FIREWALLS AND NETWORK SECURITY

Learn to perform the duties of a **Network security engineer** through **expert-level** knowledge of Cisco firewalls.

From Beginner to Advanced

- No previous security experience necessary



DR JONAS BIRCH

9 789152 749807

Prerequisetes:

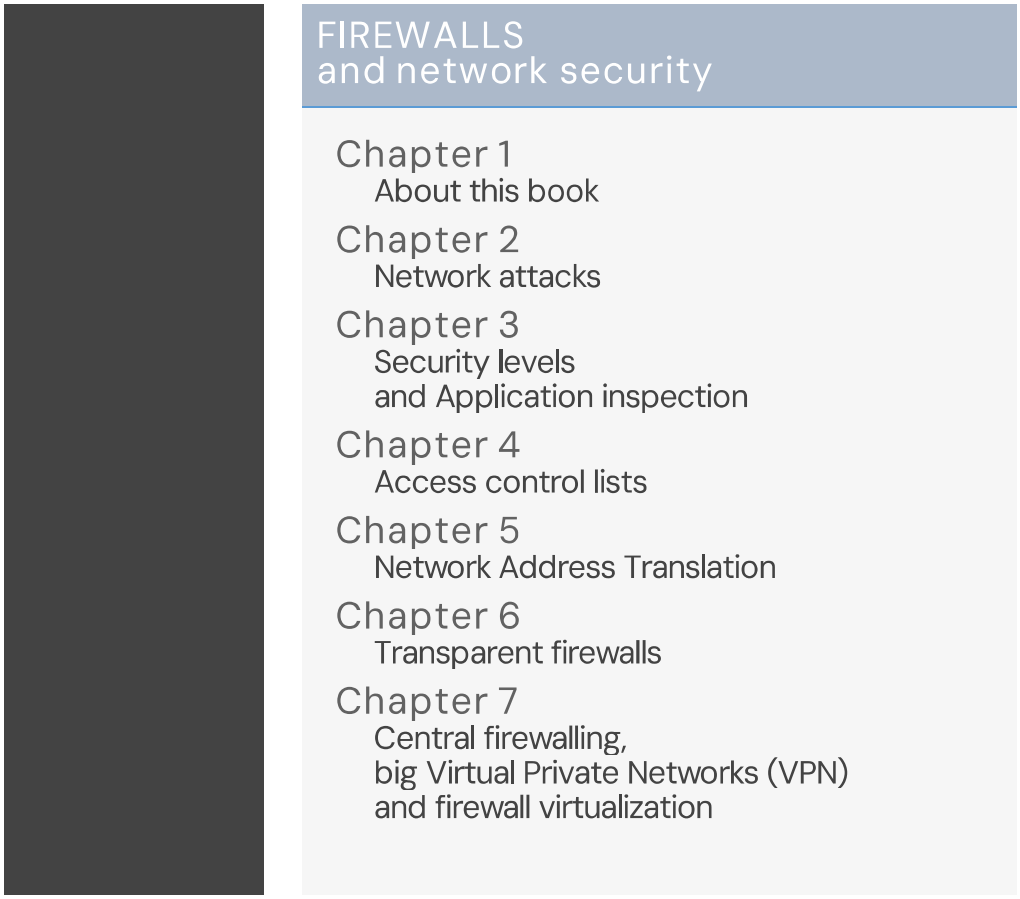
- You need to know the basics of IP networks

Art.no 2
ISBN 978-91-52-74980-7
Edition 1:1
© 2026 BJOERKULTUR EF. All rights reserved. No part of this book may be reproduced in any form without written permission from the author, except for brief quotations in reviews or if you've purchased a printable PDF license. You may only print as many copies as you've purchased.
Stockholm, SWEDEN
doctorbirch.com

Firewalls and Network Security

DR JONAS BIRCH, 2026

Contents at a glance



Chapter 1
About this book
Chapter 2
Network attacks
Chapter 3
Security levels
and Application inspection
Chapter 4
Access control lists
Chapter 5
Network Address Translation
Chapter 6
Transparent firewalls
Chapter 7
Central firewalling,
big Virtual Private Networks (VPN)
and firewall virtualization

Table of contents

Contents at a glance 3
Chapter 1: About this book 9
1.1 Foreword 9
1.2 About this book's author 10
1.3 Outline 11
Chapter 2: Network attacks 14
2.1 Mac spam 14
2.2 How a switch reacts to mac-spam 15
2.3 Protection against mac-spam 15
2.4 Mac spoofing 16
2.5 IP spoofing 16
Smurf attacks 17
2.6 Arp spoofing and IP sniffing 18
2.7 DHCP snooping and arp inspection 18
uRPF 19
2.8 Denial of Service 19
Click nuke 19
Winnuke 20
Generic DoS attacks 20
2.9 DDoS 20
2.10 Protection against DDoS 21
Scrubbing traffic with a "washing machine" 22
Modern scrubbing techniques for syn flood 22
2.11 Encryption 23
2.12 Symmetric encryption 23
2.13 Asymmetric encryption 24
2.14 Secure Socket Layer and certificates 25
2.15 SSH 25
2.16 Spam 26
2.17 Lab: Basic configuration of your firewall 27
Chapter 3: Security zones and application inspection 33
3.1 Security zones 33

Access Lists 34
Demilitarized Zone 34
Firewall as a Gateway 35
3.2 Application Inspection 36
Return Traffic 36
The Connection Table 37
3.3 TCP and UDP 38
New TCP Connections 38
Tearing Down TCP Connections 39
Handling UDP 39
3.4 Domain Name System 40
The DNS and IP Headers 40
How the Firewall Handles DNS 40
Authoritative DNS Responses 41
DNS Forwarders 41
Example of DNS Application Inspection 42
3.5 Configuring Application Inspection 43
Access Lists 44
Classes 45
Inspection Policies 45
Policy Maps 46
Activating the Policy 46
3.6 TCP Intercept 47
Configuring TCP Intercept 47
Chapter 4: Access Control Lists (ACL) 49
4.1 Access Control Lists 49
4.2 How Access Lists Work 50
Applying ACLs 50
4.3 Different Types of ACLs 50
4.4 Standard Lists 51
Remark 51
Permit and Deny 51
Implicit Denial 52
Most Specific ACE at the Top 52

4.5 Extended Lists 53
Filtering by Protocol and IP Addresses 53
Ports 54
Username 54
Interface 55
Logging 55
Disabling ACEs 56
Renaming 56
Inserting Lines 56
Time ranges 57
4.6 Web Lists 58
URL-Based Web Lists 59
TCP-based web lists 60
4.7 ACL activation 61
Inbound ACLs 61
Configuring an Inbound ACL 61
Outbound ACLs 62
Configuring an Outbound ACL 63
Global Access Lists 63
4.8 Object-Based Lists 64
Objects 65
Object Groups 66
Chapter 5: Network Address Translation 69
5.1 Network Address Translation 70
5.2 The NAT process 70
5.3 Return Traffic 71
5.4 Dynamic NAT 72
5.5 Static NAT 74
5.6 Configuring dynamic NAT 74
5.7 Configuring Static NAT 77
5.8 Configuring an ACL for static NAT 79
5.9 Auto-NAT 80
5.10 Manual NAT 81
5.11 Configuring Manual NAT 82

5.12 PAT and port forwarding 84
5.13 Configuring port forwarding 85
5.14 Unidirectional NAT 88
5.15 Identity NAT 88
5.16 Translating destination addresses 92
5.17 The technology behind Port Address Translation 96
5.18 Twice NAT 98
Review questions 102
Chapter 6: Transparent firewalls 106
6.1 Traditional Layer 3 Firewalls 106
6.2 Why Transparent Firewalls? 106
6.3 Existing Networks 107
Within a Local Network 107
Non-IP Network Protocols 107
6.4 Bridge domains 108
6.5 Configuring Transparent Firewalls 109
Our example network 109
Switching to Transparent Mode 109
Preparing ports and IP addresses 110
Configuring NAT and access lists 111
Configuring the router 112
Hardening the Server Further 113
Chapter 7: Central firewalling, big VPNs and virtualization 114
7.1 MPLS VPN 114
7.2 Ethernet over MPLS 115
7.3 Virtual Private LAN Services 116
7.4 L2VPN with internet access 117
7.5 Disadvantages of L2VPN 118
7.6 L3VPN 118
7.7 MPLS L3VPN 119
7.8 Central Firewall (Corporate Network) 120
7.9 Central Firewall (ISP Network) 121
7.10 Virtualization 123
7.11 Our Example Environment 123

7.12 Contexts 125
7.13 Configuring Virtualization 126
Firewall Mode 126
The System and Admin contexts 127
Basic Port Configuration 127
Creation of contexts 128
Allocation of ports 129
Allocating Resources 130
Shared interfaces 131
7.14 Summary 131
Appendix 1: Reference list 133
Appendix 2: Alphabetical index 134

Chapter 1: About this book

DURING a time where more and more tech jobs are being taken over by the machine, many are migrating towards a job as Network security engineer. This will be the last job to ever be taken over by AI – if it even happens at all.

–Why? The reason is not technological, but social. In case of a major security incident in a computer network, there must be somebody responsible. Imagine a bank telling its customer who lost all their savings to hackers, that "well, we put a machine in charge of our cyber security, and the machine got hacked…"

1.1 Foreword

If you already have a basic understanding of IPv4-based networks (perhaps from my other book, *Foundation of network technology, 2024*), and you manage to learn every single thing of this book...

...then you will be able to perform 80% of the duties of a network security engineer.

This includes setting up a secure computer network from scratch and configuring the firewalls according to the best practices of the industry. And also, by "perform" I am not talking about just theoretical knowledge, this book will teach you how to type in the actual commands to the firewall, in addition to learning all the relevant technologies.

This book will give you all knowledge necessary for the first half of CCIE Security ver. 6.0, the most prestigious network security certification in the world, and its holders earn hundreds of thousands of US dollars per year on average.

– dr Jonas Birch, Nov 2026