von Systemen aus.

ab) 2 Punkte

- IDS-System (XXX): Hardware und/oder Software zur Erkennung von Angriffen auf ein Computersystem oder Computernetz.
- SPI-Firewall (Staful Packet Inspection): Analyse von Datenpaketen hinsichtlich bestimmter Kriterien und ggf. Verhinderung der Weiterleitung

ba) 2 Punkte

- DHCP-Server können IP-Adressen und damit im Zusammenhang stehende Informationen zentral verwalten.
- Mit dem DHCP-Server erfolgt die dynamische Zuweisung einer IP-Adresse und weiterer Konfigurationsparameter an Clients in einem Netzwerk.

bb) 2 Punkte

QoS beschreibt die Güte eines Kommunikationsdienstes aus der Sicht der Anwender, d. h. wie stark die Güte des Dienstes mit deren Anforderungen übereinstimmt. QoS ist eine Menge von Qualitätsanforderungen an das gemeinsame Verhalten beziehungsweise Zusammenspiel von mehreren Objekten.

c) 6 Punkte, 6 x 1 Punkt

Schichten (ISO/OSI-7)	**Protokoll**
7 – 5	SNMP
4	TCP, UDP
3	IP, IPsec
2	L2TP
1	–

da) 2 Punkte

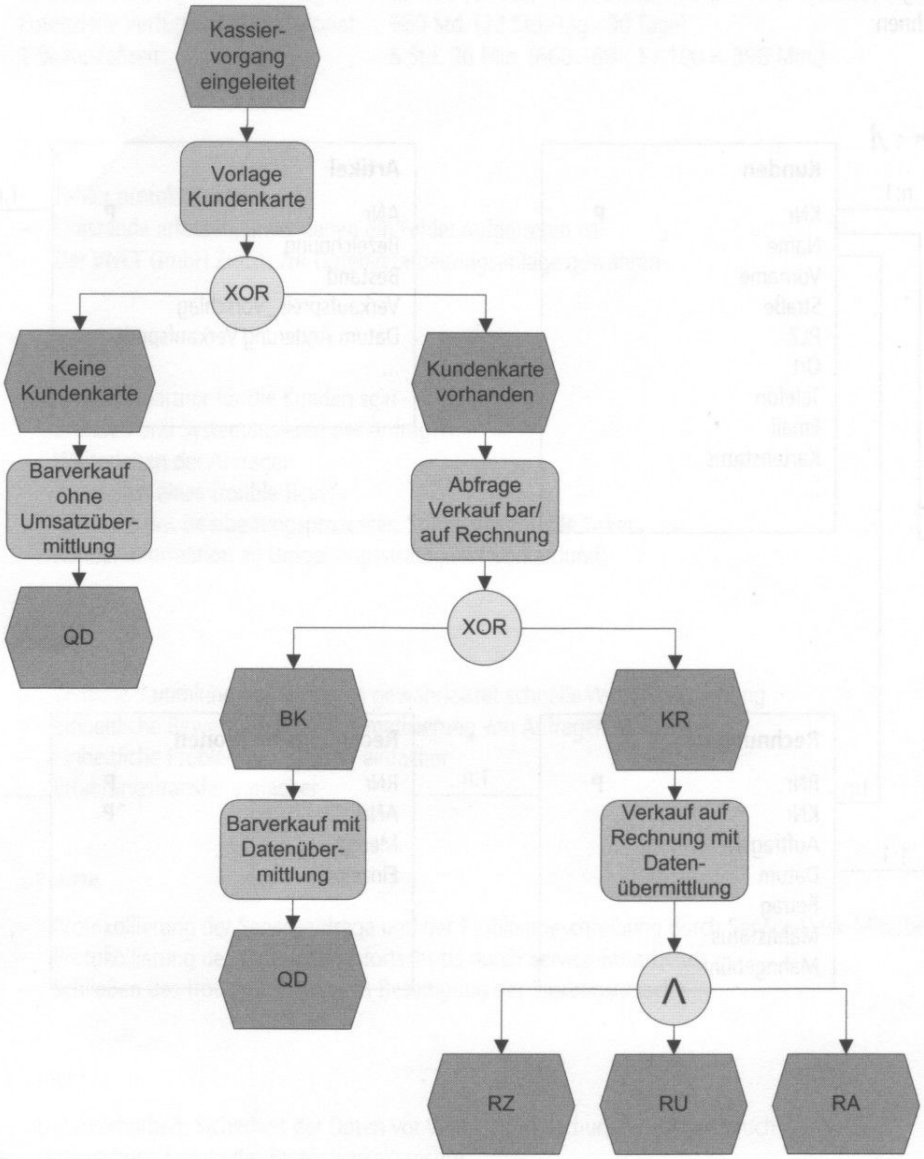
Verhinderung von Abhörversuchen durch Verschlüsselung der Datenpakete

db) 2 Punkte

Verhinderung von unberechtigter Veränderung von Datenpaketen

4. Handlungsschritt (20 Punkte)

a) 12 Punkte, 12 x 1 Punkt



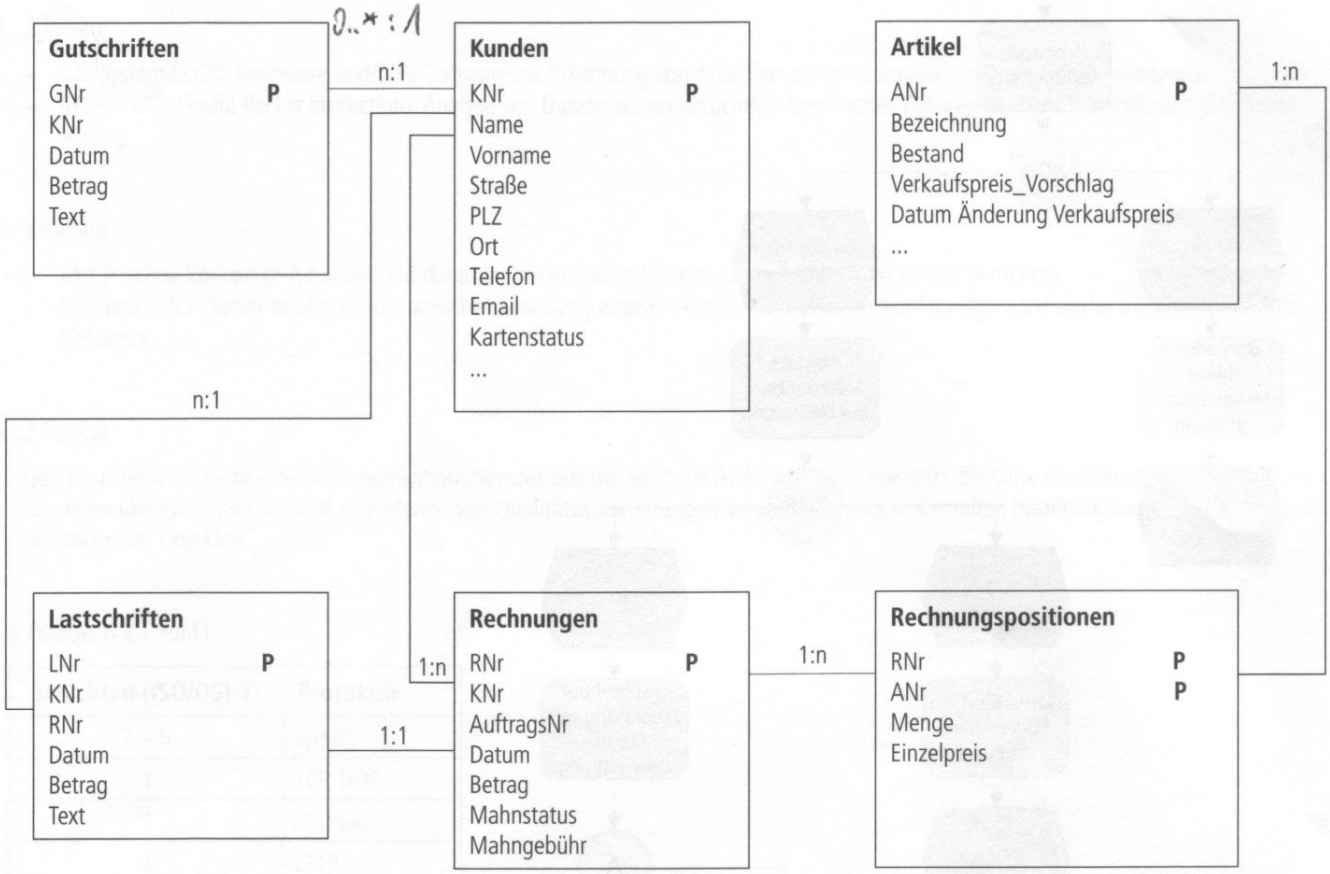
b) 8 Punkte, 4 x 2 Punkte

	Euro
Barzahlungen:	101,94
Rechnungen:	2.548,49
Nettoumsatz:	2.650,43
Bonus:	39,76

5. Handlungsschritt (20 Punkte)

a) 16 Punkte

4 Punkte: Attribute der Tabelle Rechnungspositionen
6 Punkte: Die Primärschlüssel kennzeichnen
6 Punkte: Beziehungen



ba) 2 Punkte

Daten mehrfach gespeichert

bb) 2 Punkte

Es ist darauf zu achten, dass keine Tupel gelöscht werden, die aus einer anderen Tabelle aufgerufen werden können und dass keine Tupel aufgerufen werden, die (noch) nicht existieren.

6. Handlungsschritt (20 Punkte)

aa) 3 Punkte

Potenzielle Verfügbarkeit pro Tag:	22 Std. (24 Std. – 2 Std. planmäßige Wartungszeit)
Potenzielle Verfügbarkeit pro Monat:	660 Std. (22 Std./Tag · 30 Tage)
1 % Ausfallzeit:	6 Std. 36 Min. (660 · 60 · 1 / 100 = 396 Min.)

ab) 2 Punkte

- Fehler protokollieren
- Umstände erfassen, unter denen ein Fehler aufgetreten ist
- Der VNET GmbH Zutritt zur Datenverarbeitungsanlage gewähren

ba) 3 Punkte

- Ansprechpartner für die Kunden sein
- Erfassen und Systematisieren der Anfragen
- Weiterleiten der Anfragen
- Ausstellen eines Trouble Tickets
- Kontrolle des Bearbeitungsprozesses, Status des Trouble Tickets
- Kundeninformation zu Umgehungsstrategien (workaround)

bb) 2 Punkte

- Zentrale Sammlung von Anfragen gewährleistet schnelle Weiterverarbeitung
- Einheitliche Bewertung und Systematisierung von Anfragen einfacher
- Einheitliche Problembehandlung einfacher
- Erfahrungstransfer einfacher

bc) 3 Punkte

- Protokollierung der Serviceanfrage und der Problembeschreibung durch Service-Desk-Mitarbeiter
- Protokollierung des Bearbeitungsfortschritts durch Service-Mitarbeiter
- Schließen des Trouble Tickets nach Beseitigung der Störungsursache

c) 4 Punkte

- Datensicherheit: Sicherheit der Daten vor Verlust, Verfälschung und Missbrauch
- Datenschutz: Schutz der Persönlichkeitsrechte
- Gemeinsamkeit: Gewährleistung der Datensicherheit personenbezogener Daten

d) 3 Punkte

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Zusammenführungskontrolle