

## 15-Minutes Guide to Firewalls



V0.031

---

---

---

---

---

---

---

---

## Trainer

- Matthew Cook
- Senior IT Security Specialist (Loughborough University)
- UKERNA Contracted Trainer
- Further details available at: <http://escarpment.net/>



V0.031

---

---

---

---

---

---

---

---

## Course Materials



V0.031

---

---

---

---

---

---

---

---

## Default Allow and Default Deny

- Two types of firewall policy
  - Default Allow
  - Default Deny
- Initially blocking a few malicious attacks
- Migrating to Default Deny
- Explicit Allow or Deny

```
trainingrouter> sh access-list 101
```

```
access-list 101 deny tcp any any log
access-list 101 deny udp any any log
access-list 101 deny ip any any log
```

VO.031

---

---

---

---

---

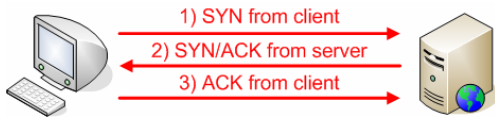
---

---

---

## Stateless and Stateful

- Initially stateless
- Stateful firewalls – connection tracking
  - IP Address
  - Port
  - Direction of flow
  - Sequence Numbers



VO.031

---

---

---

---

---

---

---

---

## Level of Inspection

- Deep Packet Inspection (DPI) or Layer 7
- Examines Payload (IDS/IPS like functions)
- Packet: dropped, tagged, rate limit or logged
- Overhead, performance and ASICs
- Mitigation early in packet life cycle
- Wirespeed issues



VO.031

---

---

---

---

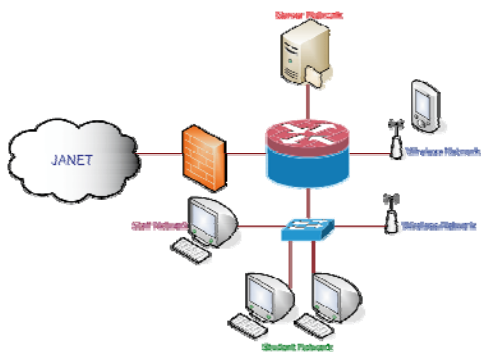
---

---

---

---

### Isolating different classes of user



VO.031

---

---

---

---

---

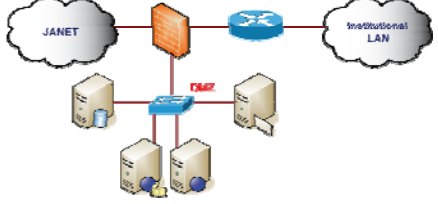
---

---

---

### DMZ

- Demilitarized Zone
- Third interface
- Network which hosts servers
- NAT/PAT protection typically Static NAT



VO.031

---

---

---

---

---

---

---

---

### Failover



VO.031

---

---

---

---

---

---

---

---

## Rules

- Corner stone of firewalls
  - Sequence
  - Line number
  - Matching in strict order
- Performance
  - Group rules
- IP Addresses instead of DNS
- Be specific
- Block everything, then allow one by one

VO.031

---

---

---

---

---

---

---

---

## Criteria for product selection

- How many interfaces?
- What mode of operation?
- What is the wire speed throughput?
- What firewall functions are included?
- Load balancing and fault tolerance?
- Virtual Firewalls
- ...and don't forget
  - Optional upgrades
  - Feature upgrades

VO.031

---

---

---

---

---

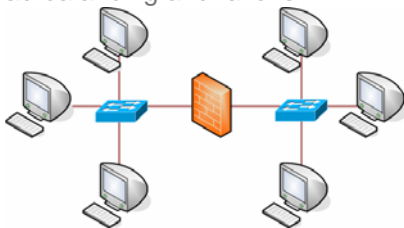
---

---

---

## Development and Testing

- Testing Configuration
- Testing under load
- Firewall functionality
- Load balancing and failover



VO.031

---

---

---

---

---

---

---

---

## Cleaner Feed

- Increasing network traffic and threats
- Struggling existing firewalls
- Cleaner feed technology
  - Removes DoS attacks, Port Scans, restrict ICMP and use DPI to mitigate threats.



V0.031

---

---

---

---

---

---

---

---

## Integration with IDS and IPS

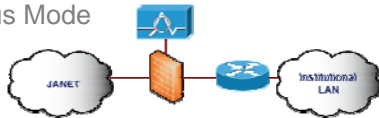
External IDS/IPS



Inline Mode



Promiscuous Mode



V0.031

---

---

---

---

---

---

---

---

## UKERNA Training

- Portfolio of network based training
- Over 10 different courses
- Training venues in many locations
- Comprehensive course workbook + CD
  
- Firewalls: Planning and Implementation
  - April 26<sup>th</sup> Cambridge
  - December 4<sup>th</sup> Glasgow

V0.031

---

---

---

---

---

---

---

---



## 15-Minutes Guide to Firewalls

### Questions

<http://www.janet.ac.uk/services/training/>

V0.031

---

---

---

---

---

---

---

---