SerNet

NGFW - Next Generation Firewalls

Oct. 22nd 2018 – ICANN63

Johannes Loxen

SerNet GmbH

about

since 1996	
Open Source Software:	Linux, SAMBA, verinice.
Information Security:	GDPR, ISO 27001
IT Security:	Firewalls, VPN
Interoperability:	Linux, Mac, Windows

verinice.

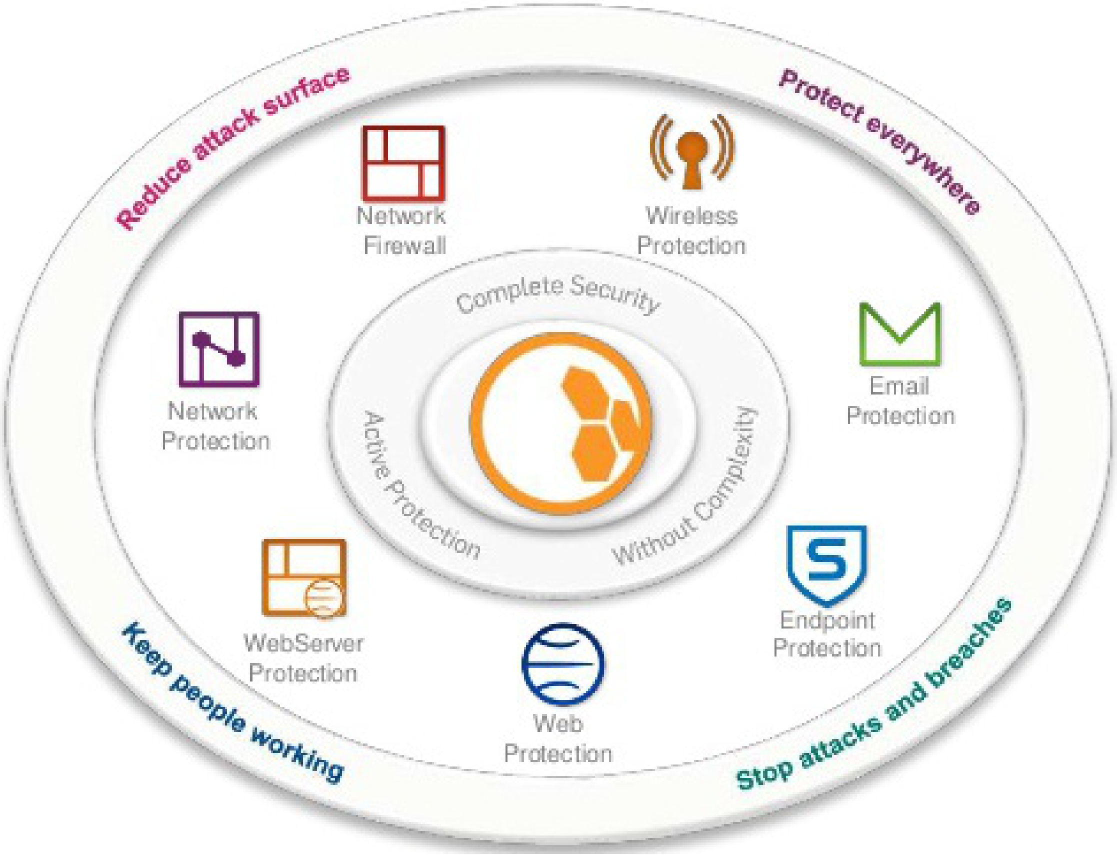
SAMBA+

firewalls

- packet filter firewalls: IP:Port
  - almost gone: 21, 23, 25, 80, 110, 143
  - still alive: 53, 123, **443**, 465, 587
- Proxy: rule based, pattern based, subscription based
  - user, time, AV pattern, block lists, heuristics
  - lots of snake oil AV or questionable helping block lists
- reverse Proxies: WAF against injection, XSS, ...
- Open Source firewalls: no secrets!

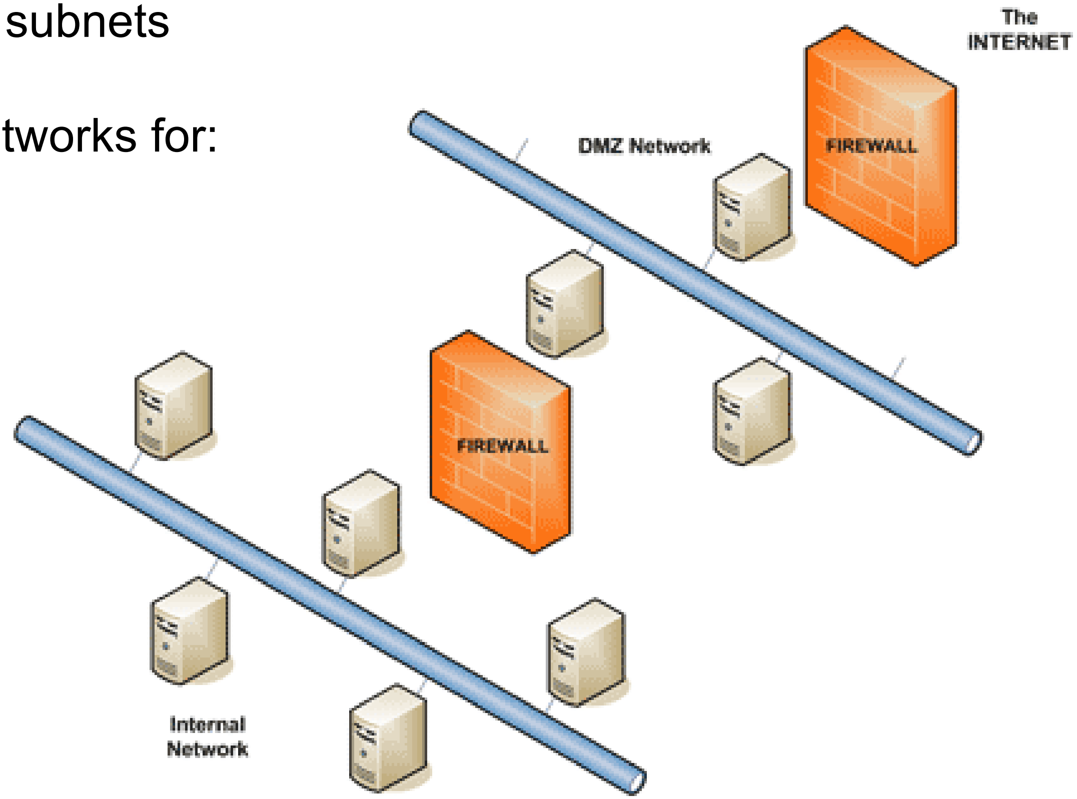
UTM: Unified Threat Management is a threat

- UTM firewall: everything build on top of on one OS kernel:
- firewall
- ALG &Proxy
- Mail
- Anti Virus
- VPN
- Web
- Wifi
- IDS & IPS



compliant firewall setup

- different machines, different OS, complex architecture
- external Firewall: border control
- internal Firewall: screened subnets
- a bunch of DMZ or LAN networks for:
  - VPN (client access)
  - VPN (site2site)
  - Proxies
  - Mailer
  - Webserver
  - Datebase



challenges

- internet of platforms
- more and more services via port 443
- the Browser is the new OS (DoH)
- zero days
- DDoS
- phishing and other social engineering

Next Gen Firewalls: UTM reloaded

paloalto
NETWORKS

FORTINET®

SOPHOS

JUNIPer®
NETWORKS

Check Point®
SOFTWARE TECHNOLOGIES LTD.

CISCO

problems with current NGFW

- UTM: everything on one kernel connecting internet and LAN
  - full awareness: packet – application – session – identities
- GDPR issues
  - identity management: corporate compliance based on Active Directory
  - SSL decryption
- closed source OS and applications
  - no public bug tracking
  - Fortinet, Juniper, Sophos, Cisco:
    CVE score 10 entry every year, each of them
- no open source solutions in sight :-(

what to do

- build firewall sandwiches, multi tiered
- protect and observe your NGFW
- utilize your ISMS, reflect and implement controls and measures
- know your information security and data protection officers
- carefully evaluate cloud services for firewalls (better don’t use them)

- collaborate on open source solutions!

Dr. Johannes Loxen, jl@sernet.de

SerNet GmbH
Bahnhofsallee
37081 Goettingen

tel +49 551 370000-0
fax +49 551 370000-9

https://www.sernet.de

references: https://danielmiessler.com, SOPHOS, misc vendors