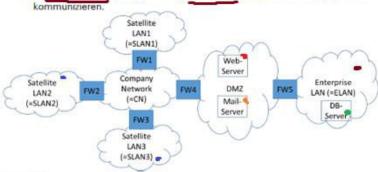
14.7 Aufgabe: Paketfilter-Regeln in verteilten Subnetzen

Die folgende Abbildung zeigt ein verteiltes Unternehmensnetzwerk. Geben Sie die durch die folgenden Kommunikationsbeziehungen definierten möglichst restriktiven statischen Paketfilter-Regeln in Form der in Kapitel 3.1 eingeführten Tabelle an:

- Jeder Host darf mit dem Web-Server kommunizieren (TCP Port 80).
- Jeder Unternehmens-Host (Enterprise + Satellite LAN) darf mit dem Mail-Server über SSL kommunizieren (TCP Port 993).
- Hosts in den Satellite-LANs d

 ürfen mit dem Datenbank-Server kommunizieren (TCP Port 66).
- Hosts in LAN 1 dürfen über SSH (TCP Port 22) mit Hosts in LANs 2 und 3 kommunizieren.
- Hosts in LAN 3 dürfen über SSH (TCP Port 22) mit Hosts im Enterprise LAN



Hinweise:

- Definieren Sie geeignete Gruppen und nutzen Sie geeignete Abkürzungen.
- · Die Firewalls verwenden kein NAT.

MailServer Gruppe: Enterprise + Satellite LAN

Web-Server Gruppe: Alle

Rule	NIC	IP-Src	IP-Dest	Protocol	SrcPort	DestPort	ACK	Action
1	NICX	WSGr	WS	TCP	80	80	Any	Permit
2	NIC2	WS	WSGr	TCP	80	80	Yes	Permit
3	NIC2	WS	WSGr	TCP	80	80	Any	Permit
4	NICX	WSGr	WS	TCP	80	80	Yes	Permit
3	NIC3	MSGr	MS	TCP	993	993	Any	Permit
4	NIC4	MS	MSGr	TCP	993	993	Yes	Permit
5	NIC4	MS	MSGr	TCP	993	993	Any	Permit
6	NIC3	MSGr	MS	TCP	993	993	Yes	Permit
7	NIC5	SLAN1	DB	TCP	66	66	Any	Permit
8	NIC6	DB	SLAN1	TCP	66	66	Yes	Permit
9	NIC7	SLAN2	DB	TCP	66	66	Any	Permit
10	NIC6	DB	SLAN2	TCP	66	66	Yes	Permit
11	NIC8	SLAN3	DB	TCP	66	66	Any	Permit
12	NIC6	DB	SLAN3	TCP	66	66	Yes	Permit
13	NIC5	SLAN1	SLAN2	TCP	22	22	Any	Permit
14	NIC7	SLAN2	SLAN1	TCP	22	22	Yes	Permit
15	NIC7	SLAN2	SLAN1	TCP	22	22	Any	Permit
16	NIC5	SLAN1	SLAN2	TCP	22	22	Yes	Permit
17	NIC5	SLAN1	SLAN3	TCP	22	22	Any	Permit
13	NIC8	SLAN3	SLAN1	TCP	22	22	Yes	Permit
13	NIC8	SLAN3	SLAN1	TCP	22	22	Any	Permit
17	NIC5	SLAN1	SLAN3	TCP	22	22	Yes	Permit
18	NIC8	SLAN3	ELAN	TCP	22	22	Any	Permit
19	NIC6	ELAN	SLAN3	TCP	22	22	Yes	Permit
20	Any	Any	Any	Any	Any	Any	Any	Deny