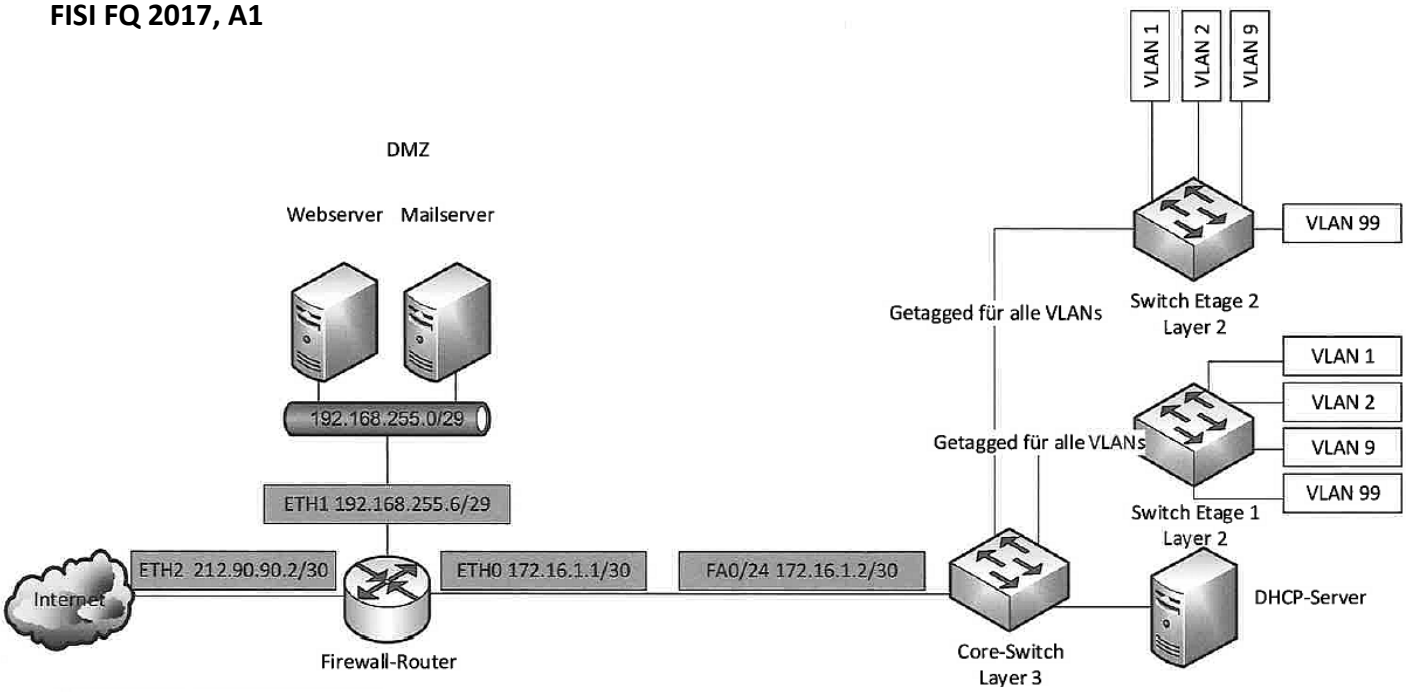
FISI FQ 2017, A1



e) Zur Absicherung des Netzes wurden auf dem Core-Switch die folgenden Firewall-Regeln aufgestellt:

Nr	Aktion	Protokoll	Quell-IP	Ziel-IP	Q-Port	Z-Port	Von Interface	Nach Interface
1	Permit	IP	192.168.9.0/28	Any	-	-	VLAN9	ANY
2	Permit	TCP	192.168.1.0/24	Any	>1023	80	VLAN1	FA0/24
3	Permit	TCP	192.168.1.0/24	Any	>1023	443	VLAN1	FA0/24
4	Permit	TCP	192.168.1.0/24	Any	>1023	25	VLAN1	FA0/24
5	Permit	TCP	192.168.1.0/24	Any	>1023	110	VLAN1	FA0/24
6	Permit	UDP	192.168.1.0/24	Any	>1023	53	VLAN1	FA0/24
...								
N	Deny	IP	Any	Any	-	-	Internet	IN

Erläutern Sie die Regeln 1 – 6 und N mit eigenen Worten. 7 Punkte

Regel	Erläuterung
1	
2	
3	
4	
5	
6	
N	

FISI FQ 2016/17, A3

In der MITTIG GmbH wird der Webserver durch eine Firewall in einer Demilitarisierten Zone (DMZ) geschützt.

b) Durch die DMZ ist das lokale Netzwerk der MITTIG GmbH gegenüber Angriffen aus dem Internet besser geschützt.

Beschreiben Sie die organisatorische Maßnahme, die diesen Schutz bewirkt. 3 Punkte

c) Für die externe Firewall der MITTIG GmbH wurden folgende Regeln aufgestellt:

Regel-Nr.	Aktion	Protokoll	Quell-IP	Ziel-IP	Q-Port	Z-Port	Interface	Richtung
1	Permit	TCP	ANY	Webserver der MITTIG GmbH	>1023	80	Internet	IN
2	Permit	TCP	ANY	Webserver der MITTIG GmbH	>1023	443	Internet	IN
...								
99	Deny	IP	ANY	ANY	-	-	Internet	IN

Erläutern Sie die Regeln 1, 2 und 99. 6 Punkte

Regel-Nr.	Erläuterung
1	
2	
99	

d) Eine Stateful Packet Inspection Firewall (SPI-Firewall) hat gegenüber einem reinen Paketfilter weitere Sicherheitsmerkmale.

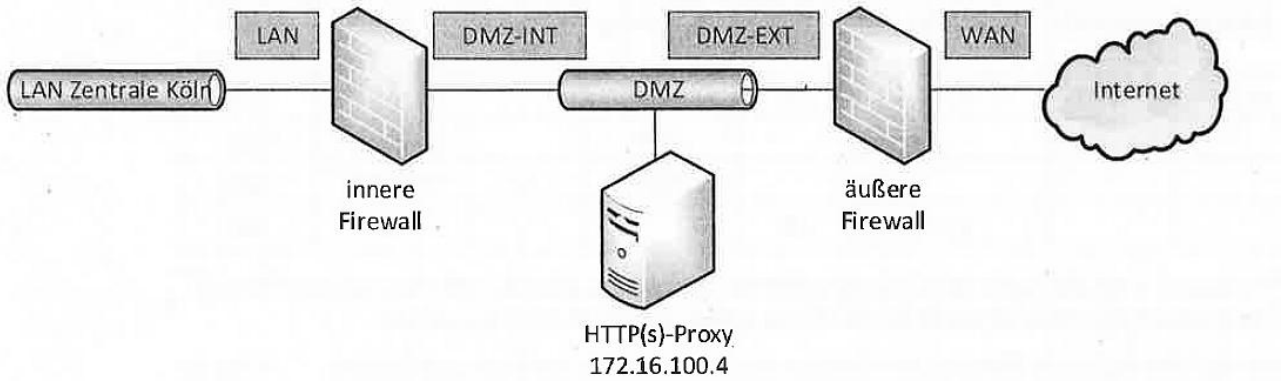
Nennen Sie die Bezeichnung eines Feldes im TCP-Header, welches nur von der SPI-Firewall analysiert wird. 2 Punkte

e) In der MITTIG GmbH wird diskutiert, einen HTTP Proxy einzusetzen.

Erläutern Sie eine grundsätzliche Funktion eines HTTP Proxy. 4 Punkte

FISI FQ 2015, A2

Die IT-Revolution AG soll für die TeNi GmbH eine DMZ einrichten. In dieser DMZ soll ein HTTP(s)-Proxyserver implementiert werden.



a) Nennen Sie zwei weitere Dienste mit den entsprechenden Portnummern, die in einer DMZ sinnvollerweise platziert werden sollten. 4 Punkte

b) An der inneren Firewall (Stateful Packet Inspection) zwischen dem internen Netz und der DMZ werden folgende Firewall-Regeln für den HTTP(s)-Proxy aufgestellt.

Nr	Aktion	Protokoll	Quelle	Ziel	Quell-Port	Ziel-Port	Von Interface	Nach Interface
1	ACCEPT	TCP	10.0.0.0/22	172.16.100.4/32	ANY	3128	LAN	DMZ-INT
..	...		...	...	...	...		...
n	DENY	IP	ANY	ANY	-	-	ANY	ANY

ba) Erläutern Sie stichpunktartig die Firewall-Regeln 1 und n. 4 Punkte

Firewall-Regel 1

Firewall-Regel n

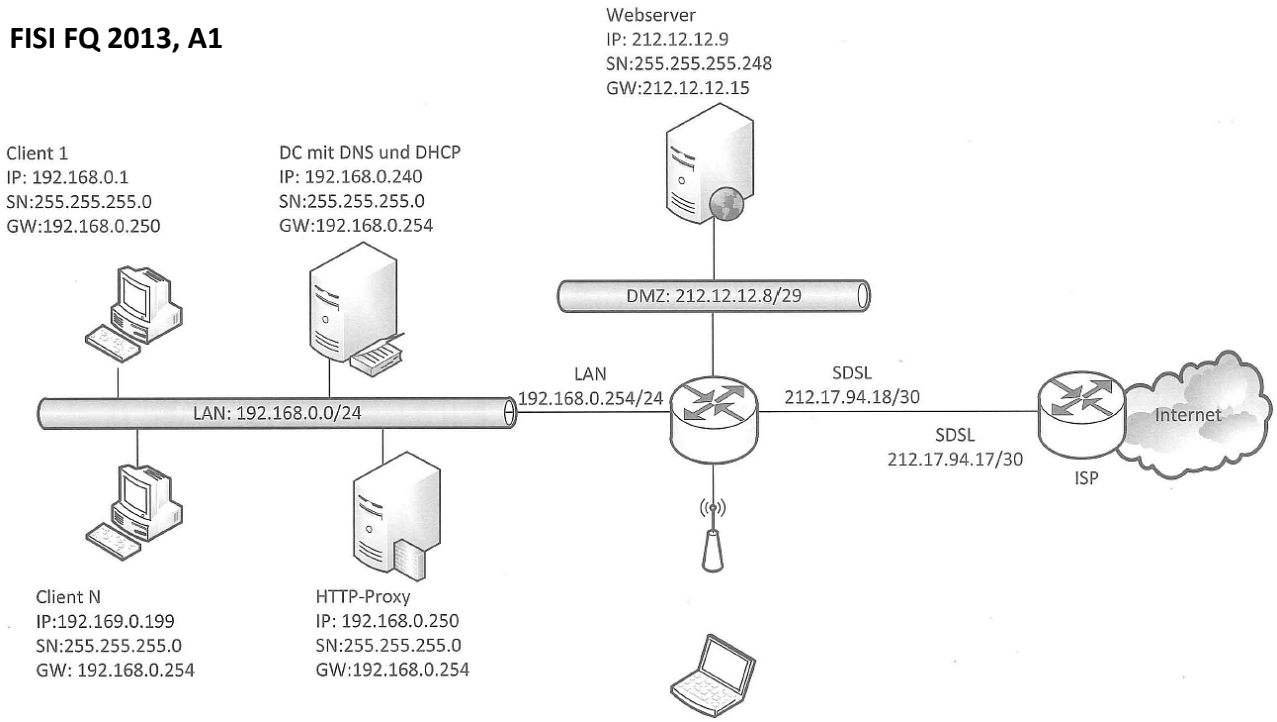
bb) Ergänzen Sie für die **äußere** Firewall (Stateful Packet Inspection – SPI) die Regeln, damit der HTTP(s)-Proxyserver ordnungsgemäß arbeiten kann. Der übrige Datenverkehr ist zu sperren. 4 Punkte

Nr	Aktion	Protokoll	Quelle	Ziel	Quell-Port	Ziel-Port	Von Interface	Nach Interface
1	ACCEPT	TCP	172.16.100.4/32	ANY	ANY		DMZ-EXT	WAN
2					ANY		DMZ-EXT	WAN
3					ANY	53	DMZ-EXT	WAN
4			ANY	ANY	-	-	ANY	ANY

c) Über den HTTP-Proxyserver in der DMZ sollen keine unerwünschten Internetdomänen erreichbar sein. Dazu soll eine Filterung mittels Domainsperre anhand einer Blacklist stattfinden. Ein Kollege schlägt vor, eine Whitelist einzusetzen.

Erläutern Sie unter Berücksichtigung der Sicherheit der Filterlisten die Funktionsweisen von Black- und Whitelists. 6 Punkte

FISI FQ 2013, A1



c) Auf dem Router ist eine Firewall eingerichtet, die nach dem Prinzip einer Stateful Packet Inspection (SPI) arbeitet.

ca) Erläutern Sie das Arbeitsprinzip der Stateful Packet Inspection im Unterschied zu einem reinen Paketfilter. (4 Punkte)

cb) Für die SPI wurde der folgende Regelsatz aufgestellt:

Erlauben/ Verbieten	Protokoll	Quelle	Ziel	Quell-Port	Ziel-Port	Interface	Richtung
Permit	TCP	Proxy	Any	Any	http	LAN	IN
Permit	TCP	Proxy	Any	Any	https	LAN	IN
Permit	IP	DC	Any	-	-	LAN	IN
Permit	TCP	Any	Webserver	Any	http	SDSL	IN
Deny	IP	Any	Any			Egal	Egal

Am SDSL-Interface kommen nun die folgenden Pakete an.

Erläutern Sie, wie die Firewall mit diesen Paketen verfährt. (8 Punkte)

Hinweis:
Auf der Firewall ist NAT/PAT für das interne Netz eingerichtet. Zunächst wird der NAT/PAT-Prozess durchgeführt, dann werden die Firewall-Regeln angewandt.

Paket 1

Quell-IP	Ziel-IP	Protokoll	Message
66.65.101.23	212.12.12.9	ICMP	echo request

Paket 2

Quell-IP	Ziel-IP	Protokoll	Quellport	Zielport
66.65.101.23	212.12.12.9	TCP	1050	80

Paket 3

Quell-IP	Ziel-IP	Protokoll	Quellport	Zielport
194.12.193.127	192.168.0.250	TCP	80	1090

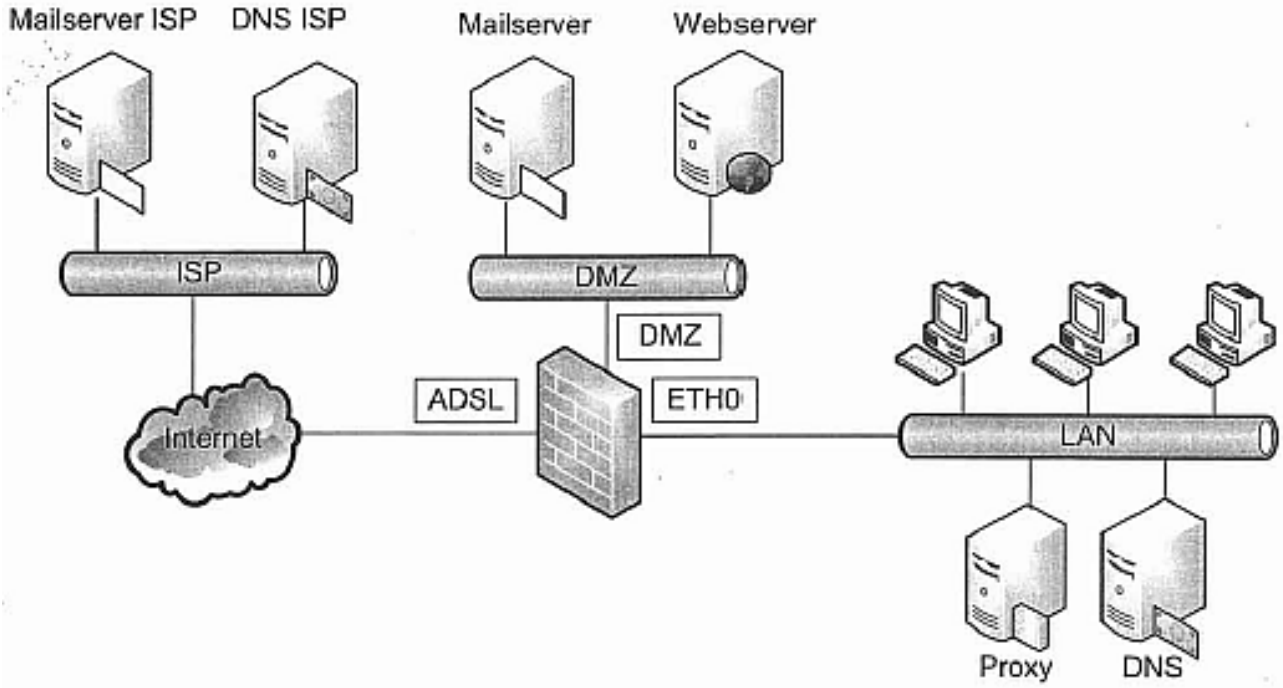
Paket 4

Quell-IP	Ziel-IP	Protokoll	Quellport	Zielport
84.235.217.19	212.12.12.9	TCP	1090	22

FISI FQ 2011/12, A2

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)

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