

Table of Contents

Preface	xv
Free Benefits with Your Book	xxi
Chapter 1: Understanding the Core Technologies	1
Technical requirements	2
Understanding the zone-based firewall	2
Expected behavior when determining zones	5
Understanding App-ID and Content-ID	7
How App-ID gives more control • 7	
How Content-ID makes things safe • 9	
<i>Inline evaluation</i> • 10	
The management and data planes	10
Authenticating and authorizing users with User-ID	12
Summary	12
Chapter 2: Setting up a New Device	15
Technical requirements	15
Gaining access to the user interface	16
Accessing the management interface • 19	
Connecting to the web interface and CLI • 20	
Adding licenses and setting up dynamic updates	23
Creating a new account • 23	
Registering a new device • 24	
Activating licenses • 26	
<i>Activating licenses via the customer support portal</i> • 26	
<i>Activating licenses via the web interface</i> • 28	
Downloading and scheduling dynamic updates • 30	

Upgrading the firewall	35
Understanding the partitions • 35	
Upgrade considerations • 36	
Upgrading via the CLI • 39	
Upgrading via the web interface • 41	
Limiting access via an access list • 45	
Accessing internet resources from offline management • 48	
Admin accounts • 50	
<i>Dynamic accounts</i> • 50	
<i>Role-based administrators</i> • 51	
<i>Password security</i> • 53	
External authentication • 55	
<i>The TACACS+ server profile</i> • 55	
<i>The LDAP server profile</i> • 56	
<i>The RADIUS server profile</i> • 57	
<i>The Kerberos server profile</i> • 59	
<i>The SAML server profile</i> • 60	
<i>The MFA profile</i> • 61	
<i>Setting up the authentication profile</i> • 62	
Understanding the interface types	66
VWire • 66	
The Layer 3 interface • 68	
<i>Exploring the interface</i> • 68	
VR • 75	
The Layer 2 interface and VLANs • 78	
Tap interfaces • 80	
The Decryption Port Mirror interface • 81	
The loopback interface • 82	
The tunnel interface • 83	
Subinterfaces • 84	
HA interfaces • 85	
AE interfaces • 85	
Summary	87

Technical requirements	89
Understanding and preparing security profiles	89
The Antivirus profile • 90	
The Anti-Spyware profile • 94	
The Vulnerability Protection profile • 99	
URL Filtering profile • 102	
<i>Custom URL categories</i> • 102	
<i>Configuring the URL Filtering profile</i> • 103	
<i>URL filtering priorities</i> • 108	
The File Blocking profile • 109	
The WildFire Analysis profile • 110	
Custom objects • 112	
<i>The Custom Spyware/Vulnerability objects</i> • 113	
<i>The custom data pattern</i> • 118	
Security profile groups • 119	
Understanding and building security rules	119
Dropping “bad” traffic • 120	
<i>Action options</i> • 123	
Allowing applications • 124	
<i>Application dependencies</i> • 127	
<i>Application-default versus manual service ports</i> • 128	
Controlling logging and schedules • 129	
Address objects • 131	
Tags • 131	
Policy Optimizer • 132	
<i>The Apps Seen column</i> • 133	
Creating NAT rules	134
Inbound NAT • 134	
Outbound NAT • 136	
<i>Hide NAT or one-to-many NAT</i> • 137	
<i>One-to-one NAT</i> • 139	
<i>U-turn or hairpin NAT</i> • 141	
<i>Enable DNS Rewrite</i> • 142	
Summary	144

Technical requirements 147

Controlling the bandwidth with quality-of-service policies 147

- DSCP and ToS headers • 148
- QoS enforcement in the firewall • 149
 - Creating QoS profiles* • 150
 - Creating QoS policies* • 157

Leveraging SSL decryption to look inside encrypted sessions 162

- SSH proxy • 162
- SSL forward proxy • 162
- SSL Inbound Inspection • 170
- Forwarding sessions to an external device • 171

Redirecting sessions over different paths using policy-based forwarding 172

- Redirecting critical traffic • 172
- Load balancing • 174
 - Policy based forwarding* • 174
 - IPSec redundancy via virtual routers* • 177
 - Equal cost multipath as an alternative* • 177

Summary 179

Chapter 5: Services and Operational Modes **181**

Technical requirements 181

Applying a DHCP client and DHCP server 182

- DHCP client • 182
- DHCP server and relay • 183

Configuring a DNS proxy 186

Setting up high availability 188

- Active/Passive mode • 189
- Active/Active mode • 190
- Clustering • 191
 - Firewall states* • 193
 - HA interfaces* • 193
- Setting up Active/Passive mode • 196
- Setting up Active/Active mode • 200
- HA1 encryption • 206

Enabling virtual systems	207
Creating a new VSYS • 208	
Administrators in a multi-VSYS environment • 211	
Inter-VSYS routing • 212	
Creating a shared gateway • 215	
Managing certificates	217
Summary	223
Chapter 6: Identifying Users and Controlling Access	225

Technical requirements	225
User-ID basics	226
Configuring WMI probes • 227	
Setting up a User-ID agent • 228	
<i>Configuring the User-ID agent • 229</i>	
<i>Adding the User-ID agent to the firewall • 232</i>	
Setting up a Terminal Server agent • 234	
<i>Configuring the TS agent • 234</i>	
<i>Adding the TS agent to the firewall • 237</i>	
Agentless User-ID • 237	
Configuring group mapping	241
The Cloud Identity Engine • 247	
Configuring Entra ID (Azure) enterprise applications • 254	
Setting up a captive portal	258
Authenticating users • 259	
Configuring the authentication portal • 263	
Using APIs for User-ID	266
User credential phishing prevention	269
Summary	271

Chapter 7: Managing Firewalls Through Panorama **273**

Technical requirements	273
Setting up Panorama	274
Initial Panorama configuration • 276	
Panorama logging • 283	
<i>Adding disks to Panorama • 284</i>	
<i>Log collection options • 284</i>	
<i>Deploying Log Collectors • 285</i>	

Device groups	290
Adding managed devices • 291	
Preparing device groups • 295	
Creating policies and objects • 296	
Important things to know when creating objects in device groups • 300	
Setting up default attributes • 301	
Setting up templates and template stacks	303
Leveraging variables to customize common configurations • 305	
Panorama management	307
Device deployment • 307	
Migrating unmanaged to managed devices • 309	
Panorama HA • 310	
Replacing one device with another • 311	
Tips and tricks	312
Summary	315

Chapter 8: Managing Firewalls Through Strata Cloud Manager 317

Setting up Strata Logging Service	317
Activating Strata Cloud Manager	318
Creating a subtenant • 320	
Activating Strata Cloud Manager from the hub • 322	
Activating AIOps or Strata Cloud Manager for NGFW • 325	
Configuring Strata Cloud Manager	328
Starting with the Manage tab • 328	
NGFW and Prisma Access • 330	
Security rules • 333	
Snippets • 334	
Security profiles • 338	
Access management • 339	
Associating devices to Strata Cloud Manager	341
Managing devices and device configuration through Workflows	343
Device Onboarding • 344	
Folder Management • 346	
Device Management • 347	
Device Settings and Global Settings • 349	
Exploring dashboards	352
Summary	356

Technical requirements	357
Documenting key aspects	358
Upgrade considerations • 358	
Upgrade path • 360	
Preparing for the upgrade	360
The upgrade process	363
Upgrading a single Panorama instance • 364	
Upgrading a Panorama HA cluster • 364	
Upgrading log collectors (or firewalls) through Panorama • 366	
Upgrading a single firewall • 367	
Upgrading a firewall cluster • 368	
After the upgrade • 371	
The rollback procedure	371
The downgrade procedure	372
Special case for upgrading older hardware	373
Summary	374

Chapter 10: Logging and Reporting

Technical requirements	375
Log storage	376
Configuring log collectors and log collector groups	378
Leveraging Strata Logging Service	381
Logging to an external syslog	383
Configuring log forwarding profiles	384
System logs • 387	
Firewall logs • 388	
Filtering logs	392
Predefined reports and creating custom reports	397
Predefined reports • 398	
Custom reports • 399	
Using the Application Command Center	405
Summary	410

Technical requirements 411

Configuring GRE 412

Configuring the IPsec site-to-site VPN 413

- Setting up a (phase 1) IKE Crypto profile • 413
- Setting up a (phase 2) IPsec Crypto profile • 416
- Setting up the IKE Gateway • 418
- Setting up the tunnel interface • 423
- Creating the IPsec tunnel • 423

Configuring GlobalProtect 427

- Setting up the portal • 428
- Clientless VPN • 439
- Setting up the gateway • 443
- HIP objects and profiles • 447

Summary 450

Chapter 12: Advanced Protection 451

Technical requirements 451

Creating custom applications and application overrides 451

- Application override • 452
- Signature-based custom applications • 455

Creating custom threat signatures 460

Implementing zone protection and DoS protection 464

- System protection settings • 465
 - Packet Buffer Protection* • 465
 - TCP settings* • 466
- Configuring zone protection • 468
 - Packet Buffer Protection and L3 & L4 Header Inspection* • 475
- Configuring DoS protection • 478

Summary 482

Chapter 13: Troubleshooting Common Session Issues 483

Technical requirements 483

Using the tools in the web interface 483

- Log files • 484
- Packet captures • 488

<i>Configuring filters</i> • 488	
<i>Configuring capturing</i> • 490	
<i>Capturing packets on the management interface</i> • 491	
Botnet reports • 492	
Interpreting session details	494
Understanding session states and types • 494	
Terminating and clearing sessions • 497	
Viewing session data from the CLI • 497	
Applying filters • 500	
Using the troubleshooting tool	501
Testing policies • 502	
Testing connectivity • 503	
Testing with traceroute • 505	
Using Maintenance Mode to resolve and recover from system issues	507
Summary	512
Chapter 14: A Deep Dive Into Troubleshooting	513
<hr/>	
Technical requirements	513
Understanding global counters	513
Finding issues through counters • 519	
Analyzing session flows	521
Preparation • 525	
Execution • 525	
Cleanup • 526	
A practical example • 527	
Debugging processes	542
CLI troubleshooting commands cheat sheet	544
Summary	554
Chapter 15: Cloud-Based Firewall Deployment	555
<hr/>	
Technical requirements	555
Licensing a cloud firewall	556
Deploying a firewall in Azure	558
Bootstrapping a firewall	570
Creating a new storage account • 570	

Creating a bootstrap file share • 573	
<i>The init-cfg.txt file</i> • 575	
<i>The bootstrap.xml file</i> • 578	
Bootstrapping a firewall on Azure • 579	
Putting the firewall in line	582
Adding a new public IP address • 584	
Adding the Untrust subnet to an NSG • 584	
Creating a server subnet • 586	
Setting up routing • 586	
Forcing internal hosts to route over the firewall • 588	
Setting up a load balancer	590
Summary	598
Appendix A: Advanced Features	599
<hr/>	
Enabling the Advanced Routing Engine	599
Activating cloud logging without centralized management	601
Troubleshooting SLS connectivity • 603	
Prerequisites • 603	
<i>Testing connectivity</i> • 603	
<i>No logs showing in Strata Logging Service</i> • 605	
Summary	606
Appendix B: Unlock Your Exclusive Benefits	607
<hr/>	
Other Books You May Enjoy	611
<hr/>	
Index	615
<hr/>	