Die Futur GmbH möchte die Sicherheit und Systemstabilität ihres Netzwerkes erhöhen.

a) In der Futur GmbH wurden VLANs für die drei Schulungsräume (VLAN-S1, VLAN-S2, VLAN-S3) und das Verwaltungsnetz (VLAN-Verw) eingerichtet.

Erläutern Sie zwei Gründe, warum diese Maßnahme sinnvoll ist. 4 Punkte

- bessere Lastenverteilung
- Sicherheit höher, weil räumlich getrennte Netze (nur öffentliche IP ist von außen erreichbar)

b) Auf dem Core-Switch wurde eine Firewall eingerichtet.

ba) Für den Schulungsraum 1 wurde der folgende Regelsatz konfiguriert:

Nr	Aktion	Protokoll	Quell-IP	Ziel-IP	Q-Port	Z-Port	Von Interface	Nach Interface
1	Deny	IP	192.168.1.0/27	192.168.0.0/24	-	-	VLAN-S1	VLAN-Verw
2	Deny	IP	192.168.1.0/27	192.168.2.0/27	-	-	VLAN-S1	VLAN-S2
3	Deny	IP	192.168.1.0/27	192.168.3.0/27	-	-	VLAN-S1	VLAN-S3
4	Deny	IP	192.168.1.0/27	172.16.0.0/22	-	-	VLAN-S1	VLAN-WLAN
5	Permit	TCP	192.168.1.0/27	Any	>1023	80	VLAN-S1	Internet
6	Permit	TCP	192.168.1.0/27	Any	>1023	443	VLAN-S1	Internet
7	Permit	UDP	192.168.1.0/27	Any	>1023	53	VLAN-S1	Internet
8	Deny	IP	192.168.1.0/27	Any	-	-	VLAN-S1	Any

Erläutern Sie die Regeln 1 bis 8.
Es sind die jeweiligen Anwendungen bzw. Dienste anzugeben. 10 Punkte

Regel	Erläuterung
1 - 4	Das VLAN-S1 erreicht kein anderes internes Netzwerk (VLAN-Verw, VLAN-S2, VLAN-S3, VLAN-WLAN) (Deny [verweigern])
5	Das VLAN-S1 erreicht das Internet auf dem Port 80 (HTTP)
6	Das VLAN-S1 erreicht das Internet auf dem Port 443 (HTTPS)
7	Das VLAN-S1 erreicht das Internet auf dem Port 53 (DNS Domain Server)
8	Das VLAN-S1 erreicht keine weiteres Netz

bb) Nach der Aktivierung der Firewall-Regeln führt ein Teilnehmer im Schulungsraum 1 an einem Rechner den Befehl `ping 8.8.8.8` durch und erhält die folgende Fehlermeldung:

```
Ping wird ausgeführt für 8.8.8.8 mit 32 Bytes Daten:
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.

Ping-Statistik für 8.8.8.8:
   Pakete: Gesendet = 4, Empfangen = 0, Verloren = 4
   (100% Verlust),
```

Erläutern Sie, warum es zu diesem Fehler kommt. 3 Punkte

siehe Regel 8, darf keine anderes Netz erreichen

bc) Der Drucker im VLAN-S1 soll seinen Toner selbstständig per E-Mail beim Lieferanten bestellen. Der Drucker hat die vorletzte IP-Adresse im Subnetz.

Erstellen Sie die notwendige Firewall-Regel. 4 Punkte

Aktion	Protokoll	Quell-IP	Ziel-IP	Q-Port	Z-Port	Von Interface	Nach Interface
Permit	TCP	192.168.1.29 /32	Any	> 1023	25 (SMTP)	VLAN-1	Internet

c) Das Internetgateway verfügt über eine integrierte Firewall-Appliance mit Sandbox-Funktionalität.

Beschreiben Sie den Zweck der Sandbox-Funktionalität. 4 Punkte

Eine Sandbox ist ein isolierter Bereich, in dem sich Software ausführen lässt, ohne dass diese auf die eigentliche Systemumgebung Zugriff hat.
... Eine Sandbox stellt der auszuführenden Software alle benötigten Funktionen bereit.