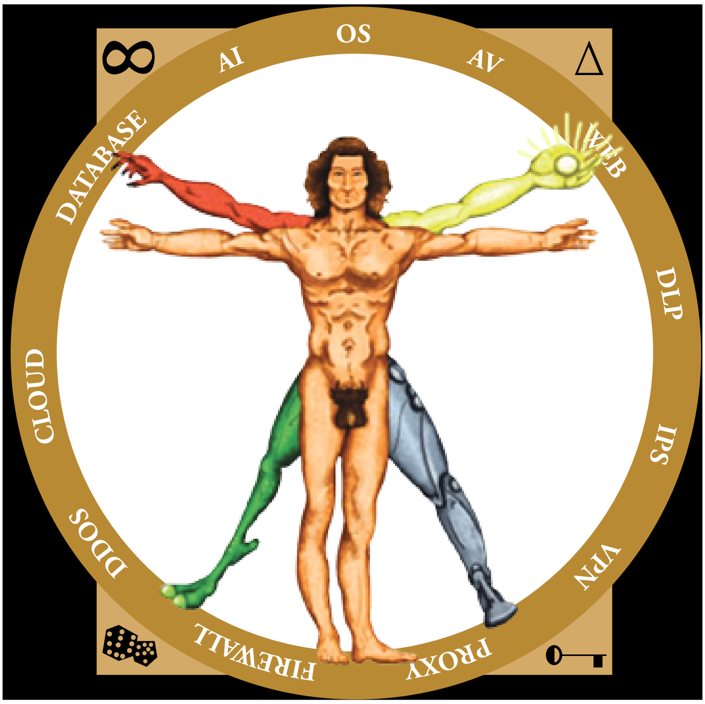

OS
AV
WEB
DLP
IPS
VPN
PROXY
FIREWALL
DDOS
CLOUD
DATABASE
AI

DISCLAIMER

This book is intended for mature readers, 18 or older. Those sensitive to religious and cultural provocations should seek other books. Similarly, if local law forbids ownership of provocative materials, please do not read.

This is a work of fiction. Names, characters, businesses, places, events, locations, and incidents are either fictitious or used in a fictitious manner. Any resemblance to actual persons, living or dead, or actual events, is purely coincidental.

The views expressed herein come solely from the author's imagination and do not reflect that of his employer. Any technologies mentioned—especially Palo Alto, Check Point, Juniper, Cisco, Arbor, F5—are mentioned without consent or endorsement. The author would like to stress this is a work of fiction and an exercise in freedom of speech. As such, the author does not promote hatred toward religions, races, creeds, etc. What follows is pure imagination; fiction interweaved with a handful of the author's personal opinions.

The information provided within this book is for general informational purposes only. While every effort is made to keep the information up to date, the author makes no guarantee, explicit or implied, about the completeness, accuracy, reliability, suitability, or availability with respect to the information, products, services, or related graphics contained herein. Information is to be used at the reader's risk.

Please email any questions, concerns, criticisms, disputes, feedback, or suggestions to readers@jasebastin.com. Also, please visit our website at www.jasebastin.com for more details about this book and new releases.

Publisher: StarkSecurity
Paperback: ISBN: 978-0-9898675-2-8

ABOUT THE BOOK

Let's Learn Palo Alto NGFW is the first-ever technical manual marrying information security technology to a rich, fictional narrative. The combination of fact and imagination strives to engage, inform and entertain.

The narrative follows Nielair. He is a man of many names: a digital security guru, an industry unto himself, a trailblazer. Hernyka works the counter at an NYC hole-in-the-wall electronic store. Their chance meeting on a sweltering summer morning kindles discovery and adventure. Hernyka thirsts for knowledge. Nielair desires a student. Together they lose days in the comparative study, configuration, and management of Palo Alto, Check Point, Juniper, Cisco, Arbor, SourceFire and F5 products. Guided by the mysterious Nielair, Hernyka dives deep into next-generation firewall concepts, networking fundamentals, NAT, Layer 2/3, Tap and VWire deployment methods.

Hernyka's curiosity isn't confined by digital trends, though. The spark between student and teacher is explosive. Hernyka and Nielair challenge each other on politics, religion and philosophy. Conspiracy theories, the new world order, flat earth theory, cults, porn and countless mysteries bounce between them.

The pair embarks on an adventure through New York and beyond. Their road is paved with hacking, pen-testing, open-source tools, hardware specifications, API management, and securing applications and operating systems. Nielair's guidance molds Hernyka into a master of App-ID, vulnerability protection, content and URL filtering, Intrusion Prevention System (IPS), Web Application Firewall (WAF), proxies, authentication, VPNs, failover, the Panorama management tool, and troubleshooting.

Through Hernyka, readers will learn to build—and then break—an NGFW. Nielair teaches network security and network hacking alike. His lessons illuminate NMAP and other scanning tools, information gathering, password management, cracking, and hacking using Kali Linux. Do you want to build a Trojan? Reverse engineer viruses? Master Cyber Threat Intelligence? Hernyka learns malware analysis, digital data elimination, device encryption, anonymous networks like TOR, evading mass surveillance, and more.

Let's Learn Palo Alto NGFW is a complete guide for security professionals and IT experts. Even seasoned pros often lack confidence in key areas. Fear no more; Hernyka and Nielair cover Wireshark packet captures with essential TCP/IP concepts (for amateurs as well as pros), BGP, and HTTP. Every lesson is in clear, concise language. *Let's Learn Palo Alto NGFW* will leave IT novices and pros alike with the utmost confidence in their day-to-day work.

Once out from New York, though, Nielair and Hernyka face impossible decisions. What is their relationship? Who are they, truly? Are they student and teacher…or something more? The whole of North America opens before them, infinite with possibility. They can (and will) be anyone. Do they start an IT company and set the world on fire? Do they part ways? Or do they follow the open road all the way to Alaska's coalfields?

A FEW TIPS FOR READING, LEARNING, AND EXPLORING

Here are a few tips to help readers better comprehend *Let's Learn Palo Alto NGFW*:

1. Any bolded text within single quotes, such as 'show config', indicates a command meant for input.

2. Read the book in its entirety. Those skipping chapters run the risk of missing key technical points and breaking the continuity of fiction. For novices, reading in order allows lessons to build one atop another. For experts, reviewing information strengthens the foundations of knowledge.

3. The text includes several suggested websites for in-depth details on each subject. Exploring these sites will deepen your knowledge. This includes searching the sites of mentioned tools for additional tools, KB documents, and whitepapers. As you read, it may be helpful to make notes of these sites to explore further after finishing the book.

4. DO NOT test anything learned from this book in a production environment. All experiments should be conducted in a lab or with the express consent of a network administrator. The author of this book refuses any responsibility for the stupidity of overeager readers. Be responsible and smart!

Expect to spend a year or more to master the information security concepts written here. Online forums can be a big help if you become stuck on a topic. Also try talking to friends, or reaching out to experts via social media. If nothing else, if you out to me, I will do my best to help. Packet captures, logs, CLI outputs, debugs, and config checks can help figure out any problem. No books, videos, or training courses can teach you everything. It is only your self-initiation, vigor, and enthusiasm that will make you a strong engineer and expert. Explore thyself!

On the other hand, I'd advise against researching any unfamiliar characters, events, or persons mentioned in the fictional portions. Just continue reading. Also, keep in mind this is a work of fiction. Two notorious characters talk freely about the world as they see it. Please don't fret over personal disagreements regarding certain topics. Hopefully, progressing toward the end will reveal answers to all humanity's problems. Be patient.

Have fun reading…I guarantee you will be thrilled!!!

BACKGROUND

I began writing this book shortly after being laid off by a pervert and pimp company. I pray that such people should no longer exist. After publishing fiction, however, I lost the drive to complete my savvy Palo Alto project. My dearest friend, Amanda Lankford, insisted I continue. She offered to purchase me new Palo Alto gear for the project; I refused. At this time, I left NYC for India, the wonderful land of my birth. There I saw oppression. I saw hope destroyed, poverty, depression, and a society of the selfish rich. Sorrow broke my heart.

I traveled to Asia, visiting almost 30 countries. And while some Asian nations prosper, the squalid living conditions in many equaled India's. I wondered: are all third world countries destined to be poor? Are the oppressed destined to live under the heel of rich elites? I was supposed to return to NYC after my travels, but couldn't. For the first time in my life, I realized that I belonged to a hopeless, inferior crowd. I saw the same in country after country—despite preaching equality, in every nation, a person is their money, their race, their family's heritage, caste, passport, citizenship, and creed.

Despite numerous opportunities to leave India, I decided to stay. I wanted to improve the peoples' lives and unite the world. But what could I do? India is most famous for computer science. Almost every major corporation has an IT office here. I saw brilliant scientific and mathematical minds working like dogs for faceless multinational corporations. Creativity, innovation, motivation and free thinking were practically forbidden. I saw my fellow countrymen and women made intellectual slaves to Western civilization's Renaissance inventions.

It was this feeling of wasted creativity that resurrected the Palo Alto NGFW book. I returned to it, interweaving a fictional narrative. With this book, I aim to destroy the notion that tech books are for nerds, and that engineers are humorless, non-creative automatons. If that were true, what a dull profession technology would be! My good friend in India helped me buy a Palo Alto gear to begin this project. I went to all the training institutes and finally got a PA box.

The first draft of this Palo Alto book resembled a romance novel. Through revision, it slowly became more like the movie *Mr. & Mrs. Smith*, discussing global politics and religion, history and cults, and science to the singularity. With a broken Internet connection and derision from my friends, I rose with utmost zeal and, pen in hand, started my journey against a land of hopelessness and impossibility.

Mr. Ravikumar Ramachanadran, who I call my "lab master," helped me set up the lab; a big kudos for him. I convey my special thanks to my cook, dearest Suma, my maid Radhika, my building manager Mahadevappa SR, and my electrician Nagaraj B. C. who helped and supported my stay in India. Without these wonderful people, I wouldn't have ever finished this book.

I don't belong to an affluent family or superior race. I do not claim the magical birth of Jesus or Buddha. I am from an oppressed class. I sincerely hope good and evil will one day unite. You don't need to accept my path or follow me. This book, born in India, will hopefully grow to be the gospel of technology. I hope the world rightly recognizes India as one of the great early civilizations, rich with culture, religion, literature, and poetry. Now, in this modern world, this mighty suppressed third world country has delivered the first fictional technology book. You can change anything and rise together!

REFERENCES

As the author, I want to thank those responsible for the following books, websites, videos, discussion forums, wikis, knowledge bases, archives, manuals, administration guides, quick tips, and blogs used as a reference for this book. I used the following resources mostly as cross-references. From some I extracted information in the hopes of better articulating their ideas in a more readable format. I sincerely appreciate the knowledge relayed by these references' authors. Without them, this work would have been impossible. If time permits, I hope to personally meet everyone to extend my deepest respect and thanks. Sincerest apologies to anyone missed. I have done my best to include as much as possible.

www.paloaltonetworks.com
www.juniper.com
www.f5.com
www.ibm.com
www.symantec.com
www.kali.org
www.ietf.org
www.mcafee.com
www.techrepublic.com
www.wikipedia.org
www.snort.org
www.novell.com
stackoverflow.com
stackexchange.com
www.tldp.org
www.oracle.com
www.owasp.org
github.com
www.udemy.com
www.coursera.org
www.ciscopress.com
www.rapid7.com
www.smashingmagazine.com
superuser.com
www.checkpoint.com
www.cisco.com
www.microsoft.com
www.netscout.com/arbor
www.norton.com
www.sourcefire.com
www.rackspace.com
www.wireshark.org
www.searchnetworking.techtarget.com
www.serverfault.com
www.metasploit.com
www.ehowstuff.com
www.tcpdump.org
www.brocade.com
www.sophos.com
www.trendmicro.com
php.net
www.cbtnuggets.com
www.udacity.com
www.howtogeek.com
www.netgear.com
www.tradepub.com
ftp://ftp.uni-duisburg.de/LDAP
www.grc.com

reddit.com
www.watchguard.com
www.w3.org
www.nist.gov
www.scribd.com
www.fireeye.com
www.gigamon.com
www.bitpipe.com
www.safaribooksonline.com
www.exploit-db.com
www.gartner.com
www.technet.com
www.tumblr.com
www.berkeley.edu
www.nsa.gov
www.cs.princeton.edu
www.mit.edu
www.ics.uci.edu
www.apple.com
www.linuxjournal.com
www.ieee.org
www.zdnet.com
www.pcworld.com
www.techcrunch.com
www.thegeekstuff.com
www.defcon.org
www.w3schools.com
dde.binghamton.edu
www.apache.org
www.brighttalk.com
www.nmap.org
resources.infosecinstitute.com
philpolstra.com
www.noasolutions.com
www.wordpress.com
www.lifehacker.com
sourceforge.net
code.tutsplus.com
www.docs.djangoproject.com
distilnetworks.com
www.sans.org
www.arstechnica.com
www.securityweek.com
www.oreilly.com
www.tcpipguide.com
www.computerweekly.com
www.highscalability.com
www.redhat.com
www.mozilla.org
www.superuser.com
www.mashable.com
www.networkworld.com
blog.steveklabnik.com
www.informit.com
www.intel.com
www.stanford.edu
www.ehow.com
www.wired.com
www.technologyreview.com
www.hp.com
www.blackhat.com
www.fortinet.com
www.kernel.org
www.vmware.com
www.radware.com
brightcloud.com
www.offensive-security.com
www.cert.org
sumuri.com
www.slideshare.net
www.eetimes.com
www.techtarget.com

packetlife.net
stationx.net
www.hitmanpro.com
www.infosecwriters.com
www.netresec.com
www.capasystems.com
www.cybersecurityschoolonline.com
www.dynatrace.com
www.fir3net.com
packetbomb.com
www.cse.iitk.ac.in
www.sekuda.com
noahdavids.org
blog.smartbear.com
community.spiceworks.com
www.lifewire.com
www.internet-computer-security.com
auth0.com
www.isode.com
blog.varonis.com
panopticlick.eff.org
www.whatismybrowser.com
community.fastly.com
gironsec.com
www.cs.wustl.edu
www.josephspurrier.com
rednectar.net
networklessons.com
srijit.com
www.routerfreak.com
techslides.com
yara-generator.net
www.creativebloq.com
forum.linode.com
www.hcidata.info
blog.ipspace.net
www.packetu.com
www.qacafe.com
www.paloguard.com
biot.com
alumni.cs.ucr.edu
www.lovemytool.com
www.freekb.net
notalwaysthenetwork.com
www.isi.edu
www.stuartcheshire.org
www.enterprisenetworkingplanet.com
blog.mosinu.com
www.w3schools.com
www.ijcncs.org
help.ubnt.com
itbundle.net
opensourceforu.com
www.gracion.com
www.differencebetween.net
psykotedy.tumblr.com
www.radicalresearch.co.uk
www.quirksmode.org
www.hurl.it
glynrob.com
www.virendrachandak.com
www.fourmilab.ch
www.firewall.cx
gcharriere.com
bestitsource.com
wiki.hashphp.org
www.tnu.edu.vn
www.bsk-consulting.de
www.mail-archive.com
blog.michaelfmcnamara.com
www.networking-forum.com
www.plugthingsin.com

www.indeni.com
caws.nsslabs.com
blog.webernetz.net
www.tunnelsup.com
www.linkedin.com/in/infinitytech
training.alef.com
scadahacker.com
www.cybertraining365.com
meyerweb.com
www.scom.uminho.pt
httpd.apache.org
www.networksorcery.com
www.hurricanelabs.com
raymii.org
kalilinuxtutorials.com
wiki.aanval.com
www.hackingtutorials.org
www.cccure.org
www.philadelphia.edu.jo
wijmo.com
jsonip.com
dtrace.org
www.sciencebooksonline.info
www.cloudping.info
woss.name
coding.pressbin.com
www.pinkbike.com
scobleizer.com
duartes.org
fishbowl.pastiche.org
tomazkovacic.com
swarm.jcoglan.com
stevelosh.com
www.jformer.com
fzysqr.com
isobar.com
sectools.org
www.asp.net
51sec.weebly.com
pynet.twb-tech.com
www.rklhelp.com
www.stallion.ee
www.bradreese.com
books.gigatux.nl
www.arrowecs.cz
www.moserware.com
sumuri.com
philpolstra.com
www.roesen.org
www.brighttalk.com
jonathansblog.co.uk
colesec.inventedtheinternet.com
www.cs.northwestern.edu
www.cs.columbia.edu
www.vtcif.telstra.com.au www.telerik.com
shiflett.org
blog.phusion.nl
ocw.mit.edu
www.cryptomuseum.com
www.b3ta.com
probablyinteractive.com
nichol.as
www.diffbot.com
news.ycombinator.com
codefastdieyoung.com
www.andrewault.net
avsquid.com
ejohn.org
www.mnxsolutions.com
rewordio.us
www.contrast.ie
www.mongly.com

bashcurescancer.com
www.quora.com
blogmal.42.org
openmymind.net
compbio.cs.uic.edu
tagstore.ist.tugraz.at
blog.programmableweb.com
www.techradar.com
freebsd.org
www.rlgsc.com
qconlondon.com
networkworld.com
www.codemeh.com
www.igvita.com
www.lighterra.com
babbledrive.appspot.com
krebsonsecurity.com
www.cs.cmu.edu
www.schneier.com
www.rayninfo.co.uk
blog.dansingerman.com
www.coderholic.com
igoro.com
blog.mikecouturier.com
www.learndevnow.com
boredzo.org
www.braintreepayments.com
crockford.com
tools.pingdom.com
pdp11.aiju.de
mlpy.fbk.eu
www.httpsnow.org
www.stanford.edu
ruslanspivak.com
videolectures.net
www.ccs.neu.edu
betterthangrep.com
blog.tiptheweb.org
www.intermediaware.com
blog.sucuri.net
nodeguide.com
archive.codeplex.com
stevehanov.ca
www.heroku.com
tong.ijenko.net
geehwan.posterous.com
journal.paul.querna.org
www.eff.org
i.min.us
devblog.factual.com
broadband.mpi-sws.org
ruby.railstutorial.org
netpoetic.com
www.threatpost.com
cloudfoundry.com
devblog.eduhub.nl
getmnpp.org
madebyevan.com
www.w2lessons.com
www.crashie.com
digg.com
www.goosh.org
matt.might.net
jqfundamentals.com
www.mathworks.com
blog.bolinfest.com
andy.edinborough.org
nodebeginner.org
gogs.info
browsermob.com
www.r-bloggers.com
nist.gov

bashcurescancer.com
archfinch.com
www.vupen.com
www.webkit.org
wonko.com
kkovacs.eu
bellard.org
www.mnot.net
www.onlineschools.org
edweissman.com
spotifyontheweb.com
www.aosabook.org
www.cc.gatech.edu
markmaunder.com
pansentient.com
danwebb.net
telehack.com
www.mcdowall.info
blog.stateless.co
uxmag.com
web2db.ssl.dotcloud.com
www.pitt.edu
bellard.org
resizemybrowser.com
kkovacs.eu
ipinfo.info
rosettacode.org
www.codinghorror.com
www.jmarshall.com
shouldichangemypassword.com
www.open-mike.org
www.phantomjs.org
morethanseven.net
codahale.com
www.quirksmode.org
www.devttys0.com
crowdflow.net
www.pitt.edu
www.nordsc.com
garmahis.com
htmlemailboilerplate.com
www.franciscosouza.com
nefariousdesigns.co.uk
www.xenoclast.org
archive.cert.uni-stuttgart.de
kkovacs.eu
chem-eng.utoronto.ca
www.measurementlab.net
memagazine.asme.org
ontwik.com
apcmag.com
mldemos.epfl.ch
xqueryguestbook.my28msec.com
johnpapa.net
ontwik.com
www.lowendbox.com
mitmproxy.org
blog.dynatrace.com
www.heroku.com
www.technologyreview.com
freddie.witherden.org
htmlcompressor.com
www.thefilterbubble.com
www.tokbox.com
www.xml.com
oasis-open.org
www.epipheostudios.com
citeseerx.ist.psu.edu
keystream.subgraph.com
www.kurzweilai.net
gent.ilcore.com
learn.appendto.com

robohash.org
collusion.toolness.org
h.ackack.net
www.gabrielweinberg.com
www.ixibo.com
www.jamesbreckenridge.co.uk
blog.scoutapp.com
windowsteamblog.com
www.internetsecuritydb.com
hyperpolyglot.org
mocko.org.uk
jcooney.net
www.w3.org
mikeos.berlios.de
www.sourcefabric.org
blog.restbackup.com
nicolasgallagher.com
www.nextthing.org
www.jamesmolloy.co.uk
www.cleveralgorithms.com
acid3.acidtests.org
www.macobserver.com
bethesignal.org
net.tutsplus.com
www.awgh.org
robert.accettura.com
enterprise.neosoft.com
jeremiahgrossman.blogspot.com
gigaom.com
readwriteweb.com
www.makeuseof.com
www.techradar.com
www.labnol.org
www2.opensourceforensics.org
notanumber.net
rdist.root.org
www.privacychoice.org
tomayko.com
itproportal.com
urlblacklist.com
toolchain.eu
tumblr.jonthornton.com
blog.passpack.com
nerdiversary.com
www.semicomplete.com
www.devttys0.com
zombie.labnotes.org
www.webmproject.org
arborjs.org
stevehanov.ca
hoisie.com
jsfiddle.net
seventhings.liftweb.net
rdf.dmoz.org
eli.thegreenplace.net
george.hedfors.com
www.lightbluetouchpaper.org
tools.securitytube.net
nerdgap.com
lab.arc90.com
www.htaccessredirect.net
blog.ksplice.com
hackaday.com
mobile.darkreading.com
setiquest.org
arstechnica.com
zdnet.co.uk
www.telegraph.co.uk
tryhaskell.org
simplestcodings.com
www.theopeninter.net
patelshailesh.com

www.iet.ntnu.no
www.secretgeek.net
mylifescoop.com
ascii.textfiles.com
www.getnetworking.net
bgphelp.com
www.ripe.net
www.iana.org
www.radiotap.org
feeding.cloud.geek.nz
www.metageek.com
www.acrylicwifi.com
www.netspotapp.com
www.tomsguide.com
www.debian.org
www.aircrack-ng.org
www.wardriving.com
sectools.org
www.cyberbit.com
www.tutorialspoint.com
www.serverframework.com
www.slant.co
linode.com
www.usenix.org
www.aescrypt.com
esqsoft.com
linoxide.com
support.passware.com
support.passware.com
www.exiv2.org
www.digitalconfidence.com
www.brightfort.com
exifdata.com
www.makeuseof.com
www.intsights.com
iraj.in
gizmodo.com
disattention.com
browsershots.org
www.catonmat.net
www.ciscozine.com
blog.ine.com
www.potaroo.net
crnetpackets.com
discourse.criticalengineering.org
wiki.archlinux.org
www.vistumbler.net
www.nirsoft.net
www.wifipineapple.com
blog.sevagas.com
www.tldp.org
wigle.net
www.canarywireless.com
venturebeat.com
blog.malwarebytes.com
www4.cs.fau.de
andreafortuna.org
gitlab.com
superuser.com
www.peazip.org
www.blancco.com
www.fileshredder.org
cocoatech.com
www.lostpassword.com
www.yubico.com
www.steelbytes.com
www.imagemagick.org
mat.boum.org
loc.alize.us
www.beencrypted.com
www.windowsecurity.com
www.adines.fr

www.illumio.com
seann.herdejurgen.com
www.techopedia.com
www.avolio.com
www.darkreading.com
www.vtcif.telstra.com.au
securityworld.worldiswelcome.com
www.comptechdoc.org
www.math.ucla.edu
forum.wordreference.com
www.starhub.com
users.cis.fiu.edu
www.nta-monitor.com
juniper.mwnewsroom.com
tech.lds.org
www.gossamer-threads.com
www.networkstraining.com
ciscoskills.net
worldtechit.com
www.cnet.com
www.fundinguniverse.com
www.hackmageddon.com
resources.intenseschool.com
www.cpug.org
networkology.net
www.firewall.cx
www.quirksmode.org
www.hurl.it
www.virendrachandak.com
www.fourmilab.ch
srijit.com
www.tnu.edu.vn
www.watchguard.com
www.plugthingsin.com
blog.webernetz.net
www.rklhelp.com
www.schuba.com
www.cs.unm.edu
docstore.mik.ua
www.ranum.com
www.cs.columbia.edu
www.cccure.org
www.ccnahub.com
blog.threatstack.com
www.cs.utexas.edu
www.linktionary.com
blogs.brisbanetimes.com.au
www.openstack.org
www.cc.com.pl
www.e-spincorp.com
www.jma.com
www.educause.edu
mellowd.co.uk
www.ciscofiles.com
www.bradreese.com
successstory.com
www.wikinvest.com
packetflow.io
rumyittips.com
www.maxpowerfirewalls.com
www.santlive.com
www.radicalresearch.co.uk
community.fastly.com
.cs.wustl.edu
www.josephspurrier.com
rednectar.net
bestitsource.com
tomahawk.sourceforge.net
www.networking-forum.com
www.indeni.com/community
www.networksbaseline.com
training.alef.com

www.stallion.ee
www.redmine.org
www.smeegesec.com
www.slashroot.in
openwall.info
www.computernetworkingnotes.com
globalconfig.net
raymii.org
www.hackingarticles.in
www.computersecuritystudent.com
www.crunchbase.com
rationallyparanoid.com
hackertarget.com
null-byte.wonderhowto.com
jonathansblog.co.uk
www.shelltutorials.com
samsclass.info
codingstreet.com
etutorials.org
fireverse.org
www.shanekillen.com
www.rutter-net.com
www.optiv.com
itsecworks.com
www.webtorials.com
lists.gt.net
www.vology.com
scadahacker.com
www.yilmazhuseyin.com
www.nczonline.net
www.blackmoreops.com
www.rebeladmin.com
www.techworld.com
www.netcraftsmen.com
www.netmanias.com
www.fuzzysecurity.com
www.dvwa.co.uk
0daysecurity.com
www.commsolutions.com
www.giac.org
www.trustwave.com
opensourceforu.com
www.peerlyst.com
forums.codeguru.com
www.empirion.co.uk
somoit.net
phoneboysecurity.posthaven.com
forums.cabling-design.com
what-when-how.com
danielmiessler.com
www.drchaos.com
www.junosworkbook.com
lamoni.io
netfixpro.com

Juniper SRX Series (book) by Brad Woodberg, Rob Cameron
The Antivirus Hacker's Book by Elias Bachaalany and Joxean Koret
HTTP: The Definitive Guide by David Gourley

CONTENTS

Chapter 1

DIGITAL WORLD, VIRTUAL BOUNDARIES (GENESIS)

Raggedy pigeons swooped down over 53rd Street, hungry for the crumbs surrounding a nearby garbage can. A giant of a man, six feet tall with shoulder-length black hair, stood on the midtown curb, watching the birds descend. His grey suit and wavy hair dancing in the breeze gave the air of an outlaw. Except instead of guns, this desperado slung LEDs and a clamshell; the brown leather bag in his hand was packed full with them.

Seeing the pigeons pecking dirty crumbs, he went into a nearby Starbucks. He returned a moment later, a double-shot macchiato in one hand and a bag of cookies in the other. He slowly approached the birds, his giant hands kneading the bag. The cookies crushed to crumbs, the man crouched, placed them on the ground close to the curb. He whistled softly to attract the nearby birds' attention.

One brave pigeon hopped close. It looked to the man, paused, then pecked at the cookies. Others followed their dirty leader. Soon the whole pack enjoyed their lavish gourmet cookie feast. They ate with frenzied abandon.

Slowly, gently, the man reached out to rub one of the pigeons on the back. Stroking softly, he murmured, "Wall Street should find you a table and napkin."

The man stood and walked to a mid-sized, somewhat nondescript, electronics shop. An array of gadgets and gizmos burst from its worn seams. Cameras, TVs, and laptops glinted with morning sun from their open shelves. PDAs, tablets, and smartphones sat safely locked in a glass cabinet behind the counter, far from the reach of would-be thieves.

A young girl, bespectacled in jeans and a bright red t-shirt, managed the shop. She jumped to attention as the man entered. She attempted small talk while he browsed the gadgets: "This Summer weather is driving away all the bargain hunters. Have you found it's a lot quieter in shops recently?" She absently spun a pen on the countertop. "Sundays are the worst. Everyone is either relaxing in the sun or going to Church. They don't want to shop in small shops like these. I don't blame them though, Gods before gadgets, I'd say!"

"Religious?" the man chuckled.

"Only when I'm sick or playing the lottery."

She moved the pen aside, adjusted her glasses. "Did you come in for something in particular or are you here to take advantage of the air conditioning?"

"No need for AC yet, sweetheart. The sun isn't very strong this time of morning."

He walked toward the counter and noticed *Networking for Dummies* hidden, tucked back near the register. Surprised to see a tech book in a retail store, he asked, “Is that yours?”

“Oh! Yeah, the title makes me look a bit stupid, but it's good for a beginner. Or so I heard.”

He gave an encouraging grin. “A book's title doesn't define its reader's intelligence.”

“Said the evangelist in his suit.” She extended her hand dramatically toward him.

He took her hand and shook it in greeting. “I'm Nielair”

“Just kidding about the suit. You look great. Call me Hernyka. Nice to meet you.”

Nielair reached out, began to flip through the book. “It's been years since I read something like this. Time has changed some of my knowledge, I suspect, but… Yes, I am on my way to church. Are you studying to be a networking guru?”

“Trying,” Hernyka shrugged. “I want to go for a CCIE, but I've got to begin with a CCNA. The courses are expensive, so I'm sticking with dummy editions to cement my foundation.”

“That's a common problem. There are plenty of free online resources and cheap training courses. Have you tried one of those? I'm sure you know how to use Google.”

She chuckled. “Yeah, I've checked out those online courses. I find most of them idiotic. A recorded training session isn't going to replace a real-life teacher. At least not for me. I'm a beginner and I have a ton of silly questions. I listened to a recording once. It was impressive, but it went in through one ear and came out the other. The next day when I woke up, and still couldn't remember what an IP was. It might as well have stood for *iP*od or *I*n *P*erson.” Exasperated, Hernyka threw her hands in the air.

Nielair sympathized. The girl was trying to build a career but finding only roadblocks. “I'd be happy to teach you Internet security,” he said, “maybe firewalls, if you're interested.”

Hernyka was taken aback. “All the IT folks I've asked say to learn networking basics first. Then move on to network security. That's where the money is.”

Nielair shook his head. “Trust me, you'll learn faster talking with me than by listening to some IT monkey who's just collecting paychecks. Most of them leave the business at the mercy of hackers anyway.”

She pursed her lips. Her eyebrows knit together for a moment. Then, her decision made, her expression relaxed. “I don't think I can pass up such a generous offer. Please tell me more.”

Nielair leaned against the counter and took a breath, ready to begin her first lesson. Before he could even speak she interrupted, “Will you start like everyone else? With pre-requisite preaching about how everyone needs basic TCP/IP knowledge, blah, blah, blah…”

Nielair grinned. He raised his arms and craned his neck. Face to the heavens, he preached from his imaginary pulpit, “Let all who thirst for knowledge come to me. English, hard work, and inquisitiveness are all one needs.” He gestured dramatically to one side of the store, then the other, saying, “Today: children. Tomorrow, expert scholars. No one shall be left behind in the information security era.”

He dropped the preaching act, leaned to Hernyka. “Now let's begin.”

Know Your Symbols and Guidelines:

"Our lives revolve around symbols and guidelines. In the case of networking, the Open Systems Interconnection (OSI) model provided the first rules representing communication and functions between two devices. It does not define specific procedures, protocols, or software. Like a restaurant menu, the OSI model provides a description of the items. It does not explain the taste and smell of individual dishes."

"So the OSI model is like a prototype jet displayed in a museum," Hernyka said.

"Good example!" Nielair said. "But the OSI model is theoretical; it does not define protocols. It is a seven-layer stack designed in the late 1970s by the International Organization for Standardization (ISO) and International Telegraph and Telephone Consultative Committee (CCITT). Many say that the ISO built OSI.

"At the same time, the Defense Advanced Research Projects Agency, or DARPA, an arm of the United States Department of Defense (DoD), funded a project to build a Transmission Control Protocol/Internet Protocol suite TCP/IP. It was similar to the OSI model, but had only four-layers."

Hernyka smiled, enjoying the story. "I read about TCP/IP being a four-layered protocol stack… Why would someone use less? Is it more efficient than the OSI model's seven layers?"

Nielair took a moment, sucked his teeth. Eventually he said, "That is a common misconception. Even experienced networking folks aren't sure about which is better: the OSI model by ISO or the DoD's TCP/IP. Both serve the same purpose: allowing devices to communicate with each other. The difference between OSI and TCP/IP is similar to metric units versus imperial units. No one cares whether a filet mignon is weighed in pounds or kilos, or if a car covers a distance in miles or kilometers. The quantity or output is the important part.

"The engineer and design teams for the two models often interact. The OSI model, in fact, was influential in the development of the TCP/IP standard, which is why so much OSI terminology is applied to TCP/IP.

"TCP/IP faced a number of, shall we say, evolution problems in the 1980s. Less layers meant some functionality was bundled together—which caused stability and performance issues. This led to the release of the second TCP/IP version that consisted of five layers. That five-layer version is the most dominant networking model used currently.

"Many ask why the OSI/ISO model failed. In reality, our government pushed via the National Institute of Standards and Technology (NIST), and through contractual policies and legislation from many U.S states, to standardize all hardware and software vendors to implement OSI model. Its implementation would have greatly reduced manufacturing costs."

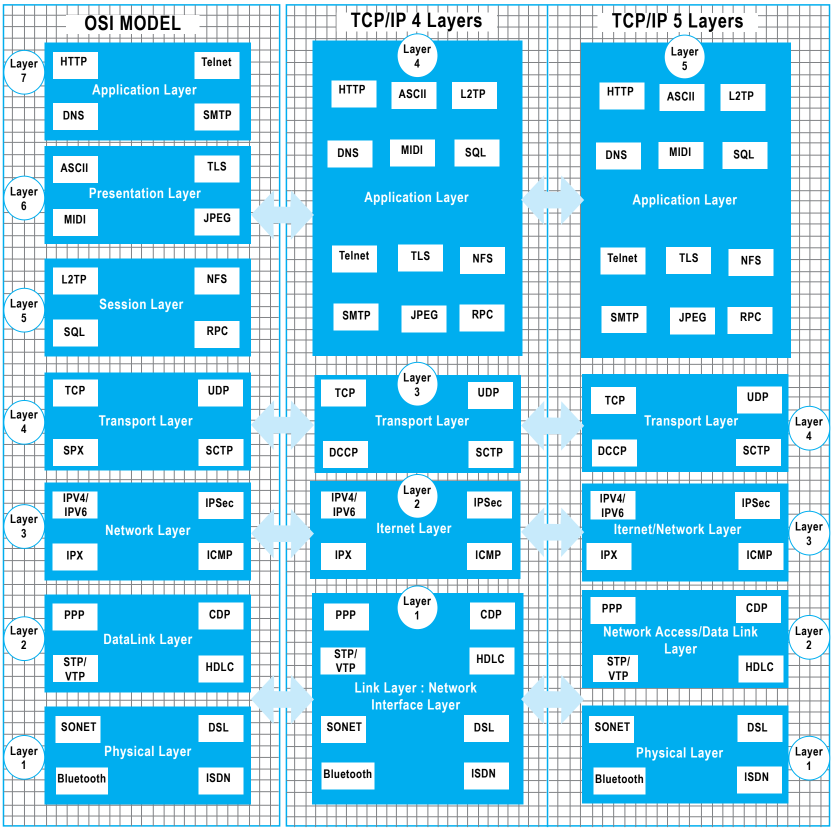
"Unfortunately, the ISO's model of protocols and standards launched late. By then, it was incompatible with most computer systems. TCP/IP was cheaper, CPU-efficient, and available to all operating systems (OS). TCP/IP also had the advantage of being taught in college curriculums everywhere. While TCP/IP had a slow connection setup, lower flow, and error controls, it was a better choice due to its fast standardization, technical documentation and promising development cycle. So the OSI model became obsolete. Not because OSI wasn't better, but because it wasn't as easily available."

"Then why did the US and NIST push the promotion of OSI?" Hernyka asked.

"Now you're talking politics." Nielair smiled. "That's a different beast altogether. But from what I've read, the UNIX operating system wasn't equipped for commercial applications. The poor security, management features, memory, etc., made it less preferred. To fix this, developers invested more time and money to make UNIX OSI-compatible. At the same time, the first implementation of TCP/IP on Cal Berkley's UNIX system, called Berkeley Software Distribution (BSD), was free and relatively effective. Things that are easier to use are nearly always more effective."

Hernyka fidgeted with excitement. "My book didn't cover it that well at all. About the layers, though, could you show me what they mean?"

"Sure." Nielair pulled his laptop out of his bag. "Here are the three gatekeepers of the networking world." He opened a file on his desktop. "This is what connects people."



Hernyka examined the chart, chewed her lower lip. "Is that a Linux operating system?"

"Yeah, it's Debian, the most trusted and preferred OS for anyone who cares about security and privacy."

"I agree," Hernyka nodded. "Windows users are begging hackers to steal their files and data. And I still can't believe that Jennifer Lawrence was so careless with her iPhone security, leaving her private photos exposed to the world's hackers."

The girl was a quick study. Nielair smiled, looking at the image on his laptop.

Hernyka rested her head in her hands and stared appreciatively. "That's a masterpiece, mister! Did you draw it?"

He couldn't resist the quick laugh. "They're just boxes. I'm no Rembrandt… but thank you. It's nice to receive a compliment."

"I really like it. It's eye-catching." Hernyka leaned toward the screen, traced part with a finger. "What are those small boxes? Are they the protocols for each layer?"

"Yes, they are." Nielair's grin sparked with tinges of pride.

"Ok, though." Hernyka leaned back, like a spring drawn back, again ready. "Could you please explain each layer? The concepts of TCP/IP still feel a little out of my grasp."

"Tell you a secret?" Nielair said. "The only people who know TCP/IP really well are its inventors and the people who designed its source code. Everyone else knows just enough to sound like they know what they're doing. If someone is trying to understand TCP/IP, they should jump into the packet capture or source code segment. It's easier and faster than reading books or additional release notes about how a bug was fixed."

She smiled wickedly. "Are you one of those people, Nielair?"

He chuckled. "I'm eco-friendly: I don't waste any more paper on TCP/IP than I have to. I'm definitely not a virtuoso, but I can certainly show you the correct path to build a strong pyramid of TCP/IP."

"This is like the Matrix movies." She extended her arms with flair and bowed her head to him. "Master Morpheus, show me thy path."

Her reply captivated Nielair. He couldn't turn away such openness, such excitement. He took a breath, began to build the world of TCP/IP. "The OSI model's seven hierarchical layers provide an important reference. Remember TCP/IP drew great influence from the OSI model majorly. So I will explain the differences while talking about the OSI model, then summarize TCP/IP."

Layer 7, 4, or 5: Application

"Imagine if King Louis XIV of France had built a grand mansion in Sweden for his six girlfriends. No wait," Nielair paused, "girlfriend sounds too modern. Let's call them 'concubines.' Tired of the War of the League of Augsburg, King Louis wanted to romance his lovers. But his heart belonged to only one of them: Sanna. He wrote Sanna daily letters from his war-worn desk. These letters spoke of how war stole away his humanity. King Louis wrote his love for Sanna often lifted him above from the bloodied battlefields and relit the humanity, the compassion in his heart. Back then, Louis XIV's letters served the same purpose of today's cell phones, iPads, and computers. They were communication tools. Email, chat, text, and social networking are all modern versions of King Louis' letter writing. And they are classified as 'applications.'

"The Application Layer, the topmost layer in any model, does not define the application itself. Rather, it defines services. It is an interface between the actual application—email client or the browser—and communicates to the underlying network. This is how messages are transmitted. For example, the HTTP protocol defines how web browsers can pull the contents of a web page off a web server. There are tons of applications. I've only listed a few in the diagram like as HTTP, Telnet, DNS and SMTP.

"For Louis XIV, after he wrote his letter, what do you think his next step was? As a royal authority, he might have added a dash of perfume and stamped it with his wax seal."

Hernyka giggled. "The French do love their perfume!"

"Exactly. For us, hitting "Send" on an email causes the email program—let's say Outlook—to interact with the application layer. Outlook adds the server address of the destination email as well as the available sender information. This step turns the email into a piece of data. The term 'data' is an encapsulation of the units in networking terminology. The data, along with its header, footer, and trailer, is then sent to the next layer, known as the Presentation. Just like water flows from top to bottom, data in both the OSI and the TCP/IP models move downward."

Layer 6: Presentation

"Before sending his love letter, Louis XIV prepared a suitable way to carry the letter. Like other royals of his time, he would have put his letter in a silver-lined cover. He would have sealed it with the emblem of the French monarchy to ensure no one tampered with his personal correspondence. In a similar fashion, during the Presentation layer, the syntax layer performs the following operations to the data received from the Application layer…"

1. "Formatting/Conversion/Encoding (all three are the same): Let's consider that the letter "A" sent by the application layer needs to get converted into the machine language of 0s and 1s. To do so, the system follows the process below:

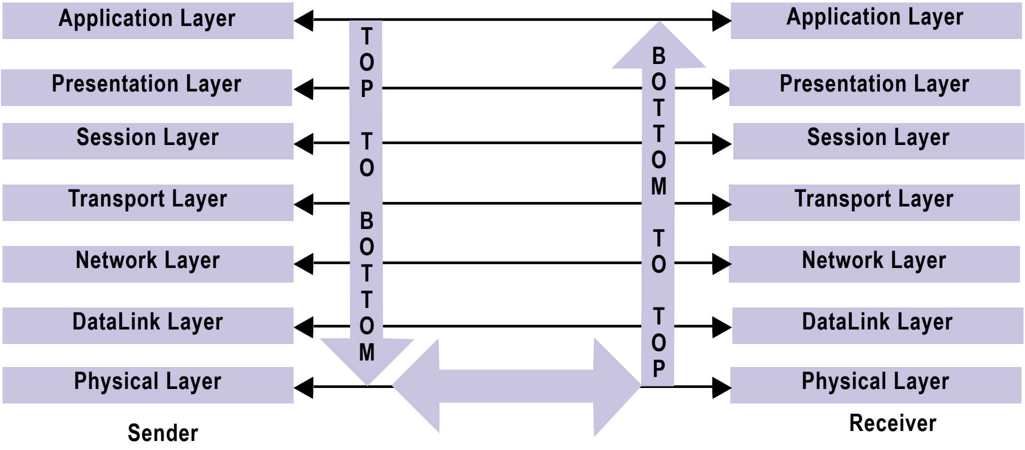
   (i) Encoding prepares the application data for conversion into 0s and 1s so lower layers can understand the data and function. Due to the limitation of ASCII character set, most encoding processes involve a wide range of character sets/code points/code units, which have a million character codes for any language on Earth, e.g., EBCDIC, UTF-8/16/32, Base 64, MIME, etc.

   (ii) If we attach a video or picture file to an email, MIME encoding is used to convert to a machine recognizable format. It's important to note that the encoding used for format conversation entirely depends on the application interface being used. Formatting also includes adding line breaks such as CR (Macintosh), CR-LF (Windows) and LF (UNIX).

2. Compression/Decompression: This step reduces the number of data bytes via compression. This reduces bandwidth and uses less storage space. Gzip, Deflate, JPEG, MIDI, and MPEG are all compression and decompression algorithms.

3. Encryption/Decryption: This step makes data confidential. It ensures that no one will tamper with the data or interpret it when it's sent through the wire. The most popular example of this is TLS (please note: SSL is outdated and its successor is TLS)."

Hernyka feverishly wrote in her notebook, hastily pulled from under the counter. Nielair waited for her to finish, then said, "Before I move on, have a look at this diagram."



"The sender processes the data from top to bottom. The receiver processes it bottom to top. Each of the layers on one side corresponds, agrees, negotiates, and communicates with its other side virtually, as if they are neighbors. The Presentation layer encapsulates all the necessary information into one block, appends the relevant header and footer, and passes the data to the Session layer."

Layer 5: Session

Nielair glanced at Hernyka's notebook, saw Louis XIV's scribbled again and again. He smiled, continued the metaphor to lighten the tempo of the topic: "As you can see, Louis XIV put in quite a bit of effort to safely send the letter. However, let's imagine that for whatever reason, Sanna did not want to read it. If Sanna tossed his letter aside, it could have even been opened and used to blackmail the king. The king had to take that risk; he could only kiss the letter and hope that his sweet Sanna accepted it and correctly interpreted his loving French prose."

"Did Sanna know French?" Hernyka asked.

Nielair grinned at her cheek. "It is just an example. Louis didn't have an online translator. Sanna probably knew French, though…it was a requirement for all the king's concubines.

"Kind of like that translator, though, the Session layer in the OSI model offers full-duplex or half-duplex operations. This handles connection, establishment and negotiation, maintenance, and termination of two applications on different machines. If the peer machine is busy and cannot accept the new connection, the primary machine must hold the data until resources are free on the other side. So, to transfer data, we need a session established on both sides.

"The Session layer also provides synchronization, using breakpoints at planned intervals. For example, if there is a file with 100 pages, a checkpoint is added every 20 pages to ensure it is received and acknowledged properly. This ensures that the transferred data is tracked and no part goes missing in case of a connection error between the two machines. The protocols that use this layer are NetBIOS and RPC. The Session layer encapsulates its own header, footer, and trailer information, passing the data to the Transport layer."

Layer 4, 3, or 4: Transport

"To ensure his letter is delivered to Sanna and not one of the other concubines, King Louis XIV had to write her name on the cover and instruct his messenger to deliver the letter directly into her hands. The courier also had to make sure that the letter wasn't ruined by water or dirt. He had to handle it with the utmost care, under pain of death. Similarly, TCP and UDP protocols are the concepts used as messengers to transfer data via ports to ensure safe and secure transmission of data. Applications have defined port numbers: HTTP is TCP 80 and DNS is UDP 53. On the receiving end, the application knows the client wants to connect to the server. The whole process is similar to someone having a nametag on their shirt at a conference. Instead of everyone having to constantly ask each other's names, the tag displays it for everyone's convenience."

During this speech, Hernyka nudged forward an unopened bottle of water. Parched, Nielair took a swig. "Obviously, the King's passion would have filled several pages. To ensure his lover read his message as intended, he would have numbered the pages in sequence. Similarly, the Transport layer sequences the packets so the recipient gets the packets in the right order. But what if our Louis was so prolific a writer that fitting all the pages inside one cover was impossible? He would have to divide his letter into piles of, say, 10 pages. In the same way, a humongous amount of data is broken down into segments of smaller units and encapsulated with the TCP header. This information is called *segment* in Layer 4, but from Layer 5 to 7 it is called *data*. If the Transport layer deals with this information in the UDP protocol, it is called a *Datagram*.

"The Transport layer also performs error checks on the packets and provides control information such as message start flags and message end flags so that the message boundaries are recognized at the receiving end. In a nutshell, the OSI model's Transport layer performs sequencing, segmentation, error control, and defines boundaries.

"Now here comes the fun part!" Nielair swiftly tapped the counter, eyes alight with glee. "The TCP/IP model can either be a Layer 4 or Layer 5 model. For sake of simplicity, we will use the more practical and popular Layer 5 model. Connection establishment, negotiation, maintenance, and termination are carried out by the Transport layer. This is not the same in the OSI model, where it is performed by the Session layer. A TCP three-way handshake in the OSI model is done in the Session Layer. In the TCP/IP model this is done in the Transport Layer. Some might say that a few functions have been moved from the Session Layer to the Transport Layer in the TCP/IP model. Others will argue that there is no equivalent to the Session layer in TCP/IP. As network engineers, all we need to know is which layer takes care of the three-way handshake.

"This segregation begins with the two different models. In today's TCP/IP protocol implementation, there are advanced features such as segmentation of data streams, acknowledgment timers, buffer management, three-way handshakes, error and duplicate analysis, sequence number inception, windowing, Nagel algorithm, TCP selective acknowledgment and many others."

Layer 3, 2 or 3: Network

Hernyka walked to a kettle, perched in a corner atop a precarious pile of books, scrunched up paper bags and tangled wires. She twisted one of the wires between her fingers as the kettle boiled. Nielair watched her intently. She prepared two cups of coffee, hers with sugar, his strong and black. Handing Nielair his coffee, she motioned to a small corner table. There weren't any customers; the two could sit and continue their lesson with more ease.

Nielair appreciated the gesture. He sat, glad for the relief, and spoke in a matter of fact voice: "The phrase 'All roads lead to Rome,' probably doesn't sound appealing to a French king. Nonetheless, let us consider that war has been declared in France. The King would instruct his messenger to take the shortest, safest path to deliver his message to Sanna. This is the role that the Network layer plays in the TCP/IP world. For example, if someone wanted to send an email from South Korea to California, it would have to travel through network points in North Korea, Russia, then to Pakistan, Afghanistan, Iran, Turkey, and perhaps even Cuba before finally arriving in California. Not only is the route slow and lengthy, but more importantly, it is also not secure.

"The Transport layer helps encapsulate the data segments, then sends them forward to the next layer, called the Network layer. This layer performs traffic routing, traffic control, fragmentation, and logical addressing. There are at least three different protocols used in IP protocol: ICMP (ping), IPX, and IGMP (multicast). These three protocols all use the IP address to communicate with the destination.

"The most popular among them is the IP protocol: it's used almost 99% of the time on the Internet. The basic fields you should know are the IP address details (sender and receiver), appends to the header checksum, the TTL field (for ping command), the IP version (IPV4/IPV6), the protocol number field that identifies the transport layer protocol (ICMP=1, TCP=6, UDP=17) and the total length (header + payload(data)). The advanced fields are the Differentiated Services Field (used by traffic shaping for managing, controlling, or reducing the network traffic), the frame fragmentation field (a router can fragment a frame if the frame size is more than the maximum transmission unit (MTU)), the explicit Congestion Notification field, the Fragment Offset, and the IP address field used for traffic routing. The encapsulation of the header, footer, and trailer in this layer is called a packet. Apart from the routing features, IPSec is the encryption method that works on this layer."

"The next two layers are plebeian," Hernyka blew dismissively across her nails. "They are the low-level workers."

"That's not quite fair," Nielair gently corrected her. "Without actual 'low-level,' everyday work, society as you and I know it would fall into ruin."

"I didn't mean it that way." Hernyka sat upright. "But why can't all the layers be sophisticated like the Application layer? Where's the equality? To hell with the hierarchical society! Maybe one day there will be a vertical society." She thumped the table with sudden passion.

Nielair grinned. Clearly he'd have to return to King Louis to illustrate his next point.

Layer 2: Datalink

"Okay. Well. Consider how King Louis' messenger needs to prepare for his journey. He must arrange for transportation, food, clothes, and so on. That's the Datalink layer. It is an interface that prepares access to the physical media and for data transmission.

"The Datalink layer has two sublayers: the Logical Link Control (LLC) and the Media Access Control (MAC). The LLC supports fields in the link-layer frames that enable multiple high-layer protocols to share a single physical link. The functions of LLC include link establishment and the termination of the logical link between two nodes, frame traffic control when no frame buffer is available, frame sequencing, acknowledgment, error checking, retransmitting, delimiting, detection, and recovery of transmitting and receiving of frames.

"The main MAC sublayer function refers to a physical address (the MAC address). It splits your data into frames and readies them to be sent across the wire to their destination. It controls how a network device accesses the data, obtains permission to transmit it, and enables multiple devices to communicate. For security, it can perform MAC filtering. For example, in your wireless points, you can define the MAC addresses that can connect to your wireless network or you could enable Network Admission Control (NAC) platforms to act as a substitute to MAC filtering in big networks.

"There are also other functions like store-and-forward, QoS, data packet queuing, LAN switching, Spanning Tree Protocol (STP), Shortest Path Bridging (SPB), and VLAN Trunk Protocol (VTP). VLAN and Frame relay can be used on the networking devices like switches and routers to process packets and interconnect them in the network."

Hernyka looked up from her quick jotting as Nielair finished speaking. "What will be the protocols that are used in the Datalink for computers to interface with physical media?"

"Those are Ethernet, PPP (used with a modem), IEEE 802.11/16 (WiFi), FDDI etc. In the case of network devices, the protocols that are used in Datalink include Ethernet, Frame Relay, ATM, trunking protocols, and so on. The most important function of the Datalink layer is to convert the frames into bits (0s and 1s)—the machine language—to easily transmit them through the wire. The encapsulation unit in this layer is called the 'frame.' "

Layer 1: Physical

Nielair continued, "Now Hernyka, the physical barriers like the land, mountains, oceans, lakes, and icebergs that separated King Louis XIV and Sanna would one day be eclipsed. As its name states, the physical layer is the actual medium. It is the hardware itself that the packet flows to and from. The functions of the physical layer are modulation of signals, line coding for digital communication, carrier sensing, collision detection, signal equalization, auto-negotiation, bit interleaving, channel coding, and forward error correction.

"Finally, the data is represented as bits, streaming as zeroes and ones through the wire. The standards that deal with the physical layer are connectors, pins, electrical currents, encoding and decoding, light modulation, signals, voltages, Ethernet (RJ45, copper port), wireless Ethernet, cables, network cards, hubs and many others. Basically, the physical layer deals with all the parts that help transport electrical signals between machines."

"The protocols involved in transmitting the electrical signals include synchronous optical networking (SONET), ISDN, USB, Bluetooth, DSL, Infrared Data Association, and few more."

Let's Settle Down

Nielair settled back in his chair, coffee between his hands. "So do you feel you've learned something useful about the OSI and TCP/IP model, young lady?" He looked across the table expectantly.

Hernyka smiled. "Yes, sir. I only wish that our Louis XIV and Sanna got married. Maybe humanity will one day have a layer where the magic of true love really occurs. I do still have lots of questions, though. I'm looking at my notes, I want to make sure I didn't miss anything. Could you maybe give a quick summary of everything so far?"

Nielair had expected exactly this question. "Fair enough, I will outline it for you."

1. For decades, OSI and TCP/IP struggled in a standards war. It ended with TCP/IP becoming the most widely used protocol and the standard. We shouldn't forget, though, that the two are brothers. OSI is the reference model and TCP/IP is the prominent networking protocol.

2. The next thing to keep in mind is whether you need to follow the 4-layered or 5-layered TCP/IP model.

   You must understand, though, that many companies self-define the number of requisite layers and name new systems after them. Cisco, Tanenbaum, Comer Kozierok and Mike Padlipsky, amongst others, have even proposed a three-layer model. In the five-layer model, Tanenbaum calls the second layer the Datalink layer. Stallings calls it the Network Access layer. Maybe one day, we'll resolve these quirks with a one-layer model. Until then we have to think about our universe: it exists in layers. It has outer space, stars, planets, dust, and the Milky Way. Each is a layer in its own right. The world may define a one-layer protocol for the sake of simplicity, but sub-layers will always exist. Without the concept of layers…society, science…even heaven could not exist or define itself!

3. Because of this multi-layer approach, there may be conflicts about which protocols fit in which layers.

   For example, ARP (Address Resolution Protocol) is disputed to be either a Layer 2, a Layer 2 ½, or a Layer 3 protocol. Rather than argue, think about it for a moment. Does the ARP protocol interact with Layer 3 in any way? Where does the actual ARP address reside? The answer to the first question is that ARP protocol interacts with Layer 3 at the IP address, but encapsulation doesn't take place there. The second answer is that the MAC addressing is in Layer 2 and encapsulation begins from there. So just because a protocol uses a layer for interaction doesn't mean it belongs to that layer. It also has to be encapsulated to stake claim to the layer. So, does that mean that ARP is a Layer 2 protocol? The choice is yours if you still feel like giving credit to Layer 3 for sharing the IP information.

4. We need to know why the OSI model has failed.

   In simple terms, it lacked a robust, practical implementation; the Session and Presentation layers were barely used. There were also redundant integrity checks in each layer, lethargy in transmission and difficulty in defining the role of each layer when considering security and actual codes.

5. Almost 95% of the protocol used on the Internet today is based on TCP/IP, making it the default industry standard. Variations of TCP/IP have been invented, but the base remains the same. So just stick with it— TCP/IP is fun!

6. The next obvious question would be whether protocols can be used for a single media. Not necessarily. PPP is a full-duplex protocol, using a variation of High Speed Data Link Control (HDLC) for packet encapsulation that can be used on various physical media. This includes twisted pairs, fiber optic lines, and satellite transmission.

7. When learning about networking systems, you should also be familiar with the elements defining TCP/IP, such as TCP/IP sockets, RPCs, APIs, etc.

8. Should you consider TCP/IP as software or hardware?

   In modern networking, the L1 and L2 layers and the driver codes are burned into a hardware circuit board. The other three upper layers are software…but the code resides on the hard disk. The better question here is, 'Does the entire TCP/IP stack come with an operating system?' Well yes, it does! You also need to understand how to troubleshoot TCP/IP and view its details. For that, packet capture is your best friend. Apart from the network perspective of viewing packet details, every application has debugging information, which will give an insight into how the socket is opened, the various processes and threads, the memory management of network data, kernel details, etc.

9. When a new protocol is launched, there are certain specifics you should keep in mind:

Is the new protocol an enhancement of any current protocols? How will the encapsulation work? What fields will it support? Also, what's the speed, performance, OS dependencies, and the RFCs it was built upon? Is it open standard or proprietary? Such info can be overwhelming to find. The best way to get answers is to ask the vendor what layer the new protocol works with.

"So, Hernyka," Nielair said, "these summarized points form the basics of networking theory. Our discussion could go on for days. I hope I have, at least strengthened your fundamental knowledge about TCP/IP." Nielair finished with a sip of coffee.

Hernyka nodded, strong and confident. "I do feel better," she said, "but can I ask another question? What about firewalls? They are, after all, the foundations of network security."

Welcome to the World of Firewalls!

Nielair shifted in his seat. Outside the door, pedestrians passed, none of them giving their wonderful little session the slightest mind. Nielair again smiled, leaned forward against the table. The girl would need some history, another story.

"Back to the very first humans, we've used boundaries to protect ourselves against strangers, wild animals, and trespassers. Don't we feel safest, after all, with a fence around our house? The actual term, 'Firewall' dates to 1851. It was, quite plainly, 'A physical wall built to prevent the spread of fire in a structure.'

"So what, if you'll pardon the pun, 'sparked' the firewall's invention? A lack of trust. Broken trust leaves a wake of insecurity and paranoia. After World War II, the Internet allowed people to openly share ideas, without regard to barriers or physical boundaries. A virtual paradise emerged, and within it laid the prospect to truly connect with each other. It was an opportunity to unite mankind as brothers and sisters on an unprecedented scale.

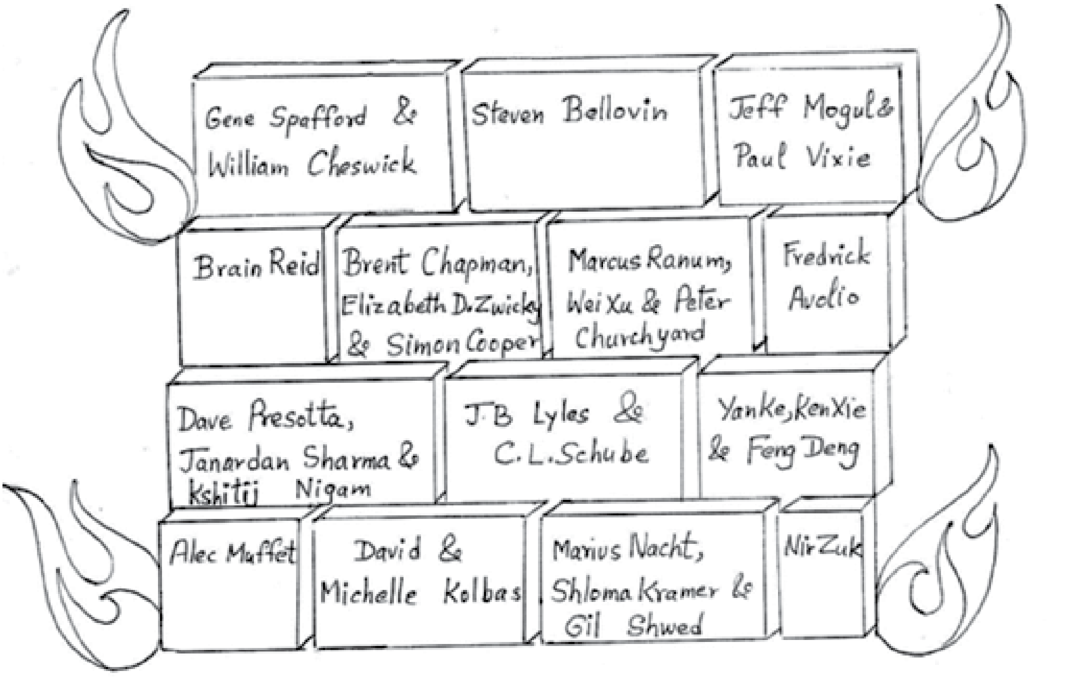
"But like Eden's serpent, the Morris worm took a bite from the Internet in 1989. It was the first widely-distributed and covered Internet virus. It broke the Internet's mutual trust and sharing. After, incidents such as Clifford Stoll's discovery of German spies tampering with his system, Bill Cheswick's "Evening with Berferd," and others popped up like weeds in Eden. There were almost 4000 security attacks between 1988 and 1994.

"Sadly, human nature often seeks loopholes to exploit new technology. These events led people to build fences in their virtual world. These fences were to protect against intruders gave birth to today's firewalls. Very soon, we began to redefine our culture, religion, language, the meaning of patriotism, business, trading, and commerce in the digital paradox.

"Rather than asking who invented the actual firewall—it's a muddy question—we'll use our time to talk about the legendary creators of firewall technology. Many claim to be 'fathers of the firewall.' To pick anyone would be debatable. Honestly, all involved deserve credit for their work. It would be nice to see the global community build a hall of fame plaque and imprint all their names on it.

"What is worth noting is that while select few actually designed the firewall, many others contributed to the technology's growth through white papers and books. Others supplied valuable abstract ideas and proposals crucial in laying the foundations of the firewall."

He opened a file and swiveled his laptop to Hernyka. A screen listed the names of the firewall's inventors, along with those who contributed to its creation. Hernyka glanced through the list, asking after each, in turn, their names and respective roles in building the firewall.


Gene Spafford & William Cheswick
Steven Bellovin
Jeff Mogul & Paul Vixie
Brain Reid
Brent Chapman, Elizabeth D.Zwicky & Simon Cooper
Marcus Ranum, Wei Xu & Peter Churchyard
Fredrick Avolio
Dave Presotta, Janardan Sharma & kshitij Nigam
J.B Lyles & C.L.Schube
Yanke, KenXie & Feng Deng
Alec Muffet
David & Michelle Kolbas
Marius Nacht, Shloma Kramer & Gil Shwed
NirZuk

"Wait." She paused, looked over the screen to Nielair. "Shouldn't the firewall symbol be a pyramid with a fire icon?"

Nielair paused, brooding. "Are you…trying to cause trouble? Just stick with my design. Besides, pyramids are bullshit."

Hernyka shook back, mocking fear and shock with hands up, "Whoa! Not a fan of Egyptian history?"

"Let's please return to the topic of discussion." Nielair smiled, but couldn't hide the annoyance pushing his tone down, or the frown lines crossing his forehead.

What is a Firewall?

"A firewall is a piece of software programmed into a network's hardware or server that provides a perimeter defense by interconnecting networks that have different levels of trust. Basically, it allows authorized traffic and denies unauthorized traffic. Think of a firewall like a country's immigration department. It checks the credentials of everyone entering, allowing the good and turning away the bad. During this process, each person must produce a valid passport and visa. Similarly, a firewall uses authentication to prove a user's identity before allowing access to the network.

"Once these documented good people enter the country, it doesn't mean they are free to do absolutely everything. It's the same inside the firewall. Traffic is monitored, audited, logged, and scanned. Any abnormal behavior triggers an alarm. Allowing and denying access to network via a firewall is subject to the rules and regulations laid down by network owners. Think of it like a controversial foreign leader, a Muammar Gaddafi-type, applying for a visa to visit America. He'd probably be allowed to visit, but his whereabouts would be tracked after his legal entry.

"A key to understanding the functionality of different types of firewalls is knowing their different generations. Now," Nielair took a breath, shook his head, "I'm not going to discuss the generations of firewalls like others would. I describe them based entirely on the time when they emerged. This means, over time, a particular firewall generation may have incorporated new security and functionality while retaining the basic operating principle of its base model. Strictly speaking, there are only two types of firewalls. Any additional components are merely enhancements."

Firewall: Type I

"The Type I firewall is known as a packet filter. After the Internet was hit by attack after attack in the late '80's, the first basic firewall was built. It was a packet filtering firewall. Its main function was to protect internal users from external network threats (inbound traffic). The name "packet filter" originates from the first firewall implemented on IP routers: Berkeley's BSD operating system in the late 1980s, allowing and blocking intrusion at the network interface. These packet filter firewalls could regulate traffic based upon source/destination IPs and source/destination ports. If internal users wanted to access the Internet (outbound traffic), then the packet filtering solution that was implemented was called screening routers.

"The limitation of packet filtering firewalls was that they couldn't determine the state of the TCP connections. Packet filtering firewalls didn't have enough data to know whether the intrusion came from an existing connection or a new connection. Certain routers used limited logging features. The Application Layer 7 had no UDP support either (though within a few years, upgraded versions of packet filtering supported UDP), and managing ACLs was complicated. Packet filtering had its advantages though, including speed, scalability, and high performance.

Firewall: Type II

"The Type II firewall is referred to as a "circuit-level firewall gateway." Some may refer to circuit-level gateways as an application gateway. There are many names for this type of firewall, like a gateway firewall, application proxy, proxy firewall, firewall proxy, application gateway, firewall gateway, or simply proxy. They all mean the same thing.

"The first circuit-level firewall gateway was programmed to prevent direct connections between networks through address authorization. It operated at the Network and Transport layer, relaying TCP connections with no extra processing.

"This firewall model involves two TCP connections. One is from the user to the firewall. The second connection is from the firewall to the destination server. This type of firewall is considered to be more secure, as it doesn't allow clients to have a direct connection with the server. It is compulsory for networks to go through an intermittent security device, known as a proxy, before connecting to the destination server.

"The first firewall, built by DEC, was commercially sold to DuPont in 1991 for $75,000. This firewall was called DEC SEAL (Screening External Access Link). The DEC SEAL firewall featured two components: a packet filtering "gate" and an application proxy "gatekeeper." DEC designed the network as a "bastion host," which still exists today. Internal and external users connect to services, HTTP, FTP, DNS etc., but not directly to a server. They are allowed in through the gate packet filtering firewall.

"The connection to the gatekeeper is then made, which in turn proxies the connection to the actual servers. This design still exists in modern networks using names like Check Point, Palo Alto, Juniper, Cisco etc. These firewall's stand at the perimeter and the proxy servers resides behind them."

Hernyka, suddenly back in class, raised her pencil in the air to stop Nielair. "I've read some blogs about this? They say there are two types of proxies: application and circuit-level proxies. Are you saying they are one and the same?"

"I understand the confusion," Nielair said. "Both application and circuit-level proxies have the same characteristics, involving 2 three-way handshakes. However, they are different. Application proxies work on Layer 7 while circuit-level proxies work on Layer 4. It sounds a bit confusing, but here's why we have two camps in the firewall world.

"Contemporary to the DEC SEAL, Cheswick and Bellovin at Bell Labs were experimenting with circuit-level firewalls, and wrote a book about it. Raptor Eagle and ANS InterLock firewalls were also developed around that time. In 1992, a presented paper on SOCKS made it publicly available. SOCKS is the standard for circuit-level gateways. It was later improved to version 4 by Ying-Da Lee of the NEC.

"In 1993, Trusted Information Systems (TIS) developed the first open source firewall: the Firewall Toolkit (FWTK). This FWTK model birthed the Gauntlet application gateway. Later, BlueCoat came up with the commercial web proxies, Squid and Netscape as open-source Linux proxies, and many products emerged in the circuit-level gateway arena.

"To summarize, a packet filtering firewall acts as a router, permitting and denying traffic with one TCP handshake between the actual client and the server. The proxy firewall acts as a termination point for the client's connection, then the proxy establishes another new TCP connection to the server."

Hernyka again raised her pencil. "What happened to the followers of the packet filtering firewall?"

"Like I said, first-generation packet filters were stateless firewalls. They couldn't track or differentiate new and existing connections, nor could they analyze IP protocol ID, fragmentation flags, spoofed packets, IP options settings, multicast, and UDP traffic. The pioneer Gil Shwed, the founding CEO of Check Point, invented a stateful inspection packet filtering firewall. This breakthrough led to many market leaders like Juniper, Cisco, Fortinet, and Sonic Wall to invent their own firewalls.

"The stateful packet filtering firewall is also called "dynamic packet filtering" because the firewall behavior changes, or is dynamic, depending upon its traffic. In the case of UDP traffic, it uses the preceding rule. You can't look at an incoming UDP packet and say that it will always be accepted or rejected. For TCP, the stateful firewall will inspect, track and correlate the TCP sequence/acknowledge numbers and all TCP fields in the packet to determine whether it is a legitimate connection or not, check this Wiki page on stateful firewall https://en.wikipedia.org/wiki/Stateful_firewall."

"So which is better," Hernyka interjected without looking up from her scribblings, "the new generation packet filtering or the application gateway?"

"It's relative," Nielair shrugged. "Different companies use both models. The application gateway works on Layer 7. It has more insight into the traffic flow. But when it comes to performance, packet filtering is the best. In terms of market volume, packet filtering is widely used in all types of network topologies. Application gateways are restricted to outbound access purposes, for instance, internal users accessing web services."

"Is packet filtering still considered a bad idea?"

"Definitely not," Nielair shook his head. "In the beginning, packet filtering fans demanded a smarter device. They began to incorporate IP spoofing, authentication, zone concepts, and other defense mechanisms to block well-known network attacks (like the ping of death and a block list of malicious Internet IPs). Some vendors even had proxy features that could be enabled in packet filtering."

Nielair, seeing a question flex in Hernyka's brow, paused. She filled the silence with her waiting question: "I've heard about Intrusion Detection Systems (IDS) and Intrusion Detection systems (IPS). Where do they fit in?"

"Oh!" Nielair's face went wide with surprise. "I say IDS and IPS are siblings. James P. Anderson published a paper in 1980 about the misuse of detection for mainframe systems, along with threat monitoring and surveillance of known threats. Dorothy Denning and Peter Neumann developed the first IDS called the Intrusion Detection Expert System (IDES) to detect malicious activity. During this period, the U.S. government funded most firewall development research. Projects like Discovery, Haystack, Network Audit Director, Multics Intrusion Detection and Alerting System (MIDAS), and Intrusion Reporter (NADIR) were developed to detect intrusions. The first publicly available, commercially-released products were WheelGroup's NetRanger and Internet Security System's RealSecure. Nevertheless, commonly known attack signatures were integrated into packet filtering firewalls and blocked."

"So where does Palo Alto come into this mix?" Hernyka asked.

"The firewall became the core device to protect a network. With increasing threats, additional security devices such as IPS, ICAP antivirus servers, URL filtering proxies, and others started supplementing the packet filtering firewall with more security controls. This led to the idea of integrating all the additional security devices into a single platform. For some reason, researchers and developers came up with a flawed method called UTM (Unified Threat Management): a deep packet inspection concept. It incorporated IPS, antivirus, URL filtering, reporting, and few other functions inside the firewall. Now, while the basic packet filtering firewall had high throughput and low latency, these add-on security modules caused a slowdown in overall firewall performance. The three reasons for this sluggish behavior included multi-pass architecture, non-stream scanning engines, and the functional management of security policies.

"The Palo Alto firewall answered these problems. The slogan behind the Palo Alto Networks' firewall is, 'Scan it all, scan it once.' They achieve this with single-pass architecture. The power of this architecture lies in the Palo Alto firewall's common protocol decoding engine and signature, which is used to determine what the application traffic is. It doesn't reduce the performance of the firewall by using separate components to perform these tasks. For example, when you send a GET request to download a file, Palo Alto uses an HTTP decoder to determine the HTTP GET method, then it scans the file, knows the start and end of the connection, and completes all operations simultaneously. This significantly reduces the latency and increases the performance of the firewall."

Nielair drank some coffee, then continued. "The benefits of stream-based signature engines is that, instead of downloading the entire file before scanning the traffic, they scan traffic in real-time. While doing this, they reassemble packets as needed. This enables all traffic to be scanned by a single engine.

"The Palo Alto firewall simplifies functional management of security policies by configuring ACLs on one box rather than configuring policies on multiple devices. This greatly eases troubleshooting, lowers administrative costs, and improves processing time for network traffic.

"So," Nielair tipped his coffee back, drank the last swig, "that's my introduction to TCP/IP and firewalls. If you are interested in something specific, I would be more than happy to explain. Is there a firewall you would like to learn about? Check Point, Cisco, Juniper, Fortinet, Palo Alto or BlueCoat proxy? Or IPS solutions like FireEye and Source Fire?"

Hernyka scratched her head. "I think Palo Alto might be cool to learn. It's sleek, it has brand value, and is considered one of the market's, uh, 'sexier' security products."

Nielair laughed. "Are the other products are ugly and shabby?"

"I didn't mean it like that," Hernyka said. "I just like the name: 'Palo Alto.' I mean, IT pioneers like Steve Jobs, William Hewlett, Larry Page, Mark Zuckerberg, they're all from the city of Palo Alto. There are also tons of famous people in other fields based in Palo Alto. Like the Japanese theoretical physics wizard Michio Kaku; he built his first atom smasher in high school. But that sucker couldn't find the 'Theory of Everything.'"

"Sucker?" Nielair nodded at the girls' excitement, her sudden change in tone. "Why do you call him that?"

Hernyka gripped the table edge, leaned close. "He lied about 9/11!" she exclaimed.

"Interesting." Nielair scratched his chin. "On behalf of my government, I am sorry for the ground zero debris, the appearance of cold fusion, Nano-thermite. And certainly, history has shown my government killing its own to harbor wars. And 9/11 is this generation's Pearl Harbor. But…" Nielair took a breath. "We're getting sidetracked. You've got me rambling. You asked about Palo Alto."

Henyrka nodded. "Palo Alto."

"Let's look at Palo Alto's many, vibrant features. I can even go one further and compare other firewall vendors so that you can understand their various approaches to solving security problems. You should also remember this analogy before we dig into Palo Alto: although Ferrari is considered one of the world's best cars, most people prefer the safety, cost and comfort of a Honda or Toyota."

"Noted," Hernyka nodded. "Although I'm not a big fan of Ferrari either, pasta and lasagna are about as far as my appreciation of Italian ingenuity goes. Please don't go on to tell me that the Romans invented the firewall!"

Chapter 2

BUSINESS AND PRODUCTS SPECIFICATIONS (YANKEE DOLLAR)

The small gadget shop buzzed, its energy not from any electron or wire, but from the small table tucked in the corner. Nielair wriggled his chair back, stretched his legs.

"Before we discuss the evolution of firewall companies and their proprietary products," he said, "you need to be familiar with certain terminologies."

"Like what?" Hernyka asked, with a slightly puzzled look on her face.

Nielair put out a hand, counted the bullet points on his fingers. "Speed, bandwidth, throughput, flow, sessions, connections. These are the basic metrics which define networking system quality."

"I see," Hernyka said. "Like learning the right words before trying to speak a new language."

"Exactly. You often see industry 'professionals' with weak fundamentals using terms like speed and bandwidth, or throughput and flow, without distinction. This leads to confusion while discussing technical terms with peers."

"Like how Saddam Hussein tried to rebuild Babylonian antiquities in his Iraq to muddy the line between him and Nebuchadnezzar II."

"Now you're just talking nonsense! But history does provide a suitable example. Let's talk Genghis Khan."

"Genghis Khan?" Hernyka stopped her mad scribbling for a moment.

"Genghis Khan," Nielair nodded. "The great Mongolian invader once led his warriors into what we'd now call Eastern Europe. He waged war with the Khazars: controllers of the Mediterranean basin, the Silk Road's gatekeepers. The time it took to travel from Mongolia to Khazaria…from source to destination…is like latency. Despite some legends, Genghis Khan probably did not have flying horses. He had normal horses, which covered around 50 miles a day. A messenger ferrying dispatches would take at least 30 days to travel the 1,500 miles between Mongolia and Khazaria. This duration is the latency."

"That's one hell of a lag time."

Nielair smiled. "It is. Now imagine an upgraded Genghis Khan living in the 21st century, with access to the Internet. Instead of a messenger on horseback, Genghis Khan would likely email his declaration of war to Khazars.

"The email would reach Khazaria in around 24.1 milliseconds. The speed of light in a vacuum is 186,282 miles/sec. Optic cables slow the speed to 124,274 miles/sec, but that's still unimaginably faster than Genghis' 30 days on horseback. In other words, the 'inherent delay' caused by transmitting information using a technology—Genghis' horses or our fiber optic cable—is called 'latency.' "

"In reality, today's latency is much more than 24.1 milliseconds. Multiple segments of fiber optic cable interconnect to create a continuous path between cities, states, and nations. This causes issues. Network congestion, retransmission, and router packet processing arise. These manmade hold-ups are called 'delays.' Delays cause latency to be around 70 to 80 milliseconds.

"I can't stress this enough: delay and latency are different terms. Some claim they're the same, which is not true. To illustrate the two, let's go back to Mongolia. Although Genghis Khan the Great's army could have made it to Khazaria in 30 days, he and his men would have taken extra time. There's mountains and rivers terrain to navigate. There are villages to plunder en route, people to kill, women to rape. These would have delayed his invasion."

"I enjoy your style of explaining things," Hernyka said, "but please don't call him great! There's no glory in raping women and in killing children in China, India, Korea, all the way to Lithuania."

"Hm," Nielair paused. "You're right. I didn't think that through. What if we continued, but with Genghis Khan the Barbarian instead?"

"Genghis Khan the Abuser."

"Certainly. Here I'm talking the importance of definitions, of using the right words, and my example is off. So let's return, but this time to Genghis the Terrible."

"Yes."

"The next important concepts are bandwidth, speed and throughput. Bandwidth is the maximum amount of data that can move from one point to another over a given amount of time. Speed is the amount of data flowing through a connection.

"Remember, speed depends on bandwidth and latency. Imagine trying to download an MP3 from a server 64 miles away that has 30 Mbps bandwidth. Even though you have 100 Mbps bandwidth, you cannot claim your Internet speed is 100 Mbps. Your browser download tool shows the actual speed.

"Now. Also imagine someone with 100 Mbps bandwidth, zero miles from the same 30 Mbps server downloading a video about the New World Order exactly when you are. You won't get the full 100 Mbps; congestion and traffic load on the shared Internet pipe, limited resources on the client computer, QoS on the ISP, and the performance of the routers will slow your download speed."

"Okay, so that's speed and bandwidth," Hernyka said. "How does throughput fit into this?"

"Throughput is the total data a system can handle at a given moment. It is the number of actions executed or results produced per unit of time. Simply said, if your computer has a one 1 Gbps NIC card and a LAN connection of 10 Gbps, your computer won't be able to handle 10 Gbps of data. It can only allow a max of 1 Gbps of data at any given time due to limitations imposed by the NIC card."

Hernyka blushed. "Oh, so throughput isn't like Nibbles from the Tom and Jerry cartoon."

"Nibbles?"

"He's the little diaper-wearing mouse? He eats more cheese than his own bodyweight!"

Nielair laughed at the thought. "Then no, throughput is definitely no Nibbles."

"Another question, though, if we have more bandwidth, do we get more speed?" Mischief twinkled Hernyka's eyes. "Except this time I need another Genghis Khan example."

Nielair laughed at her sudden 180. "Genghis Khan, huh? Okay, imagine Genghis Khan and his 200 mighty men are racing horses across the London Bridge. The winner gets to kiss Queen Victoria, who is standing on the south end of the bridge. The width of the bridge is the bandwidth. The throughput is Genghis Khan and his 200 men. The speed is limited by the natural speed of a horse, let's say 45 to 50 miles per hour. If the London Bridge is wider than most British car lanes, the competition gets even more interesting. The horses get more space, meaning more men may end up crossing the finish line together and win a chance to kiss the Queen.

"To your question, larger bandwidth allows more data to the computer at the same speed. This makes the user's experience, let's say while playing video games, better. You cannot make a horse run faster than its natural limit by, say, forcing it to drink rum or making the bridge wider. But by providing a wider bridge, you enable more horses and riders to reach to the Queen of England simultaneously."

"I know how London Bridge really fell down." Hernyka shook with quiet laughter. "Which means you don't like the British very much, do you?"

Nielair winked. "I was trying to make Genghis Khan and his men holy with a kissing from the Queen."

"Poor Victoria's cheeks will fall off if all those sinners kiss her!"

Smiling, Nielair continued, "The next important concepts to learn are flow, connections, and sessions. Flow—also known as traffic flow, packet flow, or network flow—is a unidirectional sequence of packets from a source device to a destination device. The purpose of flow is to identify a session. The packet can be unicast, from one sender to one receiver; multicast, from one device to a group of devices on a network; or broadcast, from one device to all devices on a network. The packet will have at least five tuples, or attributes, in common between the source and destination, to uniquely identify a session. These attributes include source IP, destination IP, source port, destination port, and protocol type or number.

"Here we come to an important point. Some vendors put additional information into the tuples. Let's say, you come from a Cisco background. Cisco defines flow as 7 tuples: the basic 5, plus Type of Service (ToS), and input interface. Palo Alto, on the other hand, defines flow as 6 tuples: the basic 5 and security zone. However many tuples, flow is a packet-switching network terminology where the client and server identify each other's tuples via sockets. When speaking to others about flows, we must check to see what product they are referring to so you can understand the attributes used to establish and identify a packet.

"Similarly, there are three types of connection: TCP, UDP and ICMP. Most applications are TCP by default. So unless I explicitly mention a UDP connection, consider it as a TCP.

"Connection is a bi-directional flow. One flow is from the client to the server side, called forward flow or Client to Server (c2s). The other flow is Server to Client (s2c), also called reverse flow. Now, I have a question for you, Hernyka," Nielair leaned in, relished the wary shade in her eyes. "How many flows or connections are required for a packet filtering firewall and proxy firewall, respectively, to establish communication between a client and a server?"

Hernyka did not hesitate. "For a packet filtering firewall, we need two flows or one connection for a client to talk to a server. In a proxy we need four flows and two connections."

Nielair smiled. "Spot on! Good job! Now a session has several meanings depending on which application, technology or framework someone is referring to. A session has many TCP connections between source and destination.

"Let's simplify. When you visit a website and log in, the server assigns a cookie to your browser. A session exists as long as this cookie is valid. The server identifies the client cookie and requires no further authentication for as long as the cookie is configured. One cookie session may include hundreds or thousands of connections. One connection is generated for every picture, icon, html text, etc. Once the cookie expires, the client needs to re-authenticate, and a new cookie is issued for a new session.

"So with the cookie being a Layer 5 or 7 attribute, how do you think it relates to a session? Consider a session which has many connections, and in its bi-directional flow, doesn't have cookies as an attribute. Also consider a session, which is to 'have many connections,' doesn't explicitly mention that a session is only TCP connections. There are other attributes, too, that sum up a session. A session can either be a TCP session (Layer 4) or an application session (Layer 5) in the TCP/IP Layer 5 model.

"Both types of sessions exist in applications, and they are inherently different. A TCP session is required to access an application session, but an application session can exist on the client and server independently without the TCP session."

"Like squares and rectangles," Hernyka said. "All squares are rectangles but not all rectangles are squares."

Nielair considered the metaphor, head tilted. "Sort of. To really understand, let's dive deeper into what 'connection' and 'session' actually mean.

"A connection is a communication channel between a client and a server. Like we've said, it will have anywhere between 5 to 7 tuple identifiers to establish a connection. In the server, connections are short lived and affected by timeout if the connection is idle for long, although this can be configured. A session is meant to maintain the state of the client and server, or the server alone. On the client side, its purpose is in regard to the user's application, say a browser to store cookies. On the server, it is a memory chunk allocated either in the RAM or on the hard disk. So even if the TCP connection's session time expires, the application sessions can be resumed with a new TCP connection.

“The network vendors further muddied the waters with their session definition. They loosely used the term session without specifying TCP session or application session. I will provide examples to clear up any confusion, and then summarize the accurate definition of a session.

“First, imagine Sir Winston Churchill shopping on a website that runs Apache (the most commonly used web server). The default TCP connection timeout is 15 seconds and the HTTP session timeout is 300 seconds (before Apache 1.2, it was 1200 seconds). A cookie expiry timeout is 24 hours. Sir Winston Churchill adds a few items into a shopping cart but can't decide whether to buy a book about Genghis Khan or the *Sex and the City* TV show boxset. The TCP connection session timeouts in Apache, and the HTTP session time of 5 minutes (stored only on the server) expires. The cookie, though, stored in client and server is still valid. After an hour, when Sir Winston Churchill adds an item to his checkout cart, a new TCP and HTTP GET or POST connection is established. This is done by holding the cart active without the need for re-login or emptying the cart by using the cookie session timeout.”

“Okay, okay.” Hernyka nodded. “I understand the TCP connection timeout and the cookie expiry session timeout, but what is an HTTP session timeout?”

“Good question. There are three timeouts, and three levels of session. TCP timeout occurs when the communication channel sees no traffic for 15 seconds after the initial handshake and closes the connection. In the same way, after the three-way handshake, the server waits 5 minutes for the user to send a GET request. If it isn't received, the server will close the HTTP session. The cookie session timeout has a 24-hour lifespan.”

“Great explanation. By the way, what did Sir Winston Churchill end up picking?”

“*Sex and the City*.”

Hernyka grinned. “Good choice.”

“The second example is a session in Palo Alto. When you run the command in the CLI, type, ‘**show session all**’, then grab any ID, and type, ‘**show session id 63708**’. ‘63708’ is just an example. The id can be any number between 1 and 2147483648. The output will show 6-tuple information and other application information such as the application type, URL filtering, captive portal, QoS (this should be an n-tuples parameter, but Palo Alto doesn't consider it an n-tuple identifier), NAT, and byte count, among others.

“The last example I'd like to give regard an application proxy. Let's take the best product in the market: the BlueCoat proxy. The 5-tuple TCP connection can be viewed in the GUI using the URL https://proxy-ip:8082/TCP/connections. Sessions can be viewed in the GUI at Statistics → Sessions → Active Sessions, where you can see all the application related statistics such as byte caching, object caching, compression, ICAP, protocol optimization and encryption. In BlueCoat, the distinction between TCP connection sessions and application sessions is relatively clear.

“In my last two examples, I am not pitching the strength or weakness of any product. An engineer should have the clear and precise knowledge to know the difference between TCP and application sessions. When reviewing the hardware specifications, they should ask the vendor how many simultaneous connections and sessions the hardware supports. Questions?”

Hernyka shook her head happily, "You are a genius, sir. I understand the concept very well now!"

"I understand you're specifically curious about Palo Alto. But we must also know about other market vendors who do the same business as Palo Alto, but in a different way. Like the famous saying from Sun Tzu's *The Art of War*: 'If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.'

"So let's describe the history of various companies and the products they sell. First I would like to talk about Check Point."

Check Point

"Way back when the world was using black and white screens to manage firewalls, Check Point introduced the GUI system. In 1993, the company was started in Ramat Gan, Israel, by Gil Shwed, Marius Nacht and Shlomo Kramer. FireWall-1 was their first product. Stateful inspection was its core technology. Soon after, they developed one of the world's first VPN products, VPN-1.

"In 1994, Check Point signed a contract with Sun Microsystems and HP as an Original Equipment Manufacturer (OEM) in order to distribute Check Point software in the Solaris platform and HP-UX. Later, they even collaborated with IBM AIX."

Hernyka chewed her lip, brow furrowed. "Why didn't Check Point come out with their own hardware?"

"Great question. Until the mid-2000s, Check Point was adamant about calling itself a software company. They secretly observed their competitors, though, and realized that to run their software with minimum hassle, they needed to either manufacture hardware or acquire a company that could manufacture for them. That is one of the main reasons why Check Point acquired the Nokia company. In reality, there was another reason Check Point wanted to enter into the hardware segment."

"And what's that?"

"Well, you can run Check Point in Solaris, Windows, Linux, OpenBSD, or any version of Linux. But from an operational perspective, this became a pain. Users needed to be an expert in each kind of hardware and OS running Check Point to be able to implement it. So they decided to standardize their product, and as a result, you can now get a Check Point appliance with GAiA OS a Check Point Linux distribution product that unifies IPSO and SecurePlatform (SPLAT) into a single operating system."

"What happened to the original hardware vendors?"

"Check Point continues to provide support for HP, IBM, Dell, Lenovo and a few others. Customers can also run Check Point in Crossbeam blades (BlueCoat acquired Crossbeam). Now it is the customers' decision regarding whether they want to buy Check Point manufactured hardware or install Check Point on their own hardware. All I can say is it became less complex after they came out with the GAiA OS."

Hernyka looked up at the ceiling, eyes moving to and fro as she digested what Nielair had just said. Finished, she asked, "Does Check Point only have firewall and VPN products?"

"Check Point has a wide array of products: mobility, endpoint security, antivirus software, VoIP, cloud web services, anti-spam filters, IPS, DLP and email security, among others. You can find the list on Check Point's website (https://www.checkpoint.com/products-solutions/all-products/#az)."

Hernyka already had her phone ready. Her eyes grew large as she scrolled through the product list. "Did the Check Point founders invent all these?!"

"No way!" Nielair laughed. "The rule of the game is to begin a business in a garage, become successful, enroll in the billionaire club, take up yoga, drink green juice and join some cult organization to be a part of the New World Order. Back in 1994, after Check Point received its initial funding of $400,000 USD from Ventura Capitals, it entered the US and located its headquarters in Redwood City, California. The business picked up, and Check Point acquired Zone Labs, SofaWare, NFR, Nokia, Hyperwise, and a few other companies. Now Check Point has sufficient capital to buy new companies and grow their portfolio.

"Back in 1995, Gil Shwed mentioned that the company had four developers and it was hard for them to find programmers who knew network security programming. That's all changed now. Money changes everything. Well, almost everything. Check Point ran into problems while trying to acquire Sourcefire, a leading IPS vendor. The Committee on Foreign Investment in the United States (CFIUS), an arm of the US Treasury, blocked the acquisition amidst a legal dispute between Check Point and SofaWare. Etay Bogner, SofaWare co-founder, filed a shareholder derivative suit and won. A few litigations followed, and Check Point had to settle them all. So that's a brief summary about Check Point.

"There are tons of hardware models by different vendors that went through the entire manufacturing and sales cycle. The current trend is for Check Point to sell its software in its own appliances. You can see the comparison of their proprietary appliances at https://www.checkpoint.com/products-solutions/next-generation-firewalls/enterprise-firewall/check-point-security-appliances-comparison.

"Regardless of whether they sell their own appliances or act as OEM to other hardware manufacturers, the questions you should really be asking are: 'What is the throughput, max connections and sessions that are supported? How many Ethernet and SFP ports are available? What is the memory and storage? What are the dimensions of the hardware, the power consumption, the dual power supply for redundancy, the hardware-certified certifications (ISO, FIPS), and what are the details about its hardware blades/chassis?' As a case study, I will show you a snippet of the hardware specifications for the 23800 Security appliance model so you can understand what I'm talking about."

Firewall Throughput (Gbps)	*VPN AES-128 Throughput (Gbps)*	*NGTP Throughput (Gbps)*	*Concurrent Sessions (M) default/maximum memory*	*Connections per Second (K)*
43	26	3.6	10M default and 28M Max	174K

Hernyka looked at the chart. "Why is the session value 100 times more than the connections per second? Also, what are NGTP and VPN?"

"Connection is an expensive metric compared to the session. Connection happens on the network while sessions are allocated memory chunks in the firewall. NGTP stands for Next Generation Threat Prevention, a software bundle that protects against unknown threats. It follows the UTM model and bundles all advanced security features in the firewall. VPN provides encryption connections between networks. It's an established trend, and it is shipped along with the firewall module. Check Point was the first to distribute Firewall and VPN as a single package. Today, this is the default practice for every firewall vendor on Earth. As you may have noticed, the throughput significantly decreases when we enable the VPN module since it deals with encryption and decryption, which consumes more CPU power and memory. Check Point supports VSYS (virtual firewalls) in one firewall. This enables different customers to use the same hardware, but logically, different virtual firewalls."

Cisco

Nielair took a breath, Cisco already loaded into his brain, when Hernyka stopped him. "I am a Cisco patron preparing for the CCNA exam. Can I share what I've learned about Cisco so far?" she enquired.

"By all means." Nielair nodded her on.

"The husband-wife duo Leonard Bosack and Sandy Lerner founded Cisco in 1984 while working at Stanford University. They stole the original software, which was part of the work on the "Advanced Gateway Router," developed by students William Yeager and Andy Bechtolsheim. The couple, along with Kirk Lougheed, built the router in their garage, tweaking the "Advance Gateway router" into their own product. They began selling it in early 1986 through word of mouth. During their first month, the company got $200,000 in funding, and within four years, the couple walked away with $170 million. Some say that they donated 70% of their windfall to charity."

"If you already know that the Cisco founders weren't legitimate entrepreneurs," Nielair said, his voice sharp, "then why take the Cisco CCNA course?"

"I hate thieving morons." Hernyka couldn't hide her upset, the clenched fists and shaking lip. "People who steal another's work and claim it as theirs. But I have no other choice." The upset relaxed into a resigned disgust. "I desperately want a network security tech job, and industry insiders suggested Cisco is a good platform for me to start learning."

Nielair could see her mental back and forth manifest in the desperate shift of her eyes.

"But who are we to judge?" Hernyka said. "All Americans are guilty of identity theft. We stand on the graves of Native Americans while we squabble amongst ourselves as to who's the most patriotic!"

Her sudden shift in tone pushed Nielair back in his seat. He paused, adjusted his posture. "That's very true, but Cisco is an American company, and it contributes to the economy and country's growth. Let's talk about how the Firewall technology was brought to the world by the Cisco Company.

"In 1994, Network Translation Inc. conceived of the Private Internet eXchange, or PIX. Company founders, John Mayes, Brantley Coile, and Johnson Wu wanted to fix the IP address shortage by projecting Network Address Translation (NAT) as a solution to conceal a block of IP addresses behind a single IP address. Remember, RFC 1918, the standards for assigning IPs on a private network, was not yet published. In 1995, Cisco acquired Network Translation Inc. The company's engineers continued to work on the PIX firewall Finesse OS.

"At first, Cisco sold the PIX firewall as hardware. Later, to meet service providers' demands, Cisco came up with a hardware modular chassis called the Firewall Services Module (FWSM) that used the Cisco PIX OS. The FWSM could be installed on the Cisco Catalyst 6500 Series Switch or Cisco 7600 Internet Router. FWSM allowed any VLAN on the switch or a router to pass through to the device and operate as a firewall port, applying firewall policy for filtering. This greatly reduced cost and hardware space, enabling the switch and router chassis to act as a security device. As time progressed, VPN, Web sense URL filtering, and IDS were implemented on the FWSM module.

"A key point here is that, like Check Point VSYS, both PIX and FWSM support multiple context firewalls. This is basically all about having separate firewall partitions in one single hardware.

"In 2005, the Cisco Adaptive Security Appliance (ASA) firewall replaced the Cisco PIX. The ASA has since become Cisco's champion. Cisco ASA is a Linux-based OS, and it became the Unified Threat Management (UTM) that provided VPN, IDS, URL filtering, zone-based, and deep inspection. In early 2010, Cisco offered its Next Generation Firewall (NGFW) with firewall, application control, NGIPS, URL filtering, Cisco Advanced Malware Protection (AMP) and VPN. Cisco has since acquired Sourcefire and added their FirePower services in the NGFW feature set of the ASA firewall, adding robustness and security to the Cisco ASA firewalls.

"Cisco terminated the brothers PIX and FWSM in early 2010, asking customers to migrate to Cisco ASA. Apart from PIX and FWSM module firewalls, Cisco's original classical firewall implementation of the router-based stateful firewall is called CBAC (Context Based), which applies the Access Control List (ACL) on interfaces. In the CBAC, having multiple inspection policies and ACLs on several interfaces on a router made the whole system overwhelming. Limited Intrusion Detection and Prevention (IDP) policies, a handful of supported applications, and the same inspection policies on all interfaces gave way to the Cisco IOS router firewall, a zone-based firewall.

"The Cisco IOS router firewall inherited several ASA features. Payment Card Industry (PCI) standards require a router-based firewall because data in transit requires a stateful inspection firewall and auditing access. It wasn't a bad idea to have a router for networking and security purposes, but keep in mind that, although ASA has all the security components, Cisco sells IDS's and VPNs as separate hardware if you don't want to use UTM products. This same methodology also applies to Juniper and Check Point.

"Here is the hardware specification of ASA 5585-X with FirePOWER SSP-60."

Firewall Throughput only Stateful inspection (Gbps)	***Application Control (AVC) and IPS/NGIPS (Gbps)***	***Sizing throughput [440 byte HTTP]: Application Control (AVC) or IPS/NGIPS (max)(Gbps)***	***Concurrent Sessions (M) default/ maximum memory***	***Connections per Second (K)***
40	10	6	40 M	160K

"Although many companies are replacing Cisco firewalls, Cisco has a loyal fan base. They're happy with ASA products and willingly march arm-in-arm with Cisco through all its innovations. It's also worth mentioning that these test numbers are more or less realistic, since all vendors test performance in their labs. Often, the results are mentioned in goodput, which is less than the maximum theoretical data. This arises because of several factors, such as transmission overheads, latency, system limitations, bandwidth, different packet sizes, TCP receive window size, data compression, different types of data processing (TCP, UDP, again in TCP streaming, videos, static contents), protocol overhead, retransmission and packet drops, bandwidth capacity, congestion, collisions, packet queuing delays, NAT translation delays, store-and-forward processing delays, and transmission delay."

"Oh my God!" the litany overwhelmed Hernyka, hands to face in mock horror.

Juniper

"If you still feel guilty about shaping your career around the plagiarist Cisco founders," Nielair said, "Juniper will be your redeemer."

"You know what they say," Hernyka said, hands wide and open, "'the enemy of my enemy is my friend.' Maybe I should start to learn about Juniper. Thanks for that insight." She ended laughing.

Nielair shifted himself in his chair as he began, "Just like how the Hobbit began as a bedtime story, so did Juniper. Pradeep Sindhu conceived it during a 1996 vacation to India. He wanted to create packet-based routers that were optimized for Internet traffic. Sindhu started with $2 million, and after a few months, more funding offers from companies and the financial sector poured in. Juniper's original focus was building core routers for ISPs. After acquiring Unisphere in 2002, Juniper entered the edge router business, in which ISPs route Internet traffic to individual consumers. Junos OS (FreeBSD based OS) was the core OS that ran on all switches and routers.

"Juniper remained in the networking business until 2004. After acquiring NetScreen Technologies, Juniper entered the security space. NetScreen Technologies, founded by Yan Ke, Ken Xie and Feng Deng, developed a high-speed firewall. It was the first company to build a gigabit-speed firewall. In 2002, NetScreen acquired OneSecure, the IPS product. In 2003, it acquired Neotris, the market leader in SSL VPN.

"The NetScreen SSG (Secure Services Gateway) firewall was based on ScreenOS, and was among the best three firewalls on the market at the time. Later, around 2008, Juniper took the best security features from ScreenOS and integrated them into the Juniper core Junos OS. They named the newly-branded firewall SRX (Segmentation Rules eXchange). At first, the change did not appeal to many customers who were exposed to NetScreen CLI since they had to learn a new Junos OS to manage their firewalls."

Hernyka interrupted: "Speaking of learning a new OS, I've always wondered why there can't be one standardized command line interface for all vendors and technology. Like how the science use Latin. Maybe these tech companies are all computer-racist."

Nielair smiled at the statement, at this woman's puckish streak. "The new SRX series greatly improved throughput, security, extendibility, and performance compared to NetScreen. Even with the upgrade, NetScreen still supports some SSG platforms: the ISG-1000 and 2000, and NS-5200 and 5400 have customer support in place until 2021, although their sales ended in mid-2016. Juniper firewall hardware is attractive in that it supports 3G and wireless connections at low-end firewall models. This helps small businesses reap the benefits of the firewall.

"Both the networking mammoths Cisco and Juniper have a stateful firewall integrated with routers. Juniper Junos OS software allows router function in a secure context (routing + firewall) or router context (only routing). Using router context doesn't mean that Bugs Bunny can suddenly tinker with your router by ransacking some carrots. It implies that the Junos OS inherently checks for inbound traffic, and by default, it allows all traffic to pass through.

"UTM and virtual firewalls have existed in the NetScreen and SRX series for a long time. The current SRX like other vendors, has been rebranded and is known as the SRX series Next-generation Anti-threat firewall. This all-in-one anti-threat firewall has IPS, VPN, Antivirus, Anti-Spam, Anti-spyware, URL filtering, and NAC (Network Access control). Here," Nielair again brought up an image on his laptop, "have a look at the specifications of the high-end model of the SRX5800 series."

Firewall Throughput (Gbps)	***VPN AES-256+SHA-1 /3DES+SHA-1 throughput (Gbps)***	***IPS Throughput (Gbps)***	***Concurrent Sessions (M) default/ maximum memory***	***Connections per Second (K)***
320 (2 Tbps with Express path)	200	100	230 M	2 M

Hernyka looked at the space between the screen and Nielair, eyebrows raised in surprise. "That is quite impressive. Its performance is almost 10 times more than Check Point and Cisco systems. How did they achieve it?"

"Juniper started as a networking, ASIC-based, hardware data processing routing company. Cisco routers rely on software for data processing. So the UTM concept works well for Juniper, unlike their competitors, because of their superior hardware models. One more important acquisition I forgot to mention is Juniper's acquisition of the software company Funk, which brought the Network Access Control (NAC) product suite into Juniper's portfolio. Another acquisition, Mykonos, is a web security software company focused on deceiving hackers by presenting fake vulnerabilities and tracking their activity. The product is used in defense systems and the beast continues to be unrivaled in its power."

BlueCoat

Nielair paused, gathering his thoughts and his breath. Hernyka took the chance and returned to the unsteady kettle propped in the corner of the store. She poured two more coffees and returned to their little table. Nielair sat, quietly staring into space, as if contemplating something.

"The unsettled Biblical war between the descendants of Isaac and Ishmael holds similarities to the battle between the children of packet filtering and application proxies. The assumption among experts and patrons of packet filtering is that they have crucified and put the final nail in the coffin of application proxy followers such as Gauntlet, Sidewinder, Cyberguard, and a few others. But BlueCoat stands out, shining like a morning star.

"Of course, there is a flip side to the story. Open source proxies such as Nginx, Squid, CGI proxies, anonymous proxies and Onion proxy are descendants of the rivalry. Dropbox, Github, major porn sites, social networking sites, or anonymous services that don't want to use commercial vendor proxy solutions, but use these open source proxies.

"Mike Malcolm, Joe Pruskowski, and Doug Crow founded BlueCoat, formerly known as CacheFlow, in Redmond Washington. CacheFlow focused primarily on manufacturing cache appliances, hardware solutions that accelerated Internet performance and improved poor internet and intranet performance through caching. CacheFlow's main products included proxy servers, cache appliances, enterprise cache servers, and ISP caching. They were based on Secure Gateway OS (SGOS), a Free BSD homegrown OS that still runs on all BlueCoat proxy products.

"In 1999, CacheFlow named Brian NeSmith its president and CEO and went public with an IPO. Despite a crowded cache product market including Squid, Cobalt Networks, Netcache, Dell computers, and Compaq computers, CacheFlow led the market. The cache appliance struggled to store and cache data as Internet content shifted toward streaming media. Knowing their pitfalls in 2001, CacheFlow designed a new content delivery architecture called "cIQ." cIQ managed and distributed static, streaming, secure, and dynamic content. CacheFlow introduced a family of products including cIQ Edge Accelerator, cIQ Server Accelerator and cIQ Starter Kit.

"In 2002, the company moved its headquarters to Sunnyvale, California. NeSmith changed the company's name to BlueCoat and ended the caching era, ushering in a new age of web security. The new product, 'BlueCoat', performed caching, web filtering, ICAP scanning, policy-based security rules, authentication, reverse proxy, and SOCKS proxy. The company also built its own URL filtering solutions, called BCWF, Proxy AV, SSL VPN, DLP, and K9 web parental web protection. Also fervent about network performance products, BlueCoat entered the WAN acceleration market with a product called MACH5. MACH5 provided application acceleration, visibility, object caching, byte caching, protocol optimization, video stream–splitting, and video-on-demand caching. It also acquired Packet Shaper, a leading vendor in QoS.

"Thomas Bravo, an equity investment firm, acquired BlueCoat in 2011 for 1.3 billion dollars. As BlueCoat merged with the Thomas Bravo companies, they felt their existing solutions—like Proxy SG, WAN acceleration, and Packet Shaper—were outdated. The company took another big step in optimizing their proxy solutions with the support of open-source OS Linux, BCWF cloud, a new antivirus server named CAS, enhanced DLPs, and BlueCoat encrypted tap. In addition to revamping their solutions, BlueCoat acquired Netronome SSL solutions, Crossbeam, Elastica, and few more, significantly expanding their security portfolio.

"BlueCoat switched hands in 2015, from Thomas Bravo to another private equity firm called Bain Capital. Within a year, Symantec acquired BlueCoat for 4.6 Billion dollars. The company is no longer called BlueCoat; the Symantec name enjoys more popularity, even though its antivirus software sits idle while viruses and Trojans feast on your data."

"Hang on," Hernyka stopped him, hand held palm out. "BlueCoat was acquired three times in five years."

"Yes." Nielair nodded, trying to imagine what sidetrack Hernyka sprinted down now.

"That sounds very Old Testament. Like the 'designated bondmaid,' the married slave taken to her master's bed with impunity."

"Business is like any other transaction," Nielair took a breath. "Everyone gets something."

"And what about 'portfolio?' What does portfolio have to do with all this?"

"A security company's 'portfolio' is its suite of products to expand revenue and scale, while also financially insulating when one or two products fail. To build a portfolio, BlueCoat had to merge with or acquire other companies to expand its presence in the security space. Really, though security products sound fancy, their sales are small compared to the volume of servers and network devices sold worldwide. This tough security product market leaves many companies exposed to a buyout. Often, this is a better option. A company's chances of survival are higher when their portfolio of products is more diverse than others. Think of Walmart: they have a pharmacy, supermarket, wines, food and ammunitions. Perhaps in the future Walmart will expand to car and spaceship rental. Diversity is the key to success today.

"Here, consider the performance of BlueCoat's proxy."

Max Proxy Throughput (Gbps)	***Max concurrent sessions***	***Throughput (Forward Proxy / Reverse Proxy) (Gbps)***	***Concurrent connections (Forward Proxy / Reverse Proxy)***
2.4	250,000	1.2 / 2.4	30,000 / 25,000

Hernyka looked at the numbers. She gasped. "Why are the throughput, sessions, and connections so low? How can the proxy gang survive against the packet filtering beast? Do all proxies have the same performance?"

"That's how proxies emerged," Nielair replied. "They have caching, more protocol stack detection, two TCP connections, and so on. BlueCoat architecture is focused on single plane model and optimization is performed on the CPU and RAM rather than distributing the load on card processors, multiple-CPU load balancing, and logging all data in one plane. The model I have shown you, the SG500-20 can support 30,000 users. Not only do simple packet filtering firewalls handle HTTP, but they also handle DHCP, DNS, FTP, VOIP, and many other protocols simultaneously. But proxies are special breed handlers and support limited applications. The unsupported applications are tunneled."

"How are they surviving?" Hernyka asked.

"In my opinion, BlueCoat Web Filtering (BCWF) has an inherent advantage. It can categorize 8 billion websites. URL filtering in packet filtering and Next Generation Firewalls is only around one billion. The other piece to BlueCoat's survival is the philosophy of many companies and corporates. Although firewall sits on all network edges, when the HTTP traffic wants to enter or exit a network, it needs to do so via HTTP proxies. Other types of proxies are SOCKS proxy, which is different from web proxy, FTP proxy and RTSP/RTMP/MMS proxy."

"Do proxies have UTM functionality?"

"No. Like UTM firewalls, their approach is different. Antivirus and DLP can be integrated with external devices through ICAP protocol. I will explain more about this as we discuss it further."

F5

"Have you watched the movie *Twister*?" Nielair pivoted in his chair.

"I…have…" Hernyka's eyebrow raised in confusion.

"Jeff Hussey, the founder of F5, named his company after the highest tornado classification mentioned in Twister: F5."

"Is Jeff a movie geek? If he'd watched the TV miniseries *Category 6: Day of Destruction* would he have called his company C6?"

Nielair chuckled, "After turning F5 into a billion-dollar enterprise, he made it his mission to build an F6 company, so he co-founded Tempered Networks, of which he is currently the CEO."

"This guy is either trying to chase a tornado or running after superstorms, isn't he?"

He smiled warmly. "Jeff Hussey founded F5 Labs in 1996 in Seattle, Washington. Despite load balancing giants like Cisco and Nortel, F5 managed to sell its first BIG IP product in good numbers. F5 made a quarter of a million dollars in its first year. Cisco, though making 5 billion dollars in sales, tossed its Local Director load balancer into the ring to KO F5. Nortel also saw brisk profits due to market demand in the load balancing segment.

"The F5 BIGIP product was solid, though. Customers found it better than Cisco and Nortel offerings. At the right time in 1998, F5 launched the 3DNS product: a multi-location load balancer. The 3DNS stood apart from the BIGIP, which was a LAN load balancer. The product pushed F5 to $5 million in sales.

"In 1999, the company changed its name to F5 Networks and hit Wall Street with an IPO. With Cisco acquiring ArrowPoint and Nortel's acquisition of Alteon WebSystems, F5's marketplace was becoming crowded. With just 1,600 customers, the company seemed to be heading toward a dot-com crash.

"Seeing trouble, Jeff Hussey appointed John McAdam as CEO. McAdam was F5's savior. He pulled the company uphill by investing in a Traffic Management Operating System (TMOS). McAdam also aggressively acquired Swan Labs, Acopia Networks, uRoam, Traffix Systems and Versace, merging them into F5's product line.

"Despite Cisco and Nortel's competition, F5 skyrocketed and became a load balancing monopoly. However, F5 doesn't like to call itself a load balancing company. It prefers the acronym Application Delivery Controller (ADC). In addition to dominating the ADC field, F5 manufactured security products like FirePass, Secure Web Gateway Services, MobileSafe, WebSafe and Application Security Manager (ASM). The ASM is one of the industry's best Web Application Firewalls (WAF)."

"Does F5 also have proxy products?" Hernyka asked. "And is the WAF same as NGFW?"

Nielair shook his head. "No, no. To your second question, when I mentioned the different proxies, I never explained the Web Application Firewall. A WAF is different from IPS and application firewalls in its ability to understand web application protocol logic; syntax, codes, and its standards are far better than IPS or even application gateway. WAF can be a network device or host-based. It's kind of a niche field that's specialized in mitigating Open Web Security Application Project (OWSAP) and web-based attacks.

"While the Next Generation firewall (NGFW) resembles WAF, there are two main differences. NGFW can protect from web attacks, but is a network security device. In addition to web attacks, it can protect from other threats like DNS, FTP, VoIP, etc. WAF, on the other hand, is solely concerned with HTTP and HTTPS. The second difference is that NGFW protects both inbound and outbound access, while WAF only protects inbound access. It sits before the hosted web servers and protects external users accessing the web resources from web-based attacks."

"Interesting…" Hernyka twirled her pencil between adroit fingers. To Nielair, it seemed a physical manifestation of a computer's 'thinking' hourglass. "It's almost like how a local cop works to keep peace, but can't be a Marine without training."

"More or less," Nielair said.

"Does F5 have any action in the firewall market?"

"Yes," Nielair said. "In order to meet firewall market demands, F5 released their Advanced Firewall Manager (AFM). Truth be told, I think of it as opening a pizza shop around the corner from another pizza shop. The important question is, 'What extravagant new features convince me to spend my hard-earned money on their product?' F5's describes AFM with terms like NAT, Deep inspection, logging, SSL decryption, state-full firewall, etc. Put simply, it's a full-proxy firewall with SSH proxy and Consolidated Application Protection (CAP).

"CAP is catchy because no one needs to buy separate hardware for an advanced network firewall to perform functions like ADC, DDoS, SSL inspection, and application security, which you can buy on VIPRON blade and simply enable the feature. Not only does this save data center power and space, it also makes management easier and simplifies network design. F5 has two types. One is VIPRON, a blade architecture and the other is a standalone. These days, VIPRON is preferred, as it further reduces space by having one hardware with eight chassis, instead of having eight separate hardware pieces. Here are the specifications of their hardware box VIPRON 4800."

Max Proxy Throughput (Gbps)	***Max concurrent sessions***	***Connections per second***	***Blade modules supported***
640	576 million	7.5 million	8

"AFM's significant advantage is that it performs stateful inspections, has no NGFW, and the APIs can be integrated with LTM and GTM. So if you remove VIP on an LTM, the corresponding security policy is removed from the AFM module as well. This allows one-click flexibility when managing policies in load balancers and firewalls.

"I also like that F5's AFM doesn't brag about its NGFW features. Their product is marketed as a simple stateful firewall, which reduces cost, rack space, and enables easy administration when using load balancing functions from F5 by complimenting firewall functions. If we need IPS, IDS, and other scanning functions, we need to rely on other technologies like Sourcefire, FireEye, McAfee and Symantec."

"You said F5 is a full proxy firewall?" Hernyka said. "Then how come BlueCoat has 1 Gbps throughput but F5 has 600+ Gbps? Why is there such a vast difference? Is it a ploy by BlueCoat to sell more devices by reducing the throughput? A slimy underhanded sales tactic?"

"That's the billion-dollar question. Putting one's personal gain and ignorance aside, the answer to your question lies in the difference between F5 and Bluecoat's business philosophies. BlueCoat buys hardware from third-party vendors and packages it with their SGOS; F5 manufactures its own hardware. BlueCoat wanted to do all operations in their RAM themselves and never engineered multi-task processing using dedicated processors or chips. Only recently did they introduce SSL processors for processing SSL traffic, but even that looks a bit like a patched-up robe instead of a garment sewn from scratch."

"Okay, so against all odds, battling Cisco and their other competitors, how did F5 thrive for so long?"

"One reason is their focus on their primary business strength. Rather than becoming a Jack of all trades, F5 went deeper in the ADC business. They offered basic video training and trial products to anyone who signed in. Other security product companies largely follow the mantra: "Our product is only for elites." F5 developed 'Dev Central,' a community with tools and forums, where users can learn about F5 products and the company's customer outreach initiatives. IT professionals and developers who are F5's customers spend so much time and money there that it almost feels like home to them.

"F5's openness to addressing and improving collaborative products also contributes to their success. F5 worked closely with Microsoft, SAP and Oracle, providing innovative solutions so others could run their applications productively. They improved their partnerships skills, also knowing when and how to cut certain partnerships. F5 had the good sense to break ties with Nokia Corp and Dell Computer Corp, which were linked to Internet startups. Actions like these seemed to alter F5's profile amongst its customer base."

Hernyka butted in excitedly, "I'm getting a good feeling about F5. They challenged their competitors, executed their plans perfectly, and above all, they put up a good damn fight against the monopoly of corporate rogues. It definitely sounds like a company run by a tornado chaser, a company that would storm through anything standing in his way! I can imagine the F in F5 stands for 'focus,' and 5 represents the five elements of Wood, Fire, Earth, Metal, and Water."

Nielair smiled. "How very creative of you."

"But I have one more question," Hernyka said. "What happened to Cisco and Nortel in the load balancing market?"

"Cisco shut down its load balancing." Nielair leaned forward, face sharp with a secret ready to be passed. "But I've heard rumors that they're trying to acquire F5, Nortel, and, well, a lot of other smaller companies."

"Schmucks! Shame on them!" Hernyka's cried.

Palo Alto

"You, too, Brutus, will be your answer after I go through the history of Palo Alto." Nielair warned.

"You judge people far too quickly. Tell me your Shakespearian tale, then I will share my opinion."

"Nir Zuk, a former engineer at Check Point, was the principal developer of the first stateful firewall. Some claim Zuk is the father of the stateful inspection firewall. 'I am entering the Father's Day debate,' Nir Zuk had said, laughing. The savvy guy left Check Point, joined OneSecure and co-created the IPS product. In 2002, NetScreen acquired OneSecure, and he became the CTO of that company. When Juniper bought NetScreen in 2004, Nir Zuk became its Chief Security Technologist.

"Nir Zuk wanted to construct an Internet safe from dishonorable hackers. He wanted to demoralize bad actors. This led him to found Palo Alto. Yuming Mao, another Netscreen employee, followed Nir Zuk and joined Palo Alto. Juniper sued them, claiming that Mao and Zuk plagiarized Juniper's patents. Palo Alto settled the suit in 2014. Palo Alto paid 175 million dollars in cash and equity to Juniper.

"It is widely believed that Nir Zuk stole ideas, that Palo Alto heavily borrowed Check Point's stateful inspection, OneSecure's IPS concepts, Juniper's hardware design and Fortinet's GUI layout."

"Hang on a second, Nielair," Hernyka said. "I always saw Nir Zuk as an innovative developer. Like you said, he's seen as a father of stateful inspection and even IPS. The guy has his own innovation conception and he founded Palo Alto to implement his revolutionary ideas. That isn't plagiarism!" Hernyka's voice raised to match her convictions. Her gestures grew large, pointed. "Did these corporate bastards—excuse my language—really expect him to just hand over his ideas? And what if he had done that? His paycheck would have been measly, barely been enough to cover his mortgage and subway tokens, while the lazy parasites flew around in private jets."

"I'm only telling you what I heard," Nielair said. "People don't care about ideas, but when payoffs and money are involved, you will see several unknown ideals and zombies jumping on. Here are the hardware specifications for the Palo Alto models."

Model	*Firewall Throughput (Gbps)*	*Threat prevention throughput (Gbps)*	*IPSec VPN throughput (Gbps)*	*Connections per second*	*Max sessions*
7080	200	100	80	1,200,000	80,000,000
7050	120	60	48	720,000	48,000,000
5060	20	10	4	120,000	4,000,000
5050	10	5	4	120,000	2,000,000
5020	5	2	2	120,000	1,000,000
4060	10	5	2	60,000	2,000,000
3050/3060	4	2	500 Mbps	50,000	500,000
3020	2	1	500 Mbps	50,000	250,000
500	250 Mbps	100 Mbps	50 Mbps	7,500	64,000
200	100 Mbps	50 Mbps	50 Mbps	1,000	64,000
VM-1000HV	1	660 Mbps	250 Mbps	8,000	250,000
VM - 100/200/300	1	600 Mbps	250 Mbps	8,000	50,000/ 100,000/ 250,000

"The PA-4000 series is a legacy product. It's no longer on sale, but you may still find some networks running it. The PA-200 and PA-500 have only copper ports, and there are no fiber ports available. All of these hardware products are used for lab purposes, especially the PA-200. The VM firewall is becoming popular these days because it can be installed inside the VM with other servers or networks that need less physical hardware. This reduces the cost and space. If you notice in the diagram, the throughput and connections per second for all the VMs are the same. It only differs with the number of maximum sessions, which in turn depends on the license that we purchase for that particular VM model. You can go to the Palo Alto website at https://www.paloaltonetworks.com/products/product-comparison.html to get a detailed product comparison.

"For the sake of simplicity, I haven't included the VSYS, zones and virtual routers supported by Palo Alto. I'll explain them later if you're still interested. Is that alright with you, Shakespeare's daughter?"

"Definitely. But I still don't believe that Nir Zuk is guilty of unscrupulous conduct. He proved the Next Generation Firewall (NGFW) idea. Juniper was immature to sue Palo Alto. I mean, Karl Benz is the inventor of the modern car. If Benz was like Juniper, he could have sued every other car companies, claiming that the concept of the automobile belonged to him. We could all be running our vehicles on rubber tires invented by the Nazis, hailing 'Adolf Victoria Hitler.' Oops, I mean, 'Adolf Victory Hitler.' Or perhaps we would have ended up following a global rule that stated, 'Cars for the Aryans' and 'Mules for gentiles.' The city of Palo Alto is a land of creators and inventors who have enriched our world with the NGFW." Hernyka's outburst left her red-faced. She paused to take a short breath.

Nielair watched, waiting for her to calm. When she'd taken a sip of water and her cheeks looked less flushed, he continued. "Your argument is impressive, but we're talking about Corporate America. It's neither a monopoly, nor the Mafia, nor a dictator. Like Nir Zuk, Ken Xie left NetScreen in 2000. Ken Xie founded the company Fortinet. Shlomo Kramer, the co-founder of Check Point, also founded Imperva, a security company that is well known for their WAF products. The quick-change nature of the business makes tracing intellectual property difficult. Although I do agree with you that new ideas are vital and money should be distributed for a better future."

Hernyka nodded, satisfied to see the teacher agree.

Nielair sat forward eagerly as he went on, "Anyway let's rock and roll with Palo Alto, the Thor's Hammer of the next generation."

Chapter 3

GET A FEEL FOR BASIC CONFIGURATION (CONTEMPLATE)

Hernyka stopped Nielair just as he was about to continue, “Look, I don’t want to know if smartphones are good or evil. I don’t care if Newton or Einstein invented the Internet. I’m not looking for trivia on how Charles Babbage became the father of computers despite not writing a line of code. Can we jump straight to the configuration of Palo Alto’s initial settings?” She edged forward in her chair, face set, muscles in her arms strained.

Nielair smiled at her eagerness. “Every model of Palo Alto firewall features a dedicated management port to manage the configuration, reporting, route updates, and administration functions. Apart from the management port, there are data ports for user traffic and dedicated High Availability (HA) ports (which aren’t available in the PA-200, PA-500 and PA-2000 series).”

“What if I don’t have the money to buy a firewall?” Disappointment clouded Hernyka’s usually-bright face. “Is there a free version I can try?”

“Not free,” Nielair said, “but there is an inexpensive offer from Amazon’s AWS Palo Alto services software where you pay per usage. It runs around $1.50 per hour. Just search ‘Palo Alto Amazon AWS,’ and you’ll find the product page. From there, you can buy cloud VM’s. Amazon AWS VPC (Virtual Private Cloud) is a similar setup to a VMware or VirtualBox in the home network, except with this one, we need to set up in the cloud with additional routing instances and servers, which all cost a dollar or two, and they only charge for the hourly usage. For installation and setup, check out this link: https://www.paloaltonetworks.com/documentation/70/virtualization/virtualization/set-up-the-vm-series-firewall-in-aws.”

“Okay. But I think I can sacrifice the time and money of few nights out and master Palo Alto instead!”

“I like your enthusiasm Hernyka. Whether a brand-new firewall or one sitting in a lab or production network, the primary requirement for network configuration is having an IP on the Palo Alto (PA) firewall to login and manage the firewall. If you are sitting next to the firewall, you can use the management port. Or if your firewall is miles away, you can connect through the console connection. With the exception of PA-4000, which uses a serial console interface, all the other PA models use an RJ45 connector. Here is my laptop,” Nielair passed it across the table. “You type while I run you through the configurations and details. That way it will stay ingrained in your memory.”

“Thank you!” Hernyka grabbed the laptop, her fingers wiggling over the keys.

“If you’re using the serial console port, I’m going to talk about the settings you should set in the HyperTerminal. There are tons of HyperTerminals available. To me ‘Putty’ - that’s like a Swiss army knife for an engineer. Download the putty.zip file; it contains all the tools wrapped up. That way you don't have to download each *.exe individual file. Here are the connection details…"

Bits per sec: 9600

Data bits: 8

Parity: none

Stop bits: 1

Flow control: none

"The default management port is 192.168.1.1. You can change your laptop IP in that subnet either by direct connection to the firewall or via a switch."

"Why is the default always 192.168.1.1?" Hernyka asked. "To me, the default port is like always drinking tequila with salt and lime. Why not change things up? Try paprika or pickle margaritas?"

The thought of a pickle margarita soured Nielair's tongue. He laughed. "It changes with the firewall that you're using. F5's default management port is 192.168.1.245. The last decimal octet, 245, equals F5 in hexadecimal. So, if you wish to defy convention and rim your tequila glass with paprika, so to speak, you'll have to request the vendors to change their tequila recipes to suit your taste.

"Until then, just bear these numbers in mind. Palo Alto's default management port is 192.168.1.10. For Check Point, it is 192.168.1.206. Juniper's is 192.168.1.14. For Cisco, it is 192.168.1.12. And for BlueCoat, the default port is 192.168.1.248." Nielair paused after rattling off the numbers, eyes twinkling. "As to how I came up with these numbers… it's a riddle. I think you're smart enough to figure it out."

"The default account title is 'admin/admin'. And before you ask, I have no idea why the account defaults are 'admin/admin', rather than their company name or the name of American patriots like Abraham Lincoln or George Washington."

"Plain 'admin/admin' is better than 'admin/bacon' or 'admin/ham'!" Hernyka exclaimed. "By the way, how did you connect to the Palo Alto firewall? Is that in your lab?"

"Yes. A teeny-weeny PA-200. Once logged in, you'll be prompted to change the default password. If it is in a lab, use any password you like. If you want random strong passwords for each Palo Alto that's in production, I recommend this technique. The putty.zip file contains a tool called 'PUTTYGEN'. Double click it. Then move your mouse over the tool until the PUTTYGEN tool generates keys for you. I know it sounds like Voodoo trick, but your mouse wiggles can't be predicted by hackers; therefore PUTTYGEN collects the randomness of your movements to generate a key.

"The 'Key Passphrase' password option is used for SSH authentication between client and SSH server. Since our goal is to generate random keys to use as passwords, so let's skip it. Now to save, go to File → 'Save Private Key' option or click the 'Save Private Key' button. It will be saved as a .ppk file. Open the file in WordPad or Notepad++ and pick any line with random characters to use as a password in the Palo Alto firewall. This technique isn't only restricted to Palo Alto, but can also be applied to any servers or security devices that need unique passwords.

"After extracting the unique password, most people delete the file and store the password in the password vault. If, however, you'd want to store the .ppk file for future reference—in case the password vault somehow gets lost—we can use the generated .ppk file to recover it. Rename the .ppk file with the device hostname and store it where none can access it via the network. For example, you could copy the renamed .ppk to a hard disk or flash drive and lock the disk inside a steel vault. Make sure to renew the password every two years by following the same steps. This method is only for securing the 'admin' account, also called the root account or superuser account."

"Brilliant!" Hernyka said. "My research has suggested using smart phrases… For example, for the password, "LeeHarveyOswaldkilledJFK", I'd replace certain characters with special characters such as "s" for '$', "a" for '@', "I" for '1', "e" for '3', "b" for '8' and so on."

Nielair nodded, "That's known as the Leet technique. There's no harm in it, but regardless of your password technique, it is vital to create individual accounts for each administrator who is managing the box. Using RADIUS or LDAP keeps a log of all the login attempts and emails the corresponding administrators weekly. Notified of login attempts, they can then acknowledge all their attempts via web portals. The account should get locked after three to five failed login attempts. This way, the administrator is made aware of any intrusion or illegitimate attempt to logging in. RSA tokens are even more secure for administrator access."

"I didn't know all this," Hernyka spoke airily, head swimming with fascination. "Tell me something interesting about password security."

"Well, okay. I hope we're not sidetracking from the main subject."

"Not at all!" Hernyka shook her head. "What good are perfect NGFW and policies, if someone has a weak password?"

"I'm glad that you understand the importance of strong passwords. We'll explore passwords before we configure the firewall. …But I'm not going to go into great detail. It would take a week to explain. Instead, we'll summarize and I'll give you some informational links for you to read as homework. Being a real pro means doing real work. You can spot the rookies and newbies because they want to be hand-held through each step, never once using their brains. This is important because information security is a constantly changing field. New concepts can become outdated within months. Your success will hinge on your drive toward research and staying abreast of the latest market trends."

"Spoon feeding doesn't help," Hernyka said, goaded by Nielair's nods. "A real pro learns the basics and discovers the rest independently. I'll take notes as you teach, and then I'll explore."

"Good. Now, here's the ugly truth about passwords. While talking about Palo Alto's default 'admin/admin' password, you might get paranoid about the firewall getting changed as soon as the FedEx guy delivers it. It is good to be cautious about passwords. Do we change our home router password or leave it as default? If you want to know the default passwords of all the routers, check them out at http://www.routerpasswords.com and https://portforward.com/router-password. You can also check http://setuprouter.com and http://www.routeripaddress.com for default IPs and passwords.

"Usually passwords in systems are hashed, encrypted, and stored in the OS. If someone has physical access or has gained shell access to the computer, server, or database, they will try to decrypt the password file. Your first port of call if you wish to mess around with different hashed algorithms is http://www.sha1-online.com. Type the password you want to use and change the different hashing algorithms. You can then see the length and complexity of the hash. It is worth mentioning that these hashes aren't irreversible. This leads us to a hacking technique called rainbow table.

"A rainbow table is a listing of all the possible plaintext permutations of encrypted passwords specific to a given hash algorithm. Once an attacker gains access to a system's password database, the password cracker tool compares the rainbow table's precompiled list of potential hashes to hashed passwords in the OS database. The rainbow table associates plaintext possibilities with each of these hashes, which the attacker can exploit to access the network as an authenticated user.

"This is why experts recommend using complex passwords: special characters, numbers, a mix of upper and lowercase letters, and more than 12 characters. It is even safer to use a passphrase with long sentences. To defeat the rainbow table crack technique, you can employ methods like salting and iterations. Salting is using a keyword that prepends to the actual password before hashing is performed. Or you can hash the salt keyword first, prepend it's the actual password, and apply the hash one more time.

"If we keep iterating, the hash becomes more complex. To demonstrate how this works I will go to http://www.freecodeformat.com/pbkdf2.php. Let's say the password is 'TomCruise' and the salt is 'WillSmith'. Make the key length 512 bits and hit the 'Hash' button. You will get a long hash value '9313…035'. If you add several iterations, the hash output is hashed "n" number of times. Enter '**1954**' in the 'Number of iterations:' Now, the '9313…035' hash output is hashed 1954 times. This makes the hacker's job very difficult because they need to know the password and salt value in order to crack the password. The larger the iteration number, the more complex the hash becomes. Try inputting a '**6331**' iteration."

"I love it!" Hernyka exclaimed. "It's like having a digital superpower."

"Breaking the hashes is a passive method. It is obvious that we cannot use the hash for live login attempts. The active method is when someone tries to break into a system in real time by using the username and password. Technically, this is known as 'brute force' and hackers use tools like Hydra, the most popular one, which has a list of fifteen million known passwords."

"Fifteen million passwords? That is quite a lot!"

"Not really!" Nielair shrugged. "Go to https://crackstation.net. For non-salted MD5 and SHA-1 hashes, there are 1.5 billion usernames and passwords stored. Now let's do a quick check on the strength of the CrackStation tool. Go to http://www.sha1-online.com and type '**Simpsons**' in the hash column and let it be SHA-1, copy the result '30f…3ba' and paste it into the https://crackstation.net site, and it will reveal the Simpsons password from the hashes in just a couple of seconds. There's other cool stuff to explore in CrackStation. Also, check this one http://www.freecodeformat.com."

Hernyka took a moment, fingers eager as she explored the Free Code Format. Nielair watched, sipping from his mug. Hernyka finally looked up with a nod.

"Simpsons is correct," she said. "The lesson is never use 'Simpsons' as your password since its hashed value is already available in these databases."

"Yes," Nielair agreed. "https://hashcat.net/hashcat is also a worthy site for cracking a password. There is also a publicly available website for hash dumps and passwords called http://www.adeptus-mechanicus.com/codex/hashpass/hashpass.php. You can also generate password lists using a tool called Crunch. It's at this link: https://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-passwords-part-4-creating-custom-wordlist-with-crunch-0156817.

"Automated tools such as Hydra, John the Ripper, Ophcrack, and others run different defined usernames. Say you use 'admin' as username and tap into the database password list to break into a router, web server, or poorly-configured firewall. These brute force or dictionary stacks don't work well because most devices are configured to deny access after 'n' number of failed attempts. Remember, if you accidentally mistype your PayPal or Gmail password a few times, the system generates an email notifying of a possible intrusion. In a real-world scenario, a brute force or dictionary attack is difficult to perform. To prevent hackers from guessing your password using known password databases use long passphrases combined with the leet technique. Or use the PUTTY method we used before, even though it's an old-school method. There are also many online free tools to generate random passwords such as http://passwordsgenerator.net and https://lastpass.com/generatepassword.php.

"Password manager is a handy tool. It lets you generate random passwords and then store them in a vault via free software like KeePass. The website is http://www.keepass.info, and for KeePassX, it is https://www.keepassx.org.

"The latest trend in password managers is to store passwords securely and let the manager help you to login using the autofill option when websites are accessed. Popular sites like Facebook, Amazon and Dropbox use this method. I'll give you the LastPass link for password generation. They have a few Apps that help you do it. The link is https://lastpass.com. With LastPass, all you need one master password for all your ever-expanding accounts. LastPass can be installed on an iPhone, an Android phone, and desktop. There is also the MasterPassword app that has the same functions as LastApp. You can find it at http://masterpasswordapp.com. Finally, there is Truecrypt from Oracle.

"I encourage you to explore these options, but with extreme caution. Some programs passing as password managers really hide malware that will steal all your information. The websites I have given you are credible. Most people use them, but as I always say, the law of security is to never fully trust anyone. Even with all these measures, if you still want to know whether or not you are being tracked, you can check your email address against hacking at https://haveibeenpwned.com. My last advice is that when these password manager tools get breached, how fast and securely one can react, recover the password and sanctify the theft is important. Nothing is completely secured. Recuperating is tactics and art of survival.

"So… let's leave behind the mysticism of passwords and return to Palo Alto." Nielair exhaled, the track back to their original conversation like a weight lifted off his shoulders.

"Sure," Hernyka said. "You've given me many useful links. I can do the rest of the research. Thank you. Please continue what we were originally discussing, about setting up the admin password in Palo Alto."

"Of course. To change the admin password, issue the command '**set password**' at the '>' prompt, which is known as operational mode. Then enter the password. After changing, logout and re-login to confirm that the new password is in place. The next step is to configure the management IP of the Palo Alto firewall so you can administer the network remotely while sitting at any location.

"Type the command '**configure**'. This takes you to configuration mode, which allows you to perform advanced functions. If you have worked on Cisco or Juniper routers, you would have seen a custom-built CLI interface with a vendor-defined command set. Palo Alto's is similar to this.

"To change the IP address, netmask, and default gateway, of Palo Alto, issue the command '***set deviceconfig system ip-address 10.10.10.10 netmask 255.255.255.0 default-gateway 10.10.10.100***'.

"A set command will modify the configuration. You can use the question mark key if you are unsure of the options available for that command. Type '**?**' after typing, '**set deviceconfig system**'. You'll see all the options; the '**ip-address**' command is available. Another feature of Palo Alto CLI is that it autocompletes the command when you hit the 'TAB' key.

"So, Hernyka, we have now changed the management IP address of Palo Alto. Log out of the firewall and try logging in via the new IP 10.10.10.10 or whatever IP address you have configured. But as you can see, it isn't possible. And do you know why?"

Nielair paused briefly to look at Hernyka. She returned only a confused look, mouth slightly open.

"Because the configuration hasn't been committed and saved," Nielair said. "In Palo Alto, until you commit to a change in the configuration, the changes won't work. Many beginners—and even experienced personnel—make the mistake of not saving the new configuration. I don't blame them. In most technologies, we just punch in some commands and the changes automatically come into effect.

"In Cisco, any configuration change goes into effect instantly, but if you want the config to be persistent across all reboots, you have to save the configuration in a non-volatile storage device. For this, you issue the command '**wr mem**'. In Juniper, you have a concept called the 'Automatic Commit mode', wherein once you complete your configuration, you don't have to manually issue the '**wr mem**' command. The automatic commit tool does this for you.

"To check whether the changes have gone into effect, login to the firewall again with the default factory setting 192.168.1.1 IP and go to configuration mode by typing '**configure**'. Type, '**show deviceconfig system**' to see all the changes you have made. Now type, '**commit**' and wait until the operation has been completed. Since you are changing the IP address, Palo Alto will kick you off and you won't see the progress bar hitting 100%. When this happens, close the window, then login with the new IP."

Nielair looked away from their shared computer and saw Hernyka's eyes peering through the screen to a faraway point. He waited for a breath, before again interjecting. "Do you have something you want to ask?"

"Why should it always be about the JFK assassination, even in the password example you mentioned. Why not Malcolm X?"

"Maybe JFK was more important than Malcolm X? Don't get distracted….The first step is to assign an IP address and default gateway to the management interface of the firewall. Then use the GUI to configure the rest of the parameters. Try the command '***set deviceconfig system ip-address 10.10.10.10 netmask 255.255.255.0 default-gateway 10.10.10.100 hostname MalcolmX dns-settings servers primary 8.8.8.8 secondary 4.4.4.4***'.

"This is a one-shot command you can use to configure all the necessary settings. Just use the question mark to see all the options, or break the command into pieces. First configure the IP address, then add the default gateway as I initially showed you, then use the command '***set deviceconfig system hostname MalcolmX dns-settings servers primary 8.8.8.8 secondary 4.4.4.4***'. Both methods return the same output. Never forget to '**commit**' the change. Again, many times, engineers forget the commit operations and end up scratching their heads when their changes don't work. Always bear in mind this quote from *The Matrix* when working with Palo Alto: 'Buckle your seatbelt, Dorothy, because Kansas is going bye-bye.' The seat belt is your '**commit**' command. If you do it, you can take the Palo Alto Next Generation Firewall to the skies."

"Interesting." Hernyka gave a sidelong glance. "Although to digress again, I didn't ask you to name the firewall Malcolm X."

Nielair shrugged. "I felt like honoring him. Not a bad idea."

"Actually, I like it. I'm going to name my firewall Malcolm X."

GUI the Genie, CLI the Cash Line Interface

"You can configure through both CLI and GUI. As to which method to employ, I'll leave that up to you. Personally, I use GUI to configure policies and CLI to troubleshoot. Regardless, you should bear in mind that the console will come in handy when the GUI interface can't be reached through a network. Don't underestimate the power of CLI. Sometimes CLI is even called the 'Cash Line Interface' thanks to its usefulness in tricky situations!

"To explore any product, one only needs surf the GUI and click on the options. Don't make any changes in the production environment. All experimentation should occur in the lab environment, where you can surf and see how the GUI is organized. It's like taking a walk around a new neighborhood and familiarizing yourself with the various roads. Experimenting will increase your knowledge.

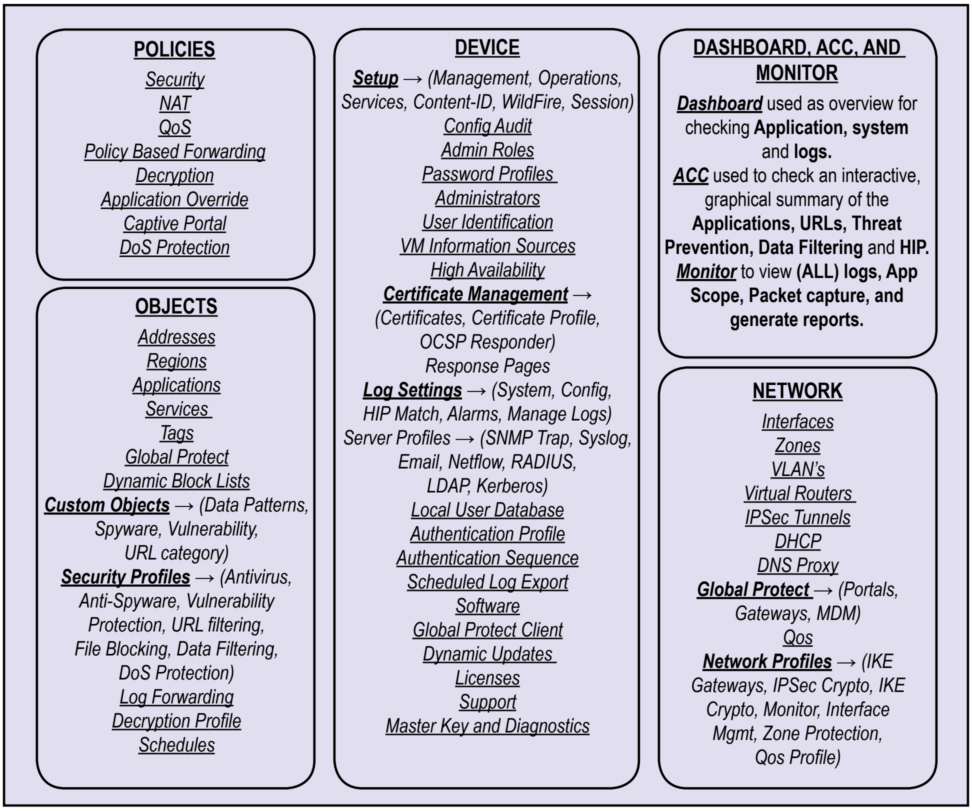
"Now, Hernyka," Nielair pushed away, stood. "I would like you to take some time to explore the menus and options in the Palo Alto firewall. Login to the firewall at https://10.10.10.10. I'll take the opportunity to examine the gadgets stocked in your store."

Nielair walked circuits of the room, always careful to keep an eye as Hernyka delved into Palo Alto's different options. Her face set, brows down and mouth a straight line as she worked. Nielair looked at the face and wondered. What strange girl, so bright and so engrossed in Palo Alto, ends up stuck in a junk electronics shop?

"Wow," she called to him some minutes into her task, "the GUI is simple and well-organized. I'm wondering, should I memorize all the tabs and the sub-menu?"

"That's not necessary," he answered. "I have created a snippet for all the tabs and included their menus inside each tab for a quick reference. Really, the more you play around with Palo Alto, the more familiar its menus and operations become. Practice makes you better. This is the truth for any product, technological or otherwise."

"Above all, though," Nielair said, "I hate the IT books. All the manuals, the training materials, filled with screenshot after screenshot like children's book. Some argue these books are formatted to help the layman, but I disagree. It's all just wasted paper promoting laziness. Let humanity visualize concepts and use their brain power. Go green!" Nielair took a breath, shook his head. "Sorry. I sidetracked myself. You'll excuse me, I get passionate about that which excites me. We were talking about my snippet guide."



POLICIES

Security
NAT
QoS
Policy Based Forwarding
Decryption
Application Override
Captive Portal
DoS Protection

OBJECTS

Addresses
Regions
Applications
Services
Tags
Global Protect
Dynamic Block Lists
Custom Objects → *(Data Patterns, Spyware, Vulnerability, URL category)*
Security Profiles → *(Antivirus, Anti-Spyware, Vulnerability Protection, URL filtering, File Blocking, Data Filtering, DoS Protection)*
Log Forwarding
Decryption Profile
Schedules

DEVICE

Setup → *(Management, Operations, Services, Content-ID, WildFire, Session)*
Config Audit
Admin Roles
Password Profiles
Administrators
User Identification
VM Information Sources
High Availability
Certificate Management → *(Certificates, Certificate Profile, OCSP Responder)*
Response Pages
Log Settings → *(System, Config, HIP Match, Alarms, Manage Logs)*
Server Profiles → *(SNMP Trap, Syslog, Email, Netflow, RADIUS, LDAP, Kerberos)*
Local User Database
Authentication Profile
Authentication Sequence
Scheduled Log Export
Software
Global Protect Client
Dynamic Updates
Licenses
Support
Master Key and Diagnostics

DASHBOARD, ACC, AND MONITOR

Dashboard used as overview for checking **Application, system** and **logs.**
ACC used to check an interactive, graphical summary of the **Applications, URLs, Threat Prevention, Data Filtering** and **HIP.**
Monitor to view **(ALL) logs, App Scope, Packet capture, and generate reports.**

NETWORK

Interfaces
Zones
VLAN's
Virtual Routers
IPSec Tunnels
DHCP
DNS Proxy
Global Protect → *(Portals, Gateways, MDM)*
Qos
Network Profiles → *(IKE Gateways, IPSec Crypto, IKE Crypto, Monitor, Interface Mgmt, Zone Protection, Qos Profile)*

Hernyka looked at the image with appreciation, "An all-in-one diagram! It looks great. I can hang this on my wall next to my desk and use it as a reference."

"Thank you! I'll briefly run you through it. There are seven tabs in the Palo Alto GUI interface, and I merged the first three tabs into one column, as they all concern viewing logs, graphical summary, and reports. The other four tabs have separate columns. An arrow key in the snippet indicates an additional sub-menu. For example, in the Objects tab, the Custom Objects menu has four sub-menus: data patterns, spyware, vulnerability, and the URL category."

General Settings and Management Interface Settings

"In the GUI, go to Device → Setup → Management. As you see in the GUI reference snippet, this is the only menu with tabs on the side. All remaining menus have sub-menus beneath. I'm not really sure why Palo Alto decided to design it like this. Perhaps they didn't want too many menus with sub-menus, which would have made the scroll bar larger.

"In the 'General Settings' panel, click the gear in the right-hand corner."

"Hang on, hang on!" Hernyka held out her hands. "Doesn't that gear icon remind you of Antikythera?

"Antikythera."

"The ancient Greek analog computer-slash-orrery?"

"Yes. It was an astrological model."

"Antikythera's gears moved to predict astronomical positions and eclipses for calendars, astrology, and Olympiads," Hernyka said. "Considering the Greeks had a computer, how did Charles Babbage, the British buffoon, become known as the father of computers?"

"Maybe we should call Zeus or Apollo the father of computers."

"The Greeks are far superior," Hernyka nodded. "We should rewrite the comp science textbooks."

Nielair chuckled. "Click the gear icon in 'General Settings'. You'll find your hostname in there and the FQDN of the firewall in the 'Domain' column (max 31 characters). There is also a 'Login Banner' column where you can enter text which will appear in the login screen below the credentials fields. If you wish, you may type something."

"Yeah, sure. Why not?" She typed, '**Any nation that builds nuclear weapons, that spends their tax money on ammunition and bombs, is a fraud, a hypocrite, sowing the seed of Satan**'.

Nielair glanced at her. He let his bubbling question pass. "Okay, save it and commit the change by clicking the 'Commit' button on the right-hand corner, then re-login. You'll see the banner message.

"Now go back to Device → Setup → Management. In the 'General Settings' config panel, we can configure the time zone, language, date and time, and where the device is physically located. Latitude and longitude are optional, but most people don't use them. This option would be useful if the firewall had been integrated with GPS on wireless cards. Imagine that! Someone could then use their gadgets connected through the firewall, even while traveling."

"If you travel, where will the power to run it come from?"

"Simple," Nielair said, "battery. We will discuss later the last two checkboxes, 'Automatically Acquire Commit Lock' and 'Certificate Expiration Check'.

"In the same 'Management' tab, click the gear icon on the 'Management Interface Settings'. It is self-explanatory. The IP address, netmask, and default gateway are configured through CLI during initial configuration. The speed should be auto-negotiated by default unless a duplex setting is specified on the switch. If you mess with the speed settings by mistake and cannot login to the firewall through either SSH or Web GUI, you will have to rely on console access. Use the command '**set deviceconfig system speed-duplex auto-negotiate**' to change back to auto-negotiate the management interface and try logging in. If it doesn't work, reboot the firewall by issuing the command '**request restart system**' in the operational mode and retry logging in. It should work now.

"In the 'Management Interface Setting' window, you will find the default services enabled in the 'Services' options such as HTTPS, SSH, and ping. This option is sufficient for a basic firewall-permitted service. If you want to monitor the device, you must enable the SNMP service. Never use HTTP, HTTP-OSCP, and Telnet services; they can cause serious security problems for the firewall since the traffic is in clear text and can be easily sniffed. I will discuss the User-ID options when I cover the authentication topic.

"The 'Permitted IP Addresses' section specifies the IP addresses' range or a single IP address. For example, the format for the IP range is 10.10.10.0/24. Until you add a restriction list, any network can access the firewall. Once you add the first IP address or mention the range, the firewall will block all unspecified address lists. So be careful and at least make sure that the administrator's network is included to access the firewall. This is a crucial config when we want to defeat dictionary or brute force password attacks since they will fail because the attacker has to be present in the management subnet to accomplish the same process."

DNS and NTP

"Although DNS and NTP are the basics of the networking world, sometimes network and security morons taunt their own family members by calling DNS and NTP engineers a waste of space. These engineers are crucial. It's similar to how society would crumble without sewer workers, babysitters, construction workers, farmers, transport workers, janitors, chef and kitchen helpers. Certainly, we wouldn't be here discussing Palo Alto!"

"Go to Device → Setup → Services to find the DNS servers that we configured through CLI. On this screen, click the gear icon on 'Services' panel to add or edit the DNS or NTP settings. Regarding DNS settings, configure the DNS server close to the firewall that's in the same data center or the closest ISP. For example, I just used a public Google DNS.

"In the 'Update server' column, you will find updates.paloaltonetworks.com, which is the CDN infrastructure used to contact Palo Alto servers for application updates, as well as threat and antivirus signature updates. Since updates.paloaltonetworks.com is a CDN infrastructure, it can contact any of the closest CDN update servers, which may be random CDN IPs. So if you have a tight security policy that specifies the need for your Palo Alto firewall to only contact a known static IP update server, change it to '**staticupdates.paloaltonetworks.com**'.

"The 'Proxy Server' section helps us to define the proxy server, port, and account information. This is in case the Palo Alto firewall is behind a proxy server, although the firewall can still reach the Internet. Check out DNS security best practices at http://www.cisco.com/c/en/us/about/security-center/dns-best-practices.html. You can also search the Internet to find some good SANS documentation on DNS."

"Wow," Hernyka said, wide eyes scanning the screen. "This option unites the Hatfields and the McCoys. I love it. Despite the differences, the firewall and proxy gangs work together like the FBI and CIA."

Nielair laughed loudly, "Your views continually impress me. So as I was saying, let's skip the 'DNS Proxy Object' radio button in the 'Services' window. In the same 'Services' window, click the 'NTP' tab. Here on this screen, we can define NTP servers to synchronize Palo Alto's clock with the servers. For synchronization with the NTP server(s), NTP uses a minimum polling value of 64 seconds and a maximum polling value of 1024 seconds. These minimum and maximum polling values are not configurable with the firewall. Once the Palo Alto Network's device goes through the initial synchronization process and synchronizes the system clock, it will poll the NTP server within the default minimum and maximum range. To check the status of NTP, type, '**show ntp**' in operational mode. If you see 'True' next to the NTP servers, it means it is functioning correctly. Otherwise, check the NTP server and restart the NTP services in the firewall in operational mode by typing '**debug software restart ntp**'. Something to keep in mind is that if an NTP server needs authentication, we can use the 'Authentication Type' column by either choosing 'Symmetric Key' for shared secrets or 'Autokey' for public key cryptography."

"How can I remember all these options and settings?"

"Great question. Do you see the question mark icon in the right-hand corner? It's the help option. For any window, tab or screen, you will find the '?' help option. It's a treasure trove of valuable information. It may not give detailed advice, but is a great place to refer to for quick support."

Management Routes

"The Palo Alto firewall features two routes. The first is the management route for handling management traffic for a management plane, and the second one is a virtual route for a data plane for the user's traffic, which we will talk about later.

"Go to Device → Setup → Services, under 'Services feature' section, click the 'Service Route Configuration' link. A 'Service Route Configuration' window will open up. The radio button on 'Use Management Interface for All' implies that all management traffic such as DNS, Email, NTP, Palo Alto Updates, RADIUS, SNMP trap, and Syslog will be forwarded to a management interface. If you want to pick and choose the applications that should be allowed to use the management interface, hit the 'Customize' radio button if by default it is not selected. Under the 'IPV4' tab, you will find all the applications listed and corresponding 'Source Interface' and 'Source Address' columns. 'Use default' indicates the service uses the management interface. If you need to change it, click any of the application links under the 'Service' column and choose the necessary interface. The source address is auto-populated.

"Separating the management's services from the user traffic has various benefits. First, it is easy to administer in case we use the management interface for services. We can easily grab the list of management IPs of all firewalls and configure it on the peer router or firewall. This allows access from the management interface IPs of the firewall to the services that are hosted. Secondly, it simplifies troubleshooting and improves security in case we need a secure connection for the management services from the firewall to the hosted services - like the RADIUS authentication traffic.

"As you can see, dividing the management and data plane traffic improves network performance and enables efficient monitoring of abnormal traffic spikes." Hernyka nodded her agreement and Nielair then continued with the next bit of their lesson.

Reboot and Shutdown

"A good nap is mandatory for humans. Sleep resets our system and refreshes our brain. Now, machines such as a computer weren't created to rest. If you go to an IBM Mainframe engineer and ask him how to reboot a mainframe, he would probably think you are on drugs or that you've escaped a mental institution. That is because mainframes are solid and strong, having no memory leaks, CPU overloads, process crashes, or disk errors. So mainframes don't need naps. I wouldn't call it a perfect machine, but in case of any problems, the machine doesn't need to be rebooted to solve them.

"Not all technologies are so efficient. For fragile technologies such as Microsoft desktops and firewalls, the first command you should learn is, "How to reboot or shut down a device." Although it sounds simple, you should know the process by heart. The CLI commands to reboot a firewall are as follows:

"To restart: '**request restart system**'.

"To shut down: '**request shutdown system**'.

"To perform through GUI, go to Device → Setup → Operations → Device Operations. You will find both restart and shut down options. Check for Palo Alto KB 'Getting Started: Setting Up Your Firewall'. That will help you when you are stuck. Now I want to ask you something slightly off-topic. Do you hate kings and their monarchies?"

"As an American, I of course hate kings and queens and subordinates. Their existence doesn't even make sense. All what monarchs did was to orchestrate wars, engage in the slave trade, exploit human rights, plunder homes, and get their faces printed on currency notes. And now these very notes and their portraits are hung on museum walls to honor these villains. Even that son of a gun Genghis Khan and the other 'Khan' dickheads still adorn Mongolian Tugriks to this day."

Nielair glanced at her. "But surely you see history had some good kings and queens?"

"I respect anyone who can justly wield power, but the bad monarchs give them all a bad name!"

Check Point

"So do you want to stick with Palo Alto or should we compare the Check Point, Cisco, and Juniper firewalls?"

Hernyka, her radical thoughts interrupted, took a calming breath. "Yes; it's vital to know and understand the different market vendors, since it will then increase my reasoning power and knowledge of the players in the field."

"Great! I'll give a quick overview of all the different concepts rather than demonstrating practical labs. I'll also share commands and show GUI navigation if it's necessary. The rest of the stuff like IP, DNS, NTP, routers and other options are the same."

"Sounds great!"

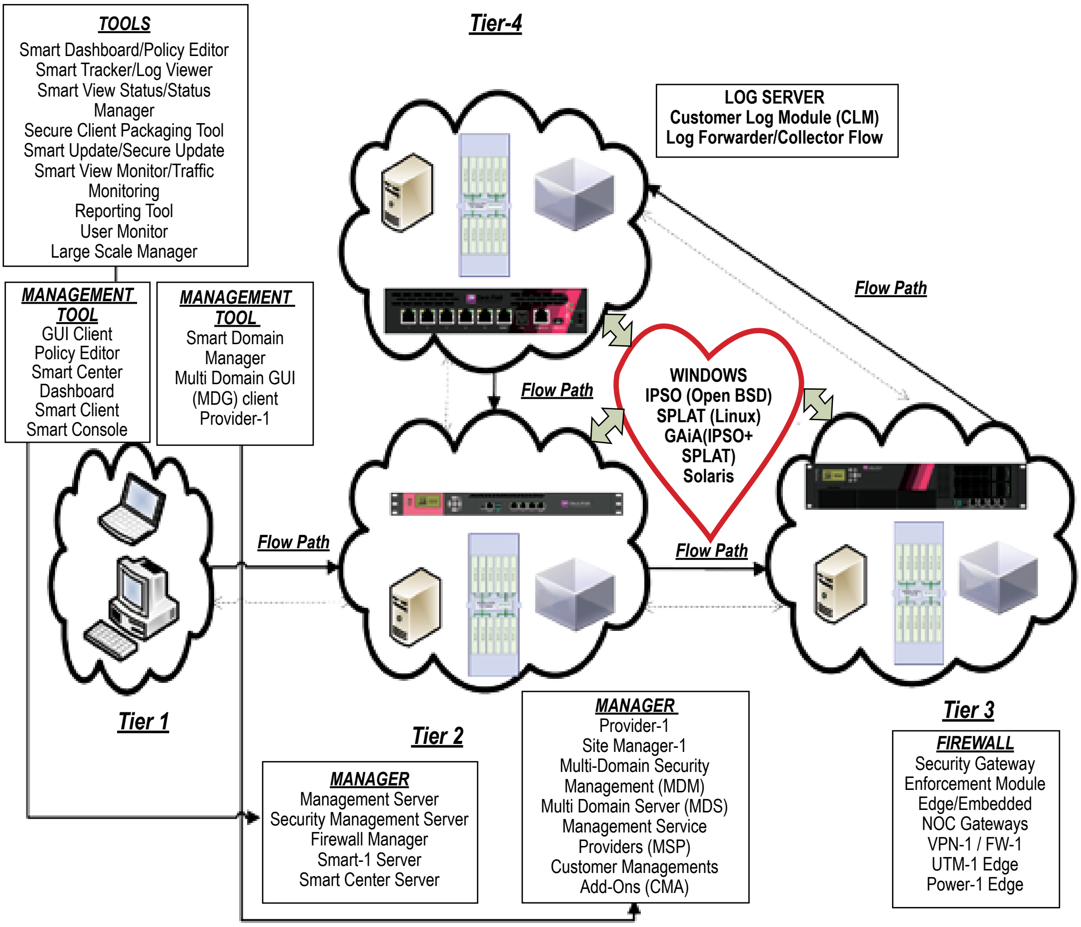
"Check Point's firewall basic model is a Tier-3 architecture. Ideally, in a big environment, it is a Tier-4 architecture. Having a Tier-3 architecture allows for improved scalability, performance, and security. Honestly, in my opinion, the architecture is fantastic, but Check Point's endless offerings of hardware, software, and OS make it a big pile of crap. The company's core product is enormous, making it unmanageable and uncontrollable.

"Ah I can see you're wondering why I'm so bothered by this Check Point? Let me explain this madness to you. Tier-1 is nothing except the Check Point client software that needs to be installed on a laptop, or even a Windows server. It is like Putty for SSH in the Palo Alto firewall or a web browser such as Chrome, IE, or Firefox accessing HTTPS GUI. In the past two decades, the Check Point client software has gone through many different names. You can see the list in the diagram. For now, you can refer to it as the Smart Console. There are two tables of management tools, which I will discuss in a moment.

"Similarly, like SSH and HTTPS, the Check Point software helps security administrator's login to the Tier-2 centralized management server where all policies, ACL, objects, and configs are stored."

"Does Palo Alto have a centralized management tool?"

"Yes. It is called Panorama. The big difference is that we can add and remove security policies directly on the firewall itself in the absence of Panorama. Plus, you can do anything with SSH and HTTPS access, but Panorama's centralized management adds more robustness and simplicity to managing hundreds of Palo firewalls. To make a long story short, without Panorama, we can configure and run the Palo Alto firewall, but without the Check Point Smart Console, we can't configure policies on the management server."



"Okay, okay," Hernyka nodded Nielair on.

"Again, the centralized manager has many names. For now, you can refer to it as a security manager or management server. In Tier-3, you have the actual firewall where the security policies are running that does the dirty work of allowing, blocking, stalking traffic, monitors the firewall, VPN, antivirus, and IPS. As you can see, there are many names for the Tier-3 firewall, so let's just stick to the firewall or security gateway. Enforcement Module (EM) is another prominent term in the Check Point community. Folks doing Check Point certification will find this called 'EM' in their books and study guides. In layman's terms, it is a security gateway or firewall. In a Tier-3 model, the firewall can forward logs to the security manager (for example, the Tier-2 is for storing logs). Generally, it is a burden for the manager to store security policies, and also manage these terabyte logs. So you need one more tier, and this is where Tier-4 comes into place. Instead of forwarding logs to the management server, the logs are forwarded to dedicated log servers whose only job is to collect and store the logs.

"The 'Flow Path' in the diagram indicates the flow from Tier-1 to Tier-4 while the dotted arrows indicate that the communication is bi-directional. Almost in the middle of the diagram, you'll see a lovely heart. This indicates the different OS on which Check Point can run. As I mentioned earlier, the software company was adamant about marketing themselves in a way that allowed major OS to run their software. To this day, the provision is still open. We can run Check Point in Windows, Solaris, and Linux. But like I explained earlier, because of the disorganized software and hardware lists, Check Point eventually came out with a new OS called GAiA. GAiA included the best bits of OS such as IPSO and Linux. IPSO is based on OpenBSD, which used to be the OS in the Nokia appliances that Check Point acquired in the late 2000s. Also, Check Point's SecurePlatform, a Check Point Linux distribution based on Red Hat Enterprise Linux, is often called SPLAT. GAiA, the new unified secure platform, is the recommended OS, and all Check Point appliances are shipped with it."

"What features of IPSO and Linux did they merge to create GAiA?"

"The usual bullshit hype," Nielair said with disdain. "They basically removed security bugs, made the system faster, re-engineered the processing speed, and simplified management, among others. There was also real-time intelligence, multiple layers of threat prevention…blah, blah, blah." Nielair tailed off with a dismissive flick of his hands.

"The best part is that they retained the commands used in IPSO and SPLAT. In the diagram I have shown you, there are two sets of central managers and two types of management tools. The first one is simply called the management server or security management server, which holds the policies of hundreds of firewalls. From the security management server, the policy gets pushed to the firewalls. It's pretty straightforward, as you can see.

"Imagine you are running an ISP. You will have different customers and a provisioned security management server for them. It works as expected, but the biggest problem is this: say that customer A, who is an administrator of the lingerie brand Victoria's Secret, can view customer B's policies, who is in charge of Aerie's security policies. That isn't a good security practice.

"For isolation, they have systems called Provider-1, among others. These management servers separate security rules as per customer request. So let's say the administrators of Victoria's Secret log in to MDS or MDM—what later versions of Provider-1 are known as—they can't then view Aerie's security policy.

"Compartmentalization isn't the only feature. Common security policies that allow admins to access common configuration objects, logging modules, and others are featured. This enables a company to use MDS product as opposed to their ISP's. This empowers all their administrators to view all policies. Isolation of policies is not the only goal, but rather ease of administration. Obviously, based on the network topology and IP address each company can have their own ACLs and manage it. To manage policies collectively, the client that needs to connect to MDS or MDM is called the MDG (Multi-domain GUI) client. The Tier-4 concept is the same.

"If we manage one company's firewall, we can use one security management server and one log server. For different companies, the practice is to go for MDS or MDM, and the corresponding log servers are called Customer Log Module (CLM), where each customer can only view their own logs. Let's just say that it's like rummaging through someone else's lingerie —it's prohibited!"

"Victoria Secret and Aerie are good examples to keep in mind," Hernyka said with a wink, "Check Point sort of sounds like a lady's kind of firewall."

Nielair smiled. "Installation and configuration are simple. Do you want me to walk you through the steps in the lab or should I just brief you?"

"Show me the steps if you have time. Otherwise a brief is fine."

"I'll show you the steps. The GAiA OS, which contains Smart Console, Security management server, MDS or MDM, and a log server, among others, is inside one ISO file. We need to install what we want to use. You'll need to register an account at https://usercenter.checkpoint.com. It is free, and they will give you a trial license for 30-days, but getting the ISO itself is tricky. I don't want you hanging around and searching for that. Use this Check Point Secure Knowledge article 'sk104859'. You can download R77.30.

"The latest one is R80, but I don't know where to get it, so the 'sk104859' is quite helpful. In the future, the 'sk' will change, but you need to adapt yourself. But for now, this can be your hometown for downloads.

"I will give you a lot of 'sk' articles. These documents are fabulous. Let's give Check Point a round of applause to for making them in the middle of their nightmarish combination lists of different hardware and software products. The link https://www.checkpoint.com/try-our-products shows all the products that we can choose for evaluation.

"It says software blades, which is what I want to focus on now. This is unlike Cisco products, which require the installation of hardware blades for more features. A license is a compulsory requirement, and we can add additional licenses as required. Without registering ourselves with an account at Check Point UserCenter, we get a 15-days license with the ISO file. With an account, we can get 30 days—just a tip! Not all licenses are enabled at the Check Point UserCenter's portal by default. We need to request the ones that are required, and they will provide them. Surf around Check Point's portal later. You will learn a lot about everything I just said in there.

"With so many tiers, I'll just start with Tier-1. It's a client software like Microsoft Word. Click 'Next', to install. I would say the best practice for installing it in a production environment is to install the security management server, then the firewall module in Tier-3. Tier-4 is just the log server; I don't consider it as important. You can find documents on the Internet or on Check Point's support site, where you can get all the information you need.

"Sometimes you may get the Smart-1 ISO file, which pretty much only has the security server management component. Always check with the Check Point manuals to know what ISO file it contains before installing or configuring it. If you want to learn Check Point, you can also install it in a VMware like VMware Workstation or Virtual Box, which is free and downloadable from https://www.virtualbox.org."

"I have VirtualBox, VMware, and GNS3 for my CCNA lab," Hernyka said. "I'm familiar."

"Great! There are some awesome tutorials on YouTube. Whenever you want to mess around with unfamiliar software, OS, network products or testing malwares, you should use VMware products. They are safe and don't inflict damage on your confidential files. Also, you can install them a thousand times without impacting the real OS. An even better option is to use VMware in a dedicated lab machine isolated from your regular laptop or desktop. This is safer, since in the event of damage or a crash, only your garage lab desktop will be affected. I recommend assembling a desktop and beefing it up with 16 GB RAM and a 500 GB hard disk for superior performance."

"Good tip," Hernyka said, "I have my old desktop, which is equipped with 8 GB RAM and a 300 GB hard disk."

"Fantastic! I have a VMware machine and it's booting up GAiA OS. We can select the keyboard type, assign the IP address/mask/gateway 209.87.209.100/24 and the gateway 209.87.209.1/24. Regarding the admin account information, the default username is the 'admin'. The password can be typed here. Then, it shows the disk partition settings.

"Since we have allocated 20 GB, the Check Point automatically assigns the partitions. If we want to change the disk settings, we can do so by clicking 'Next'. Use the Tab key to move between options, or use the UP and DOWN arrow keys. If it asks for a reboot, press 'OK'. That's all."

"It's so simple."

"Indeed. I just showed it to you in a VMware box. If we had a Check Point appliance, which I don't have on me right now, you should look for something called LOM (Lights Out Management), which is an alternate way to install Check Point and bring it into the network. LOM is used when the firewall has to sit in an isolated network where admins don't have network access to the firewall. Using LOM, a site admin can plug in locally into the firewall. Alternatively, the usual method is to connect the Ethernet interface and console port.

"When a firewall is introduced into the network, the administrator connects to the console port and does the initial setup like the one we did in the VMware, which includes setting up the GAiA keyboard, IP address, disk partition, admin account, and the reboot. Then it's finally connected via the new IP address through HTTPS. In LOM, a site engineer connects his laptop to the LOM port (whose default IP is https://192.168.0.100), he configures his laptop in the same subnet range of the LOM port, and he begins the config. Once you log in via https://192.168.0.100 using 'admin/admin' as your login, the web GUI is launched. LOM is a Java KVM, so make sure Java is installed on the connecting laptop. The Java KVM is called JViewer, which is launched automatically. The site admin can load the ISO OS from his laptop locally rather than from the network."

Hernyka searched for LOM on her smartphone. "I have a PDF about LOM. On page 7, I can see we have power controls, email settings, network configs, users, LDAP, RADIUS, and many other basic configs."

"That's right. All your initial settings can be configured here. After rebooting our VMware, we can connect it to the web portal via https://209.87.209.100".

"Wait a second…I'm confused," Hernyka's face scrunched in a puzzle. "You said all the configs are stored in the security management server and that it can be accomplished via Smart Console, the client installed tool. Can we also configure it via the HTTPS web portal? In that case, does it mean that Check Point has two ways of doing configs?"

"Good questions. Any Tier-2, 3, or 4 has SSH access and HTTPS access. The HTTPS access is not a replacement for the Smart Console. We can use it to configure the system and network settings, but that's all. Smart Console is purely for configuring security policies, such as NAT, VPN, IPS, AV, URL filtering and anti-botnet protection. With that being said, Check Point's most important warning is to not configure security policies via SSH. What I mean is that Check Point GAiA is a Linux-flavored OS, which means you can run all the Linux commands from inside SSH.

"F5 is another product that has shell access, through which we can use all the Linux commands. Even if a tool is not found, we can use the RPM package manager to install it. Through Smart Console, we can create a security policy and push it through the Firewall via the Security Management Server. In the background, though we may be able to click several icons, it is written into several files.

"Now…you may suddenly ask why we should use GUI to write in the files when we could go directly to the CLI interface and edit the file. Although it sounds logical, according to Check Point, it's suicide. The firewall will crash. You can locate the files in the /opt folder via SSH. Even for Linux legends, it is a good idea to treat Check Point Linux like a stranger."

"That's a very valid point and I think it applies to all fields," Hernyka said. "Like how a person may be a Cisco guru, but it is still crucial to go through proper training before they work with a competitor like Juniper. You need to know the product well, seek advice, clear doubts from Juniper experts and not do any stupid stuff that may end up doing more bad than good."

"Exactly," Nielair nodded at the girl's wisdom. "The web portal that I'm talking about is also called the 'First Time Configuration Wizard'. Click 'Next' in the first window. In the 'Deployment Options' window, we can do a fresh install. Boot it from the USB, or if you have a snapshot of the firewall, you can import it here. This is pretty much rebuilding a firewall crash. The next screen is the management interface setting. In VMware, if you want to have multiple interfaces, you should configure them before loading the ISO. In VMware, there is a maximum of 4 interfaces. If it is a Check Point appliance, check the hardware specifications. Click 'Next' and name the security management server '**GilShwed**'. After filling in the DNS and domain name, hit 'Next', fill out the 'Date and Time Settings', and choose NTP on the next screen if needed. Here is where we define if we want the MDS (Multi-Domain Server) or the Security Gateway/Security Management server."

"Oh, like the lingerie example!"

"Precisely. Click on the radio button, 'Security Gateway or Security Management', and hit 'Next'. This takes you to the 'Product' screen."

"Why do we have to check boxes for 'Security Management' and 'Security Gateway'? Can't we install both of them on one system?"

"You're one of the smarter students I've taught!" Pride brightened Nielair's voice. "The diagram I showed you is called distributed deployment, where we have all the components separated. There is another deployment method called standalone, where we can put all the four tiers into one system. Do not consider Tier-1 since it can always be in a laptop. Tier-2 and 3 are in one module. Tier 4 is an add-on module, so ignore it. Both the products are selected under 'Security Management' and 'Security Gateway'. Click the drop-down menu in 'Define Security Management as:' There you will find options such as 'Primary', 'Secondary', and 'Log server /Smart Event only'. You may wonder why I don't include Tier-4 in the standalone deployment. This is because the component of logging is already in the security management. Tier-4 is only needed for larger deployment when a dedicated log server is needed. Does that make sense?"

"It does. So when do we need standalone deployment?"

"If you have a startup lingerie company with 10 employees, you neither need a large scale deployment, nor can you deploy your needs in a lab environment."

"You're not letting go of that lingerie example, are you?!"

"If you'd prefer I could use the boring 'Alice and Bob' examples used by so many in the industry."

"More a joke than a complaint," Hernyka said with a smile. "Besides, I'm so bored to death of Alice and Bob. Please continue!"

"Only select 'Security Management'. The clustering option is for firewall gateways. The old protocol is VRRP and the new recommended one is Cluster XL. That option gets grayed out when we uncheck the 'Security Gateway'. You should know that this is our primary security management, so click 'Next'. In the following screen, we can change all the admin account info. The username can be 'admin' and the password can be '**earth1993**'. The next screen then helps us to define the GUI clients (for example the Tier-1 clients that can connect to the Tier-2 management server). To combat brute force or dictionary password attacks, only define the networks that can connect to this security management server. Hit the 'Next' button and click the 'Finish' button to install the security management server. This takes time, so in the meantime, we will do the same setup for the firewall module.

"I'll create it in a VMware. Make sure we put it in VMware Bridge mode since we want it on the same network. I think you know VMware concepts, right?"

"I know about the NAT mode, bridge mode, and the host-only networks." Hernyka said. "So yeah, VMware is cool stuff."

"Awesome! It's the same process for both the Security Center Server and firewall module. I am booting the ISO in VMware, defining the IP/subnet/gateway, assigning the administrator username/password as 'admin/earth1993', 209.87.209.101/24 and the gateway as 209.87.209.1/24. Once I confirm 'Ok' in the window, the package installation starts and it reboots."

"This time it didn't ask anything about disk partition, keyboard settings and other settings."

"VMware can auto-detect. It needn't necessarily show up in these messages. Once it is rebooted, log into the web portal https://209.87.209.101 using the credentials 'admin' and 'earth1993'. You'll see that the 'First Time Configuration Wizard' will appear. Click 'Next' in Deployment Options. The 'Management Connection' window will open. Name the firewall '**ShlomoKramer**' and the DNS '**8.8.8.8**'. Then hit 'Next'. We don't need NTP settings, so skip it. Select 'Security Gateway or Security Management' in the 'Installation Type' window. This is the actual firewall. Uncheck the 'Security Management' checkbox and leave clustering as cluster XL. Click the 'Next' button.

"We don't need DHCP, so skip the 'Dynamically Assigned IP' with the 'No' option. The 'Secure Internal Communication (SIC)' window is the crucial part. We have to provide an activation key. This is basically used when we add the firewall to the manager. We need this SIC key to establish communication so it won't use the 'admin' account password we have created. It needs a separate key for establishing communication with this OTP (one-time password). Let's use the activation key '**mariusnacht1948**' and confirm it again by clicking 'Next'. Finally, after hitting the 'Finish' button, you will see that our firewall has begun to install.

"Let's go back to the security manager that we first installed. We can login via the HTTPS web portal https://209.87.209.100 using the username and password 'admin' and 'earth1993'. In the overview page, you can download the SmartConsole software to complete the installation on your computer, or wherever you want to manage Security Manager. On the right-hand side, we can find all the software blades that are available with the Check Point Firewall; along with IPS, IPSec VPN, URL filtering, anti-spam and mail, DLP, application control, anti-bot, antivirus, and threat emulation.

"On the left-hand panel, we have all the basic ways we can configure the network in the firewall. Breaking it down, we have the 'Network Management' panel, where we can configure interfaces, ARP, DHCP, DNS, NetFlow, and static routes. 'System Management' can customize time, SNMP, mail notifications (or to be more precise, email notifications) and proxy settings (if our firewall is behind a proxy). This proxy option was available in the NTP setting in the first-time wizard. Other customizable lists in this section include banner messages, CLI and Web UI session timeouts, core dump, certificate authority, and system logging, amongst others. One option worth mentioning is 'Host Access'. This config method is the opposite of GUI client. While the latter is for Smart Console access, 'Host Access' enables HTTPS access to the box itself.

"We have five methods of access, namely LOM, console, SSH, HTTPS Web UI, and the Smart Console. The SSH even has an alternate name: the GAiA SuperShell.

"Incredible, isn't it? The next is the 'Advance Routing' panel, where you can set up the firewall for the DHCP relay, BGP, IGMP, PIM, RIP, OSPF, PBR, all the route-based options, and the routing monitor. Next comes the 'User Management' panel, from which you can change the admin password, add users and roles, set password policies, define authentication servers, and add GUI clients that define the Smart Console, which you must already be well-aware of.

"'High availability' helps us design the security server for HA pairs. We may only have the VRRP option, but for the firewall, we have both legacy VRRP and Cluster XL Check Point's recommended HA feature. The 'Maintenance' option helps us add licenses and take a snapshot of the system. If you recall, in the first-time config wizard, we were asked whether we wanted to freshly install or to recover the firewall from a snapshot. This snapshot is the one that is taken when the security server is stable and running, and it can be used whenever the security server faces instability problems or crashes. In this panel, we can backup, download Smart Console, which we did in the 'Overview' page, and reboot or halt the system.

"Finally, the 'Upgrades (CPUSE) Panel' helps us apply hotfixes, install minor and major versions, and schedule downloads manually. Automatic is an available option in the 'Software Updates Policy'.

"The firewall, HTTP Web UI, is similar to the security server. Let's log into https://209.87.209.101 using the earlier login credentials of 'admin' and 'earth1993'. At first glance, you will notice that in the Firewall Web UI, you cannot see the 'OverView' page that you saw on the security server."

"I know," Hernyka answered. "I've been trying to master Check Point. Smart Console software is not in the 'Overview' page of the firewall. Also, we don't have GUI client config in the 'User Management' panel."

"Praise the princess of Check Point!" Nielair gave Hernyka a little round of applause before continuing. "The 'Network Management', 'System Management', and 'Advanced Routing', panels are similar for both the security server and the firewall. You can spot the difference in the 'User Management' panel. The first three panels are the same except for the 'Smart Console' option, which is available only on the security server."

"Why do they have the routing module in security server?" Hernyka asked. "It's like the Queen Bee of Check Point. Why would it require routing? After all, it's the firewall that sits on the perimeter that needs routing functionality."

"I don't know. A lot of the processes don't make much sense. Maybe Check Point felt like giving the Queen Bee more work than usual. I believe they have a routing feature, but it's best not to enable it. You can liken it to the automobile industry, which can develop superior engines that roar at 200-miles-per-hour, but remain restricted by 70 mph speed limits."

"I disagree," Hernyka interrupted, shaking her head, "without a 200-mile-per-hour car, how will we outrun zombies, aliens, vampires, and serial killers?!"

"You watch too many movies!" Nielair laughed with her. "It is strange, though, that aliens constantly appear in the USA…" he trailed off. Gone off track, silence washed over them, guided them back to topic.

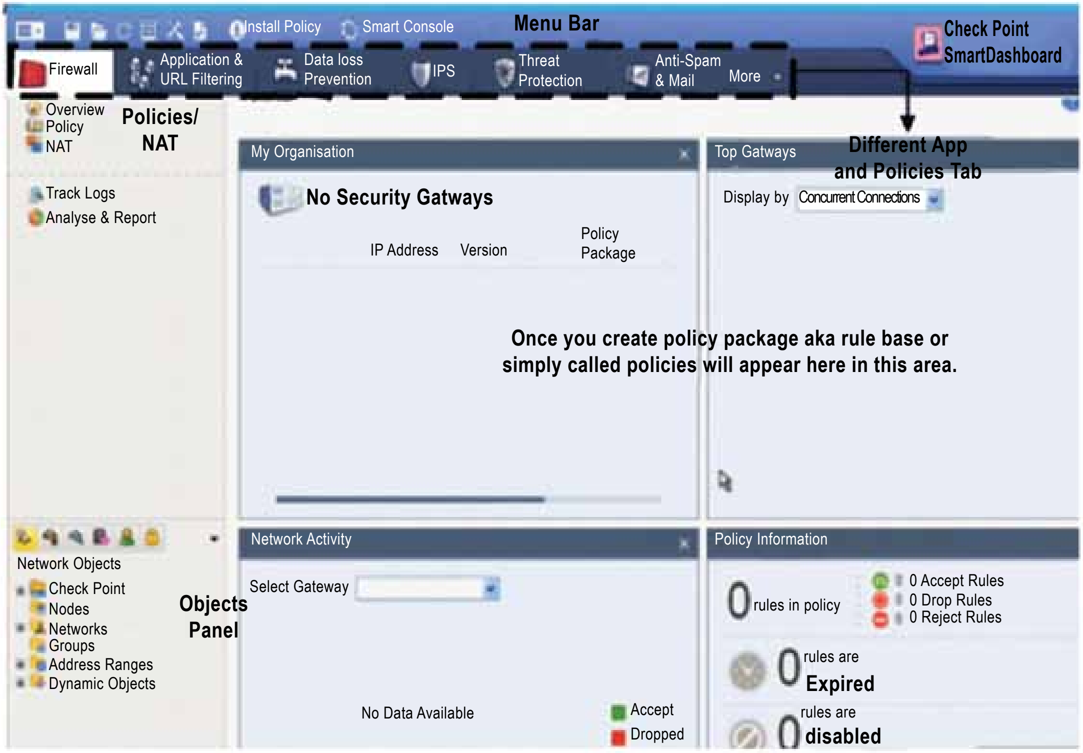
"Now that we have the security server and firewall ready, install Smart Console on one of my Windows 8 PCs. I will follow with the 'Next' button protocol to get it installed. I need to go to the start programs, and under 'Check Point SmartConsole R77,' click 'Smart Dashboard 77'. The 'Demo mode' is for beginners, where we have all policies, objects and configuration available. In demo mode, there is provision for a live simulation to get a feel for how the Check Point Smart Console looks in the real world. For now, we will login to the dashboard with the Security Server IP as 209.87.209.100 and the username and password typed as '**admin**' and '**earth1993**' respectively."

"What's this fingerprint mechanism? It sounds like a nursery rhyme!" Hernyka asked, her nose wrinkled with disgust.

"It's a mechanism to verify that we are connecting to the correct security server. Check Point calls it a fingerprint, but I prefer to call it graphology. We can verify the graphology via the SSH of a security server, and the same fingerprint will be displayed. If I type the command '**cpconfig**', a list of options will appear. Hit '7' and the same text message will appear as in the Smart Console. We don't need to save it so type '**N**' and press '**9**' to exit.

"Once the fingerprint is verified, click 'Login' to see the Check Point SmartConsole GUI. I find it beautiful. The visuals are easy on the eye. At the very top is the 'Menu Bar'. A drop-down menu in the left-hand corner has many options for creating policy packages, adding rules, SmartWork flow, set view options for different settings, and few more, as you can see.

"In the same menu bar, you will find the 'Install Policy' option. In the 'Smart Console' drop-down menu, we can see the different tools that Check Point offers for administration such as the SmartView Tracker, SmartProvisioning, SmartView Monitor, SmartReporter, and SmartEvent."



Once you create policy package aka rule base or simply called policies will appear here in this area.

"Below the 'Menu Bar', you'll find the application and policies tabs. Right now, we are discussing the firewall functions. So, to configure the URL filtering, click the 'Application & URL filtering' and to turn on the IPS, and click the IPS tab. In a nutshell, all the NGFW security features are engraved in those tabs.

"You can see the 'Policies/NAT' option on the left-hand side below the application and policies tabs. That is where you can configure the ACLs and NAT rules in Check Point. The objects panel is in the bottom left-hand corner, which we can use to create all types of objects that are needed to build policies. The center space is the 'Overview' page, which gives a summary of the products, firewalls, policies, and network activity. Once we create a policy package, which is also known as a 'rule base' or 'policies,' the overview page is changed and the rules appear in a top-down fashion, which is similar to how it appears in Palo Alto. These rules are the firewall's bread and butter. In the 'Objects' panel, expand the Check Point link, you can see 'GilShwed' security server object is automatically created for us. In the world of Check Point, all things such as firewalls, management servers, log servers, other kinds of servers, hosts like computers, desktops, and network ranges are represented as objects. These objects have properties defined in them.

"To wrap up our initial configuration, we need to create an object for the 'ShlomoKramer' firewall that we have just configured. Select 'Check Point', and right- click to select 'Security Gateway/Management' from the options. Click the 'Classic Mode' to help get a feel for the menu options in Check Point. Next, the 'Check Point Object' page will pop up. In the first link, which is called 'General Properties', name the firewall '**ShlomoKramer**'. Remember that while entering names into Check Point, there should be no spaces in the names of the objects. Check Point will throw a tantrum if you use spaces. The IP you should use is '209.87.209.101'. In the 'Platform' section, choose all the settings that are related to the hardware platform where the firewall is installed. Since we are now using VMware hardware, click 'Open Server', and you will find that all the other settings have been set up automatically.

"As I mentioned before, Check Point is a software blade solution unlike Cisco. So in the last section under 'Network Security', select the modules that you want the enforcement module or firewall to use, and check the packages that need to be added to the GAiA. Of course, you need a license to make it work, but here is the place where you can turn the buttons on. The last piece is config SIC. In the same 'General Properties' page under 'Secure Internal Communication', click the 'Communication' button and type the password '**mariusnacht1948**', which we used while configuring the initial settings of the firewall. This SIC activation key is an authentication mechanism to tell the firewall that the right SMS is connecting to it."

"So what exactly is SIC?" Hernyka asked.

"SIC is based on certificates. When our Security Management Server (SMS) is initially loaded, part of the post-installation is utilized toward initialization of the Internal Certificate Authority (ICA). The SMS is a full-featured certificate authority, and the first thing the ICA does is create a certificate for itself (the 'SMS-Cert'). The SMS-Cert is presented when we connect to the SMS by using any of the SmartConsole GUI tools to validate the identity of the SMS, or the fingerprint. The SMS-Cert is also presented to firewall gateways when a policy is being pushed to validate the identity of the SMS. You can either view the SMS-Cert in GUI or in the '**cpconfig**' command on the SMS. It can be reset using the '**fwm sic_reset**' command. This initial trust problem is solved by the use of a SIC activation key. This is essentially a pre-shared secret which is very similar to IKE Phase 1 authentication that is used to establish a one-time trust between the SMS and the Security Gateway so it can receive the FW-Cert.

"When we hit the 'Initialize' button, the SMS and the Security Gateway performs a two-way challenge, essentially convincing each other that they both have the same value for the activation key. Once the Security Gateway receives its FW-Cert, the activation key becomes invalid. After that, the activation key won't do an attacker any good. From this point, all communication between the SMS and Security Gateway is authenticated and encrypted using SMS-Cert & FW-Cert, which establishes trust between the two entities.

"The goal of initializing SIC or trust between an SMS and Security Gateway is to have the ICA create a certificate and assign it to the Security Gateway (FW-Cert). Once that is accomplished, all communication between the SMS and Security Gateway is authenticated and encrypted using a certificate exchange. Once a new Security Gateway has been loaded and placed on the network, it needs an SMS to assign it a certificate ('establish trust') so that it can receive a security policy and begin working."

"The certificates are 2048 bits and valid for 5 years. They change as security standards in the SSL paradigm evolve. Search 'Check Point ICA internal_ca' to get the admin guide, which talks about the ICA in more detail. It's always useful to have a local copy of the admin guide saved onto your desktop. Check Point has many different ones, so it's a pain to locate the correct ones. Use this link for your convenience: https://sc1.checkpoint.com/documents/R77/CP_R77_SecurityManagement_WebAdminGuide."

"Thanks for the document link! I'll download the documents for the different versions and features as we're talking."

Cisco

"Have you been to Thailand?" Nielair suddenly asked.

"I'd love to but haven't. Why?"

"King Bhumibol Adulyadej was a great man. He is considered the cornerstone of the country's modern-day prosperity. However, hung up all around the country are posters of people kneeling before him as a sign of respect. This seems against humanity to me, though the Thai's revere him as a God. They even have a lifestyle website, www.kingpower.com. It kind of sucks, don't you think?"

Hernyka crimped her lips, blew a puff of air from her nose. "Kings should go to hell, and queens doused in fire. Kneeling is horrible. May the good Lord show the ladyboy king the path of equality!"

Nielair pumped his fist skyward. "Long live the ladyboy king!" The two laughed for a moment, bright and cheerful.

"The next firewall is Cisco. As you are a student of CCNA, this should be interesting."

"I doubt it. I'm more fascinated by the Palo Alto firewall, and after our talk, I'm getting a good vibe from Check Point. Cisco, with its deep pockets, has suddenly lost its appeal."

"Let me tell you a little about the evolution of the state-full inspection process in the Cisco world. Cisco routers with IOS-based firewalls began their journey with packet filtering firewall functionality in a sophisticated way. They called it ACL (Access List). One has to write ACL policies for forward and return traffic. Sounds terrific, right? They quickly they shifted to the 'Established ACL' method. Just add the 'established' keyword at the end of the ACL. For example, '**permit tcp host 192.168.192.168 eq 80 any gt 1023 established**'. The 'Established ACL' method isn't a stateful inspection technique. It's a bumper sticker in the inspection analysis that's only meant to check the 'ACK' bit in the TCP header after a TCP handshake is completed. Understandably, the first packet in the transaction is SYN, which doesn't get checked, while all the other packets that contain the 'ACK' bit are examined. Thus, it is easy to spoof and fool the router.

"Next, they discovered a better step by introducing reflexive ACL where you could create ACL in the router as '**permit tcp any any reflect REMEMBER**'. The same methodology could be used for UDP and ICMP with a corresponding keyword in it. 'REMEMBER' is the keyword to make reflexive ACL work. Think of internal users in an office trying to access the Internet. After granting permission for them to reach the Web, the router automatically creates an ACL for the return traffic. You can verify the return ACL by issuing the command '**show access-list**'."

"My God, that sounds pathetic." Hernyka said. "This is for routers, right? Or does the Cisco ASA firewall also behave like this? This method of establishing and remembering keywords is so naïve. It's almost as if the company was taunting its loyal customers, flaunting sub-par products while knowing users will continue to purchase from them because Cisco is an established brand."

"Maybe," Nielair shrugged. "Anyway, we are talking routers. I'm briefing you about this because, these days, firewall stateful function is integrated into all switches, routers, desktop firewalls, and home wireless gears. I thought this would be helpful. Also, when you encounter networks and infrastructure that runs IOS-based firewalls, you shouldn't be surprised to have these non-stateful methods. Leaving aside this comical way of creating an automatic reverse rule for return traffic, reflexive ACL can only work from Layer 2 to 4. Since Cisco is a company with adequate capital, they got smarter and introduced the Context-Based Access Control (CBAC).

"CBAC is able to inspect all the way to the application layer, taking into consideration characteristics of a flow on a per-protocol basis (or context). CBAC allows you to define an inspection rule for each protocol that you want to monitor. I have an example to help you understand this better. To enable stateful inspection, use this command to enable all TCP traffic: '**ip inspect name Stateful-for-TCP TCP**'. The 'name' is user defined, and we can use UDP or ICMP to config routers so that we assign ACL to the interfaces by using the commands '**int fa/1**' and '**ip inspect Stateful-for-TCP out**'. You can check the ACL by '**show ip inspect interfaces**'. You will notice that the outgoing inspection is set to "stateful-for-TCP" and the inbound access list is denied. This makes the ACL stateful since inside users can reach outside and traffic from outside to inside is denied. For a specific application protocol like web traffic '**ip inspect name Internet-Web-Access http**', use 'https' if the traffic is encrypted.

"After this, Cisco came up with a zone-based firewall, a true stateful advanced inspection firewall that was more or less identical to Palo Alto, Check Point, and Juniper. It had several components and moving parts to build modular security, network, and inspection policies. Before we talk about components, you should know Cisco's traffic classification process, which is essential to performing Layer 3 to Layer 7 operations.

"There are three steps to classify traffic, also called the Modular Policy Framework (MPF). They are class maps, policy maps and service maps. These three modules aren't abstract concepts. They're actual configs that you need to edit to make them work. A class map identifies the type of traffic, whether it be HTTP, FTP, VOIP, SSH, or any supported protocol that Cisco can identify.

Once we identify the traffic, the next module, a policy map, decides what action should be taken. Allowing and denying are part of policy action. In addition, the policy map can perform actions such as doing a deep application inspection for protocol violations, passive FTP, send to the IPS or CSC module for threat prevention scanning, apply QoS, perform advanced TCP operations such as timeouts, prevent DoS attacks and others.

"So far, we have identified the traffic and defined the action that should be taken on it. Now, the final module is a service map that tells you where to apply the action such as on an interface or globally on all interfaces.

"The components that make up zone-based firewall policies are zones that are mapped to interfaces. Class maps are used to identify traffic, policy maps are for applying the actions and zone pairing is for identify the zones involved. And finally, the service policy specifies the policy that is to be used on the zone pair. Maybe you noticed that I mentioned policies while I was talking about the stateful firewall. It isn't ACL, which is a cheaper version of firewall inspection."

"I get it, but I'm confused about zones, mapping of interfaces, and zone pairing."

"No worries, I'll cover these topics as we discuss them further. Now, we dive into Cisco ASA (Adaptive Security Appliance). The baby bear model ASA 5505 doesn't have a dedicated console port; other models do. The default management address is 192.168.1.1 in the 8-port ASA 5505. We can connect to any port except Ethernet0/0. On the other hand, Management 0/0 is the default management port for all models."

"Cisco is confusing because they keep changing the standards," Hernyka said. "The default username and password was 'asa' and 'cisco'. After 8.4, I believe there isn't any password. But some say username and password is 'cisco/cisco'. It's a pain in the butt."

"I don't blame you for being confused," Nielair said. "Inconsistency from version to version is a nightmare.

"Passwords are a mystery in the world of Cisco. They can just choose to have one unique account for the entire range of Cisco products, like how they could clear up the confusion with the username 'John' and the password 'Chambers'. One thing for sure though, there's no enable password for the ASA. In virtual firewalls, or in Cisco terms, 'context firewalls', the firewall is partitioned into several logical firewalls within one piece of hardware. There can be more than one management interface. ASA 5580 has two management interfaces: Management 0/0 and Management 0/1. And ASA 5585-X has three management interfaces. In each context, no more than five concurrent Telnet, SSH, and GUI ASDM management sessions are allowed.

"Since it is a management port, it doesn't support multicast, sub-interface, or QoS. Nor does it allow user traffic to pass through. But if we have a security plus license, we can convert management 0/0 to a regular interface."

Hernyka smiled, added, "The moral of this story is that if we have money, we stand a good chance at changing the laws of nature. Not like Michael Jackson, though. He got it all wrong. He should have loved himself rather than damaging his skin and body. Sucker!"

"Well said." Nielair answered. "When a pre-sales guy preaches about his product and the user demands crazy features not supported in the current version of hardware and software, he will make it his goal to give the users what they want. And based upon their request, a new product line will emerge.

"As usual, connect to the management interface on its default IP 192.168.1.1/24 by using your computer in the same network. If it is a brand-new ASA that's right out of the box, the current version should already be running. If you have an existing firewall that you want to rebuild from scratch, use the famous copy command to load the ASA software into the flash: '**copy tftp://192.168.1.100/ asa962-smp-k8.bin disk0:/ asa962-smp-k8.bin**'. For a TFTP server, use the 3cDaemon free software, which can run FTP, TFTP, and the Syslog server."

"I use 3cDaemon. It's simple and neat."

"It's pretty easy to load the software through the management interface. There's also one more concept called ROMMON initial config. Let's say you are connected to the console or management port of the ASA for CLI access, and Ethernet0/4 is connected to the LAN switch in the network 10.10.10.0/24—the network where the TFTP resides (or it's directly connected to your computer by using a crossover cable). In that case, you should issue these commands:"

```
interface Ethernet 0/4

address 10.10.10.10

server 10.10.10.20

file asa962-smp-k8.bin

tftpdnld
```

"After the reboot when we issue the '**show ip**' command, you won't see an IP address for Ethernet0/4, so the ROMMON is a temporary placeholder for the Ethernet0/4 port IP address."

"Cool," Hernyka said with enthusiasm. "Now you mentioned ASA 5580 and ASA 5585-X. Does the X represent anything?"

"Great question. The 'X' models belong to a class of new ASA firewalls that support all the latest code from 9.5 and above. The models without 'X' still exist, but cannot be upgraded to 9.5 and above, which means they can run any code between 7 and 9.5. Now that we've got the latest and stable ASA software running, we need one more piece: the ASDM software. It is the GUI that manages the ASA firewall. Always check the compatibility between the ASA software and the ASDM, and load it to the flash memory by using copy command like '**copy tftp flash**'. The ASDM software is a bin file, which should be something like asdm-762.bin, and it should be downloadable from Cisco. Once it is copied to the flash, we need to make sure that when the ASA reboots, it loads the correct ASDM image. So issue the command '**boot system flash:/ asdm-762.bin**'. To check the settings, use the command '**show bootvar**'. To check the ASDM image, type, '**show asdm image**', and to set the image, use the command '**asdm image flash:/ asdm-762.bin**'.

“To change the IP address of the management interface, run the same commands from ASA CLI:

```
interface management 0/0

speed 100

duplex full

nameif this-is-mgt-if

security-level 77

ip address 72.163.4.161 255.255.255.255

exit

ssh 72.163.4.161 255.255.255.0 this-is-mgt-if

ssh 184.26.162.0 255.255.255.0 this-is-mgt-if

ssh 184.30.50.0 255.255.255.0 this-is-mgt-if

ssh 140.242.64.0 255.255.255.0 this-is-mgt-if
```

“You must be familiar with most of these commands. Except the ‘**nameif this-is-mgt-if**’ and ‘**security-level 77**’ commands, which I’ll talk about with zones and interfaces, they’re similar to the router. For now, in ASA, we need an interface name, and the security level is a mandatory component in creating policies. The ‘ssh’ config command allows trusted networks that have been granted prior permission to access the ASA. Those that aren’t on the list are denied access. The traffic that comes into management 0/0 with the defined subnets is allowed. This doesn’t necessarily mean that if the same subnets enter via other interfaces—for instance, via Ethernet0/4—that they won’t be permitted.

“The next step is to enable the https service by using the command ‘**http server enable**’. I know it’s kind of confusing that the command says http, but keep in mind that the service is https. Don’t forget to save the config. The ASA is the same as the router: ‘**copy run start**’ or use ‘**wr mem**’.

“Now that the ASDM image is set, we can connect to ASDM with the IP address https://72.163.4.161. There is no enabled password by default, so just press enter without entering the username and password to login. To launch the GUI, we have two options. Either we can install the ASDM launcher as an application in the desktop, or we can use the JAVA version. Once you launch the GUI, you will land on the ‘Device Dashboard’ home page, which will give you the overall statistics of the box. There are three pages in the ‘Toolbar’ that you can see below the menu bar. In ‘Home’ where we are now, there are two tabs: ‘Device Dashboard’ and ‘Firewall Dashboard’. The second page is ‘Configuration’, where we do configuration. I feel dumb mentioning all these details.”

"The third page is 'Monitoring'," she said, "where we monitor."

He chuckled, "Exactly! The 'Home' page is self-explanatory, and you can explore it yourself. Navigate to the config page and click on the 'Configuration' button, this is the place where the magic happens! Then we'll land on the 'Device Setup' panel. Depending upon the ASA software, you will have several sections in the left-hand panel. The most common ones are device management, device set-up, firewall, remote access VPN, and site-to-site VPN.

"In the 'Device Setup' config panel, let's click the 'Interfaces' link. For now, we should ignore the 'Startup Wizard' shortcut for configuring the basic settings. It's a useful tool, but beginners should navigate through each option in the ASA first. Later, after they master it all, they can use the startup wizard. The 'Interfaces' menu is used to set up interface settings such as IP address, the name of the interface, MTU, security level, MAC address, and IPV6. In my opinion, this is the most critical place because the ASA interfaces are down by default. We need to enable it. Many engineers run into this problem when they have all configs in place, but then they notice that all the interfaces are down and need manual enabling."

"Like a train without any tracks," Hernyka added.

"Yes, except that the 5505 model or any switch plus ASA model firewall only has one screen for interface configuration. On the other hand, a switched port firewall has two additional tabs: 'Interfaces' and 'Switch Ports'. The ASA 5505 is a switched port firewall that is typically used in a small office when you can't afford a router, switch and a firewall. The ASA 5505 hardware provides a router, switch and firewall functionality in one box. This doesn't mean other hardware models don't support L2 mode. They do, but for the 5505, the ports are in switched virtual interface mode. This suggests that the hardware has a switch module integrated within the firewall.

"I have an ASA 5550 model. It is an L3 firewall, and you cannot see the configs for the switch ports. I'll edit on the interface GigabitEthernet1. In the 'General' tab, we can define the interface name, which is mandatory, and provide a security level number between 1 and 100. We'll talk about this later.

"If we need to dedicate the interface to management-only purposes, check the box 'Dedicate this interface to management only'. The equivalent command is '**management-only**', and should be applied inside the interface config mode. Make sure to enable the interface using the 'Enable Interface' checkbox".

"The CLI command to bring up the interface is '**no shutdown**'," Hernyka added.

"Yes. If you want to config a static or dynamic IP, use the options below. The next tab in the interface settings is called 'Advanced', where we can set MTU. It is an interesting option, and we can use it to specify our custom MAC address. This is particularly helpful during troubleshooting. It's also useful for when attackers try to footprint the network with scanning tools because it ensures that they cannot determine the kind of device by using its MAC address. The IPV6 tab, I'll leave to the scholars.

"In the left-hand panel below the 'Interface' link, we have the 'Routing' menu. Click on 'Static Routes'. Here, we can configure the static and default routes. The next option is 'Device

Name/Password', where we can set the device name of the ASA and the domain name. The domain name is used by the ASA to append domain name to hostname configured. A good example is if the configured syslog server's unqualified name is 'dog' and the domain name is 'cat.com'. The ASA will qualify the name as 'dog.cat.com'. The enabled password lets you access privileged EXEC mode after you log in. Also, this password is used to access ASDM as the default user, which is blank. The default user shows 'enable_15' in the User Accounts panel.

"The last setting in this 'Device Setup' panel is 'System Time' where we can set the time and clock, and NTP settings. Always make sure to authenticate NTP, otherwise it is vulnerable to attacks by hackers spoofing bogus time. If this happens and our clock is set wrong, our time-based ACL will not work properly. Then access logs and audit logs will become inaccurate. Therefore," Nielair said, a note of warning in his voice, "you should not take NTP lightly.

"The next panel is 'Device Management'. Expand the 'Licensing' menu and click the 'Activation key'. This is the place where we can apply for the license that we receive upon purchase. It also shows the serial number of the box, which is important when calling Cisco support for help. The 'Perpetual' is a lifetime one, a cumulative-based validity time for the license. This means that if you have subscribed to a 1-year URL filtering license, renew it after 11 months and apply for the license, the new validity will stay for another 13 months, carrying over the old validity balance. You may notice a path to this page on the 'Activation Key' page, just below the toolbar, specifically Configuration → Device Management → Licensing → Activation Key. This will help you understand which page is being surfed and navigated.

"Under the 'Licensing' link, the System Image/Configuration → Boot Image/Configuration has options for us to load the ASA software and choose the boot order sequence."

"Simple stuff!" Hernyka said. "Wouldn't this ASDM GUI be a lifesaver compared to Cisco's black and white CLI screen. That thing looks like a movie screen from the 1940s?"

"CLI is handy on many occasions. It's like a Swiss Army knife: a tool with an importance that you cannot underestimate even if your opponent is holding a powerful gun with perishable bullets. You don't need to remember the commands. I'll teach you a few tricks to combat the old-school CLI difficulties. In the menu bar at the very top, click Tools → Preferences, and in the 'Communications' section, check the option 'Preview commands before sending them to the device'. Every time you change a setting or configuration in GUI, when you apply the change, the ASA spits out a list of commands. These are the exact commands you need when you go through the same steps of configuration via CLI. When you are working in the lab, learn all the configurations through GUI one by one, document the CLI commands using the preview CLI option, and store the commands online and on your desktop. This is particularly useful to use for reference when you are consulting and helping customers in the field. Cisco also has good documentation and Google will be your best friend. But what good are these resources when you're in a room without an Internet connection and you have to config or fix the ASA? Your personal notes and CLI skill sets will be your saviors on such occasions."

"Great tip! Thank you!"

"The 'Users/AAA' section allows us to define administrator accounts. Just go to 'User Accounts', where you can see the 'enable_15' default account. Create an adminstrator account with root admin access to the box. I don't recommend using '**admin**' as an account name because it is too easy to guess. Instead, create something like '**cisco_asa_rootadmin**' and give privilege_15 access and check the box 'Full access' (ASDM, SSH, Telnet, and Console). Also, please remove the 'enable_15' account. There are other options in the list for basic settings. Go to 'AAA Access' and only allow HTTPS and SSH under 'Require authentication for the following types of connections'. For Christ's sake, don't choose Telnet, but serial is okay if you have OOB secured network access.

"Next in the 'Device Management' panel go to 'Certificate Management'. You'll get a warning page upon launching HTTPS GUI because of the self-signed certificate. In the 'Identify Certificates' menu, we can create a self-signed certificate, which is necessary because a new self-signed certificate is generated each time the ASA reboots. That isn't good even though we've added it to the exception list, since the certificate change in reboot means that we have to accept warning messages all the time. The best method is to have an internal PKI that is trusted by the browser and import it for the ASA device certificate.

"The last important task is to stage the box with basic settings in DNS. You can find it below the DHCP menu. It allows us to define the ASA so we can use a DNS server for name resolution, and other tweakable DNS settings."

He took a deep breath and smiled, "So, Hernyka, that's the quick and dirty on basic ASA firewall settings."

Juniper

"Should we explore Juniper firewalls next?" Nielair checked before advancing.

"I'm feeling confident," Hernyka nodded. "Learning about the management interface IP's, routes, NTP, DNS and commands to reboot or shutdown are all the basic elements."

"It seems you're already bored."

"No, no! It's exciting, but… With your level of experience, the basics of any new product are the same. You can configure base network parameters, remove the defaults, either allow, block or monitor what is happening, and turn a few knobs on to get some pretty flashing Christmas lights!" she joked.

"You're funny," Nielair said. "And what you said is gospel. To learn a Juniper SRX firewall like Check Point, we can get the free trial vSRX software at http://www.juniper.net/us/en/dm/free-vsrx-trial and run it in VMware, or we can use cloud Amazon AWS to test the Juniper SRX firewall at https://aws.amazon.com/marketplace/pp/B01LYWCGDX. Sometimes you will come across the term 'Firefly Perimeter downloads', which is considered a virtual security appliance that provides security and networking services at the perimeter or the edge in virtualized private or public cloud environments. Firefly Perimeter runs as a virtual machine on a standard x86 server.

"In fact, it doesn't matter if it's a vSRX virtual software or physical SRX firewalls. The configs will be the same. Only interfaces, zones, and some defaults will vary. To me, this is a disorganized firewall when it comes to basic settings. It varies from platform to platform and requires us to update changes whenever a new version is introduced. Its predecessor, the Netscreen firewall, was much easier to configure.

"The dedicated management port in SRX firewalls is called fxp0 and has a default IP of 192.168.1.1/24. Different hardware, though, has various default IPs. For instance, the SRX 1500 model has an fxp0 default IP of 192.168.1.1/24, ge-0/0/1 IP has 192.168.2.1/24, ge-0/0/2 IP has 192.168.3.1/24 and ge-0/0/3 has 192.168.4.1/24, and so on.

"By the way, 'ge' stands for GigaEthernet and 'fe' stands for FastEthernet. Here is a link that lists all of the conventional names for the SRX interfaces: https://www.juniper.net/techpubs/en_US/release-independent/junos/topics/reference/specifications/interfaces-srx-series-port-naming-conventions.html.

"You can find additional information under different topics on the left-hand panel."

"Why are there so many default IPs?" Hernyka asked, "Is it because Juniper SRX has many different management IPs?"

"Nope, they are all IPs for the interface. It has nothing to do with management IPs. The default management IP is 192.168.1.1/24. Here, I have a few SRX boxes… Just let me log in. They're all set in the factory default, so we can configure from scratch. The default username is 'root' and there's no need of a password. The first prompt we get is 'root@>', a Linux shell prompt. Do you know Linux?"

"Here and there." Hernyka said, shrugging, "I know commands like 'ls, pwd, mkdir, and cat.'"

"Not bad," Nielair said. "Like Palo Alto and Cisco, we also have operational mode and configuration mode, but we land in the Linux shell if we log in as root. In the shell prompt, we can create directories, files, kill processes, and do other useful Linux system administration commands. To go into operational mode, type '**cli**'. Then we are welcomed to the Junos OS CLI. This is different from the Cisco command line set. First of all, I strongly suggest you spend a few hours learning taking the 'Junos OS as a Second Language' course. You can access training modules from the Juniper website, which will teach you the fundamentals of Junos OS and about how their cash line interface works.

"I will make you comfortable enough with Junos OS CLI to navigate it and get familiar with the Junos OS SRX commands. There is a laundry list of interface types and different IP settings on various platforms. You can always refer to the startup guide for this information, but you'll get the best experience and gain the most knowledge from checking the factory defaults.

"Just like Cisco's '**show ip interface brief**', the Junos OS command is '**show interfaces terse**', which will show all the available interfaces, their status, and the configured IPs. Some SRX have fxp2 as the management interface, so you should look for anything that begins with fxp."

"So the '**show**' command also works in Junos OS, right?" Hernyka said.

"Yes, '**show configuration**' displays the SRX's configuration. You may also notice that it is in a hierarchical format. I will demonstrate this with a quick example. Configuring Junos OS is similar to how we configure Cisco and Palo Alto. Go to the configuration mode using the command '**configure**'. Now we can name our firewall '**set system host-name PradeepSindhu**'. The '**set**' command allows us to configure settings in Junos OS. The changes don't take effect until we commit to the change with the '**commit**' command."

Hernyka made a surprised cluck. "What? You mean to say that committing changes isn't a proprietary command in Palo Alto? Did that Nir Zuk guy steal the commands from Juniper to found Palo Alto?!"

Nielair gasped, her suggestion was the final piece of a long-unfinished puzzle. "Hernyka, I think so! It would explain why they decided to sue him!"

"Dumbass!" Hernyka shook her head. "Had it been me, instead of a commit command, I would have made something like…" She looked up, trying to pull a word from the clouds. "'Consecrate'. That would be my commit version command."

"People generally aren't good spellers. Perhaps that's why he used the same command term as Juniper. Whatever the reason, after commit, do a '**run show configuration**', and you can see the hostname settings at the very top. By the way, we can't run operational mode commands in configuration mode, so we use the keyword 'run'. The equivalent command in Cisco is 'do'.

"Let's do a recap of the '**set system host-name PradeepSindhu**' command. 'set' is the keyword to use to tell Junos OS that we are about to configure something, 'system' is what we call the section, and inside the 'system' section, 'host-name' is the portion we want to use to edit or add config to. The alternate way of doing it is from the configuration mode. Just make sure we're at the top of the hierarchy. We can verify that by using the [edit] prompt, with the commands, '**edit system**' and '**set host-name PradeepSindhu**'.

"Notice that once you type the command '**edit system**', the tree structure changes to the [edit system] prompt. As you navigate the tree structure, it will include more paths. It is similar to the directory path of files and folders. To go up one directory, or level, or section—whatever you would like to call it—just type '**up**'. To go to the highest part of the root directory (or the [edit] prompt), use the command '**top**'. I am running the '**show configuration**' command and only grabbing the first piece of the 'system' section, and I will make the sub-sections in bold."

```
system {
  host-name PradeepSindhu;
}
  services {
    ssh;
    web-management {
      http {
        interface fxp0.0;
      }
    }
  }
  syslog {
    user * {
      any emergency;
    }
    file messages {
      any any;
      authorization info;
    }
    file interactive-commands {
      interactive-commands any;
    }
  }
  license {
    autoupdate {
      url https://ae1.juniper.net/junos/key_retrieval;
    }
  }
}
```

"The 'system' in the main section contains all the system level configurations, such as who can access SSH, HTTPS, syslogs, licensing, radius server, and NTP. In the default factory 'system' section, we have three sub-sections including services, syslog, and license. You can see the full output of the '**show configuration**' that most of the main sections are indented on the left and that the sub-sections are indented inside the main section. All the settings are tucked inside the sub-section. Something to keep in mind is that if you want to navigate to a section, you can use the 'edit' command with the section name. If you want to set some values, use the ‘set’ command inside a section that either be in the main section or sub-section. Now, I want to test your understanding of how you would navigate through the ‘syslog’ sub-section and set all the values.”

Hernyka shrugged, smug and knowing. “Easy, Nielair. At the top of the tree hierarchy structure, it should be [edit], then I should type the command ‘**edit system**’, and inside the ‘system’ section, if I type a question mark, I can see the commands related to the main section ‘system’. If I want to dive further into a sub-section such as in our example, I should type, ‘**edit ?**’ This will list all the sub-sections inside the main section ‘system’. For syslog, I need to type ‘**edit syslog**’, which will take me into the syslog sub-section, and we can confirm by the prompt [edit system syslog].”

She clicked on the question mark inside the syslog sub-section and said, “I believe there are three different settings we can use inside the syslog sub-section, including user, file messages, and file interactive commands. To execute the ‘user’ settings, we should use a ‘set’ command such as ‘**set user * any emergency**’. For ‘file messages’ setting, it is ‘**set file messages any any**’ and ‘**set file messages authorization info**’. And for the last one, which is ‘file interactive-commands’, the ‘set’ command is ‘**set file interactive-commands any**’. That’s it.”

Nielair pushed back in his seat. “I’m impressed! You learned Junos OS in no time. How did you do it?”

“Nothing major,” Hernyka said. “I used the question mark and TAB keys to figure out the process flow. But I still have a question. What are the commands inside a section and what are they used for?”

“They’re operation commands and properties. Inside [edit system], type, ‘**show**’, and it will display all the sub-sections inside it. Another useful command is ‘**status**’. It will display all the users who are editing that particular section. You will discover other commands as we explore further.”

Hernyka gave him a thumbs-up. “One problem, though. Why are you naming the firewall name after the founder of the company, Pradeep Sindhu. I want something different. Let’s call it ‘CharlieChaplin’.” Each keystroke deliberate, Hernyka typed ‘**set system host-name CharlieChaplin**’.

“Why not?” Nielair said. “Charlie Chaplin is a heck of a lot more famous than Juniper. I’m glad you have grasped the Junos OS CLI. Now that we’ve managed to get to the hostname set, we can config some basic settings by using:

set system time-zone Amercia/New_York

set system domain-name hello.CharlieChaplin.com

set system name-server 8.8.8.8

“Above the three basic settings we added including hostname, time-zone, domain-name and name server, the first thing we need to add is the password for the ‘root’ username. Use the command ‘**set system root-authentication plain-text-password**’. And for security purposes, we should add another 'admin' account for all the administrators to use by using the command '**set system login user juniper_firewall_admin class super-user authentication plain-text-password**' where 'juniper_firewall_admin' is the admin username."

"That username is dull," Hernyka stuck out her tongue. "Let's delete 'juniper_firewall_admin' and add an account named 'marilynmonroe', which hackers won't be able to guess."

He chuckled. "Then use the delete command. You're one crazy girl, you know? Let's see if you have the skills to match."

"I can fix this." She keyed a '**show configuration**', creating a flow of sections and sub-sections, and typing the two commands used to delete and create accounts '**delete system login user juniper_firewall_admin**' and '**set system login user marilynmonroe class super-user authentication plain-text-password**'. Finally, she committed the change.

"Brilliant! You're a Juniper rockstar, Hernyka. I have one last question, though. How many sub-sections does the security main section have?"

"We've got screens, policies, and zones," she answered.

"Well, then we're finished and you've mastered Junos OS. Watch the free training video to gain some more knowledge, and you're good to go as a Juniper consultant. The next crucial step is the IP address for the management interface. For that, run this command '**set interfaces fxp0 unit 0 family inet address 6.6.6.6/26**'. You must be familiar with most of the syntax, except the 'unit 0'. In Juniper, the primary IP address is designated as 'unit 0'. If you add a secondary IP address to the 'fxp0' interface, it would become 'unit 1', and so on.

"We can connect our laptop to the same subnet as the management IP of Juniper firewall. Or, if it's VMware, we could have a bridged mode. But if we want to access the network, we need to have a static route. This command will get us connected remotely: '**set routing-options static route 0.0.0.0/0 next-hop 6.6.6.1**'. Do a quick '**show configuration**' under the 'service' section, and you will notice that the allowed default management protocols are HTTP and SSH. Let's launch a browser and connect to http://6.6.6.6 where we will get connected to Juniper Web Device Manager. This is just lab testing, so don't worry. I know HTTP is insecure. It's like allowing crooks to peep inside your safe. To avoid it, we should enable HTTPS. Like in Cisco, we need to enable the service via the command '**set system services web-management https system-generated-certificate**' and then assign HTTPS service to fxp0 interface by using the command '**set system services web-management https interface fxp0**' and commit the change. Now we can connect via HTTPS.

"The Juniper Web Device Manager layout is simple to navigate. When we logged in, we landed on the 'Configure' tab. There are other tabs such as Dashboard, Monitor, Maintain, Troubleshoot, and Commit. As you know, when we do any change, we need to commit it. That isn't necessary here for some setup configs. Example, in the 'Commit' tab in the top right-hand corner, click the drop-down, select 'Preferences', and then click the 'Startup page upon login' tab. Then we can select which page we need to go to when we log in. This change doesn't require any commit function. All we have to do is log out and re-login. The reason I mentioned this little trick is because you have to go through all the windows and pages in the GUI to get familiar with the product. Once you have mastered it, you gain confidence about the firewall and its components. Make sure you do! Don't be like other lazy and unenthusiastic technicians."

"Definitely not!" Hernyka said.

"So far, we have configured and changed the root password, hostname, domain name, time zone, DNS servers, admin account, and HTTPS settings. The same CLI operations can be accomplished via GUI in the 'Configuration' tab. For that, go to System → Properties → System Identity, where we can configure hostname, domain name, root password, DNS servers, and domain search."

"I have a quick question," Hernyka said. "I'm fascinated by the Junos OS CLI interface, but does it have a preview option like Cisco? So we can get to know the commands using GUI?"

"Of course. An easy way to demonstrate it is to add some DNS servers to the 'System Identity' page and go to 'Commit'. The first option, 'Commit', saves and pushes the changes. The second one is 'Compare', where we can grab the CLI equivalent commands. It won't be a single line command, it will be in hierarchal tree format instead. Use the set or delete command to follow the path.

"In System → Properties → Management Access, click the 'Edit' button. We can configure the interface that will enable management protocols such as Telnet, SSH, and HTTPS. For HTTPS, we can generate certs in the last tab, 'Certificates'. The next link is 'User Management', where we can add users and configure RADIUS and TACACS+ settings. The last link in the system properties management access drop-down is 'Date Time', where we can specify the time and time zone manually, or add NTP servers. I have a helpful tip on how the Linux shell helps in Junos OS troubleshooting. Either type the command '**show system processes extensive | match http**' in operational mode or just add a 'run' before the 'show' in configuration mode. We will get the HTTP daemon with PID, which is the number in the first column. To go the Linux shell, either from the operational mode or configuration mode, just type '**exit**'. Finally, you will enter the Linux shell 'root@>', or from the operational mode, type, '**start shell user root**' to be in the Linux shell. The second way is similar to use the '**sudo**' command. Once you are in the Linux shell, type, '**kill -9 6000**'. '6000' is a process ID that you can grab from the '**show system processes extensive | match http**' command. To reboot a Juniper firewall, use the command '**request system reboot**'.

"And that's it. We just got the four best firewalls up and running in basic configuration." Nielair nodded, satisfied. Yet his mind returned to earlier conversation and he spoke before he could resist. "By the way, you said you hate kings. But tell me; is there one king in history who you admire?"

"Buddha," she answered with conviction. "He discarded his royal attire and became an ordinary man. He lived his life seeking utmost divinity and peace. All men and women who bask in power should leave their undeserved glory and live like regular humans."

"Well said, dear. That is the most basic setting and configuration for humans. Leave your power, glory, ego and selfishness behind."

"Amen to that!" Hernyka clasped her hands in agreement.