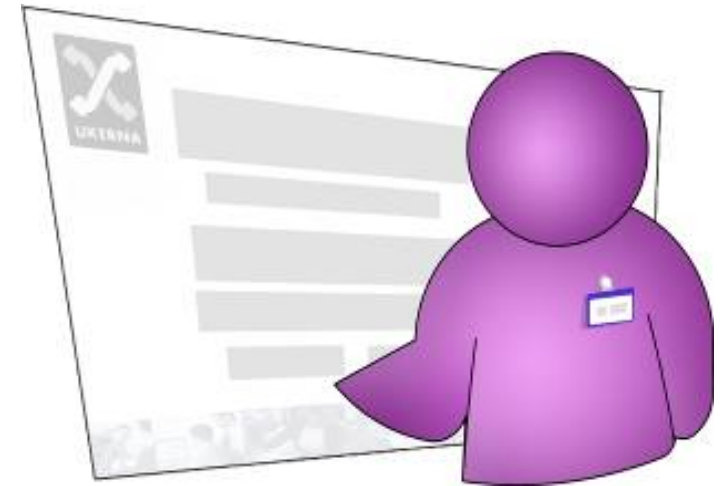


15-Minutes Guide to Firewalls

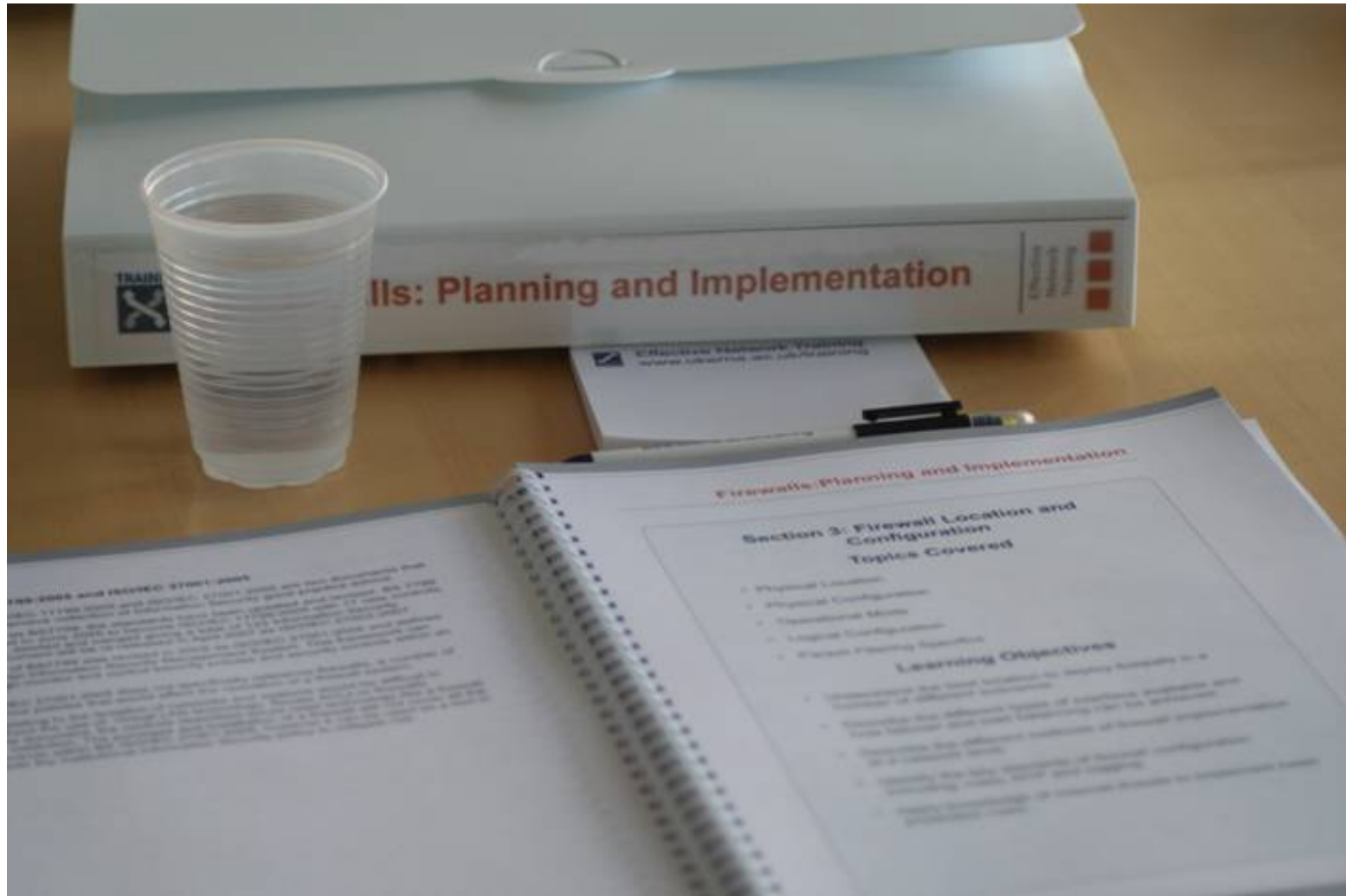


Trainer

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



Course Materials



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
```

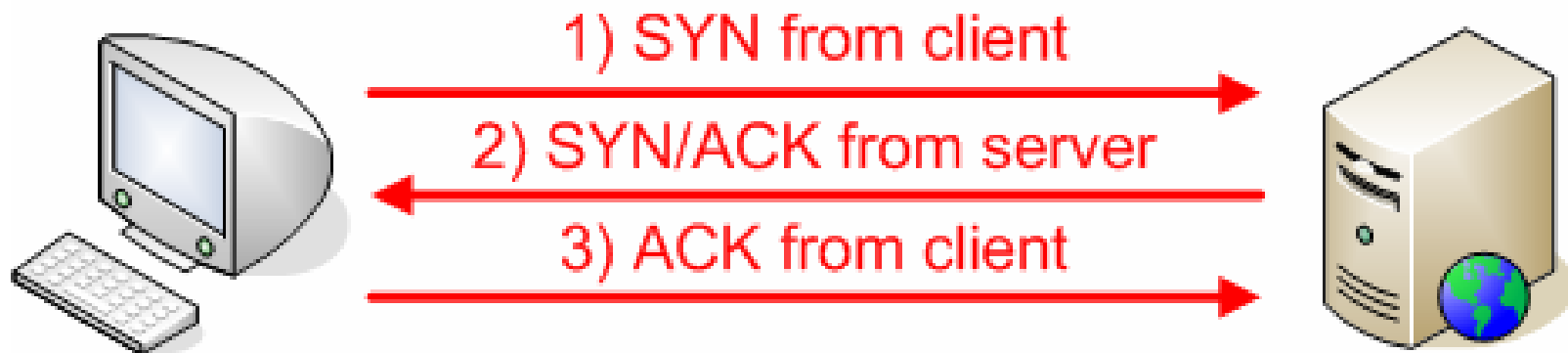
```
access-list 101 deny tcp any any log
```

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

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

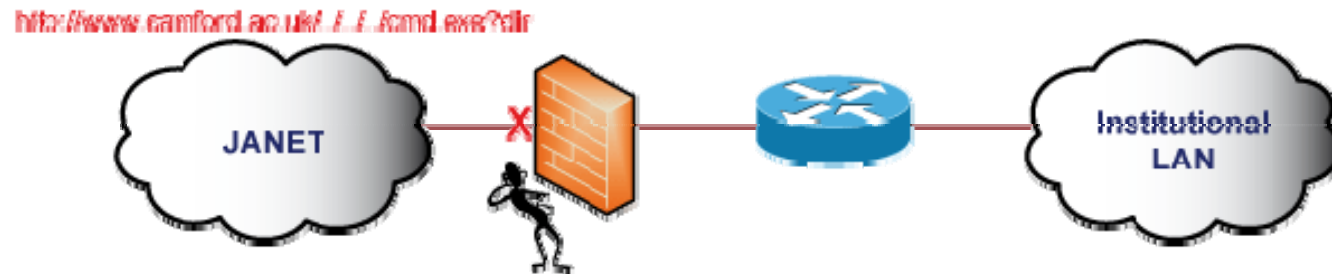
Stateless and Stateful

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

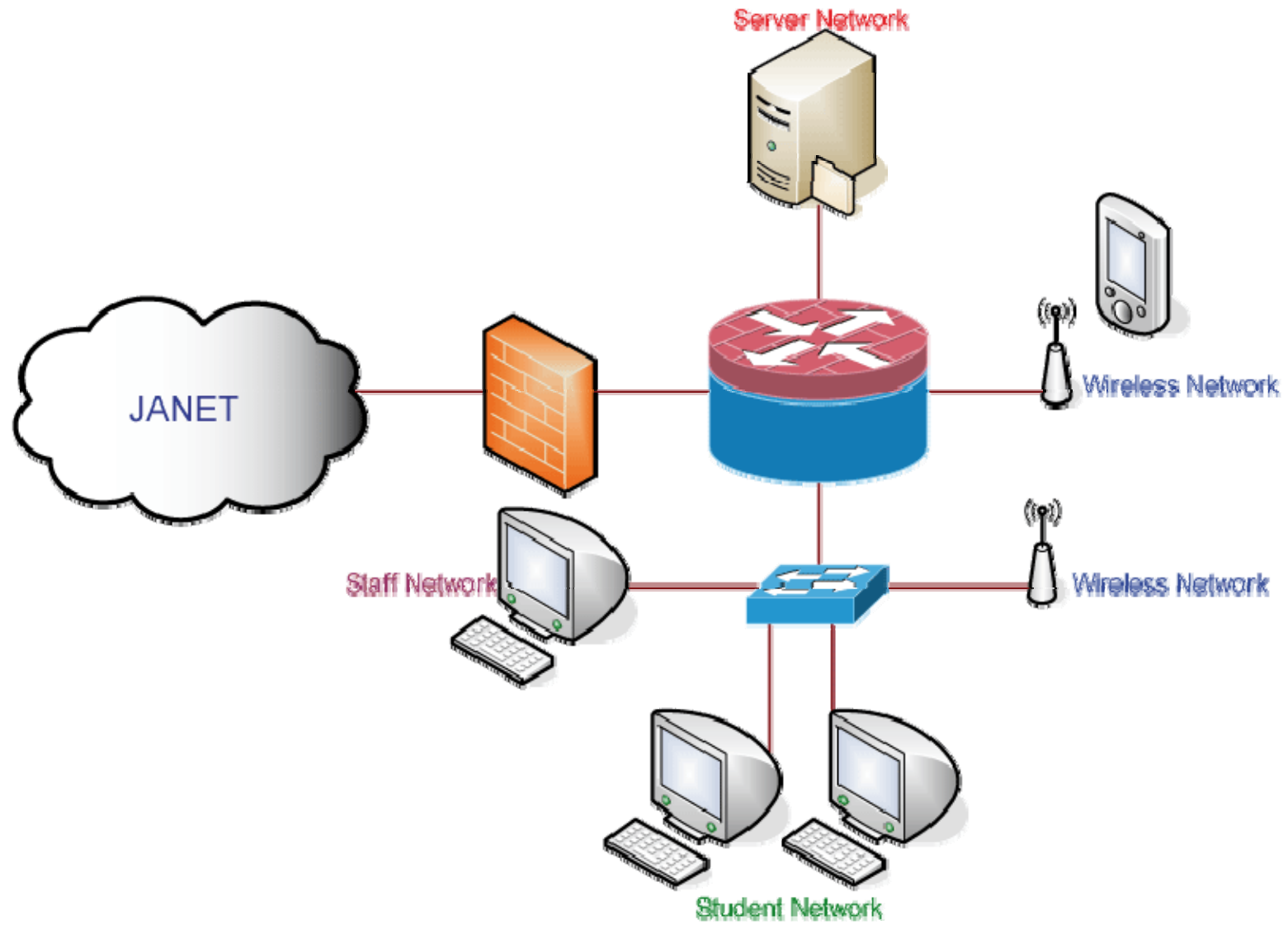


Level of Inspection

- 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

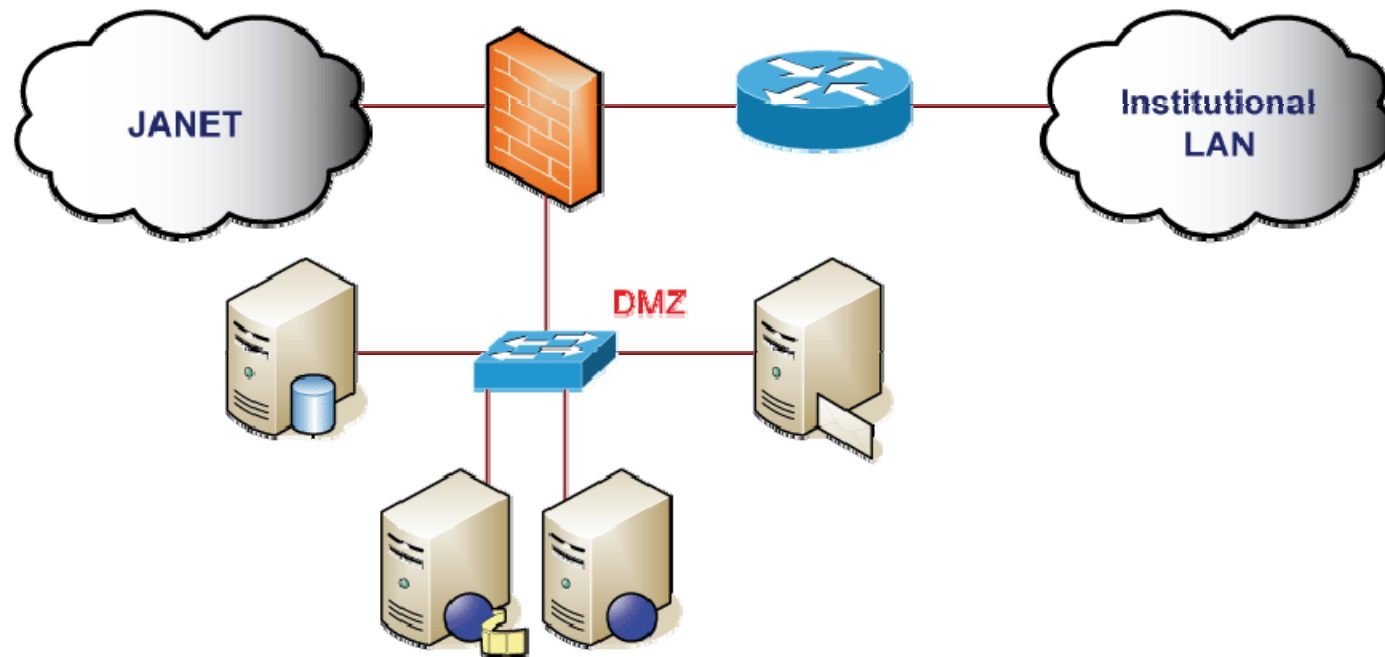


Isolating different classes of user

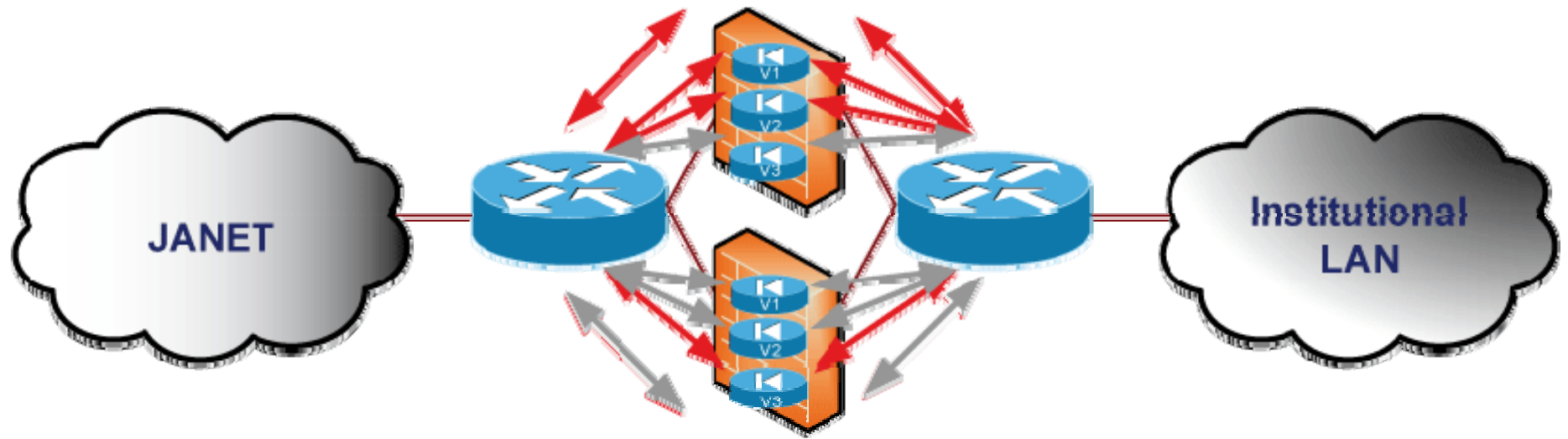


DMZ

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



Failover



Rules

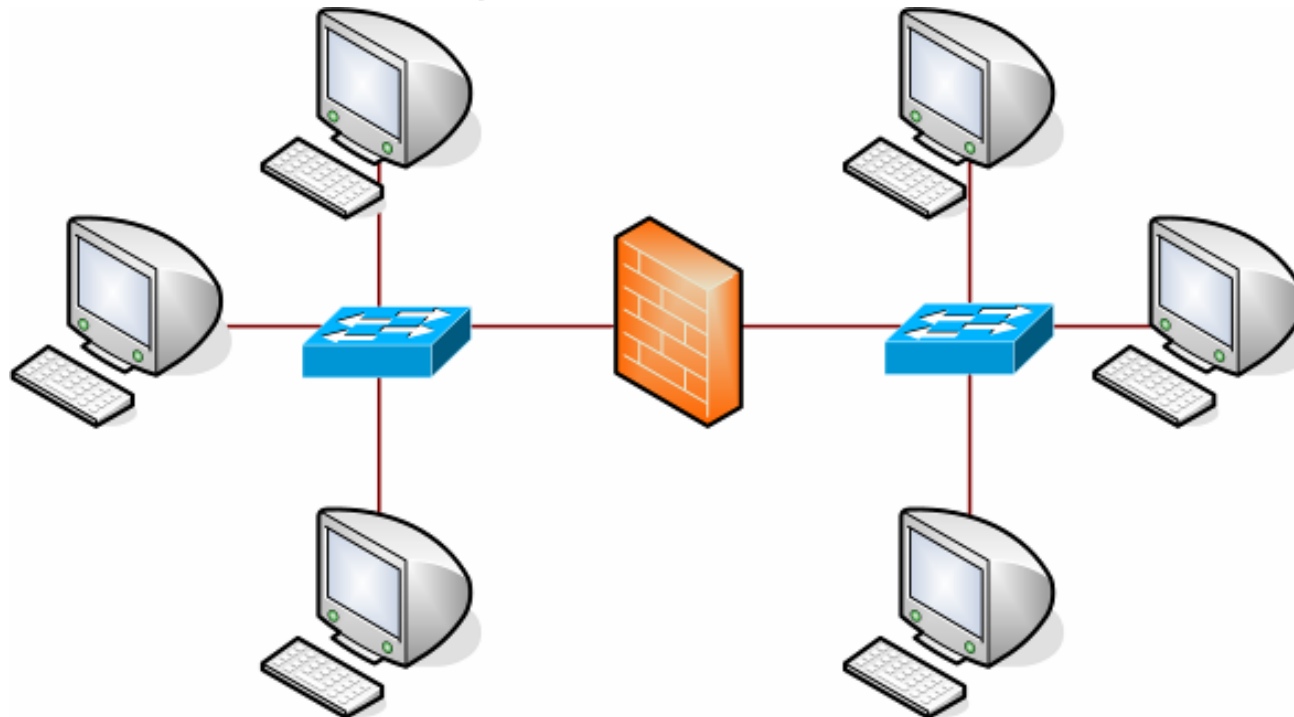
- Corner stone of firewalls
 - Sequence
 - Line number
 - Matching in strict order
- Performance
 - Group rules
- IP Addresses instead of DNS
- Be specific
- Block everything, then allow one by one

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

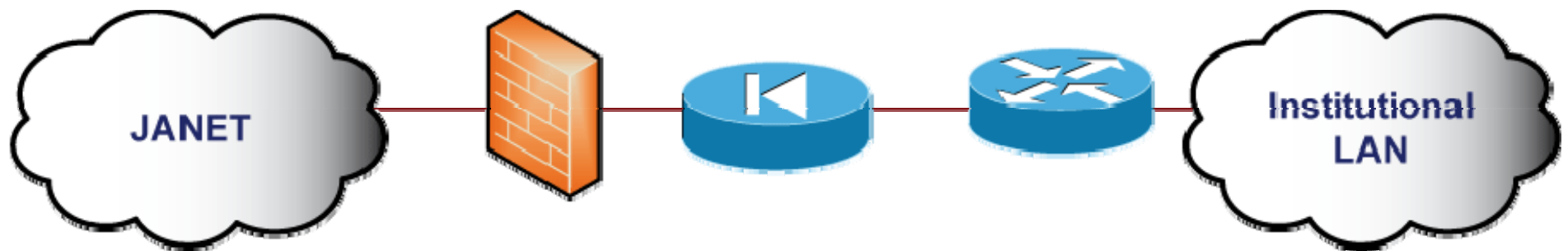
Development and Testing

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



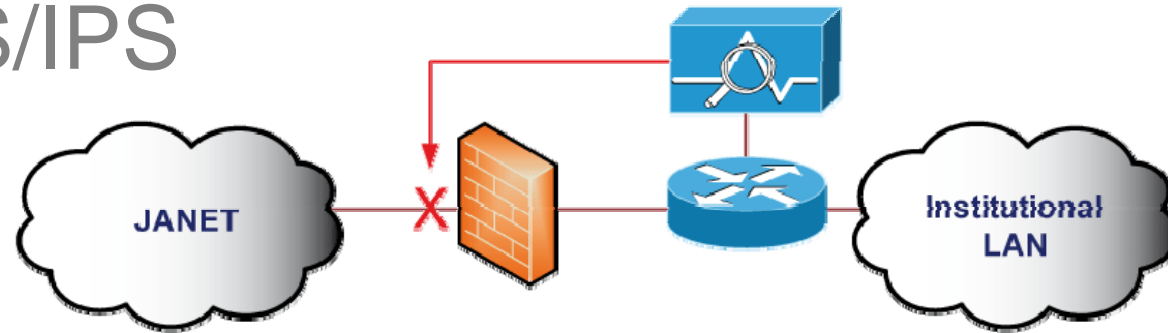
Cleaner Feed

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

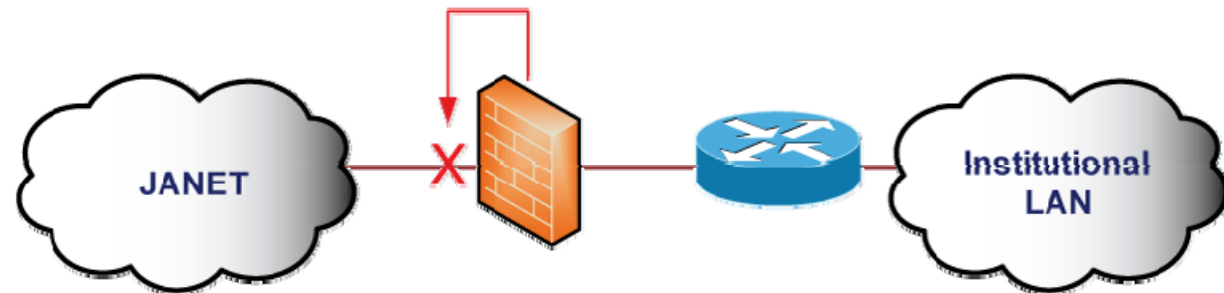


Integration with IDS and IPS

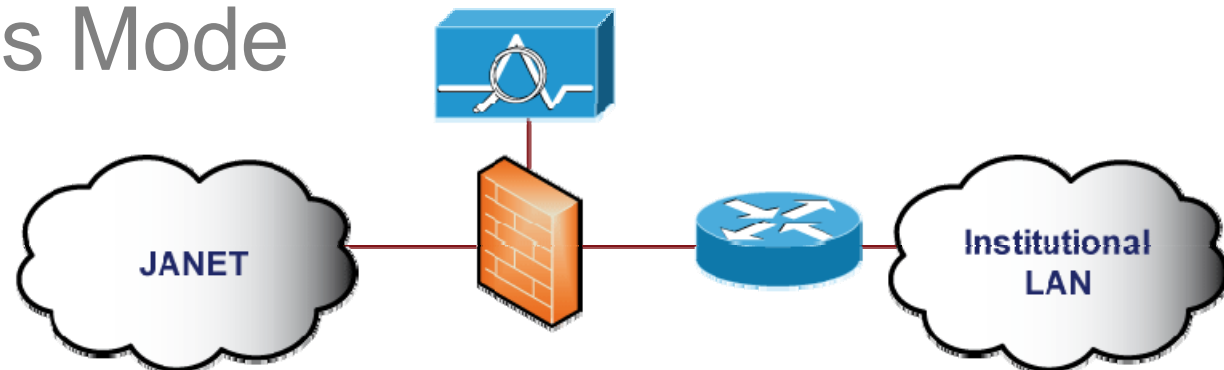
External IDS/IPS



Inline Mode



Promiscuous Mode



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 26th Cambridge
 - December 4th Glasgow

15-Minutes Guide to Firewalls

Questions

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