VLAN-Based Security for Modern Service-Provision Networks

Version 1.0

October, 2000

Bill Woodcock

Packet Clearing House

PCH
Packet Clearing House

We Have Linguistic Problems, not Technological Problems

The technology is much, *much* more flexible than most people's ability to comprehend the problem-space.

The problem is in finding a mental model which allows users to comprehend the problems and their solutions, not in finding a technology to solve the problem.

PCH
Packet Clearing House

Legacy Firewall Terminology

Historical distinction between “packet filtering firewalls” and “stateful-inspection firewalls” no longer very useful in the real world.

“inside,” “outside” and “DMZ” nomenclature limits lay-people’s ability to understand security.

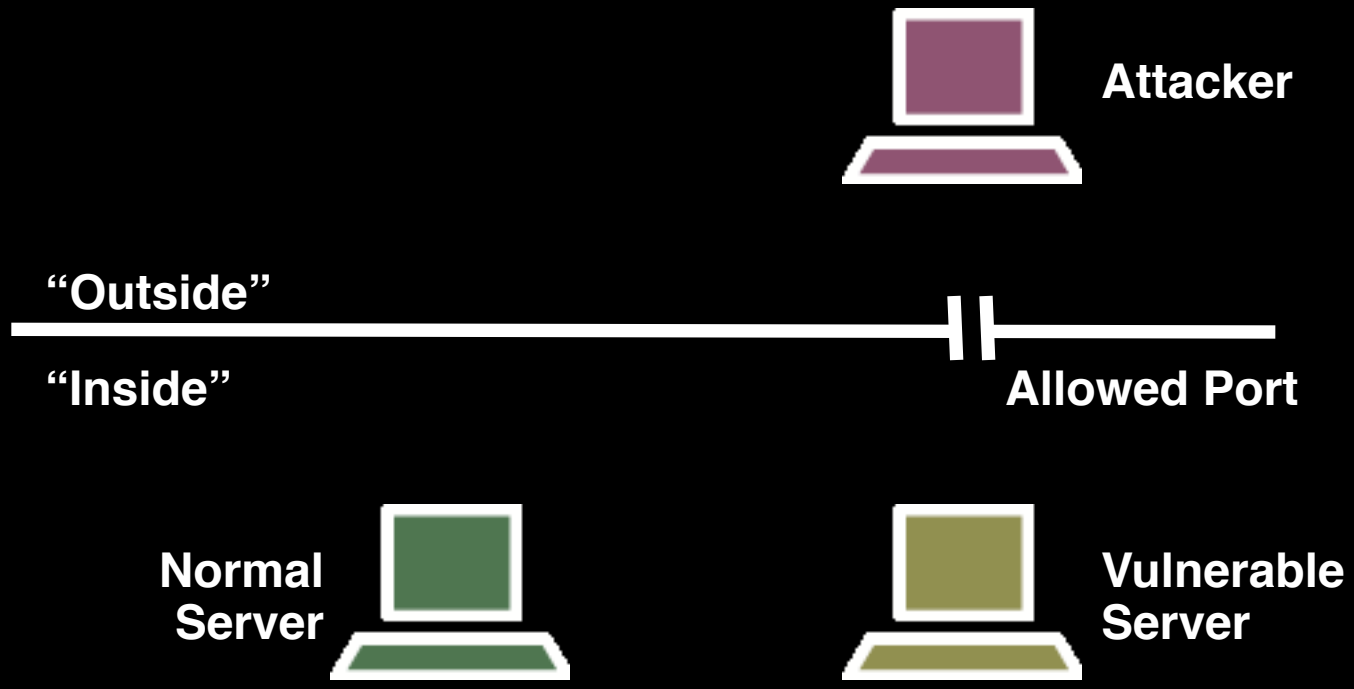
PCH
Packet Clearing House

Old Enterprise Solution:

- Stateful-inspection box
- Usually an application on top of Windows.
  - Immense differential between the complexity of the system and what's exposed to the operator.
- Usually very slow.
- Usually very low MTBF.
- Three 10/100 Ethernet interfaces.
  - No protection against stepping-stone attacks.
  - No protection against untrusted users.

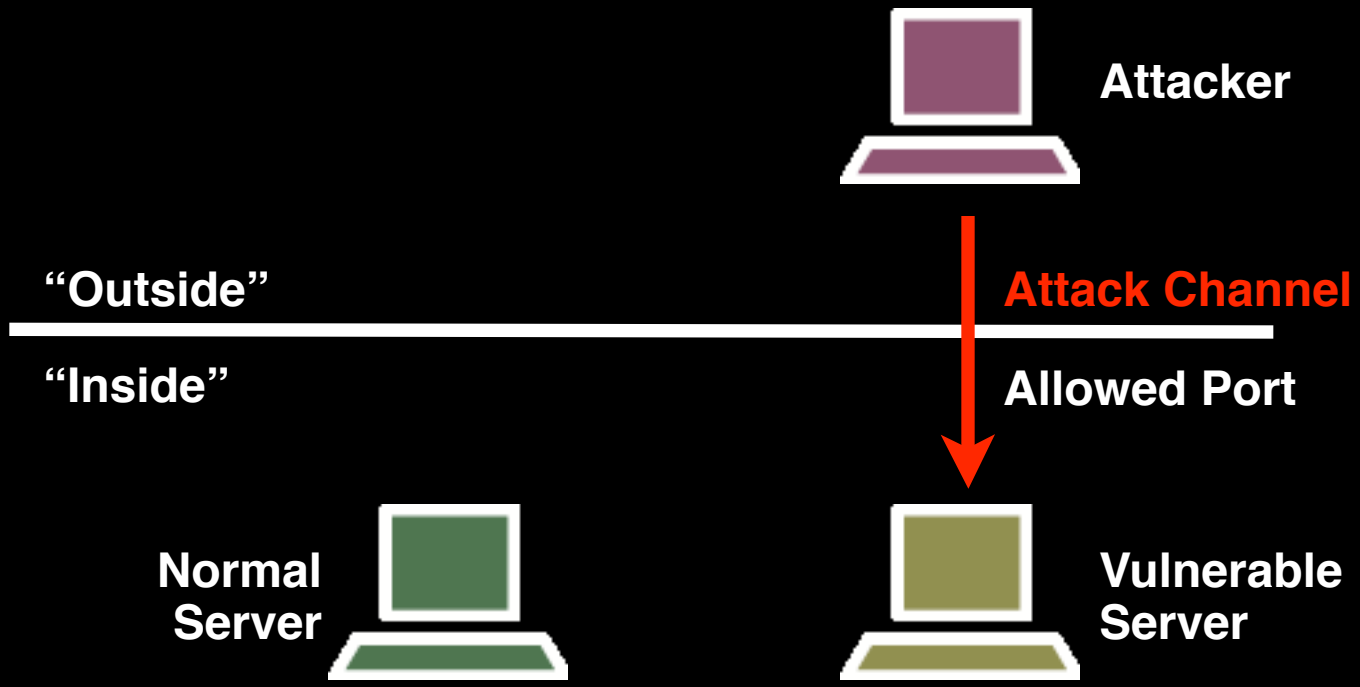
PCH
Packet Clearing House

Stepping-Stone Attack



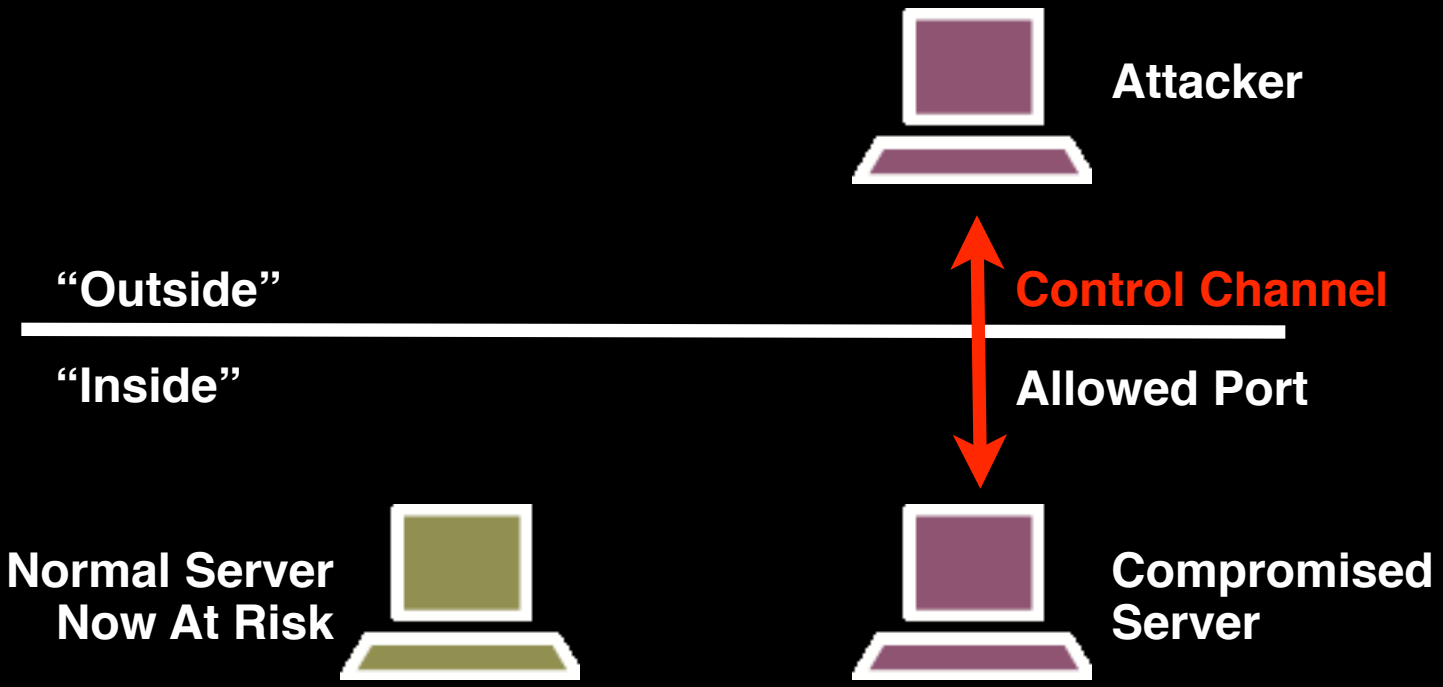
PCH
Packet Clearing House

Stepping-Stone Attack



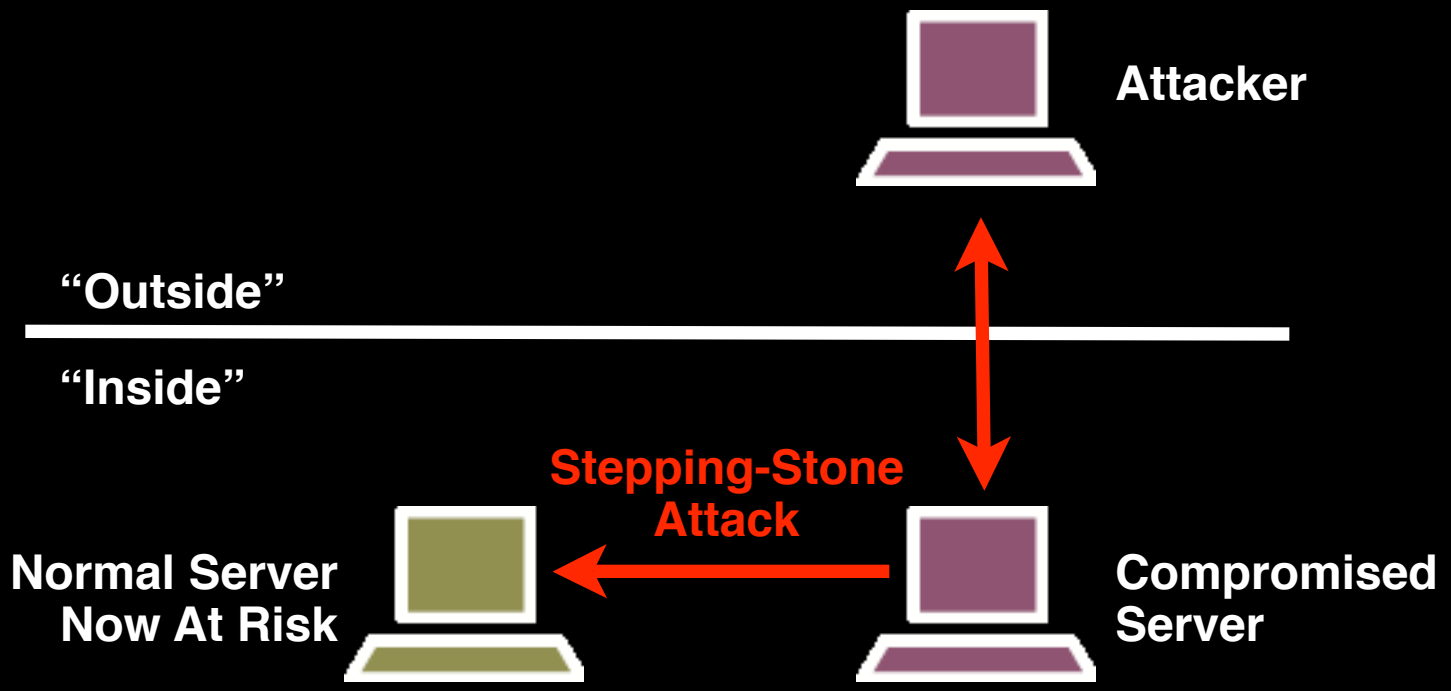
PCH
Packet Clearing House

Stepping-Stone Attack



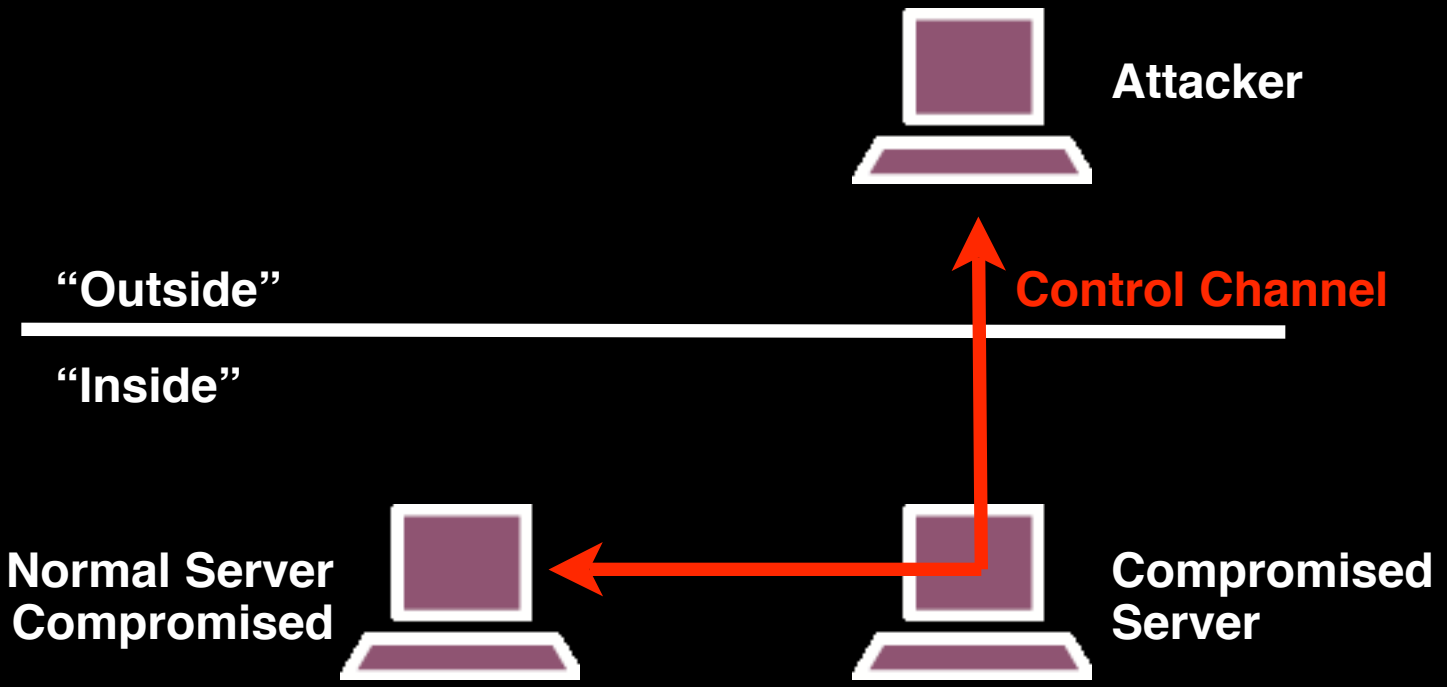
PCH
Packet Clearing House

Stepping-Stone Attack



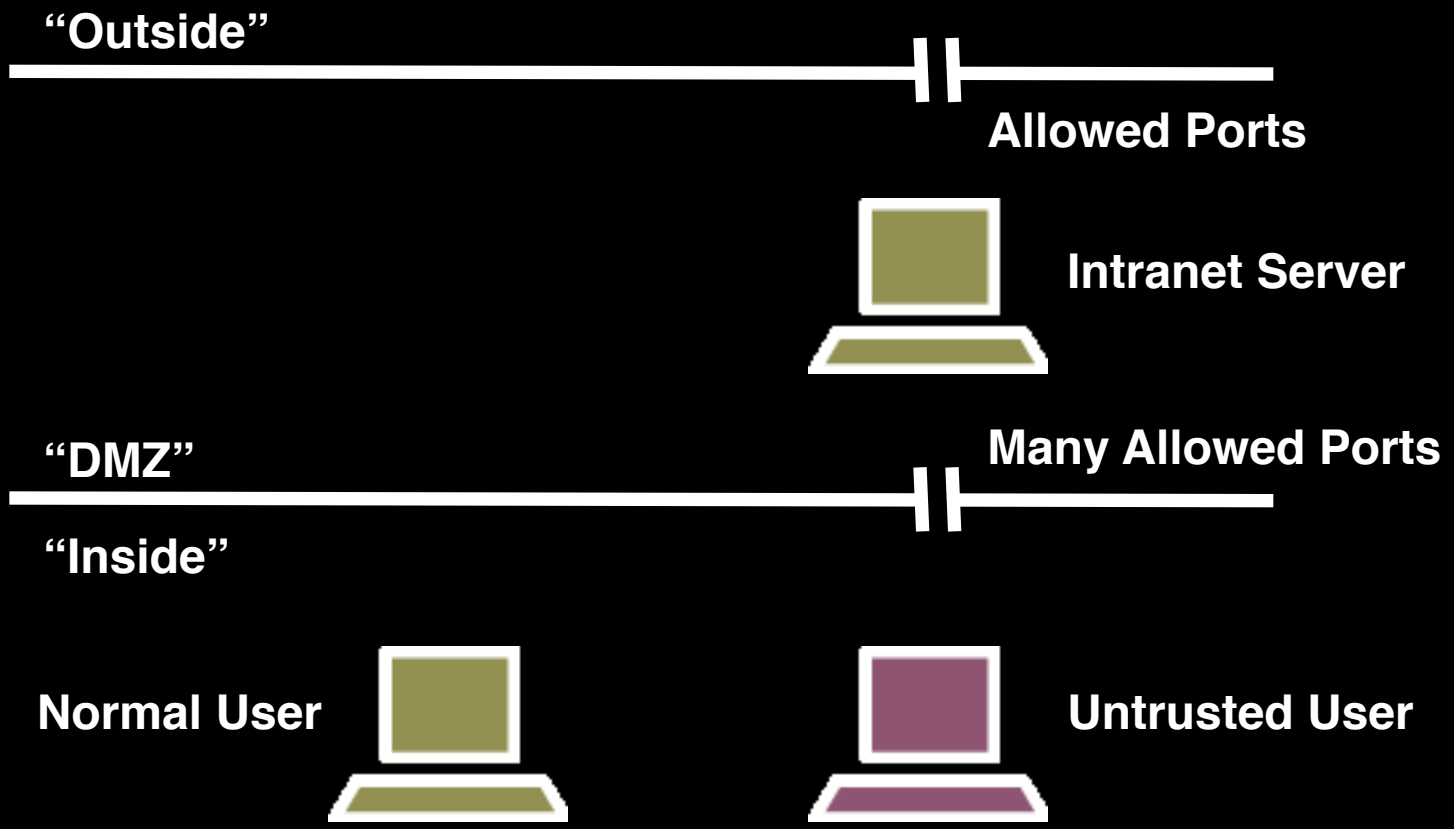
PCH
Packet Clearing House

Stepping-Stone Attack



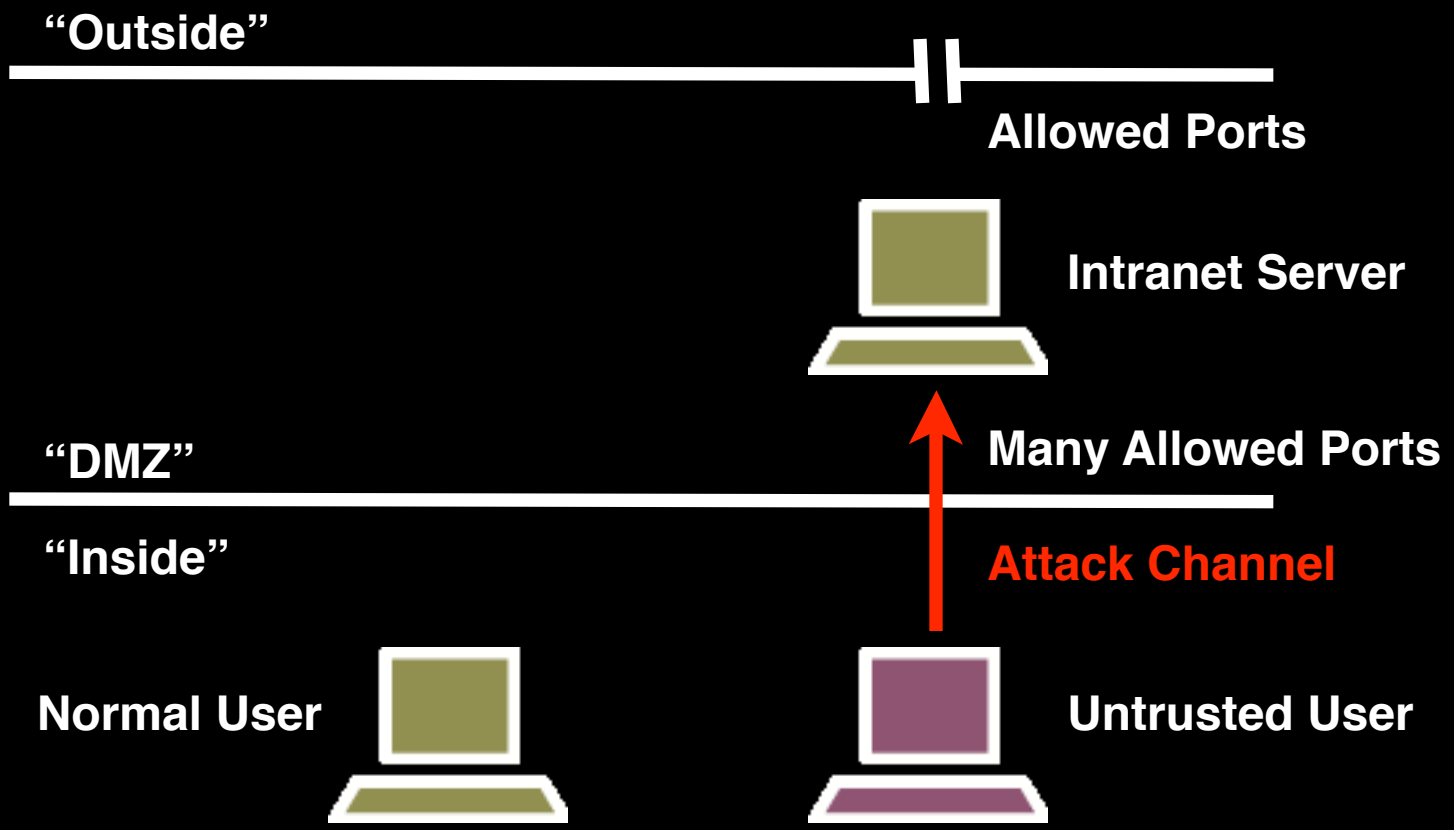
PCH
Packet Clearing House

Untrusted User Attack



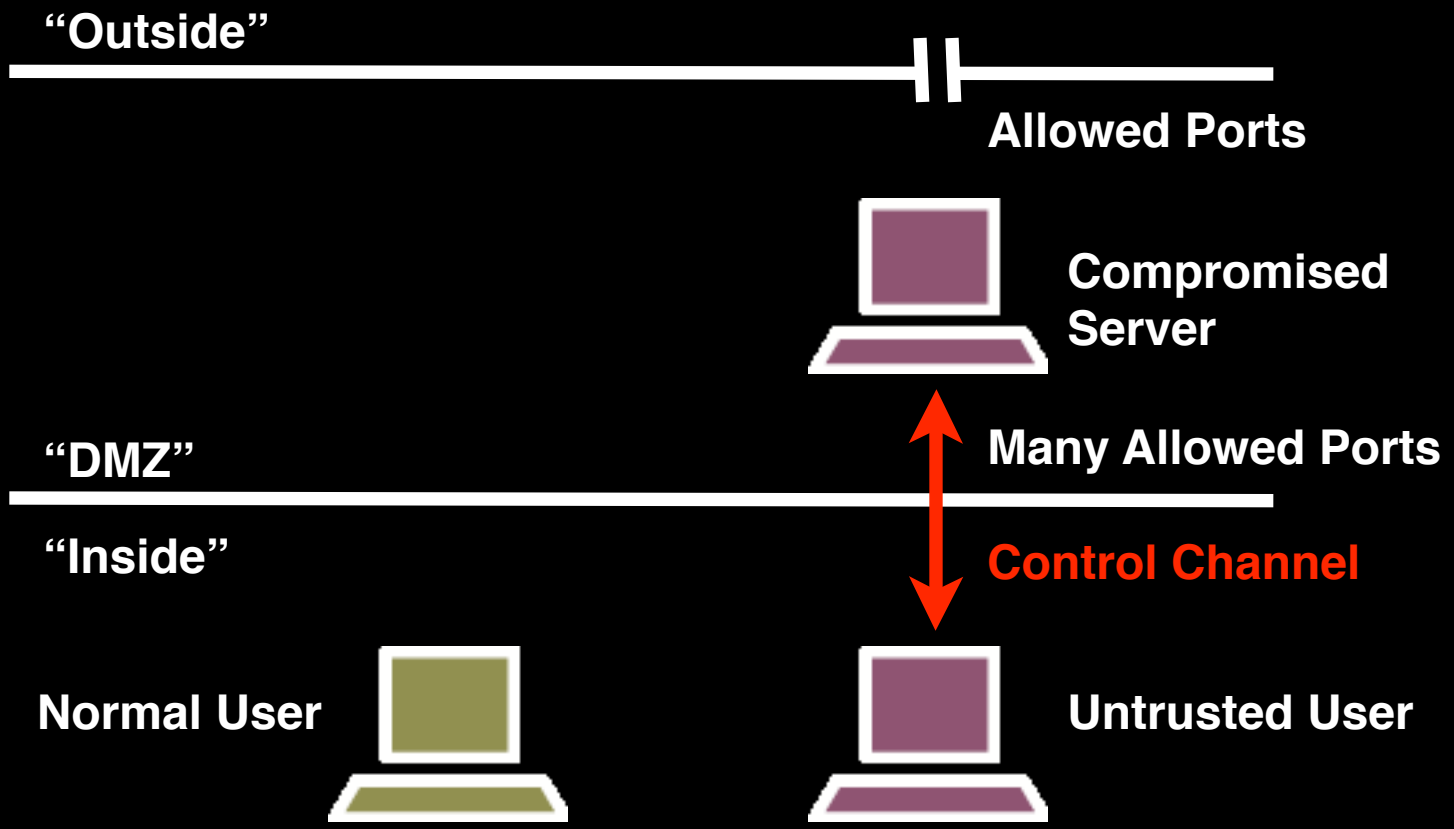
PCH
Packet Clearing House

Untrusted User Attack



PCH
Packet Clearing House

Untrusted User Attack



PCH
Packet Clearing House

Modern Firewalling

Don’t add points of failure. Make full use of the high-MTBF equipment you already have.

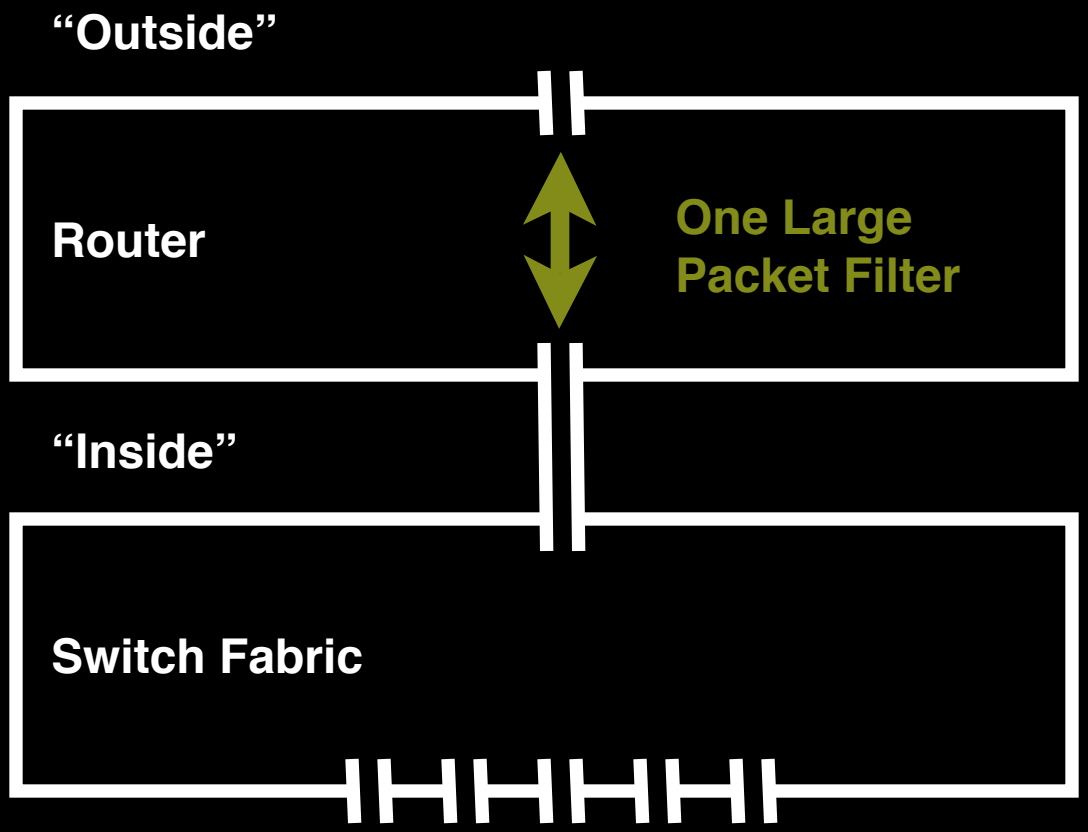
Don’t slow things down.

Don’t invite Bill Gates into your network.

Security needs should define your security policy, not some coincidental number of physical interfaces on a box.

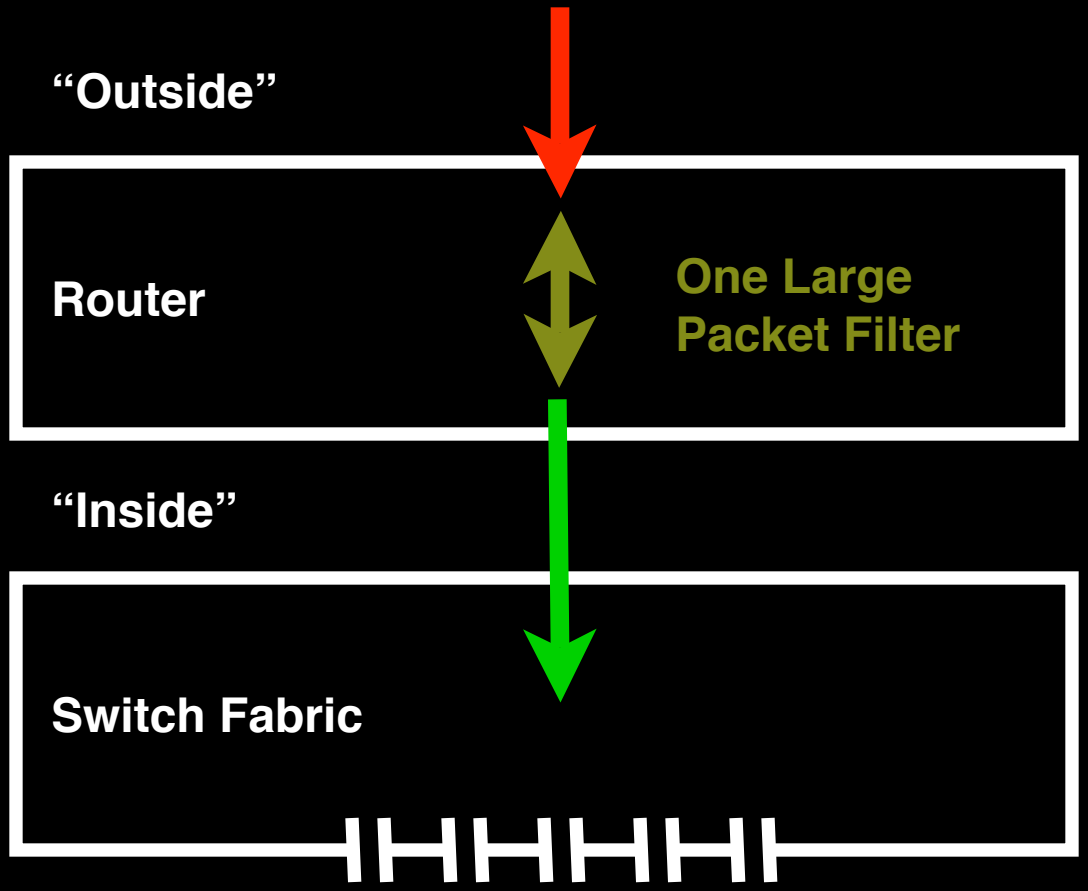
PCH
Packet Clearing House

Simple Packet Filter



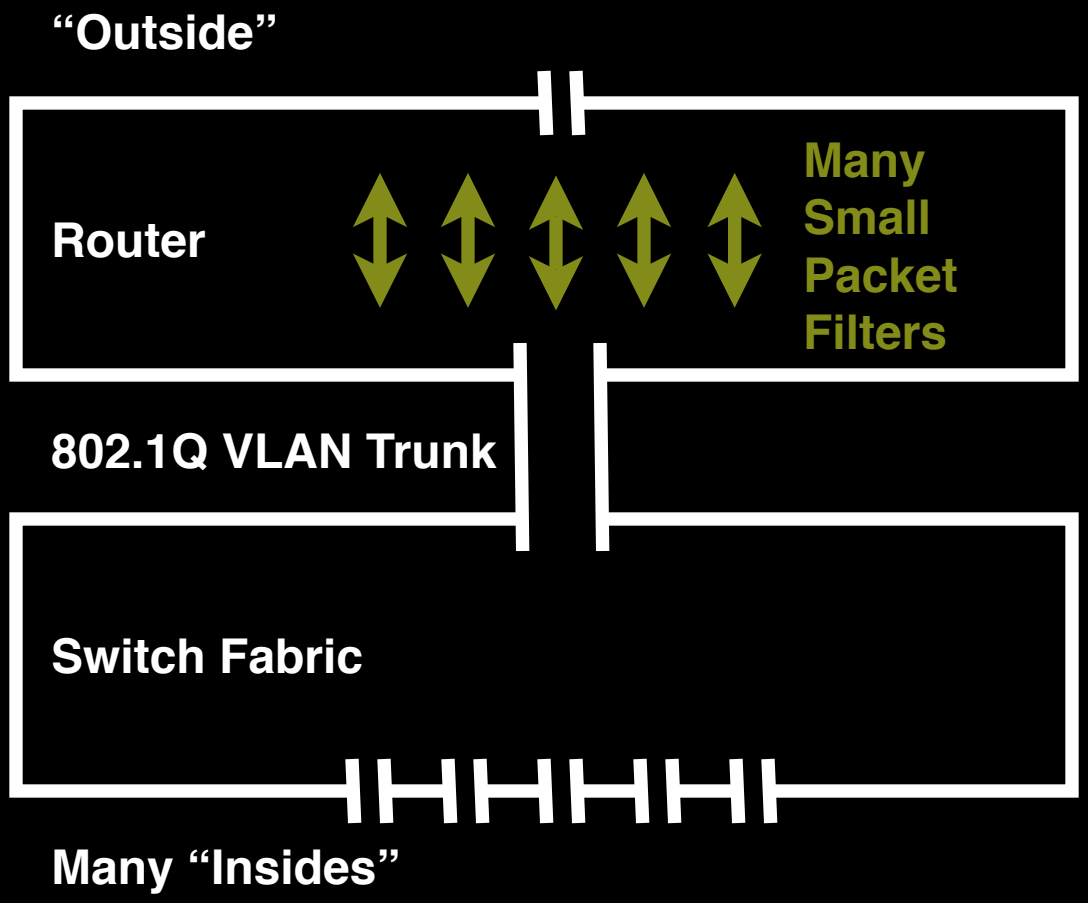
PCH
Packet Clearing House

Simple Packet Filter



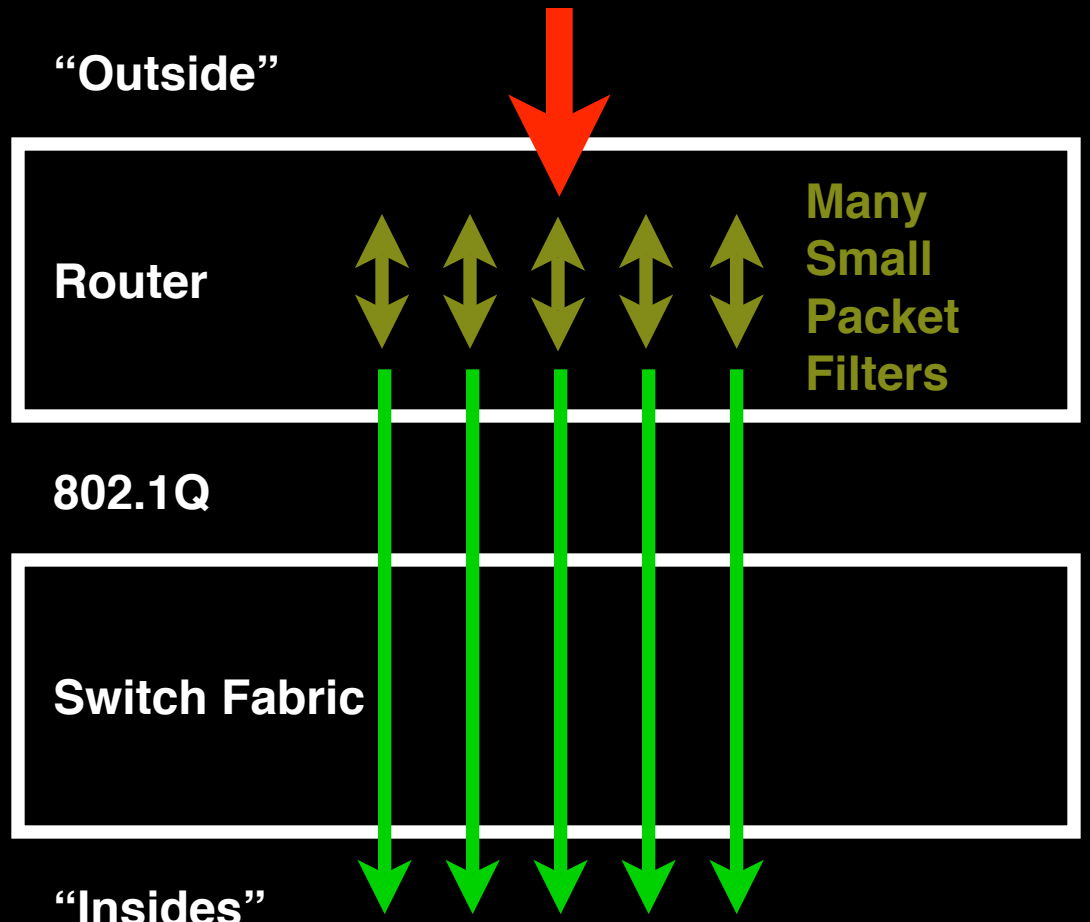
PCH
Packet Clearing House

VLAN-Based Firewalling



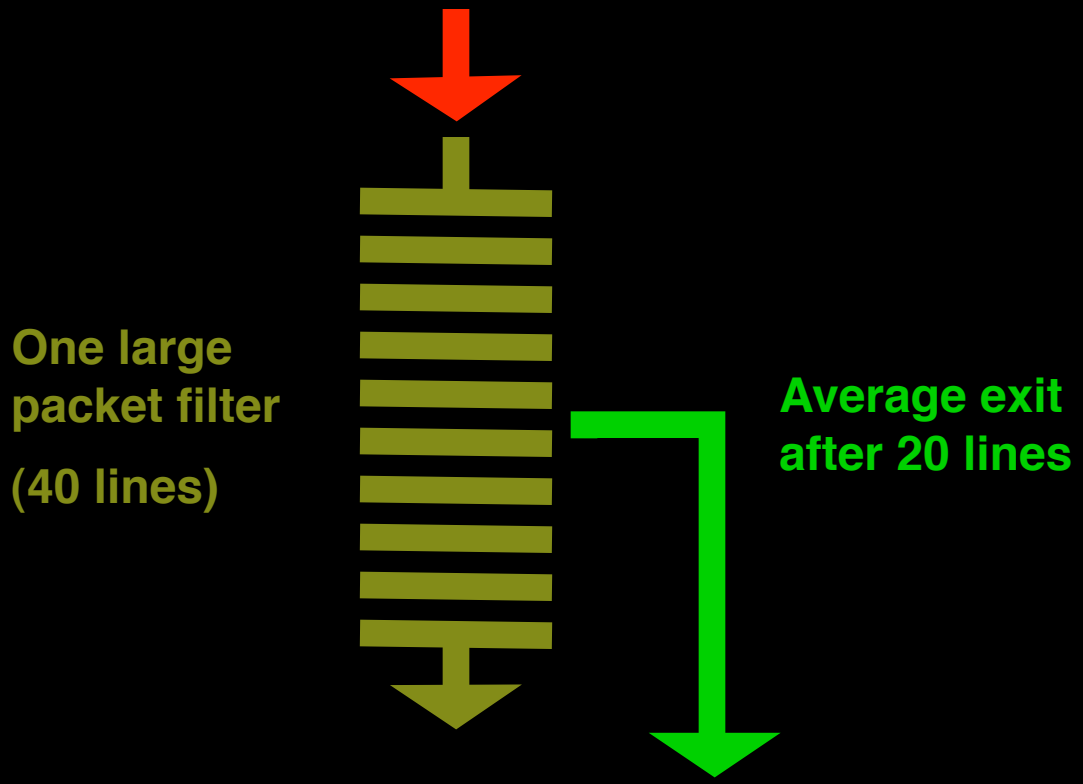
PCH
Packet Clearing House

VLAN-Based Firewalling



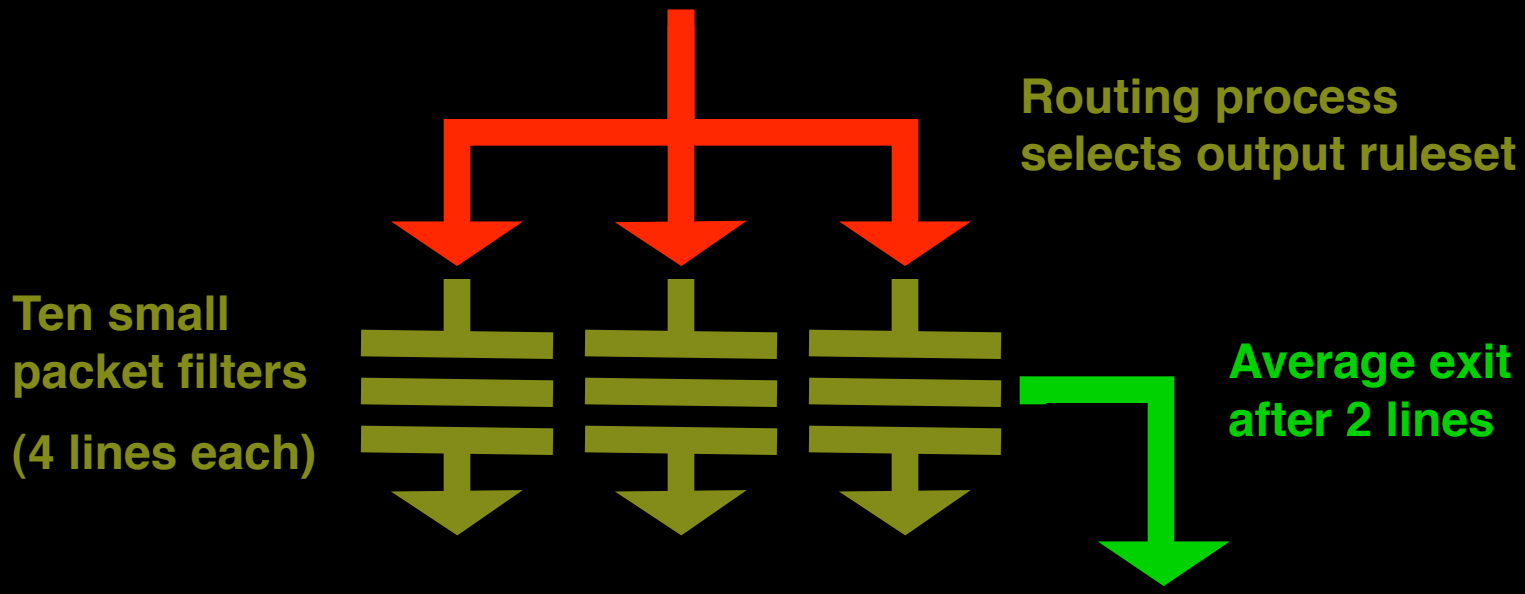
PCH
Packet Clearing House

Relative Processing Speed



PCH
Packet Clearing House

Relative Processing Speed



Routing is cheap, ruleset processing is expensive.
Use the router for what it's good at.

Packet Clearing House

What This Looks Like: Switch

```
hostname OAK-Switch-3
!
interface FastEthernet0/41
  description VLAN_341-OAK_DNS-131.161.2.0/30
  switchport access vlan 341
  speed 100
  full-duplex
```

```
OAK-Switch-3# vlan database
OAK-Switch-3(vlan)# vlan 341 name VLAN_341-OAK_DNS-131.161.2.0/30
OAK-Switch-3(vlan)# exit
APPLY completed.
Exiting....
```

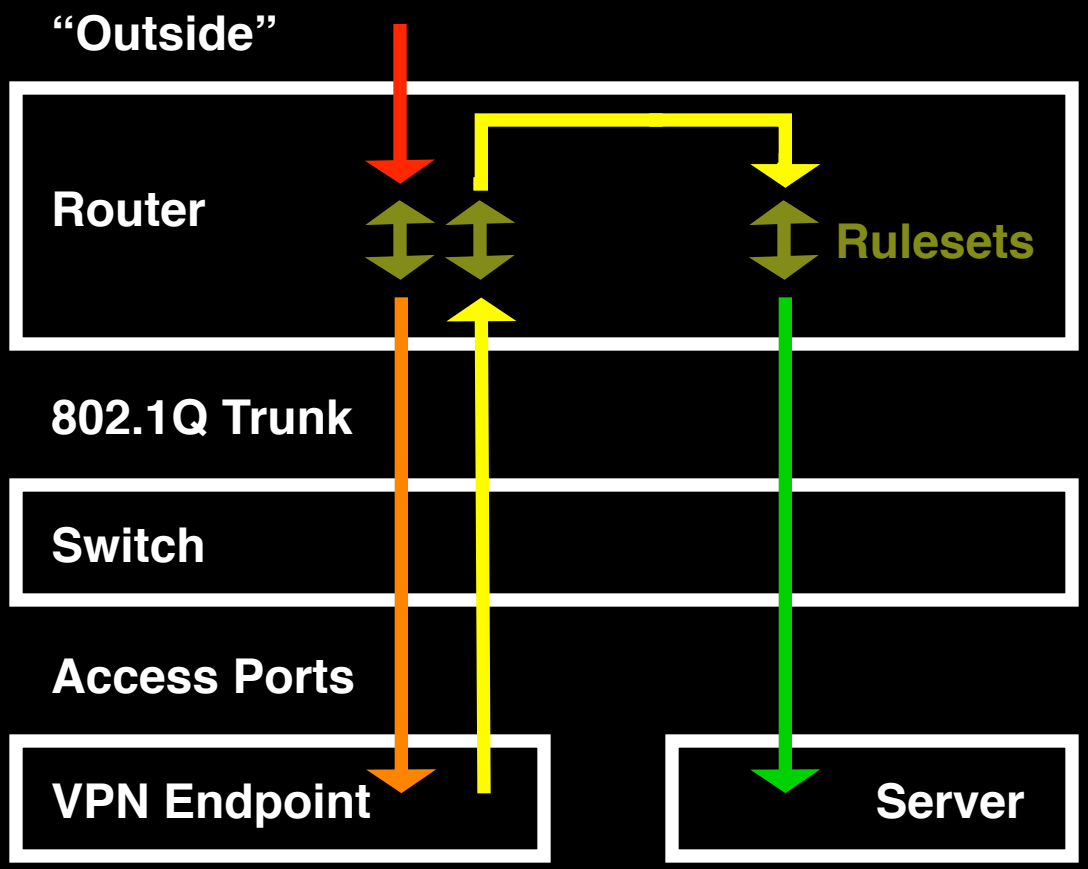
Packet Clearing House

What This Looks Like: Router

```
hostname OAK-Firewall
!
interface FastEthernet0/0
  description 802.1Q VLAN Trunk to OAK-Switch-1
  no ip address
  speed 100
  full-duplex
!
interface FastEthernet0/0.341
  description VLAN_341-OAK_DNS-131.161.2.0/30
  encapsulation dot1Q 341
  ip address 131.161.2.2 255.255.255.252
  ip access-group ACL-341-OAK_DNS-IN in
  ip access-group ACL-341-OAK_DNS-OUT out
!
ip access-list extended ACL-341-OAK_DNS-IN
  permit udp host 131.161.2.1 eq domain any
  permit udp host 131.161.2.1 any eq domain
  permit tcp host 131.161.2.1 any eq domain
  permit tcp host 131.161.2.1 eq domain any
  deny   icmp any any port-unreachable
  deny   udp any any gt 0 log-input
  deny   tcp any any gt 0 log-input
  deny   ip any any log-input
ip access-list extended ACL-341-OAK_DNS-OUT
  permit udp any host 131.161.2.1 eq domain
  permit udp any eq domain host 131.161.2.1 gt 1023
  permit tcp any any established
  permit tcp any host 131.161.2.1 eq domain
  deny   udp any any eq netbios-ns
  deny   icmp any any
```

PCH
Packet Clearing House

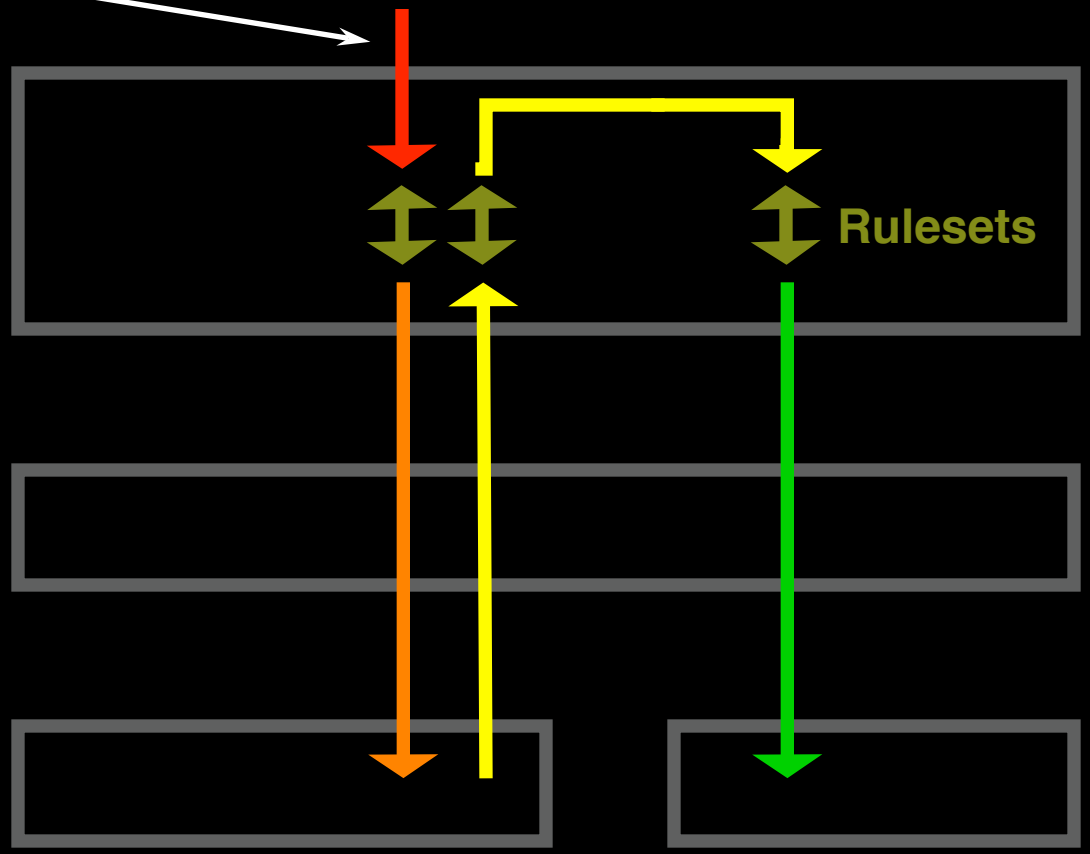
Example With VPN Endpoint



Packet Clearing House

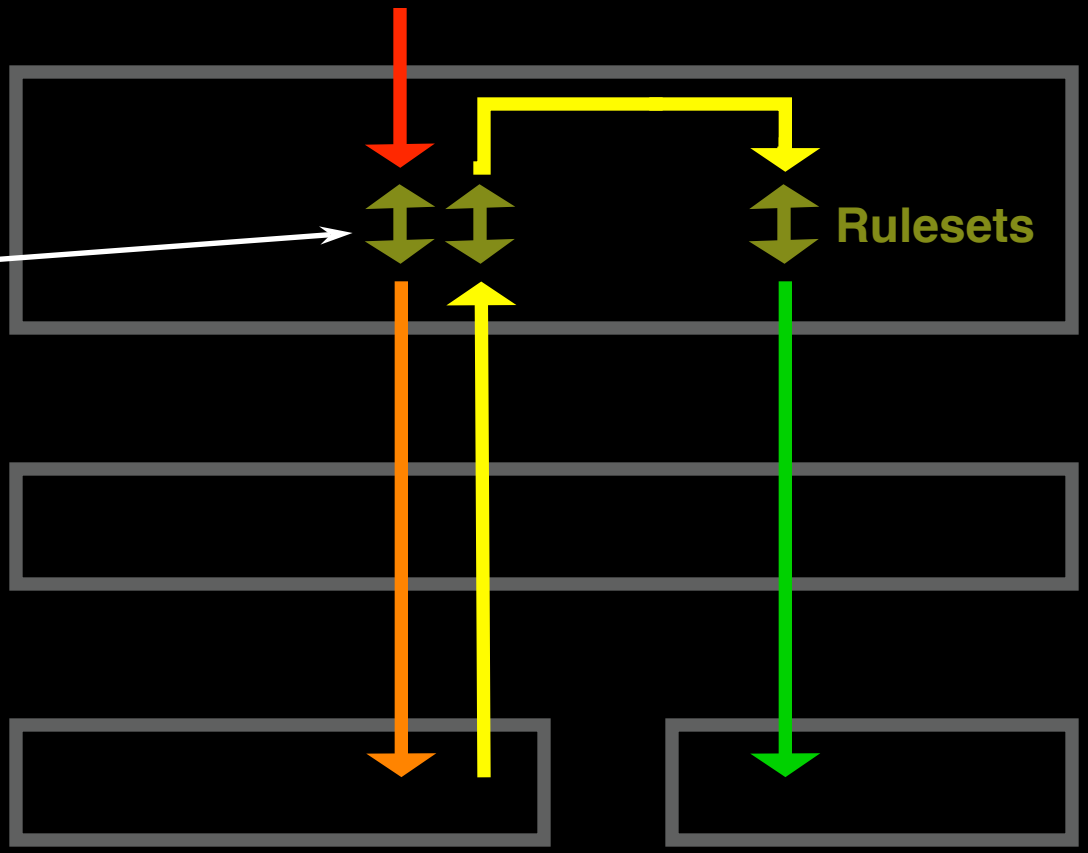
Example With VPN Endpoint

Traffic enters network from the commodity network



PCH
Packet Clearing House

Example With VPN Endpoint

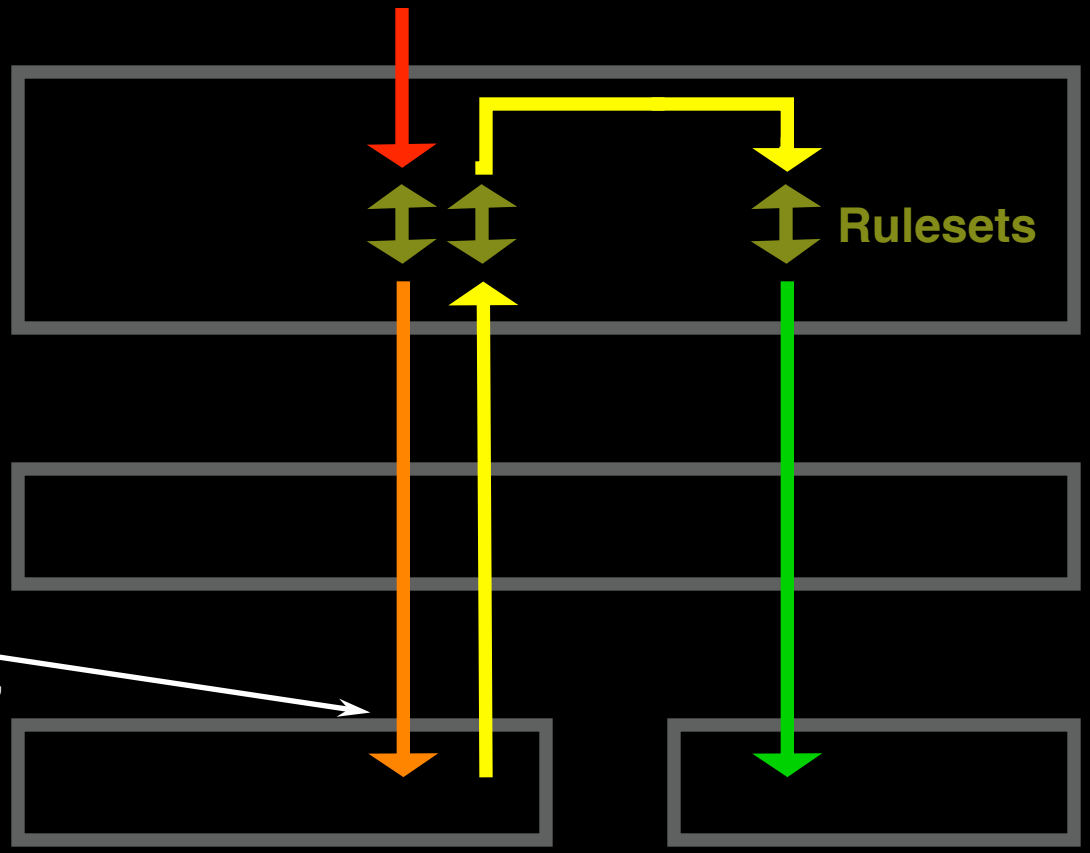


First ruleset guarantees that only IPSec traffic will reach the VPN endpoint

VPN endpoint is protected against non-IPSec attack

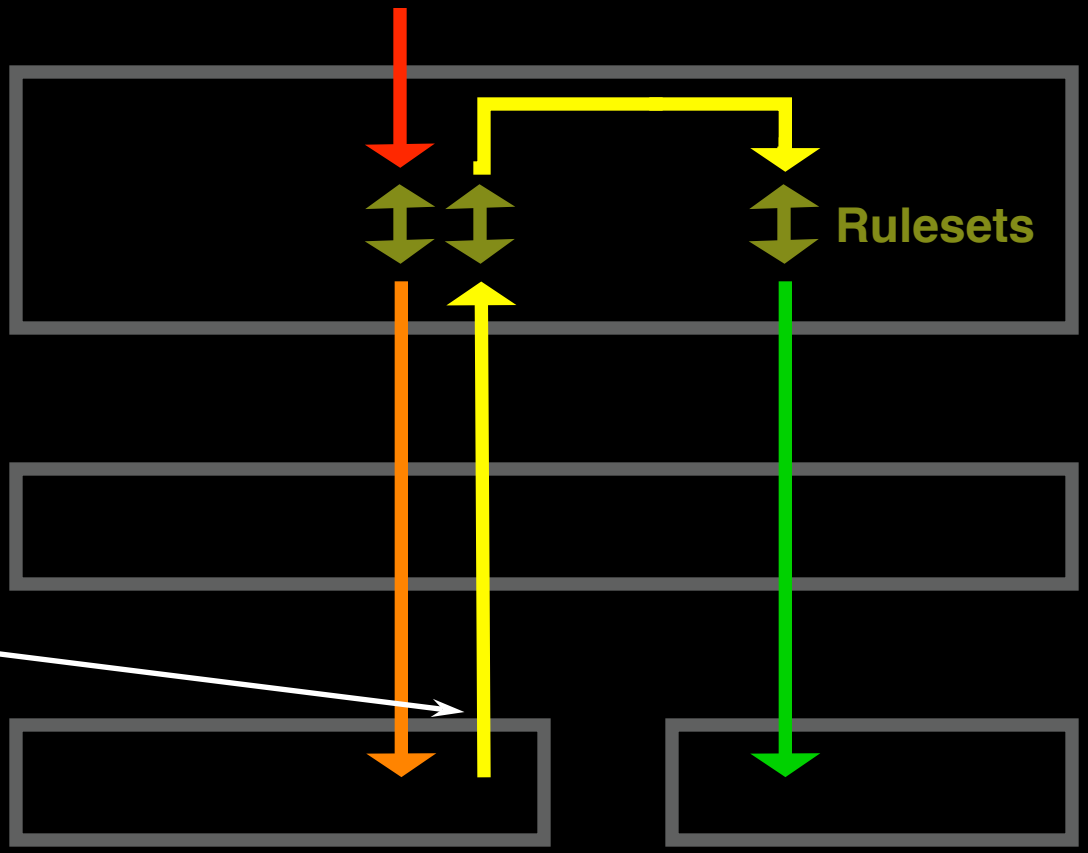
PCH
Packet Clearing House

Example With VPN Endpoint



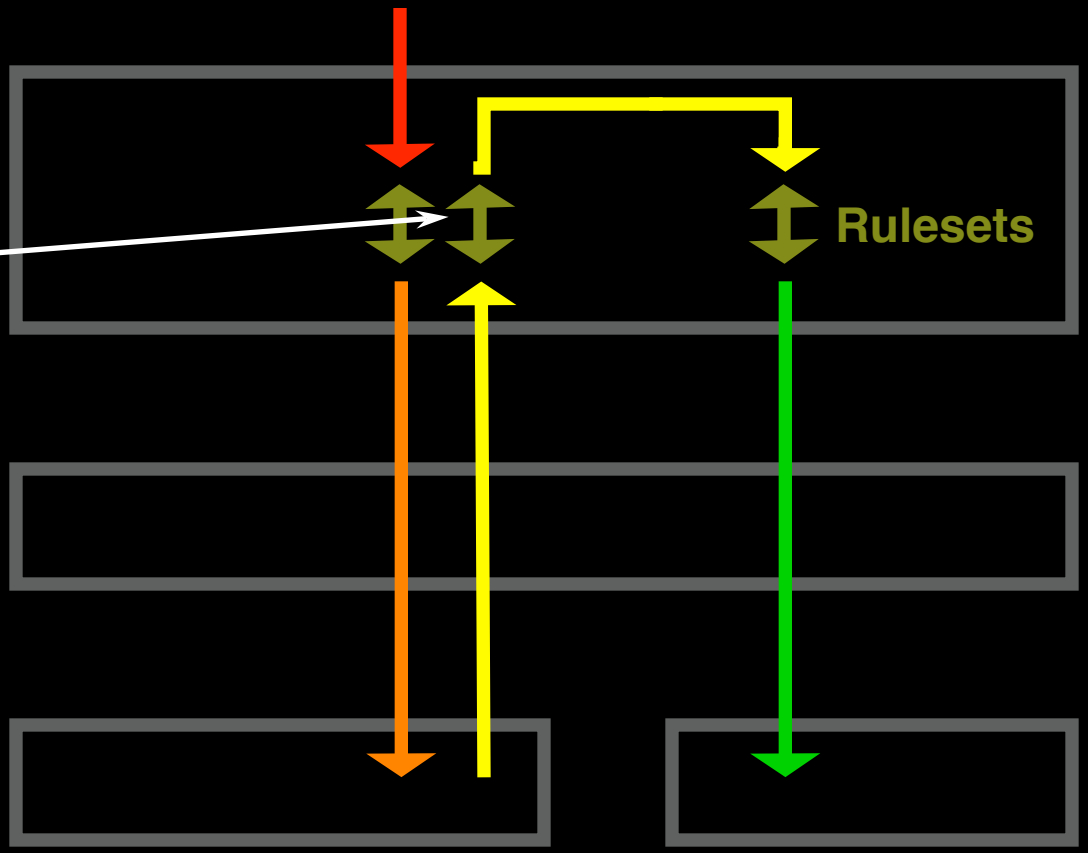
PCH
Packet Clearing House

Example With VPN Endpoint



PCH
Packet Clearing House

Example With VPN Endpoint

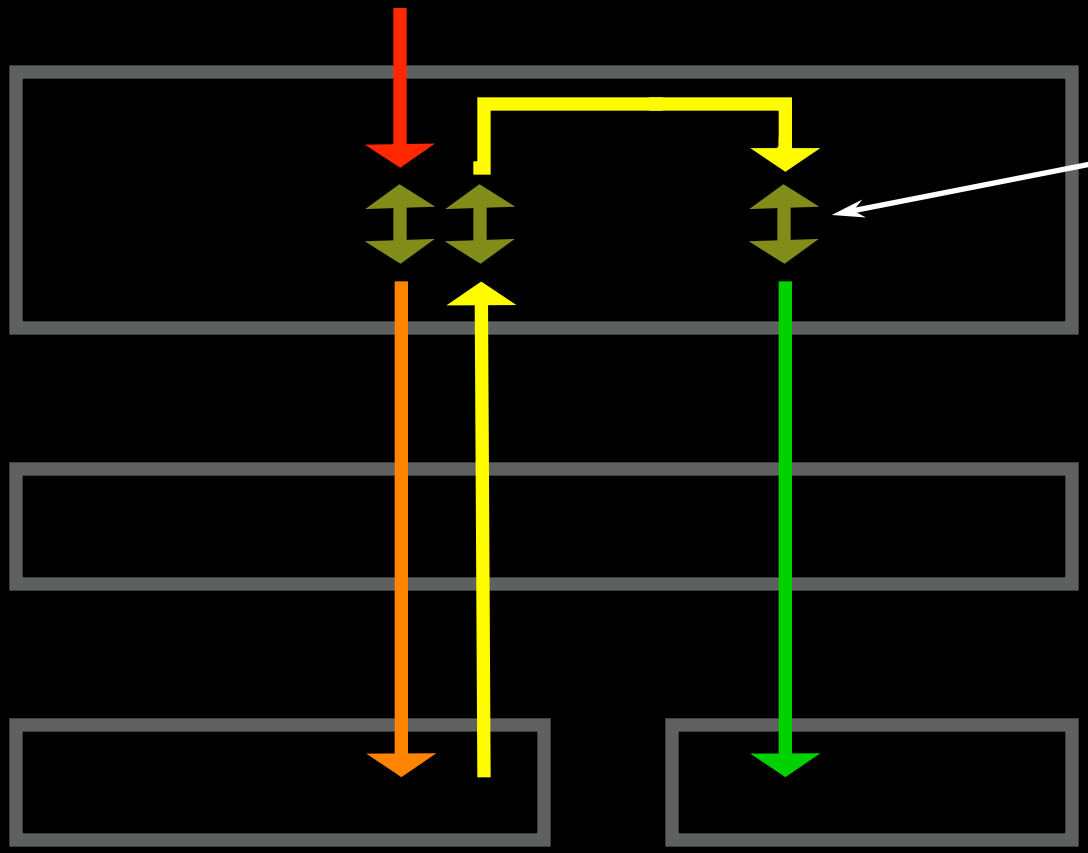


Second ruleset defines which internal resources VPN users are allowed access to

Users who have undergone visual authentication are differentiated from those who may have left a home terminal logged in

PCH
Packet Clearing House

Example With VPN Endpoint



Third ruleset defines which services are accessible on each particular server

PCH
Packet Clearing House

Thanks, and Questions?

Copies of this presentation can be found
in Keynote, PDF, QuickTime and PowerPoint formats at:

http:// www.pch.net / resources / tutorials / vlan-based-security

Bill Woodcock
Research Director
Packet Clearing House
woody@pch.net