A Honeynet Policy

06.05.2013, Garching

1 Honeynet-Architecture

The network architecture of our honeynet looks as follows:
2 Firewall Configuration

The firewall is equipped with four network interfaces:
1. **mgt**: management interface to administer the firewall
2. **ext**: external interface to the LRZ
3. **int**: internal interface to the switch with mirror port
4. **log**: logging interface to the logging server

Only the **mgt** interface has an IP address assigned, the **ext**, **int**, and **log** interfaces are bridged (i.e., it works on layer 2).

The praktikum and the management network both share the same subnet 131.159.50.0/24 and are logically separated by the I20 firewall. The honeypots themselves will be assigned IP addresses from the subnet 131.159.74.80/28.

3 Policy

During our last session, we agreed on the following policy.

**Management interface**
- **→ mgt**: Access allowed only from specified hosts
- **→ mgt**: SSH connections must always be allowed
- **mgt →**: Block all outgoing traffic, except for: DNS, NTP, SMTP

**Logging interface**
- **log → ext**: Block all traffic, except for: DNS, NTP
- **int → log**: Allow specified protocols & ports, block the rest

**Internal interface**
- **ext → int**: implement watchlist/blacklist
- **ext → int**: allow all with honeynet IPs as destination
- **ext → int**: bandwith limits: 10 MBit/s
- **int → ext**: allow all TCP/UDP/ICMP, except: SMTP, spoofed sender IPs
- **int → ext**: block known attacks with IPS
- **int → ext**: implement watchlist/blacklist
- **int → ext**: bandwith limits: 10 MBit/s
- **int → ext**: connection limits per protocol: 50 burst, rate 1/sec