

# Inhaltsverzeichnis

<b>Vorwort</b>	<b>ix</b>
Geschichte . . . . .	x
Abgrenzung zur UTM . . . . .	xi
<b>1 Quickstart</b>	<b>15</b>
Was ist die Sophos Firewall? . . . . .	15
IP-Adresse . . . . .	16
Einrichtung . . . . .	17
Übersicht . . . . .	17
Zusammenfassung . . . . .	18
<b>2 Labornetzwerk</b>	<b>19</b>
Ressourcen . . . . .	19
Virtualisierung . . . . .	20
Hardware . . . . .	23
Netze . . . . .	23
Firewall . . . . .	24
Adressierung . . . . .	24
Labor-Server . . . . .	25
Verwendung . . . . .	25
<b>3 Plattform</b>	<b>27</b>
Vorbereitung . . . . .	28
VMware . . . . .	28
VirtualBox . . . . .	34
Hardware . . . . .	38

---

Installation . . . . .	40
<b>4 Ersteinrichtung</b>	<b>43</b>
Voreinstellung . . . . .	43
Ersteinrichtung . . . . .	44
Lizenz . . . . .	46
Allgemeines . . . . .	46
Routing . . . . .	49
Namensauflösung . . . . .	50
Generalprobe . . . . .	51
Dynamische Adressvergabe . . . . .	51
Zusammenfassung . . . . .	52
<b>5 Paketfilter</b>	<b>53</b>
Die Sophos-Firewall . . . . .	54
Laboraufbau . . . . .	55
Allgemeine Einstellungen . . . . .	56
Zonen . . . . .	57
Filterregeln . . . . .	58
Logging . . . . .	60
Durchsatz . . . . .	61
Ausnahmen . . . . .	62
Best Practice . . . . .	62
Zusätzliche Filter . . . . .	64
Fehlersuche . . . . .	67
Technischer Hintergrund . . . . .	68
Zusammenfassung . . . . .	69
<b>6 Network Address Translation</b>	<b>71</b>
Laboraufbau . . . . .	72
Szenarios . . . . .	73
IPv6 . . . . .	80
Technischer Hintergrund . . . . .	81
Zusammenfassung . . . . .	81

---

<b>7 Webfilter</b>	<b>83</b>
Laboraufbau . . . . .	85
Internetrichtlinie . . . . .	85
TLS-Inspection . . . . .	90
Ausblick . . . . .	93
Technischer Hintergrund . . . . .	94
Zusammenfassung . . . . .	95
<b>8 Webserver-Schutz</b>	<b>97</b>
Laboraufbau . . . . .	97
Basisschutz . . . . .	99
Erweiterter Schutz . . . . .	100
Fehlersuche . . . . .	101
Praxisbeispiel: E-Mail-Archiv Piler . . . . .	102
Ausfallschutz . . . . .	106
Technischer Hintergrund . . . . .	106
Zusammenfassung . . . . .	107
<b>9 NetFlow</b>	<b>109</b>
Inhalt eines Flows . . . . .	109
Labor . . . . .	110
Exporter . . . . .	112
Kollektor . . . . .	113
IPv6 . . . . .	114
Fehlersuche . . . . .	114
Cloud . . . . .	115
Zusammenfassung . . . . .	116
<b>10 Cloud</b>	<b>119</b>
Logging as a Service . . . . .	119
Backup . . . . .	122
Zusammenfassung . . . . .	126
<b>11 Best Practice</b>	<b>129</b>
Factory-Default . . . . .	129
Durchsatz messen . . . . .	130
SSH-Login ohne Passworteingabe . . . . .	132

Passwort zurücksetzen . . . . .	135
Quality of Service . . . . .	136
TLS-Zertifikat . . . . .	138
<b>12 Life Hacks</b>	<b>141</b>
Zugriff von Windows . . . . .	142
Weniger Arbeitsspeicher . . . . .	142
Speedtest . . . . .	144
Application Programming Interface . . . . .	145
<b>13 Architektur</b>	<b>149</b>
Allgemeines . . . . .	149
Systemstart . . . . .	150
Cyberoam System Controller . . . . .	152
Antivirus . . . . .	152
Einbruchserkennung . . . . .	153
Datenbank . . . . .	153
Webserver . . . . .	154
Paketfilter . . . . .	154
Logging . . . . .	156
Webfilter . . . . .	156
Verschiedenes . . . . .	158
Zusammenfassung . . . . .	160
<b>Literaturverzeichnis</b>	<b>163</b>
<b>Index</b>	<b>165</b>
<b>A IP Version 6</b>	<b>171</b>
<b>B Editor unter Linux</b>	<b>175</b>
<b>C Zusatzmaterial</b>	<b>179</b>