



The Great FIREWALL 2021

- PRIMÄRE LERNZIELE
- PAKET FILTER
- STATEFUL PAKET INSPECTION
- APPLICATION LEVEL FIREWALL
- PROXY
- DMZ
- ACCESS CONTROL LIST (ACL)



PAKET-FILTER FIREWALLS

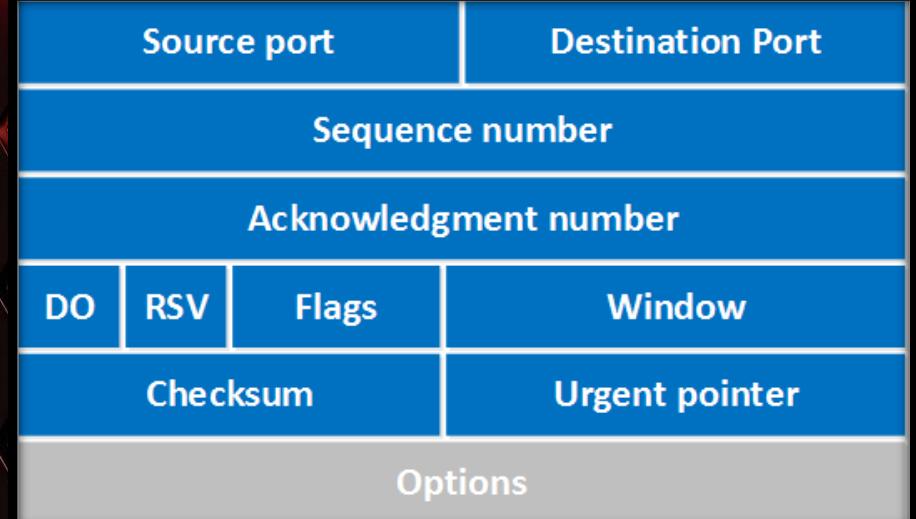
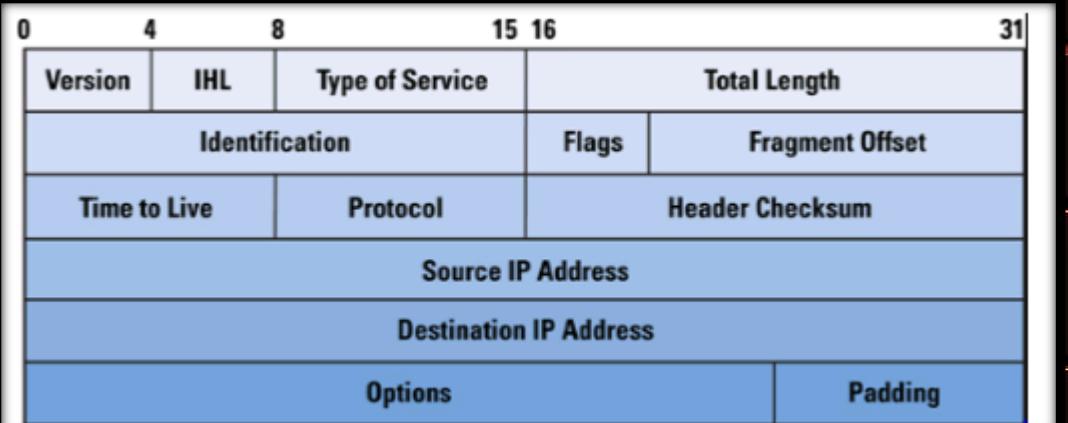
KONTROLIEREN DIE DATENPAKETE AUF DER 3./4. SCHICHT DES OSI MODELLS

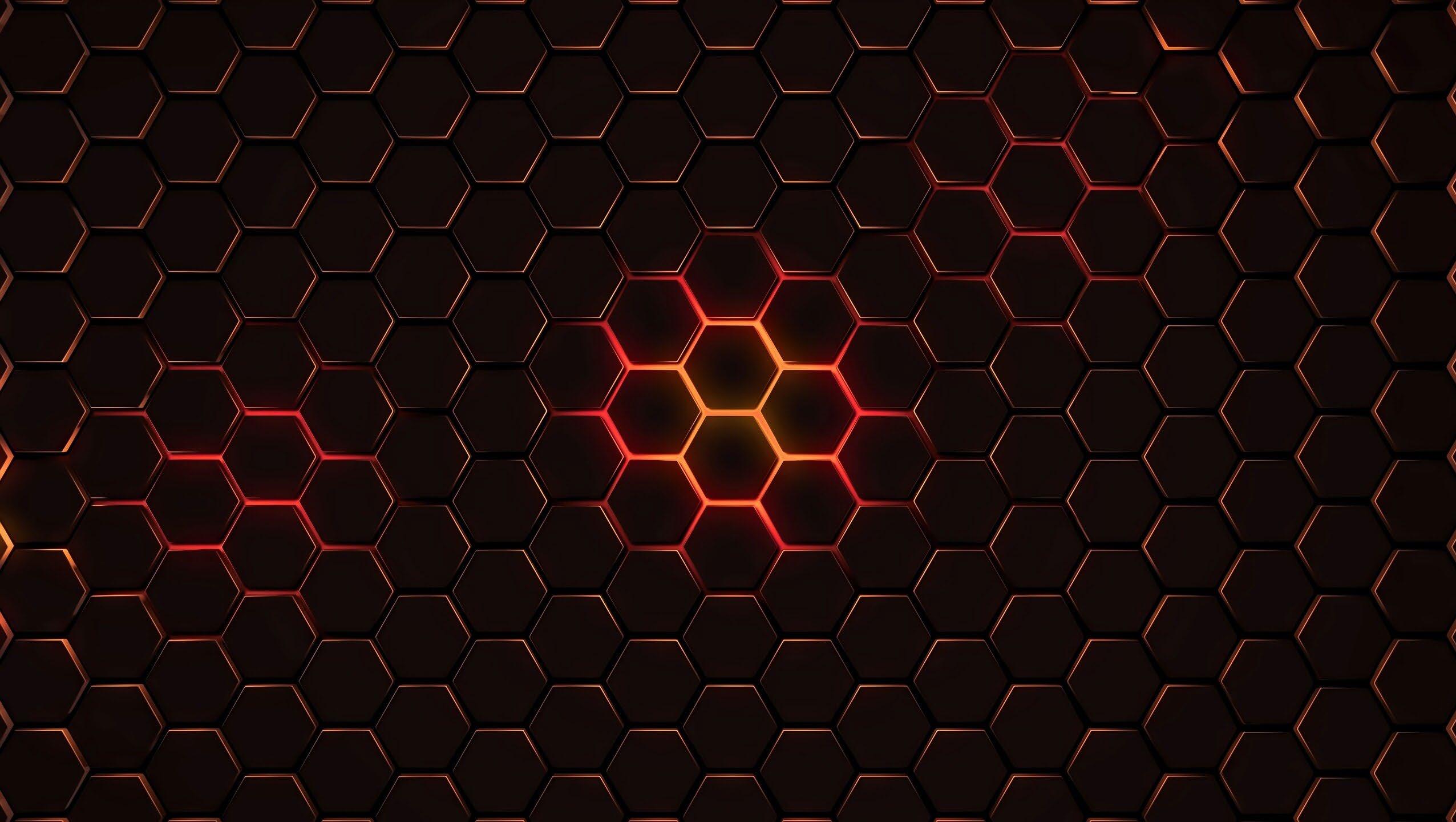


Überprüfung der Sende- und Empfangsadresse

Überprüfung der Protokollart

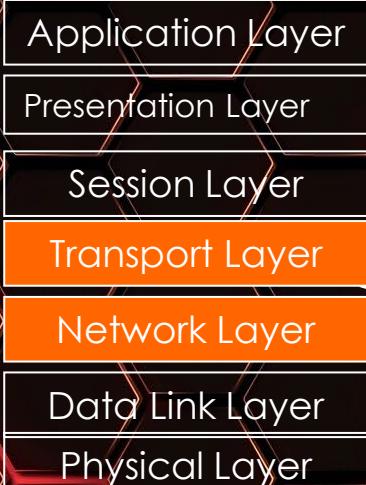
Überprüfung des Protokoll-Ports





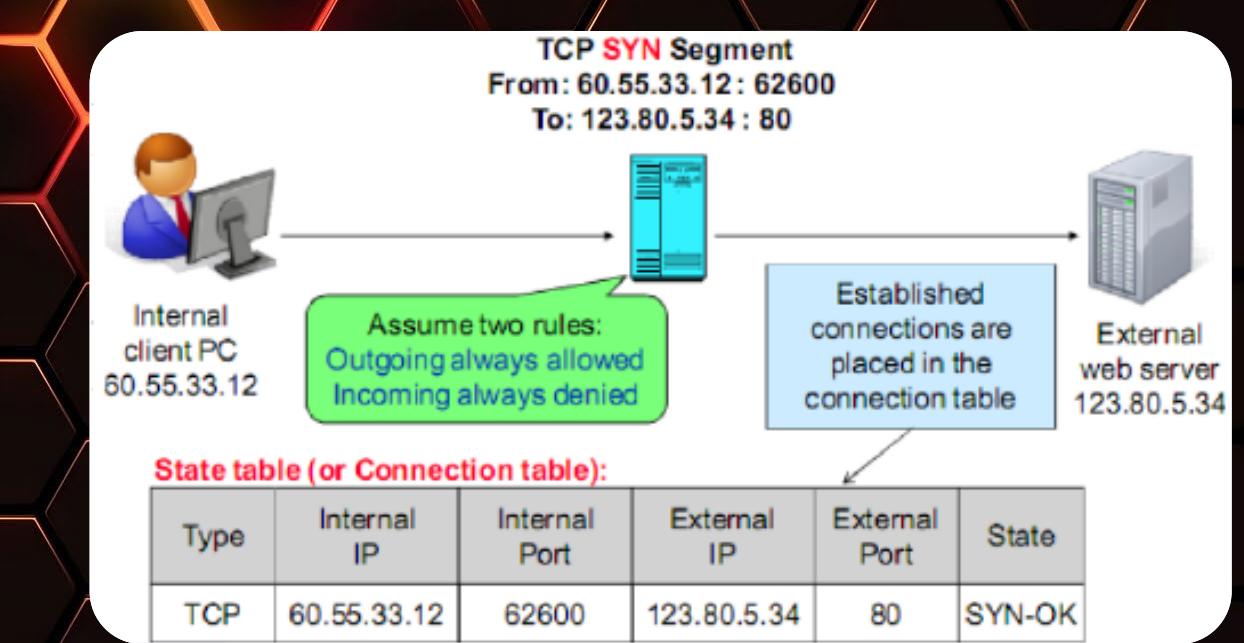
STATEFUL-PAKET-FILTER FIREWALLS (SPI)

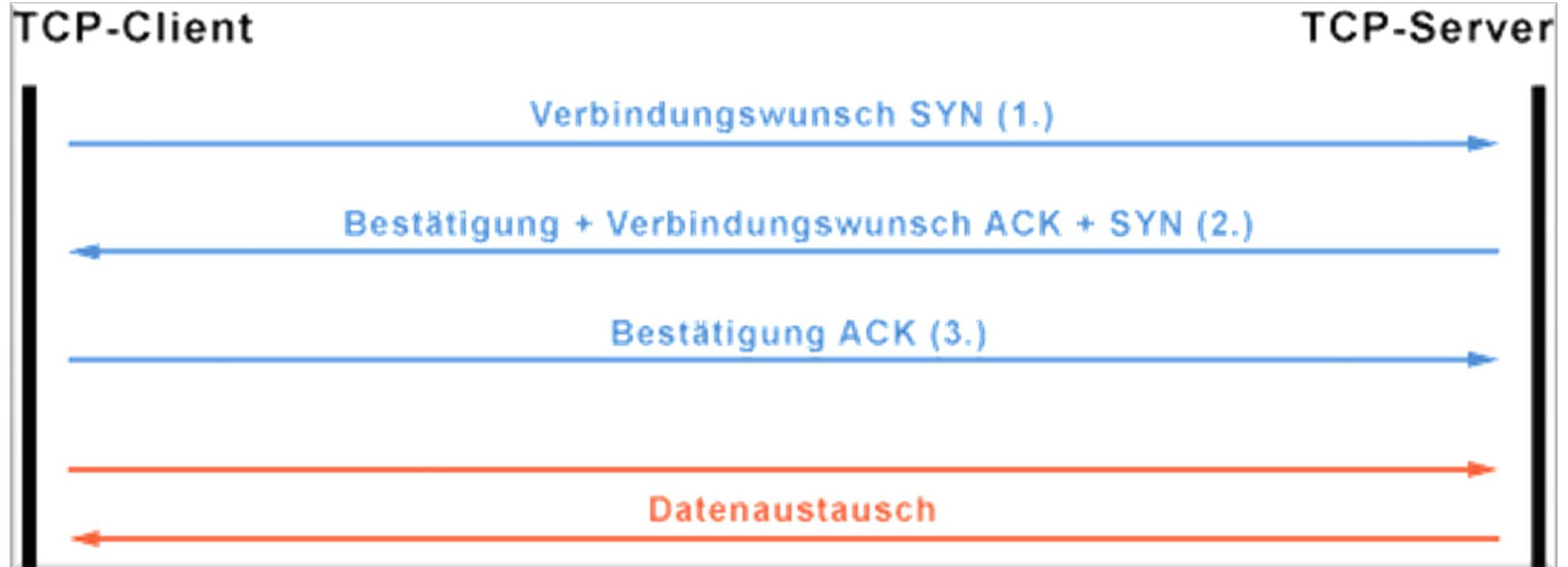
KONTROLIEREN DIE DATENPAKETE AUF DER 3./4. SCHICHT DES OSI MODELLS



- Überprüfung der Sende- und Empfangsadresse
- Überprüfung der Protokollart
- Überprüfung des Protokoll-Ports
- Überprüfung der Verbindungsdaten

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1032	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.212.212	1046	192.168.1.6	80	Established



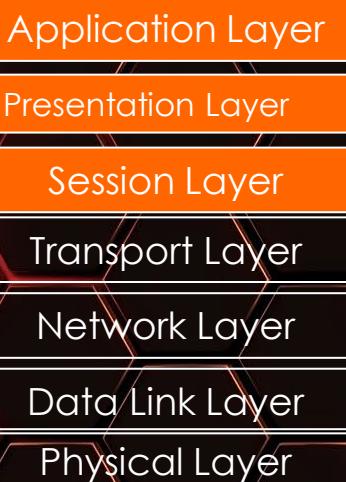


Wichtige Portnummern

1. ftp-data	20	/	TCP	File Transfer (Default Data)
2. ftp	21	/	UDP	File Transfer (Control)
3. ssh	22	/	TCP	Secure Shell
4. telnet	23	/	TCP	Telnet !!!unsicher!!!
5. smtp	25	/	TCP	Simple Mail Transfer
6. dns	53	/	UDP	Domain Name System
7. http	80	/	TCP	Hypertext Transfer Protocol
8. pop3	110	/	TCP	Post Office Protocol - Version 3
9. imap4	143	/	TCP	Internet Message Access Protocol Vers. 4
10. snmp	161	/	UDP	SNMP Simple Network Management Protocol
11. https / ssl	443	/	TCP	http Protocol über TLS / SSL
12. Smtp/ ssl	465	/	TCP	smtp über ssl
13. Ipsec	500	/	UDP	IP-Security VPN
14. Smtp/TLS	587	/	TCP	smtp über TLS
15. imaps	993	/	TCP	imap4 Protocol über TLS /SSL
16. pop3s	995	/	TCP	pop3 Protocol über TLS / SSL
17. RDP	3389	/	TCP	Remotedesktop (nie ohne VPN)

APPLIKATION LEVEL FIREWALL (PROXY)

DIE APPLIKATION LEVEL PROXY TECHNOLOGIE IST DIE UMFASSENDSTE UND GENAUESTE FIREWALL TECHNOLOGIE. HIER WIRD JEDES DATENPAKET – SOWEIT MÖGLICH UND SINNVOLL – BIS AUF DIE OBERSTE EBENE DES OSI MODELLS UNTERSUCHT:

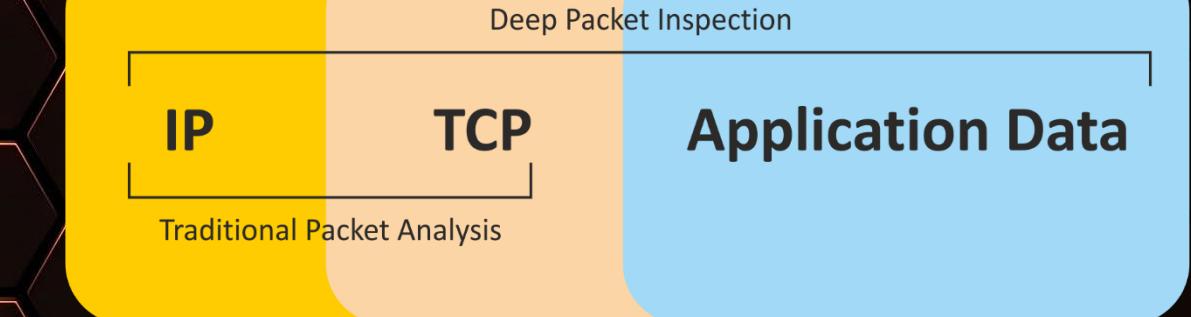


Fungieren als Proxy

Für jeden Dienst muss ein eigener Proxy angelegt sein

Next Generation Firewalls

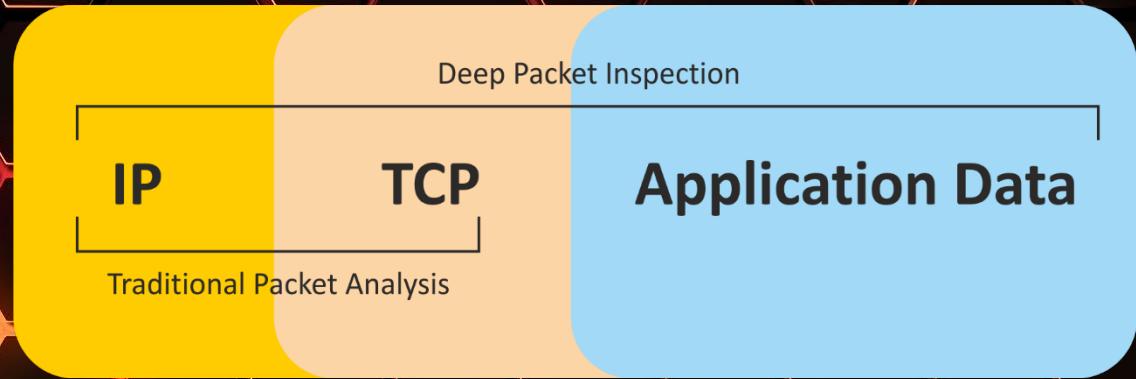
Deep Packet Inspection



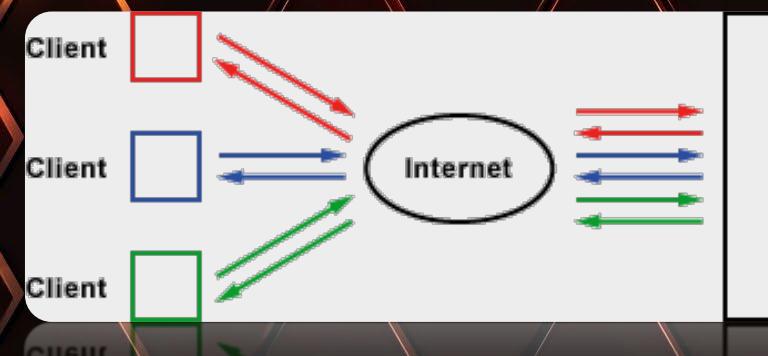
Ein Proxy Server ist ein Vermittler in einem Netzwerk, der Anfragen entgegennimmt und sie stellvertretend weiterleitet. Mit Hilfe des Proxy Servers lässt sich die Kommunikation zwischen einem lokalen Client und einem Webserver **absichern, verschleiern oder beschleunigen.**

Aufgaben eines Proxyservers:

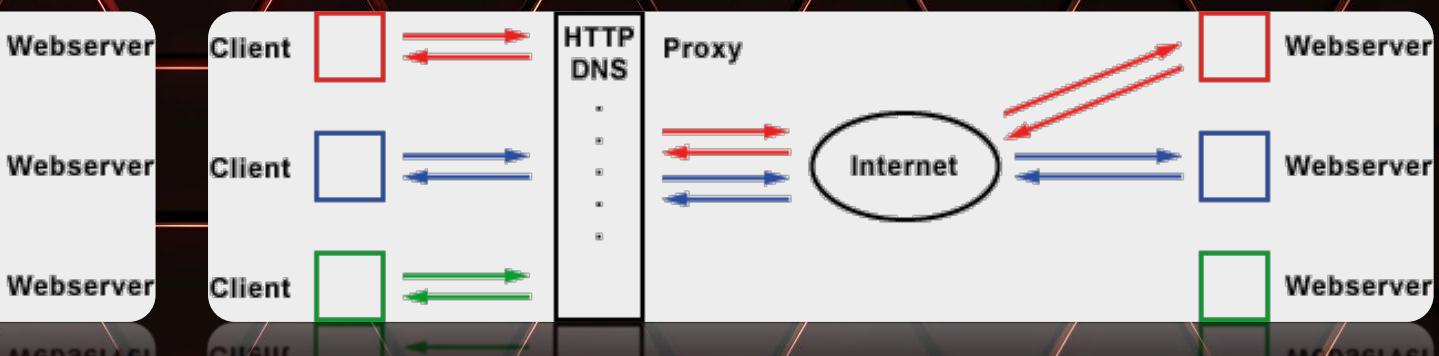
- Stellvertreterfunktion
- Filterfunktion
- User Authentication
- Caching

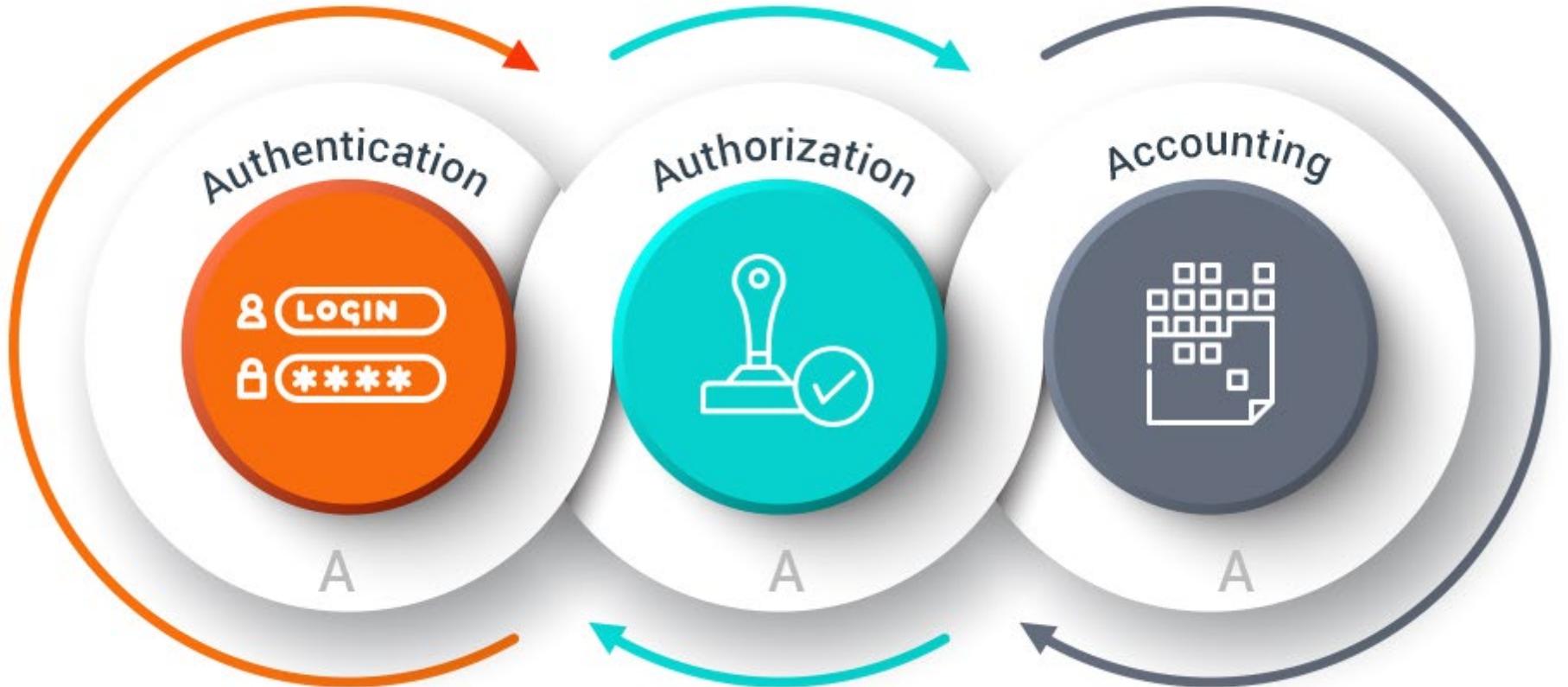


Reverse-Proxy

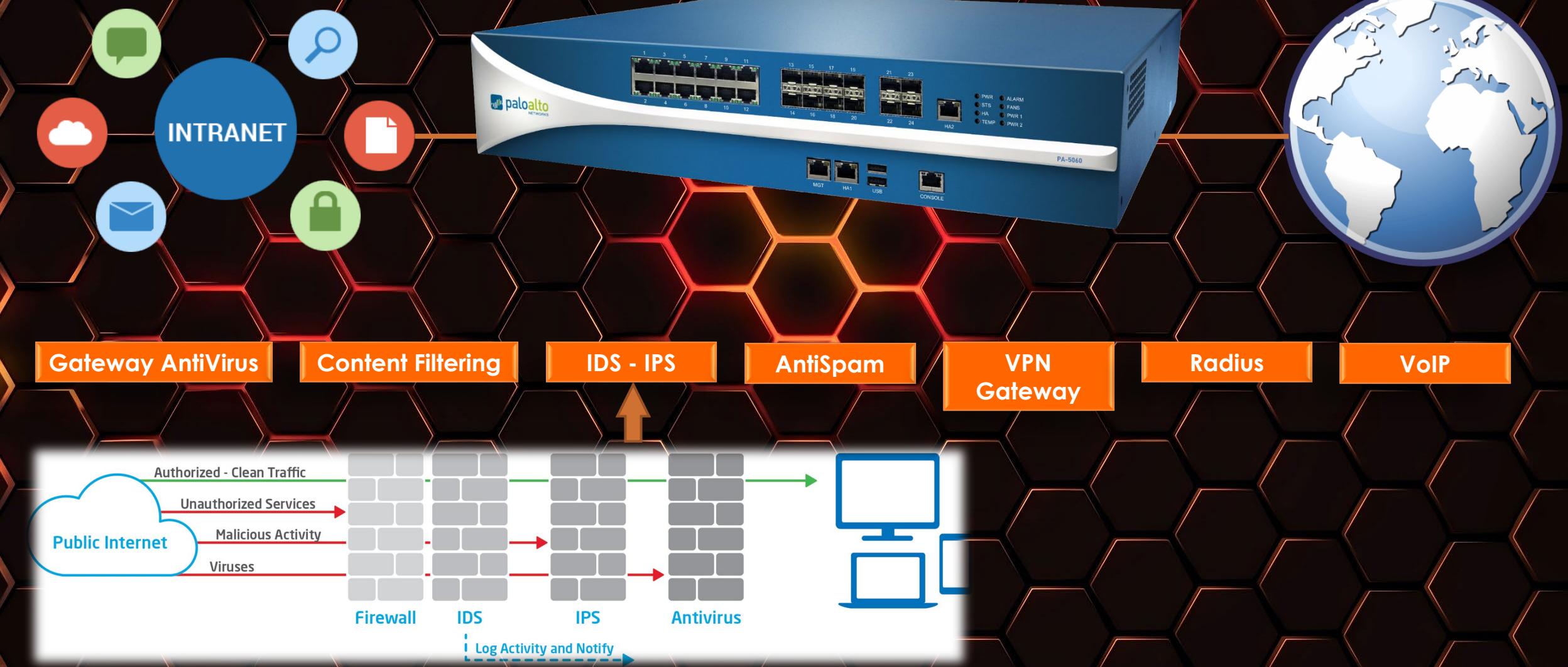


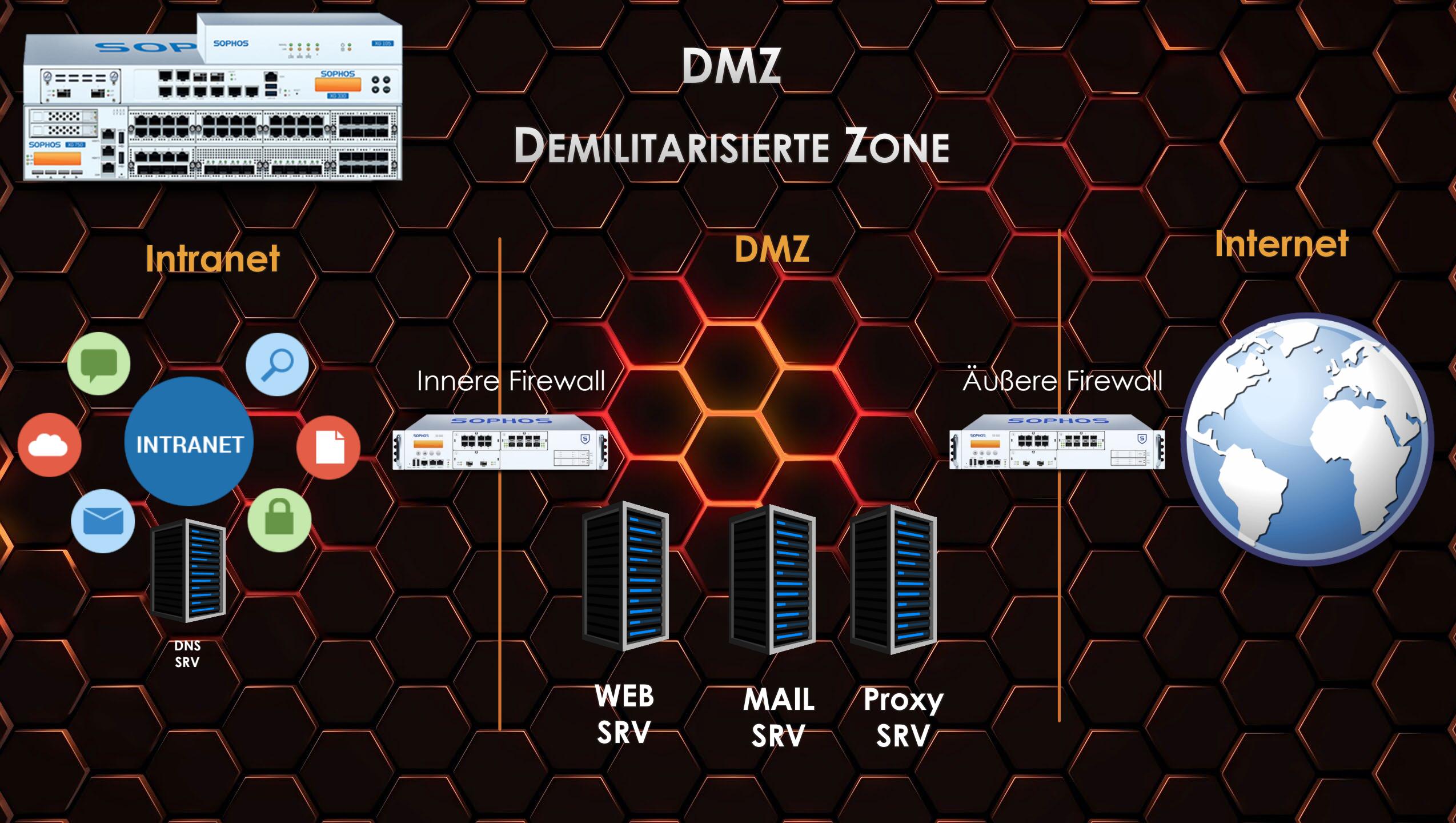
Forward-Proxy



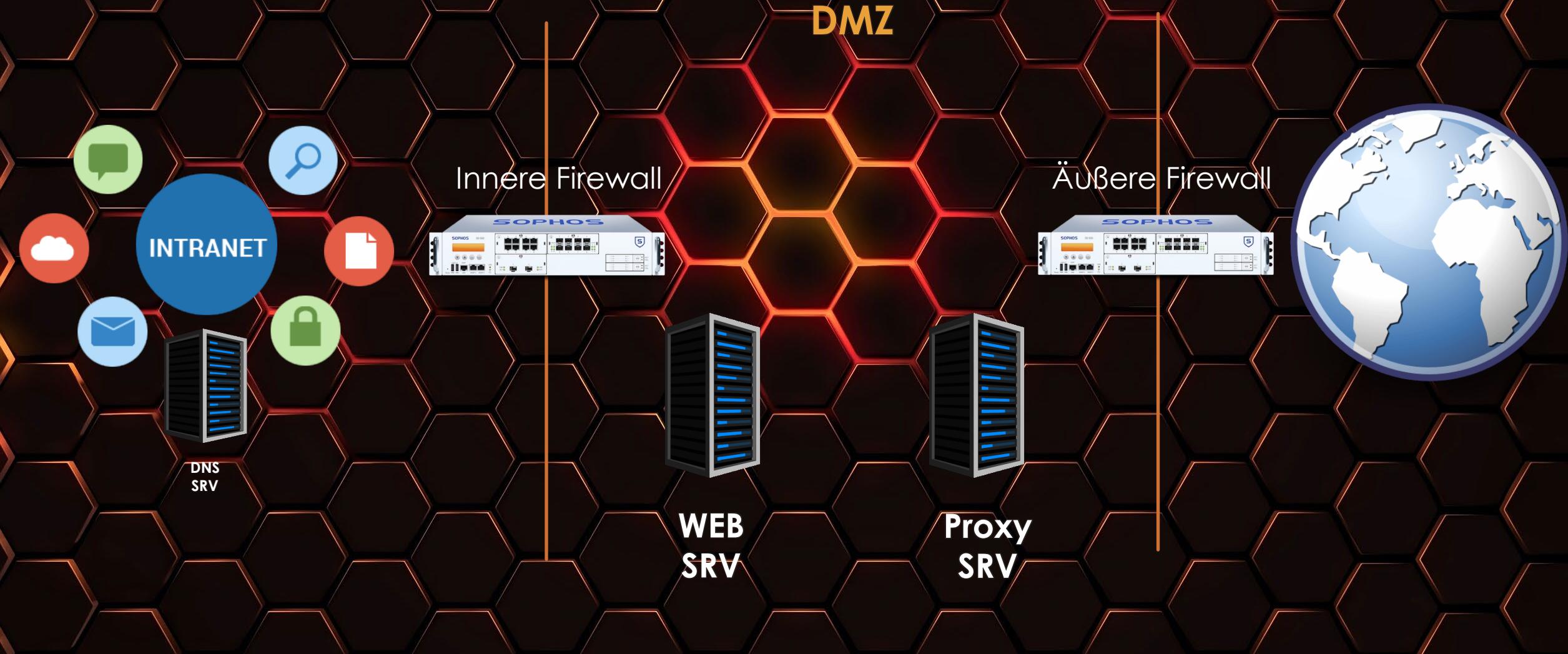


NEXT GENERATION FIREWALLS





DEMILITARISIERTE ZONE



Wichtige Portnummern

1. ftp-data	20	/	TCP	File Transfer (Default Data)
2. ftp	21	/	UDP	File Transfer (Control)
3. ssh	22	/	TCP	Secure Shell
4. telnet	23	/	TCP	Telnet !!!unsicher!!!
5. smtp	25	/	TCP	Simple Mail Transfer
6. dns	53	/	UDP	Domain Name System
7. http	80	/	TCP	Hypertext Transfer Protocol
8. pop3	110	/	TCP	Post Office Protocol - Version 3
9. imap4	143	/	TCP	Internet Message Access Protocol Vers. 4
10. snmp	161	/	UDP	SNMP Simple Network Management Protocol
11. https / ssl	443	/	TCP	http Protocol über TLS / SSL
12. Smtp/ ssl	465	/	TCP	smtp über ssl
13. Ipsec	500	/	UDP	IP-Security VPN
14. Smtp/TLS	587	/	TCP	smtp über TLS
15. imaps	993	/	TCP	imap4 Protocol über TLS /SSL
16. pop3s	995	/	TCP	pop3 Protocol über TLS / SSL
17. RDP	3389	/	TCP	Remotedesktop (nie ohne VPN)

192.168.0.0 /24

DMZ
192.168.1.0 /24

80.70.20.8 /30



Innere Firewall



WEB
SRV
192.168.1.3

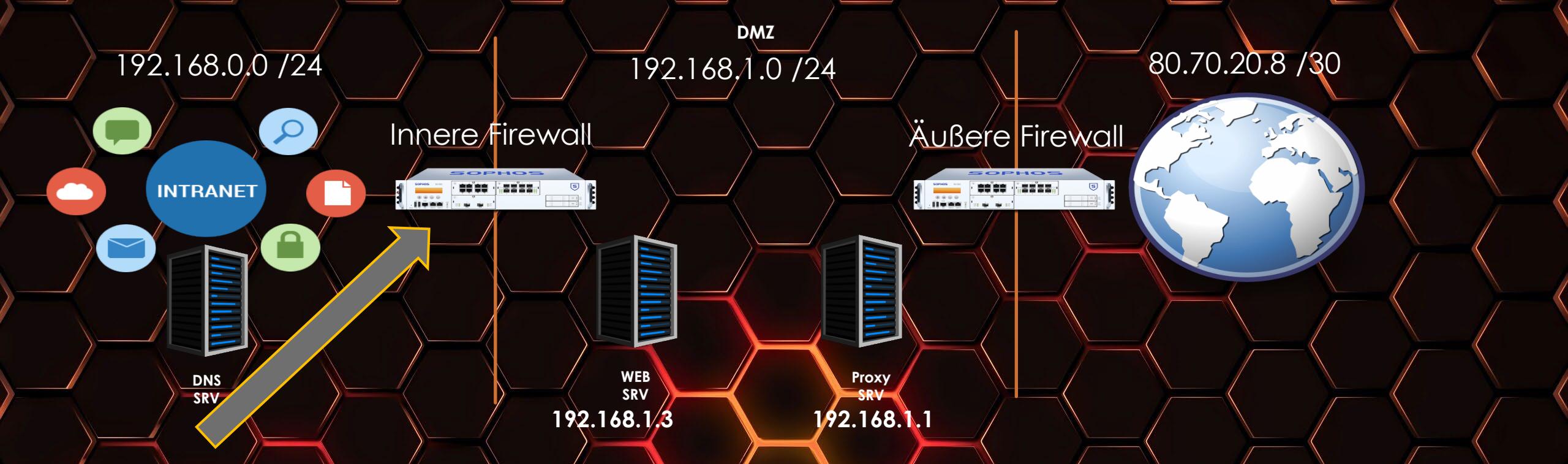
Äußere Firewall



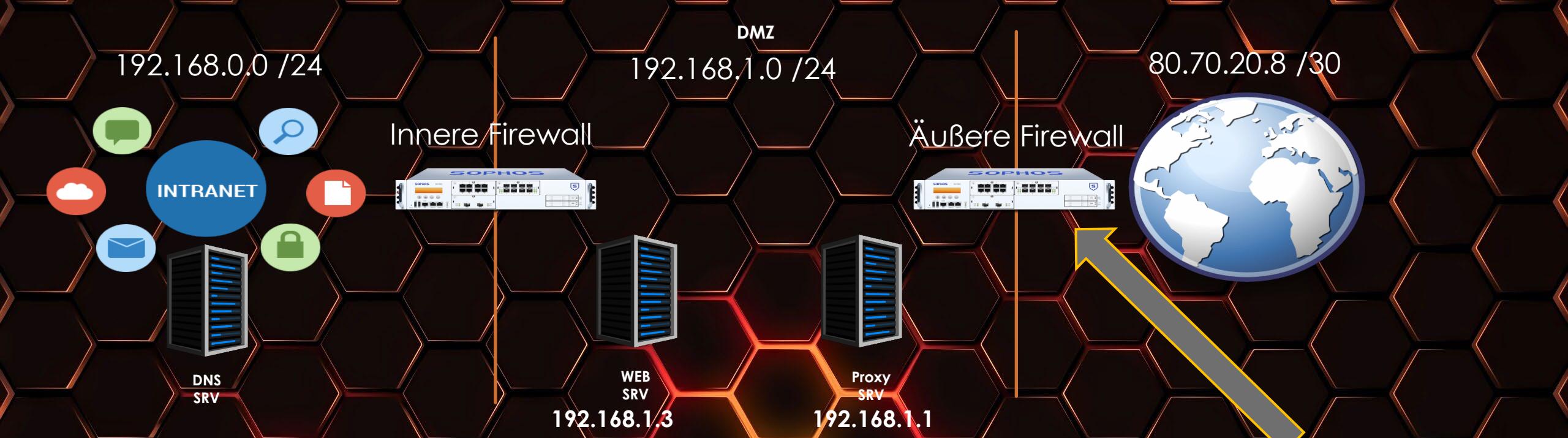
Proxy
SRV
192.168.1.1



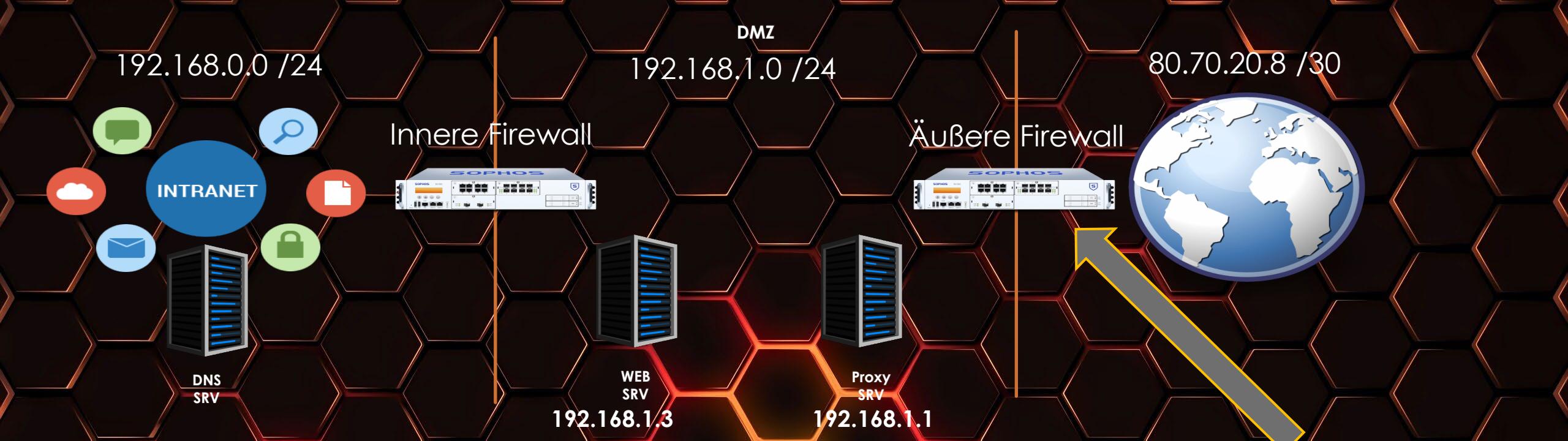
Nr.	Aktion	Protokoll	Quell-IP	Ziel-IP	Quell-Port	Ziel-Port	Richtung
1							
2							
3							



Nr.	Aktion	Protokoll	Quell-IP	Ziel-IP	Quell-Port	Ziel-Port	Richtung
1	Permit	TCP	192.168.0.0	192.168.1.1	>1023	3128/8080	DMZ
2	Permit	UDP	DNS SRV	ANY	>1023	53	DMZ
3	Reject	IP	ANY	ANY	-	-	ANY



Nr.	Aktion	Protokoll	Quell-IP	Ziel-IP	Quell-Port	Ziel-Port	Richtung
1							
2							
3							
4							
5							
6							
7							
8							



Nr.	Aktion	Protokoll	Quell-IP	Ziel-IP	Quell-Port	Ziel-Port	Richtung
1	Permit	TCP	192.168.1.1/32	ANY	ANY >1023	443	Internet
2	Permit	UDP	DNS SRV	ANY	ANY >1023	53	Internet
3	Permit	TCP	ANY	80.70.20.9 /30	ANY >1023	443	DMZ
4	DENY	IP	ANY	ANY	-	-	ANY
5							

IHK PRÜFUNGSAUFGABEN

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.

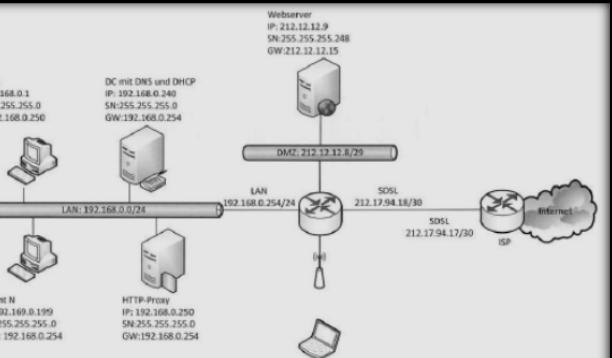
(8 Punkte)

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

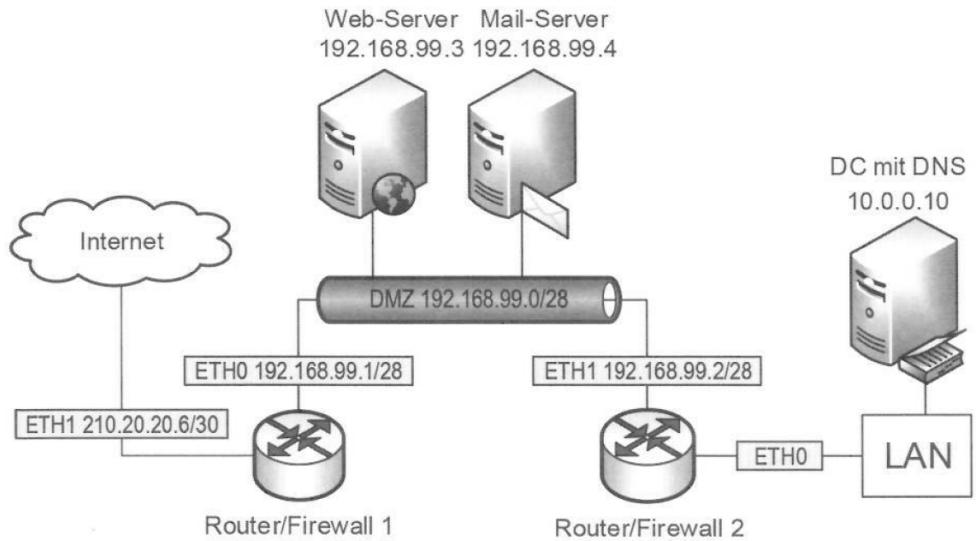
Quell-IP	Ziel-IP	Protokoll	Quellport	Zielport
66.65.101.23	212.12.12.9	TCP	1050	80

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



ab) Die SPI-Firewall 2 soll nur folgende Dienste aus dem internen Netz erlauben:

- Zugriff auf Web-Server (siehe Regelsatz) und Web-Shops
- Zugriff auf den Mail-Server in der DMZ (unverschlüsseltes Senden und Empfangen von E-Mails)
- Namensauflösung für den DC

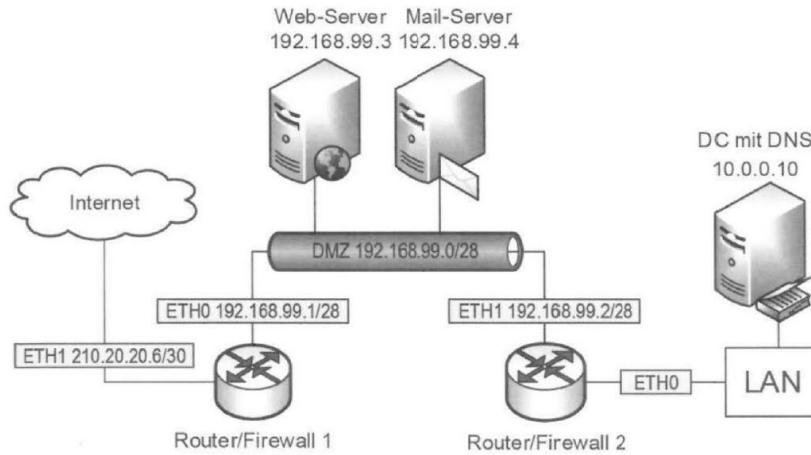
Anderer Datenverkehr ist verboten.

Ergänzen Sie den folgenden Regelsatz entsprechend dieser Vorgaben.

8 Punkte

Regelsatz für die Router/Firewall 2

Aktion	Protokoll	Quell-IP	Ziel-IP	Quell-Port	Ziel-Port	Von Interface	Nach Interface
Permit	TCP	10.0.0.0/22	Any	Any	80	ETH0	ETH1
Deny	IP	Any	Any	-	-		



ab) Die SPI-Firewall 2 soll nur folgende Dienste aus dem internen Netz erlauben:

- Zugriff auf Web-Server (siehe Regelsatz) und Web-Shops
 - Zugriff auf den Mail-Server in der DMZ (unverschlüsseltes Senden und Empfangen von E-Mails)
 - Namensauflösung für den DC

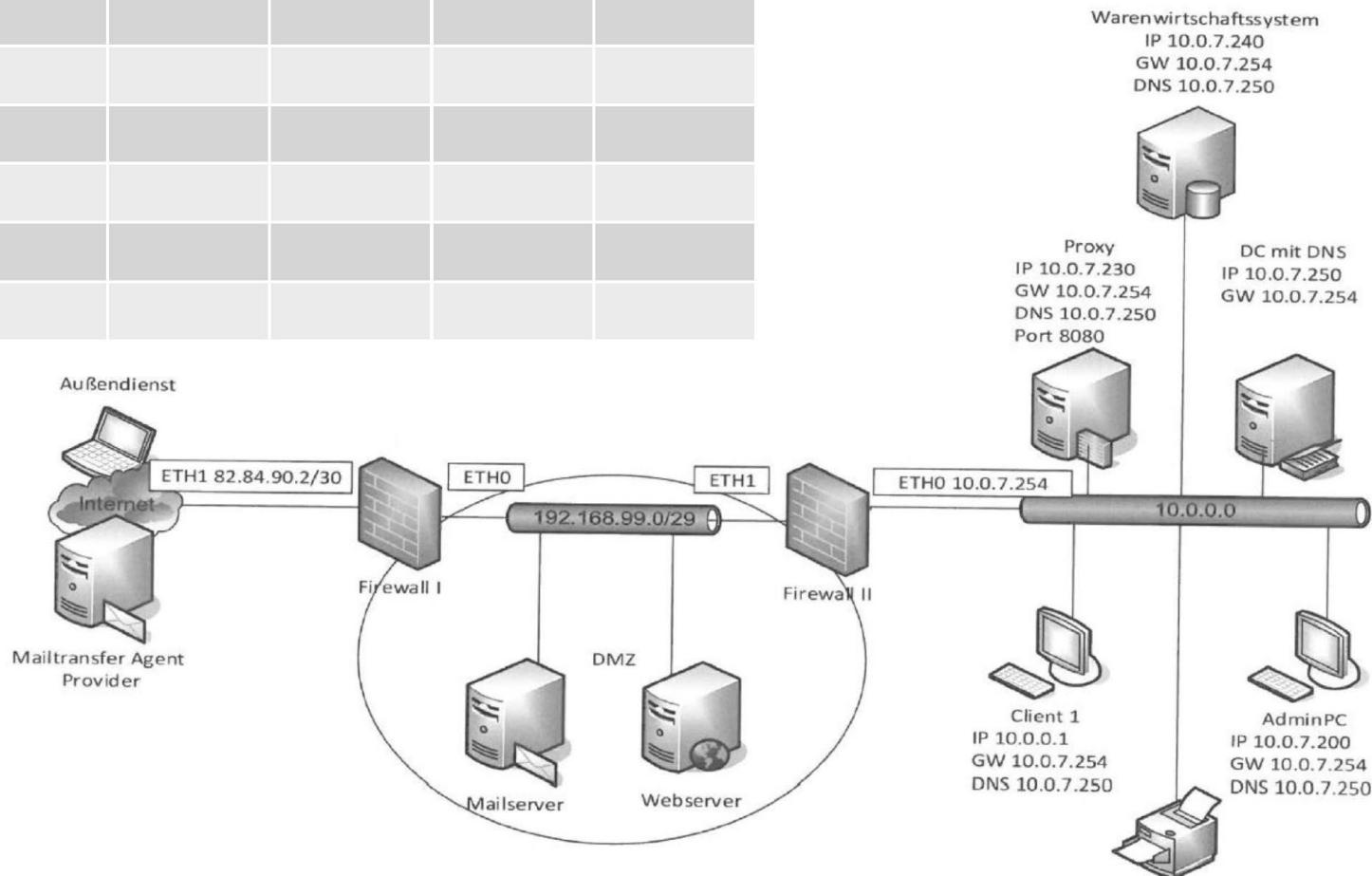
Anderer Datenverkehr ist verboten.

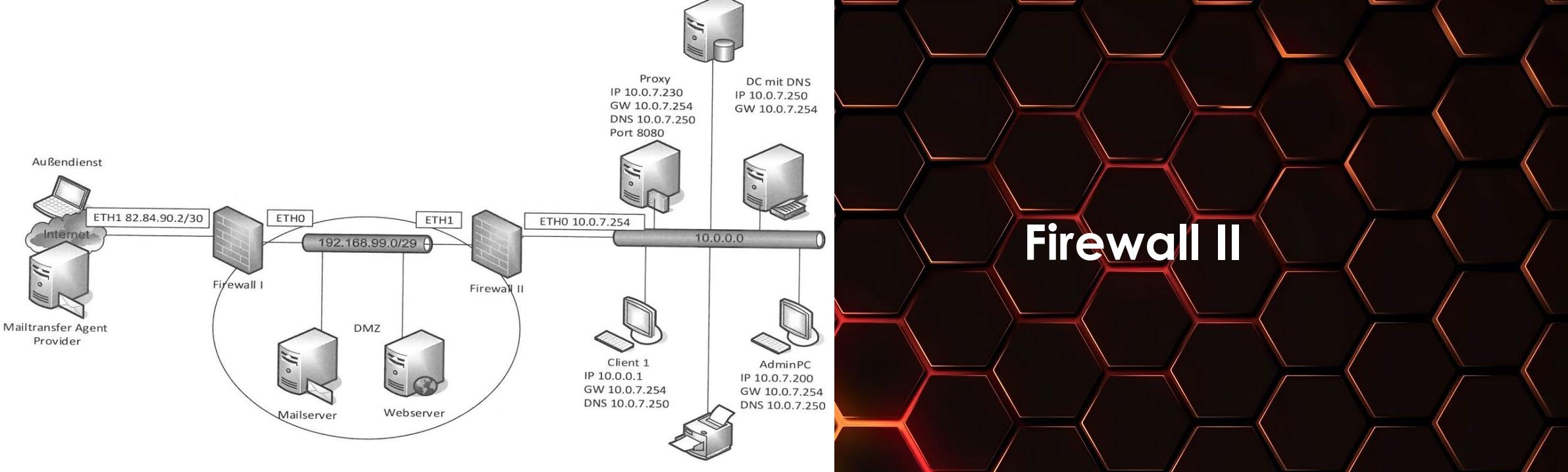
Ergänzen Sie den folgenden Regelsatz entsprechend dieser Vorgaben.

Regelsatz für die Router/Firewall 2

8 Punkte

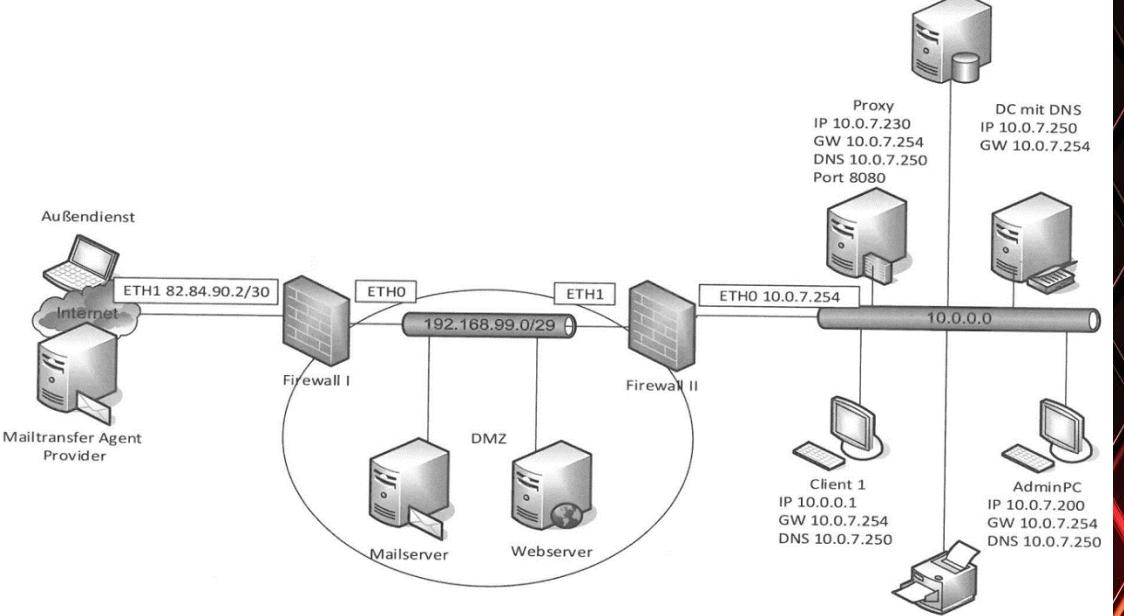
Aktion	Protokoll	Q-IP	Z-IP	Q-Port	Z-Port	Von IF	Nach IF





Firewall II

Nr.	Aktion	Protokoll	Quell-IP	Ziel-IP	Quell-Port	Ziel-Port	Richtung
1	Permit	TCP	10.0.7.230/32	any	> 1023	443	DMZ
2	Permit	UDP	10.0.7.250/32	any	> 1023	53	DMZ
3	Permit	TCP	10.0.0.0/21	192.168.99.1/32	> 1023	25	DMZ
4	Permit	TCP	192.168.99.1/32	10.0.0.0/21	> 1023	110	Intranet
5	Deny/Reject	IP	any	any	-	-	any



Nr.	Aktion	Protokoll	Quell-IP	Ziel-IP	Quell-Port	Ziel-Port	Richtung
1	Permit	TCP	10.0.7.230 /32	Any	>1023	443 (https)	Internet
2	Permit	UDP	10.0.7.250 /32	Any	>1023	53 (dns)	Internet
3	Permit	TCP	Any	82.84.90.2 /30	>1023	443 (https)	DMZ + PF
4	Permit	TCP	MTA	82.84.90.2 /30	>1023	110 (pop3)	DMZ + PF
5	Permit	TCP	Mail SRV	MTA	>1023	25	Internet
6	Deny	IP	Any	Any	-	-	Any
7							
8							

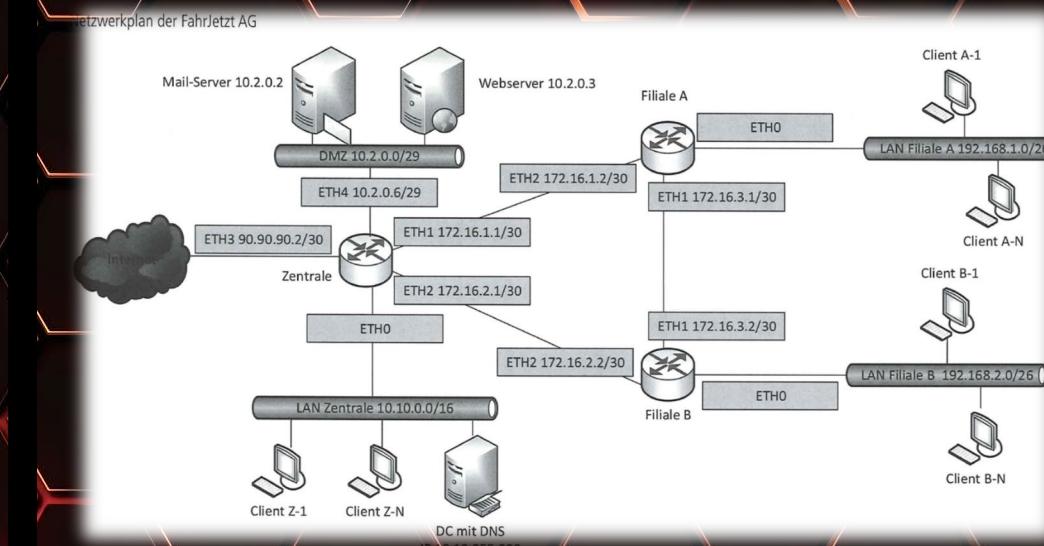
- c) Die FahrJetzt AG betreibt auf dem Router in der Zentrale eine Firewall, die nach dem Stateful Packet Inspection (SPI)-Prinzip arbeitet.

Erklären Sie die folgenden Firewall-Regeln.

7 Punkte

Nr.	Aktion	Protokoll	Quell IP	Ziel IP	Quellport	Zielport	Von Interface	Nach Interface
1	permit	UDP	10.10.255.200/32	8.8.8.8/32	ANY	53	ETH0	ETH3
2	deny	TCP	ANY	ANY	ANY	80	ETH0/1/2	ETH3
3	permit	TCP	ANY	ANY	ANY	443	ETH0/1/2	ETH3
4	permit	TCP	ANY	10.2.0.3/32	ANY	443	ETH3	ETH4

Nr.	Erklärung
1	
2	
3	
4	

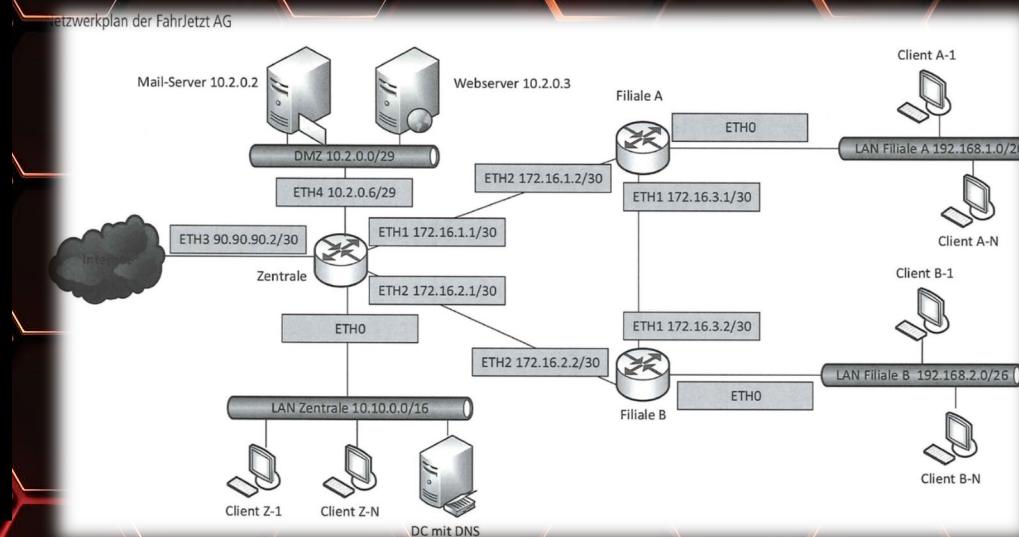


c) Die FahrJetzt AG betreibt auf dem Router in der Zentrale eine Firewall, die nach dem Stateful Packet Inspection (SPI)-Prinzip arbeitet.

Erklären Sie die folgenden Firewall-Regeln.

7 Punkte

Nr.	Aktion	Protokoll	Quell IP	Ziel IP	Quellport	Zielport	Von Interface	Nach Interface
1	permit	UDP	10.10.255.200/32	8.8.8.8/32	ANY	53	ETH0	ETH3
2	deny	TCP	ANY	ANY	ANY	80	ETH0/1/2	ETH3
3	permit	TCP	ANY	ANY	ANY	443	ETH0/1/2	ETH3
4	permit	TCP	ANY	10.2.0.3/32	ANY	443	ETH3	ETH4



Nr.	Erläuterung	Punkte
1	Erlaubt dem DNS-Server die Kommunikation mit dem Google-DNS über den DNS-Port 53	2
2	Verbietet allen HTTP-Datenverkehr aus den lokalen Netzen	1
3	Erlaubt allen HTTPS-Datenverkehr aus den lokalen Netzen	2
4	Erlaubt den Zugriff auf den Webserver in der DMZ über den HTTPS-Port aus dem Internet	2

b) Ihr Kollege hat bereits begonnen, ein Demonstrationsnetzwerk aufzubauen. Die Firewall ist bereits wie folgt konfiguriert:

FIREWALL_DENY_PORT_N='3'	#no. of ports to reject/deny
FIREWALL_DENY_PORT_1='0:19'	DENY'
FIREWALL_DENY_PORT_2='22:24'	DENY'
FIREWALL_DENY_PORT_3='26:1023'	DENY'

Erklären Sie anhand der obigen Konfiguration, welche Ports nicht gesperrt sind. Nennen Sie auch die zu den Ports gehörigen Dienste bzw. Protokolle (6 Punkte).

Antwort zu b):

Die gezeigten Einträge geben einen Bereich von gesperrten Ports an. Die Ports, die von den angegebenen Bereichen nicht abgedeckt werden, sind zugänglich.

Offene Ports:

- 20 → zugehöriges Protokoll: FTP (Datentransfer)
- 21 → zugehöriges Protokoll: FTP (Kontrollinformationen)
- 25 → zugehöriges Protokoll: SMTP (Simple Mail Transfer Protocol)

HYBRID-FIREWALLS

DIE HEUTIGE ENTWICKLUNG GEHT IN RICHTUNG HYBRID FIREWALLS.

DIESE STELLEN DIE ZWEI VORGESTELLTEN GRUNDTECHNIKEN IN KOMBINATION BEREIT.

