IPv6 Firewalls

Håkan Nohre

Cisco Systems

Test Result ☺

Cisco Firewalls Tested

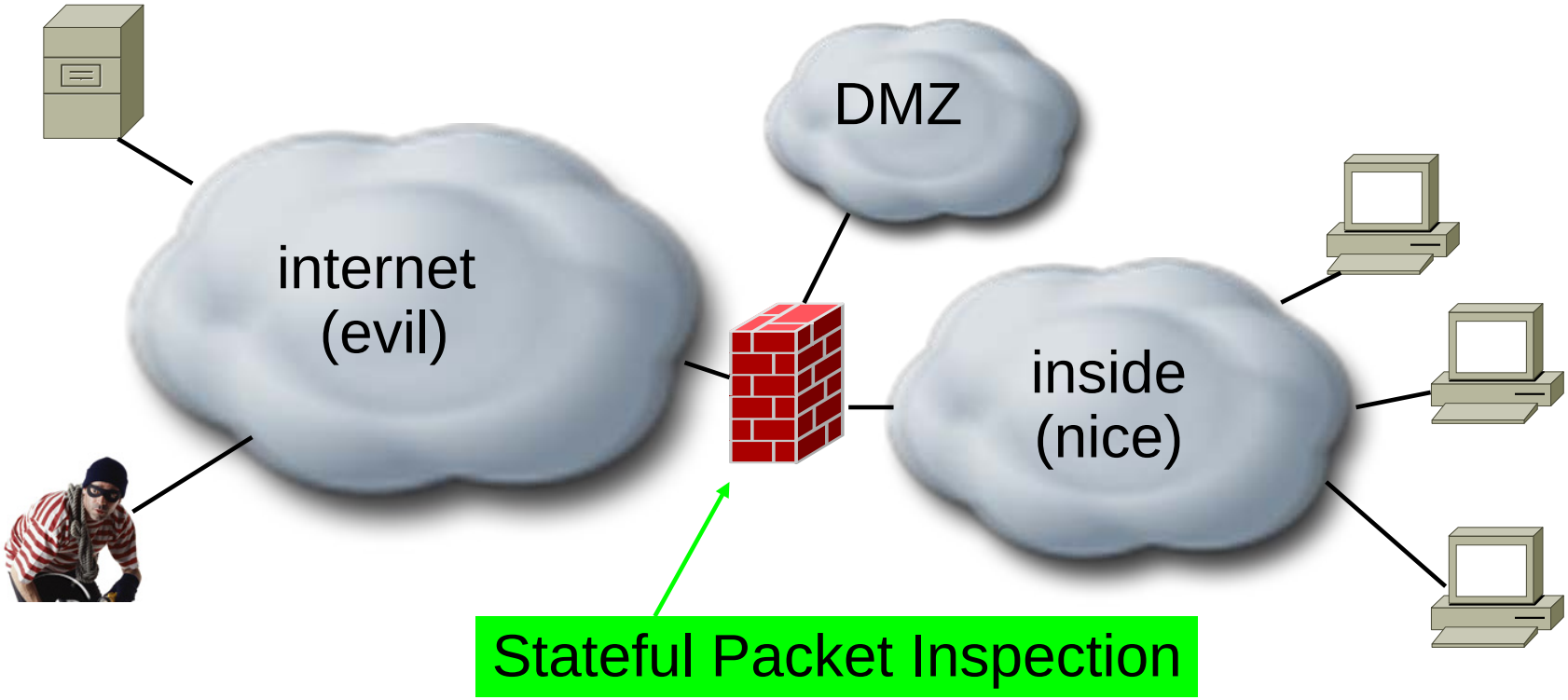
- ASA 5500 (ASA 5505)
- Cisco IOS Firewall (1800/871)

Results

- faulty cables, PC wireless issues, but...

NO IP V6 Related Issues !

Basic Firewall Functionality



IPv6 Firewall configuration ☺

```
interface Ethernet0
 nameif outside
 ipv6 address 2001:db8:c000:1051::37/64
 ipv6 enable
interface Ethernet1
 nameif inside
 ipv6 address 2001:db8:c000:1052::1/64
 ipv6 enable

ipv6 route outside ::/0 2001:db8:c000:1051::1

ipv6 access-list SECURE permit tcp any host
2001:db8:c000:1052::7 eq telnet
ipv6 access-list SECURE permit icmp6 any
2001:db8:c000:1052::/64

access-group SECURE in interface outside
```

IPv6 ACL Implicit Rules

Implicit Permit for Enable Neighbor Discovery

- The following implicit rules exist at the end of each IPv6 ACL to allow ICMPv6 neighbor discovery:

```
permit icmp any any nd-na
permit icmp any any nd-ns
deny ipv6 any any
```

- Be careful when adding « **`deny ipv6 any any log`** » at the end

For your reference

IPv6 ACL to Protect VTY

```
ipv6 access-list VTY
  permit ipv6 2001:db8:0:1::/64 any

line vty 0 4
  ipv6 access-class VTY in
```

Control Plane Policing for IPv6 Protecting the Router CPU

For your reference

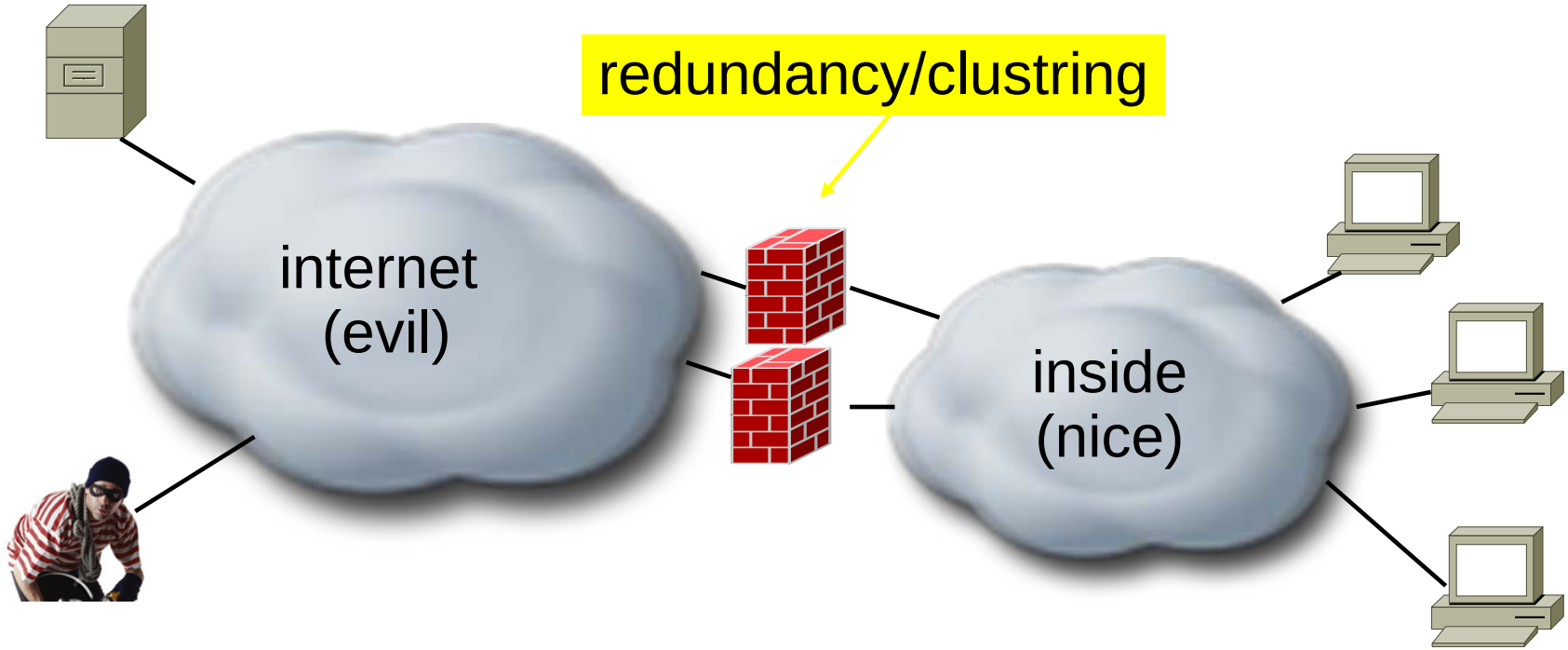
- Against DoS with Neighbor Discovery,...
- Can also throttle IPv6 traffic when processed in SW while IPv4 is in HW (legacy platform)
- If in doubts: **`show proc cpu | include IPv6`**

```
class-map match-all ipv6
 match protocol ipv6

policy-map CoPP
 class ipv6
  police rate 100 pps
    conform-action transmit
    exceed-action drop

control-plane
  service-policy input CoPP
```

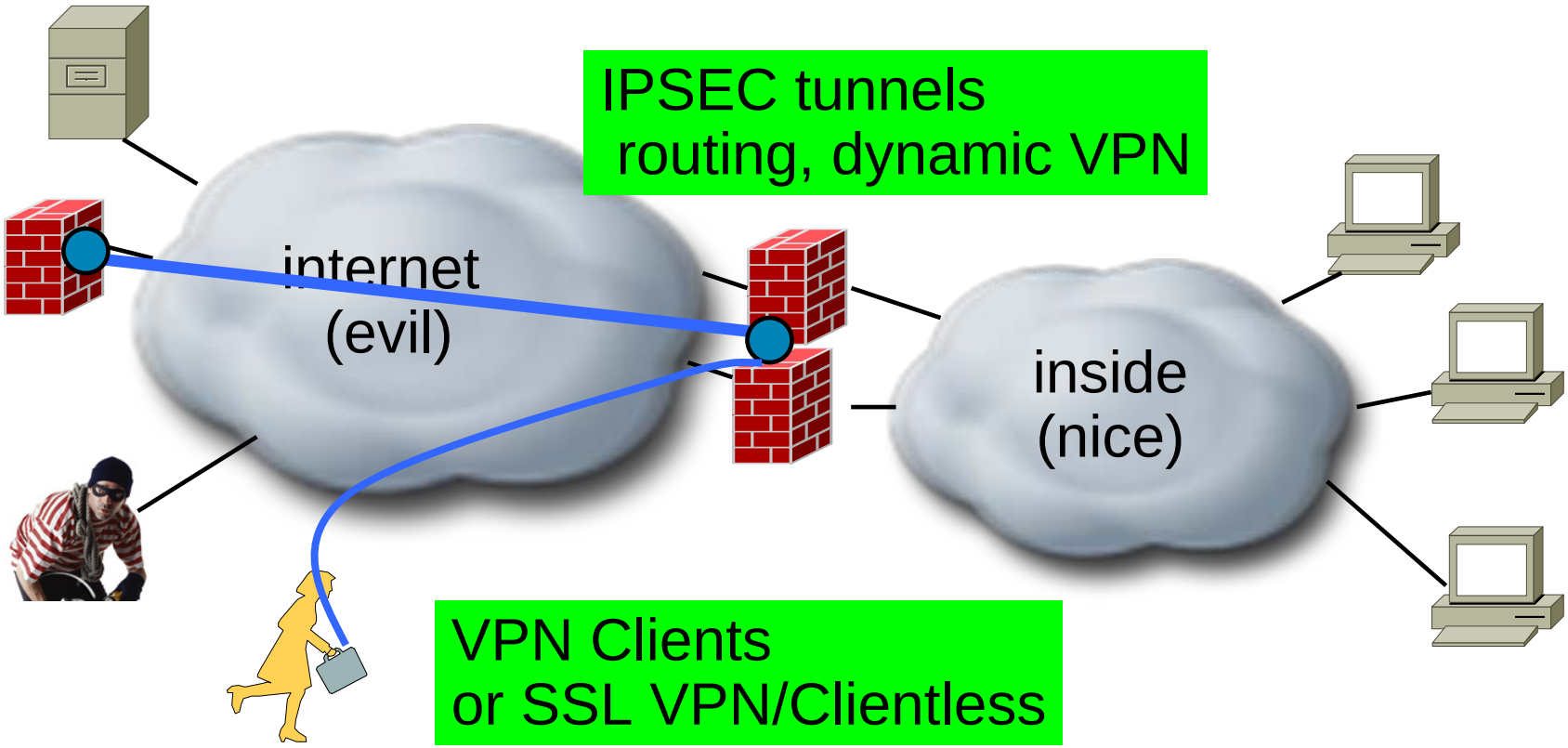
Firewalls have developed under IPv4...



Firwalls have developed under IPv4...

IPSEC site-to-site, Remote Access, SSL VPN

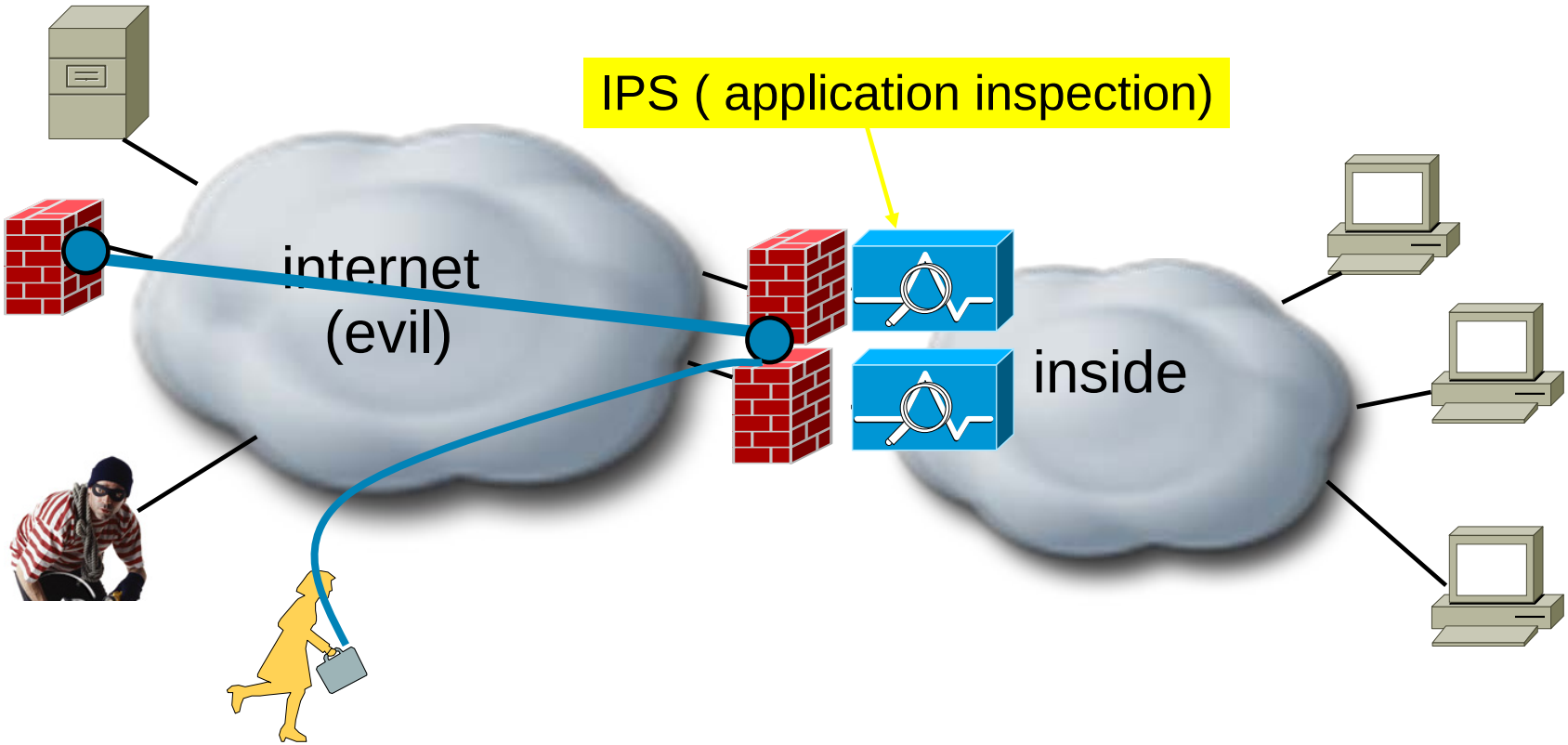
IPv6 : IPSEC mandatory ...



Firewalls have developed under IPv4

IPS (application inspection) in the Firewall

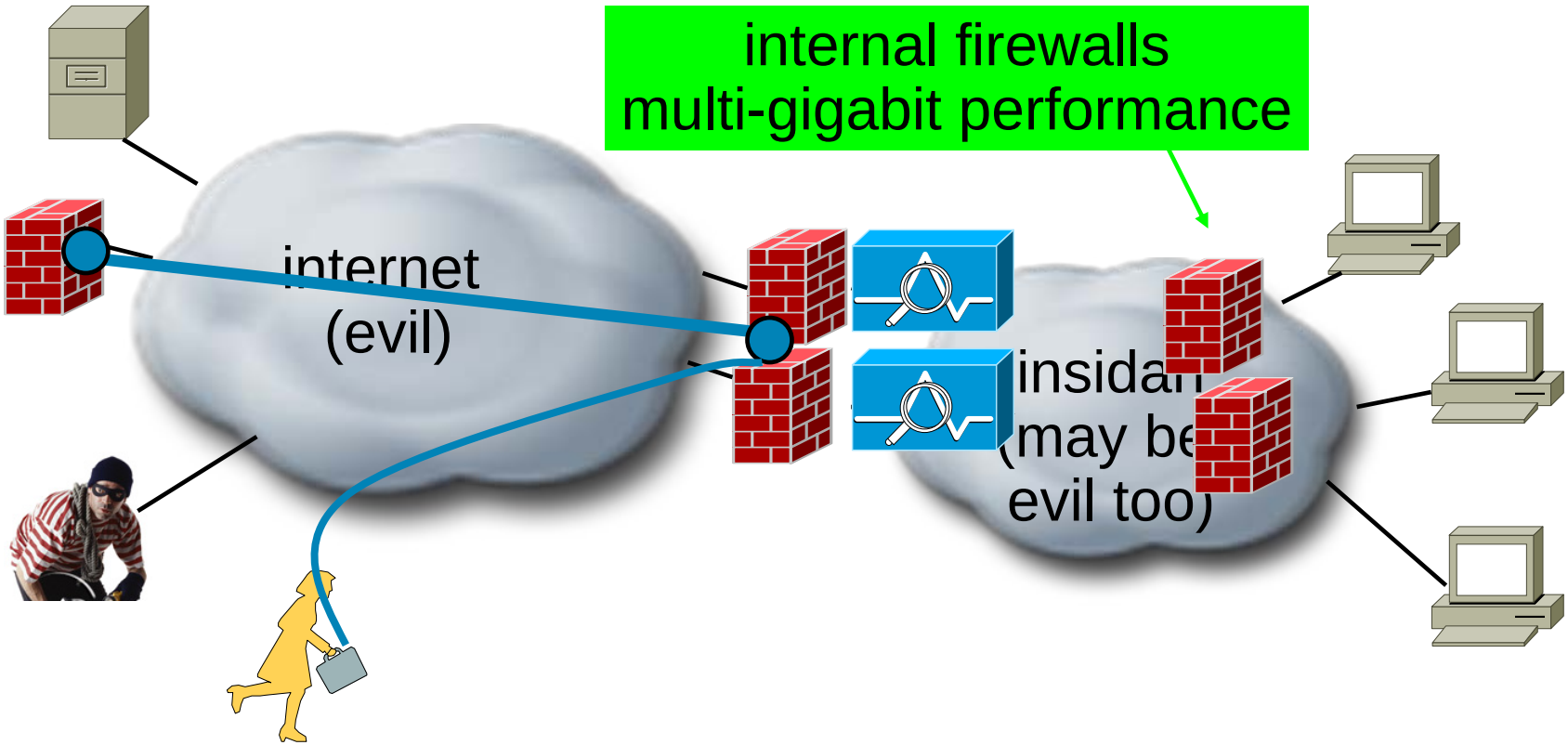
IPv6 : handling of IPv6 based IPS evasion necessary



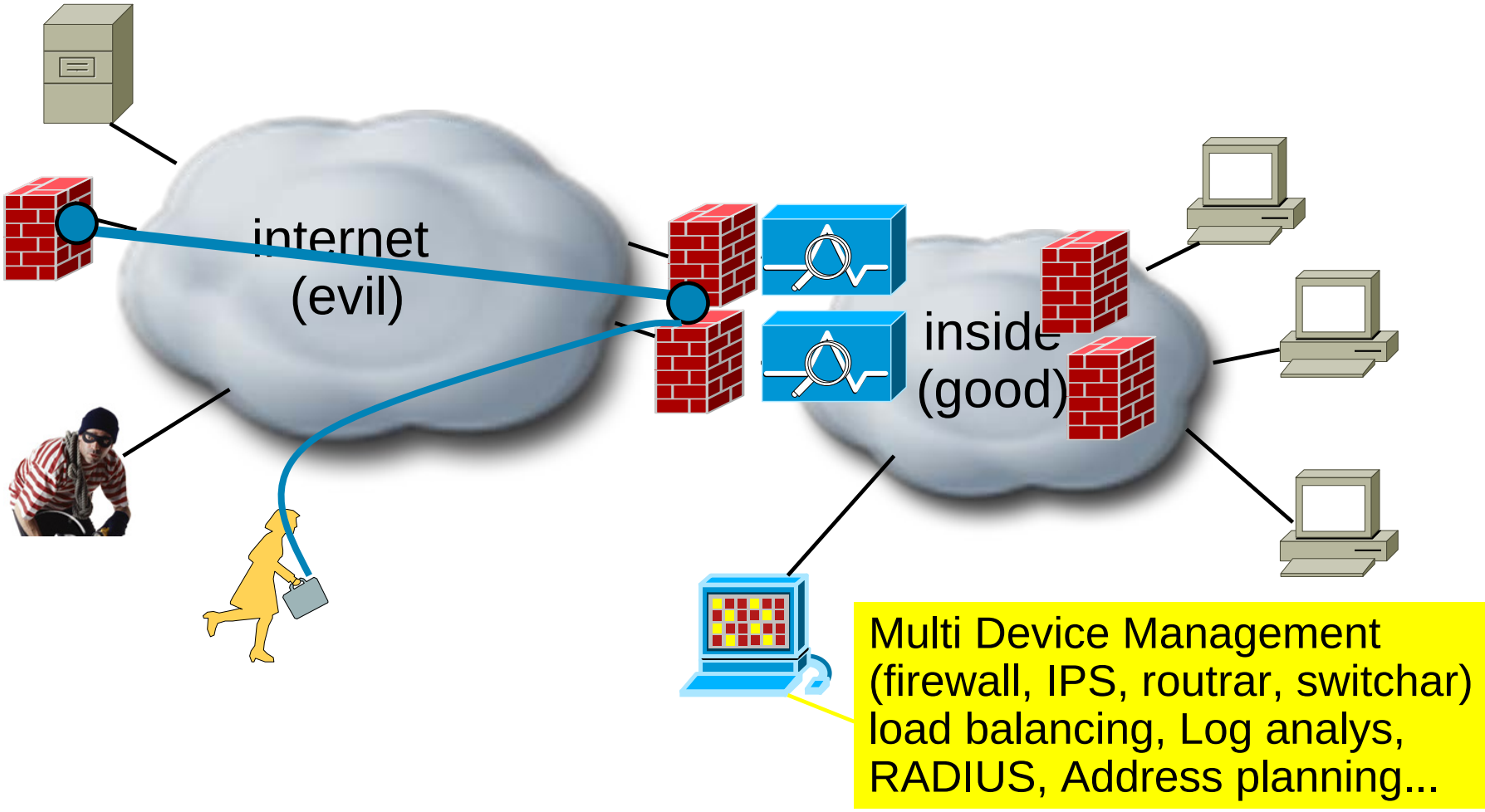
IPv4 has developed under IPv4

Multi-gig performance for internal firewalls

IPv6 firewall should be handled by hardware acceleration



System-level integration biggest challenge with IPv6 ?



Summary

- Yes.... (firewalls can do IPv6)
- ... system level integration , support systems, vendor integration may be biggest challenge
- Firewalls (IPv4) have been developing and improved thanks to customer feedback and experience
- Same will happens with Firewalls (IPv6) once adaptation accelerates