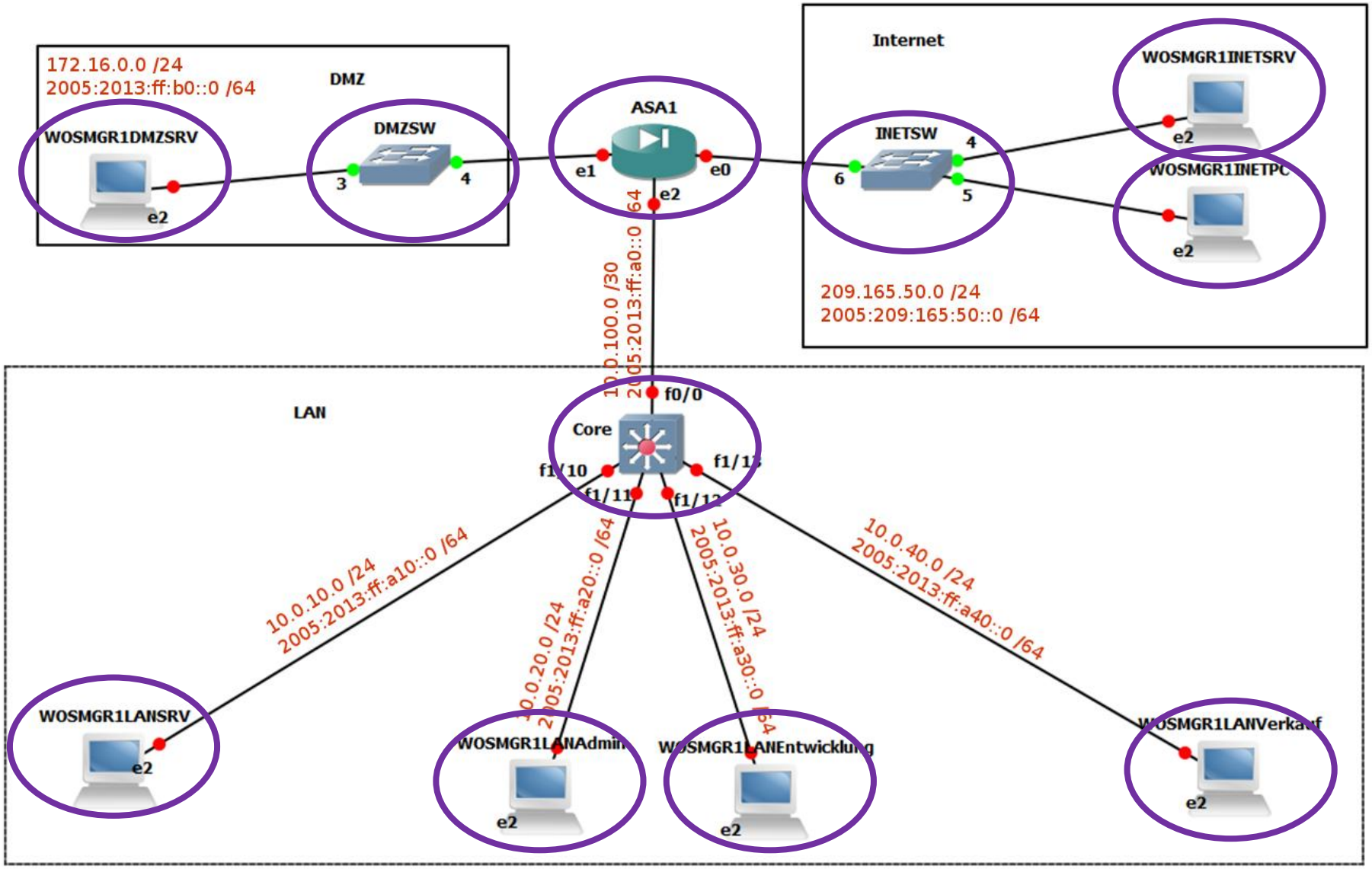
wosm

Phase 1

Tobias Lerch, Yanick Eberle,
Pascal Schwarz

Inhaltsverzeichnis


172.16.0.0 /24
2005:2013:ff:b0::0 /64
DMZ
WOSMGR1DMZSRV
e2
DMZSW
3
4
ASA1
e1
e0
e2
10.0.100.0 /30
2005:2013:ff:a0::0 /64
Internet
INETSW
6
4
5
WOSMGR1INETSRV
e2
WOSMGR1INETPC
e2
209.165.50.0 /24
2005:209:165:50::0 /64
LAN
f0/0
Core
f1/10
f1/11
f1/12
10.0.10.0 /24
2005:2013:ff:a10::0 /64
10.0.20.0 /24
2005:2013:ff:a20::0 /64
10.0.30.0 /24
2005:2013:ff:a30::0 /64
10.0.40.0 /24
2005:2013:ff:a40::0 /64
WOSMGR1LANSRV
e2
WOSMGR1LANAdmin
e2
WOSMGR1LANEntwicklung
e2
WOSMGR1LANVerkauf
e2

Adressvergabe an Clients

- IPv4
  - DHCP
  - `ip helper-address`
- IPv6
  - Autokonfiguration
  - Router Advertisement
  - DNS Server über zustandsloses DHCPv6
  - `ipv6 nd other-config-flag`
  - `ipv6 dhcp relay destination`

Bedrohungsmodell - Attacken

- ICMP ‘smurf attack’: Denial of Service
- Viren / Würmer / Trojaner
- TCP DoS (SYN-Flooding)
- DNS Cache poisoning
- Phishing
- Rogue DHCP
- MAC flooding
- ARP spoofing

Bedrohungsmodell - Priorisierung

Rang	Wahrscheinlichkeit	Schweregrad	Bedrohung	Schutz umgesetzt
1	hoch	hoch	ICMP 'smurf attack': Denial of Service	ja
2	hoch	mittel	Viren / Würmer / Trojaner	nein
3	mittel	hoch	TCP DoS (SYN-Flooding)	ja
4	mittel	hoch	DNS Cache poisoning	nein
5	hoch	niedrig	Phishing	nein
6	niedrig	hoch	Rogue DHCP	ja
7	niedrig	mittel	IP spoofing	ja
8	niedrig	mittel	MAC flooding	nein
9	niedrig	mittel	ARP spoofing	nein

Bedrohungsmodell - Defense

- ICMP ‘smurf attack’: Denial of Service
  - ACL: ICMP Pakete blockieren
- IP spoofing
  - Verify reverse-path
- TCP DoS (SYN-Flooding)
  - SYN Cookies
  - connection conn-max
  - connection timeout
- Rogue DHCP
  - ACL: Port 68 für DHCP Antworten blockieren

Demo