

Inhaltsverzeichnis

Vorwort	ix
Geschichte	x
Abgrenzung zur XG-Firewall	xi
1 Quickstart	15
Was ist Sophos UTM?	15
IP-Adresse	16
Einrichtung	17
Übersicht	18
Zusammenfassung	19
2 Labornetzwerk	21
Ressourcen	21
Virtualisierung	22
Hardware	24
Netze	25
Firewall	25
Adressierung	26
Labor-Server	27
Verwendung	27
3 Plattform	29
Vorbereitung	30
VMware	30
VirtualBox	36
Hardware	40

Installation	42
4 Ersteinrichtung	45
Setup Wizard	45
Lizenz	46
Allgemeines	47
Netzadapter	48
Sicherheit	49
Routing	49
Namensauflösung	51
Generalprobe	51
Dynamische Adressvergabe	51
Zusammenfassung	52
5 Paketfilter	53
Die Sophos UTM	54
Laboraufbau	55
Filterregeln	55
Logging	59
Durchsatz	60
Best Practice	61
Zusätzliche Filter	62
Fehlersuche	65
Technischer Hintergrund	66
Zusammenfassung	68
6 Network Address Translation	69
Laboraufbau	70
Szenarios	71
IPv6	78
Technischer Hintergrund	80
Zusammenfassung	80
7 Webfilter	81
Laboraufbau	83
Filteraktion	83
TLS Inspection	88

Ausblick	92
Technischer Hintergrund	93
Zusammenfassung	94
8 Webserver-Schutz	95
Laboraufbau	95
Basisschutz	97
Erweiterter Schutz	99
Fehlersuche	100
Praxisbeispiel: E-Mail-Archiv Piler	100
Ausfallschutz	103
Technischer Hintergrund	103
Ausblick	104
Zusammenfassung	104
9 IPFIX	107
Inhalt eines Flows	107
Labor	108
Exporter	109
Kollektor	110
IPv6	111
Fehlersuche	112
Cloud	113
Technischer Hintergrund	116
Zusammenfassung	116
10 Cloud	117
Logging as a Service	117
Backup	120
Zusammenfassung	124
11 Best Practice	125
Factory-Default	125
Durchsatz messen	126
SSH-Login ohne Passworteingabe	128
Passwort zurücksetzen	131
Quality of Service	133

TLS-Zertifikat	135
Unbenutzte Firewallregeln erkennen	137
12 Life Hacks	139
Zugriff von Windows	140
Telegram	140
Speedtest	143
Startton ausschalten	143
Application Programming Interface	144
13 Architektur	149
Allgemeines	149
Systemstart	151
Konfigurationsdienst	151
Einbruchserkennung	153
Datenbank	153
Webserver	154
Paketfilter	155
Logging	155
Webfilter	156
Backup	158
Verschiedenes	159
Zusammenfassung	161
Literaturverzeichnis	163
Index	165
A IP Version 6	171
B Editor unter Linux	175
C Zusatzmaterial	179