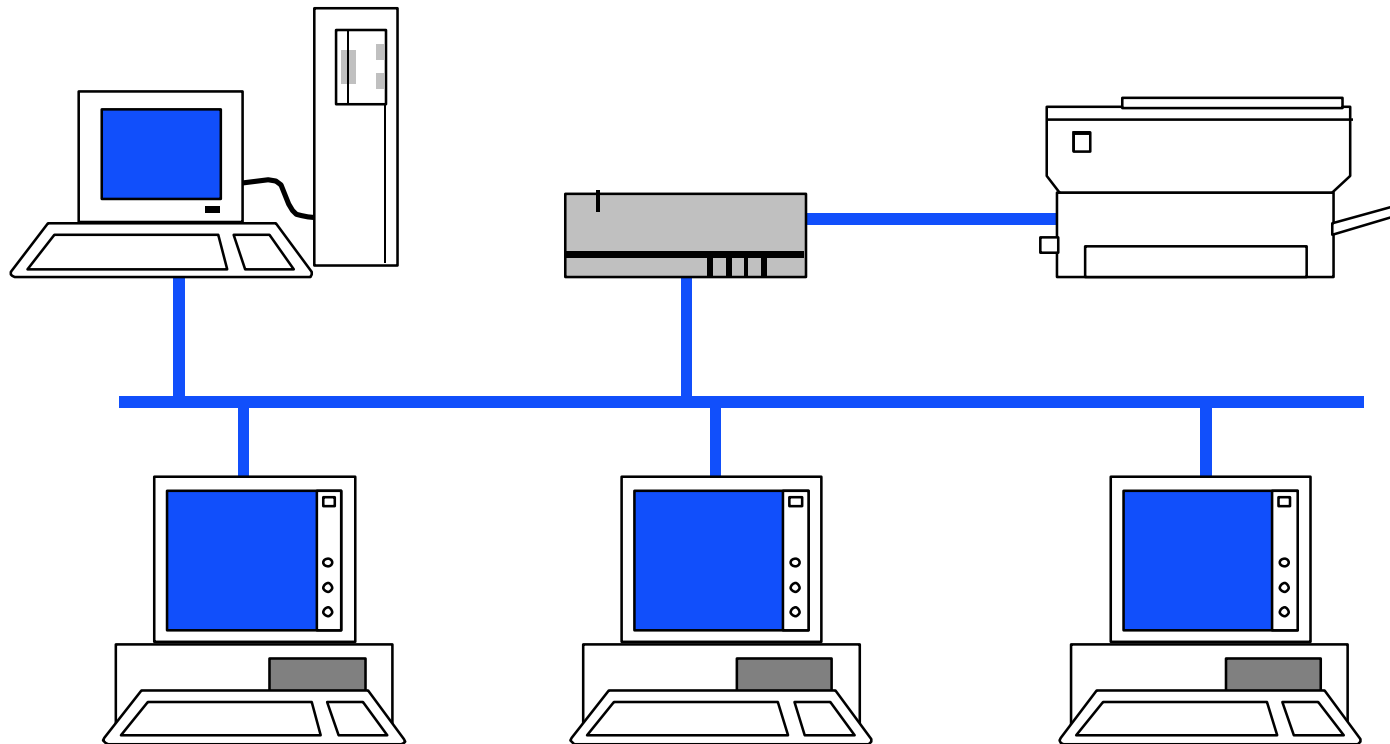


# Phion Netfence Firewall

Mag. Dr. Klaus Coufal



# Übersicht

- I. Konzepte
- II. Installation und Konfiguration
- III. High Availability
- IV. Firewall
- V. VPN Server
- VI. Management Center
- VII. Addons

# I. Konzepte

1. Grundlagen
2. Phion Notation
3. „Software Appliance“
4. Box – Server – Service
5. Layer Concept
6. Boxfirewall – Forwarding Firewall

# 1. Grundlagen

- Österreichische Entwicklung
- Firmensitz: Innsbruck
- <http://www.phion.com>
- Netfence Firewalls beruhen auf einem speziellen RedHat-Derivat als OS.

## 2. Phion Notation

- Phion benutzt ein sogenannte „Write as you speak“-Notation.
- Konträr zu CIDR-Notation
- Beispiele:

CIDR	Phion	CIDR	Phion
/24	/8	/0	/32
/30	/2	/32	/0

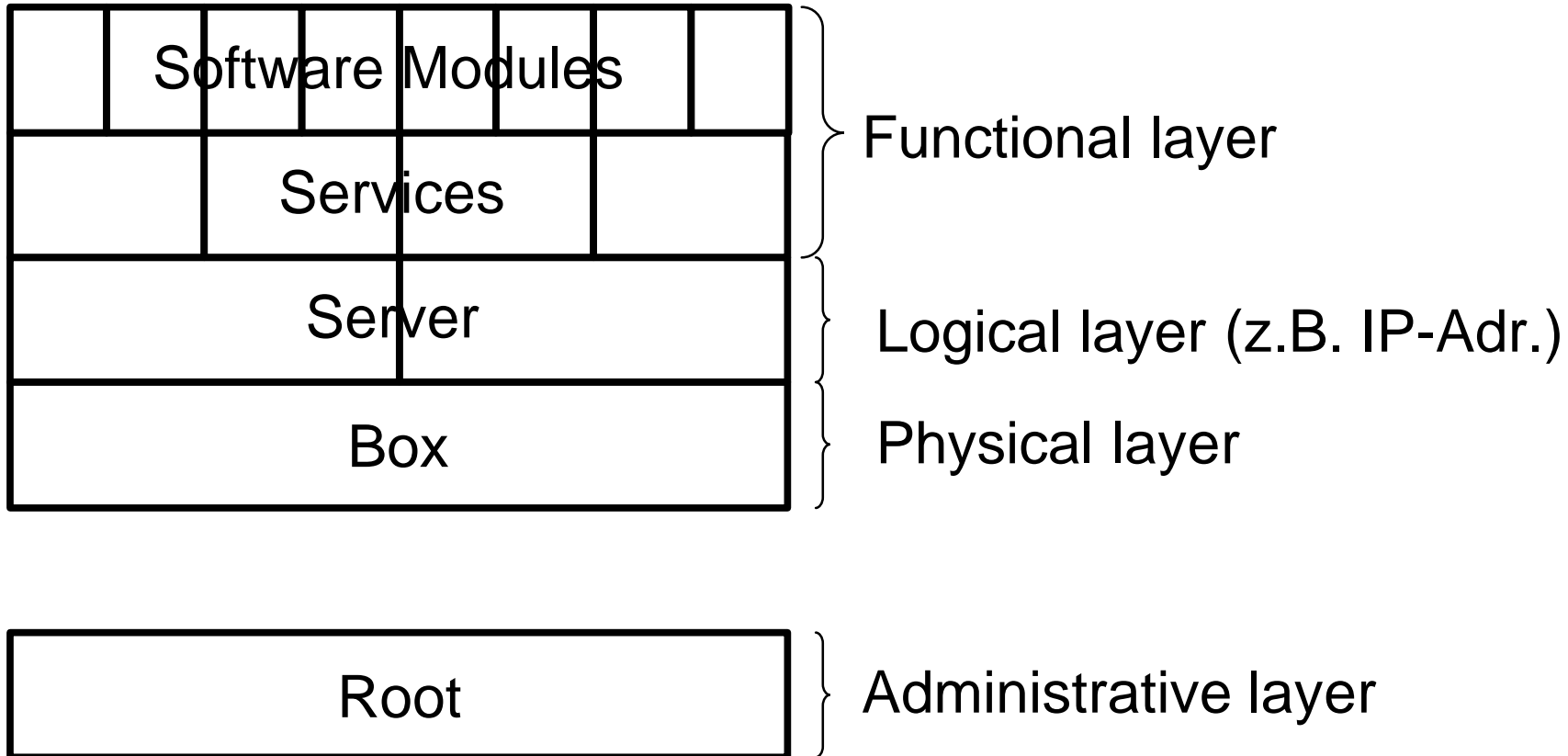
# 3. „Software Appliance“

- Die NetfenceFW versucht durch die möglichst intensive Integration des OS in die Gesamtsystematik die Vorteile einer „Appliance“ und einer Software-Lösung zu vereinen
- Ein Industriestandard-PC wird durch die Netfence-SW zur „Appliance“

# Vorteile

- Von Appliance
  - Kompakt
  - Einfache Einsetzbarkeit
  - Keine eigenen OS-Kosten
  - Keine Kompatibilitätsprobleme mit OS
- Von Software basierenden Lösungen
  - Flexibilität (Software)
  - Skalierbarkeit (Software)
  - Keine Hardwarebeschränkung

# 4. Box – Server – Service



# 5. Layer Concept

- Administrative layer
  - Root Administrator bzw. weitere Admins
- Physical layer
  - Physische Maschine inkl. Notwendiger Services (z.B.: controld, boxfw, boxconfigd, ...)
- Logical layer
  - Server inkl. Definition der IP-Adressen
- Functional layer
  - Eigentliche Funktionen (Forward-FW, ...)

# 6. BoxFW – Forwarding FW

- Wie schon vorher erkennbar gibt es zwei FW-Typen, die Box-FW (pro Box genau eine) und die Forwarding-FW (max. eine pro Box)
- Box-FW: für die Zugriffe auf die Box
- Forward-FW: eigentliche Firewall

## II. Installation und Konfiguration

- phioni (Win32) erstellt „kickstart-File“ (enthält Hardwarebeschreibung und Management-IP-Adresse)
- Phion Kickstart ist verschieden von RedHat-Kickstart
- Bootfähige InstallationsCD und „kickstart-File“ zum Installieren der Box
- phiona (Win32) Administrations-GUI

# Device Routen

- Auf der Box werden i.A. nur Device-Routen den NICs zugeordnet bzw. Gatewayrouten festgelegt.
- Erst die Server haben die IP-Adressen und machen aus den „Pending Device Routen“ echte Routen

# Sonstige Netzwerkkonfiguration

- Redundant Routes („route preference“)
- Ethernet Trunks
  - Bundle
  - Fallback
- VLANs
  - Nur auf wenigen NICs
  - <nic>.<vlanid> (z.B.: eth0.1)
- Dynamische Netzwerke (ADSL, Kabel, ISDN)

# III. High Availability

- Heartbeat-Lösung (active, passive)
- DHA(Dedicated) – mcHA
- Primary und Secondary Box
- Einfache Installation
- 10 s Intervall zum Abgleich
- Automatische Übernahme
- HA auf Serverebene (!)

# IV. Firewall

- ACPF (Application Controlled Packet Forwarding)
- TAP (Transparent Application Proxying)
  - TCP only
- Source           Quelle des IP-Requests
- Destination     Ursprüngliches Ziel
- Bind             Quelle nach FFW
- Connection     Ziel nach FFW

# Firewall Regeln

- Action Type
- Connection Type
- Net Objects
- Service Objects
- ...

# Action Types

- Beschreibt Connection als Funktion von Destination
- Block                    Paket wird verworfen
- Deny                    Paket wird verworfen aber Sender inf.
- Pass                    Paket wird durchgelassen
- Redirect                Paket wird nach Änderung durchgel.
  - Redirect Object
  - Local Redirect
- Map                    Extended NAT
- Execute                Paket wird einer Appl. übergeben
- Cascade                Weiteres Ruleset
  - Cascade Back

# Connection Type

- Beschreibt Bind als Funktion von Source
- Client            Bind IP = Source IP
- Proxy            Bind IP = NAT (Source s.u.)
  - Proxydyn
  - Proxyfirst
  - Proxysecond
  - Proxy ADSL (DHCP, ISDN)
- Explicit        Source NAT

# Net Objects

- Objekte zur besseren Lesbarkeit der Regeln
- Auch Hosts werden hier eingetragen
- z. B.:

ZentraleLAN      10.0.0.0/12

Miraculix          192.189.51.100

# Service Objects

- Services zur besseren Lesbarkeit der Regeln (Ports)
- Zusatzparameter (Timeout)
- z. B.:

BoxVPN	TCP	692
--------	-----	-----

DNS	UDP	53
-----	-----	----

FTP	TCP	21 (Plugin FTP)
-----	-----	-----------------

# V. VPN Server

- Client VPN und Site-to-Site VPN
- VPN-Server kann CA sein
- Unterstützte Verschlüsselungsalg.:
  - AES, AES256 (sicher), DES, 3DES, Blowfish (schnell), CAST
- Unterstützte Transport Methoden:
  - TCP, UDP, Hybrid, ESP (nur Site-to-Site)

# VI. Management Center

- Installiert wird eine StandardBox aber mit der MC-Option
- Auf der Box wird ein Server und die Managementservices eingerichtet (rangeconf, mastervpn, mevent, ...)
- Boxen werden im MC definiert und verwaltet
- Ports 800-820 werden benutzt

# Remote Management

- Port 692
- Boxtunnel vom MC zu den Remote Boxen
- Auf diesen müssen auf der Box eventuell die IP-Adressen ergänzt werden, damit der Boxtunnel auch ohne Server funktioniert.

# VII. Addons

- Policy Routing
- DNS
- Mail Gateway
- Proxy (Squid)
- 3rd Party
  - z.B: Trendmicro SPAM-Filter, Virenschutz, URL-Filter