

# **VLAN-Based Security for Modern Service-Provision Networks**

**Version 3.0**

**October, 2008**

**Bill Woodcock, Gaurab Raj Upadhaya**

**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.

# 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.

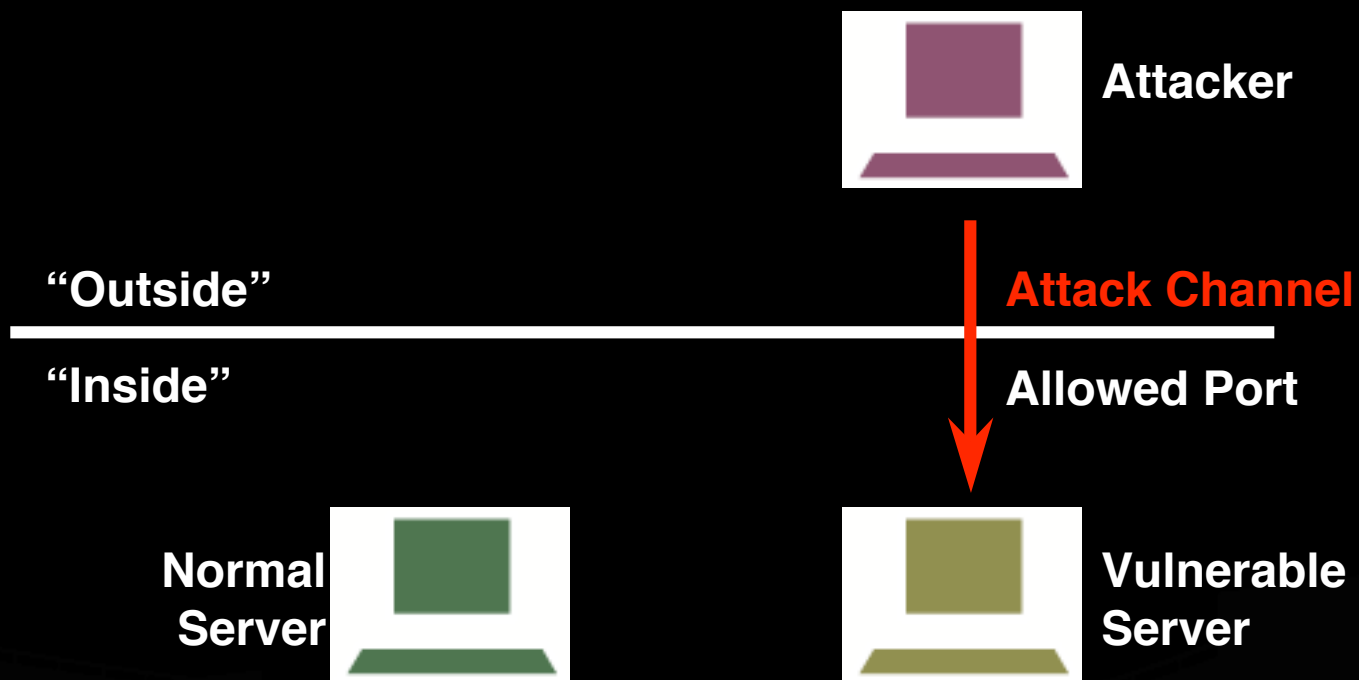
# Old Enterprise Solution:

- 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.

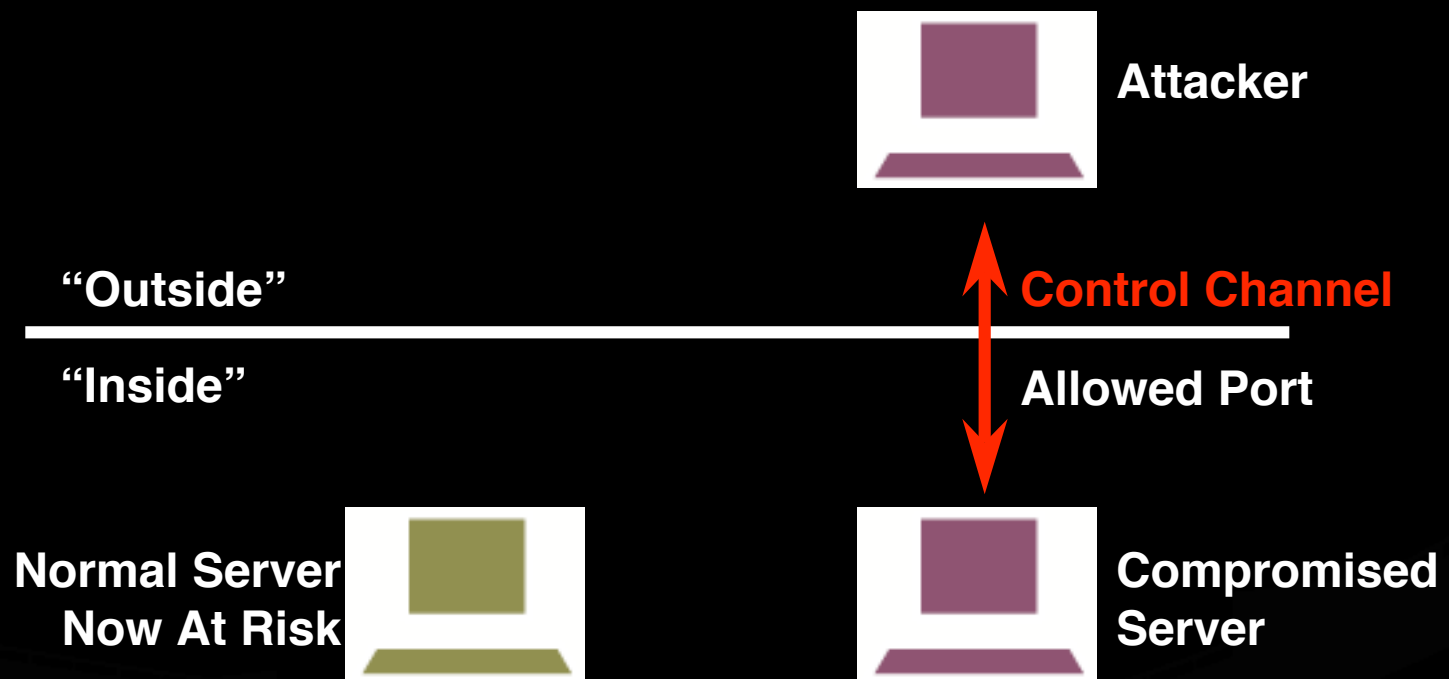
# Stepping-Stone Attack



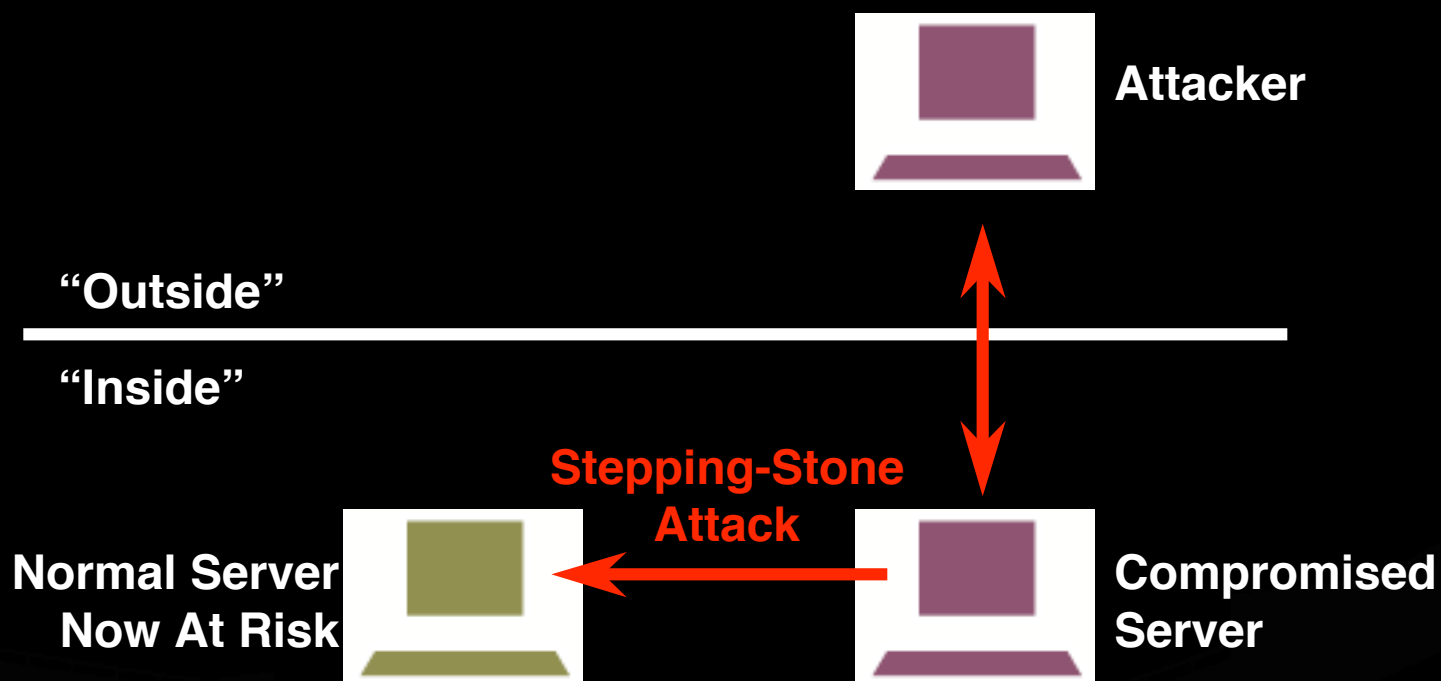
# Stepping-Stone Attack



# Stepping-Stone Attack

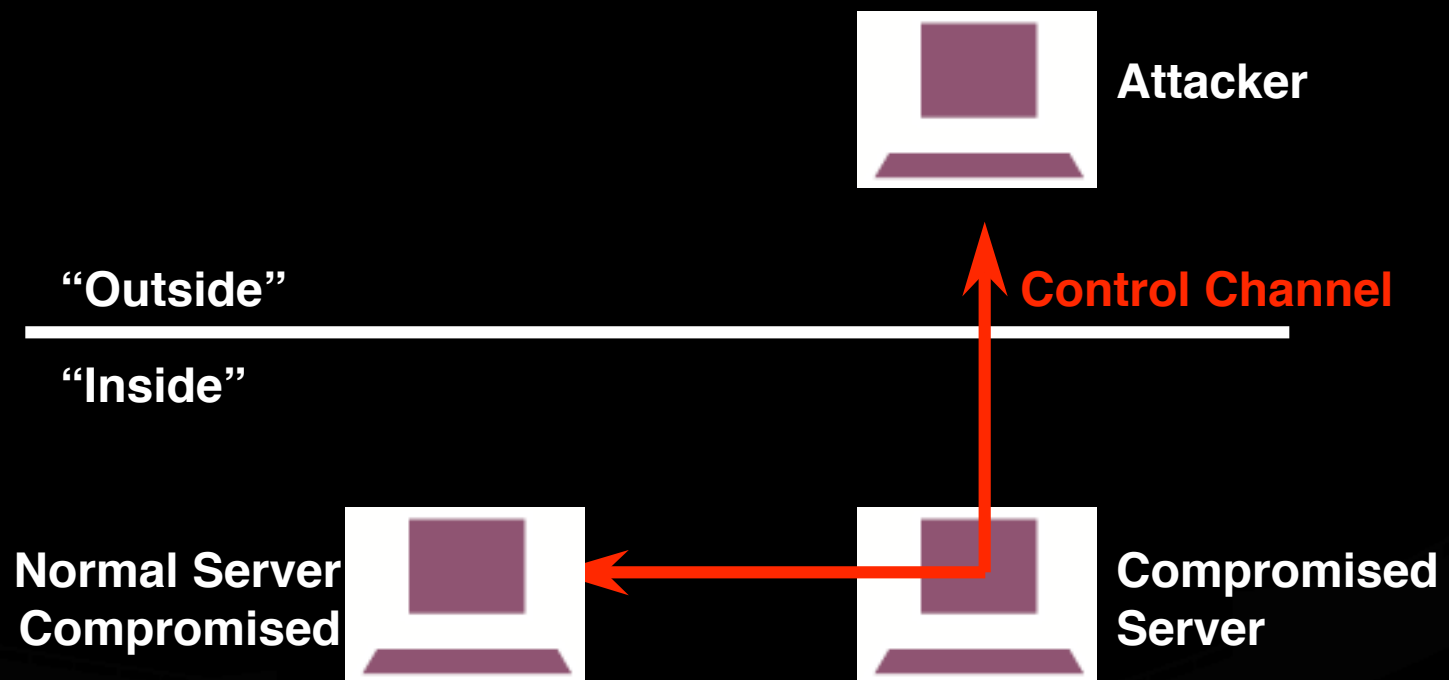


# Stepping-Stone Attack

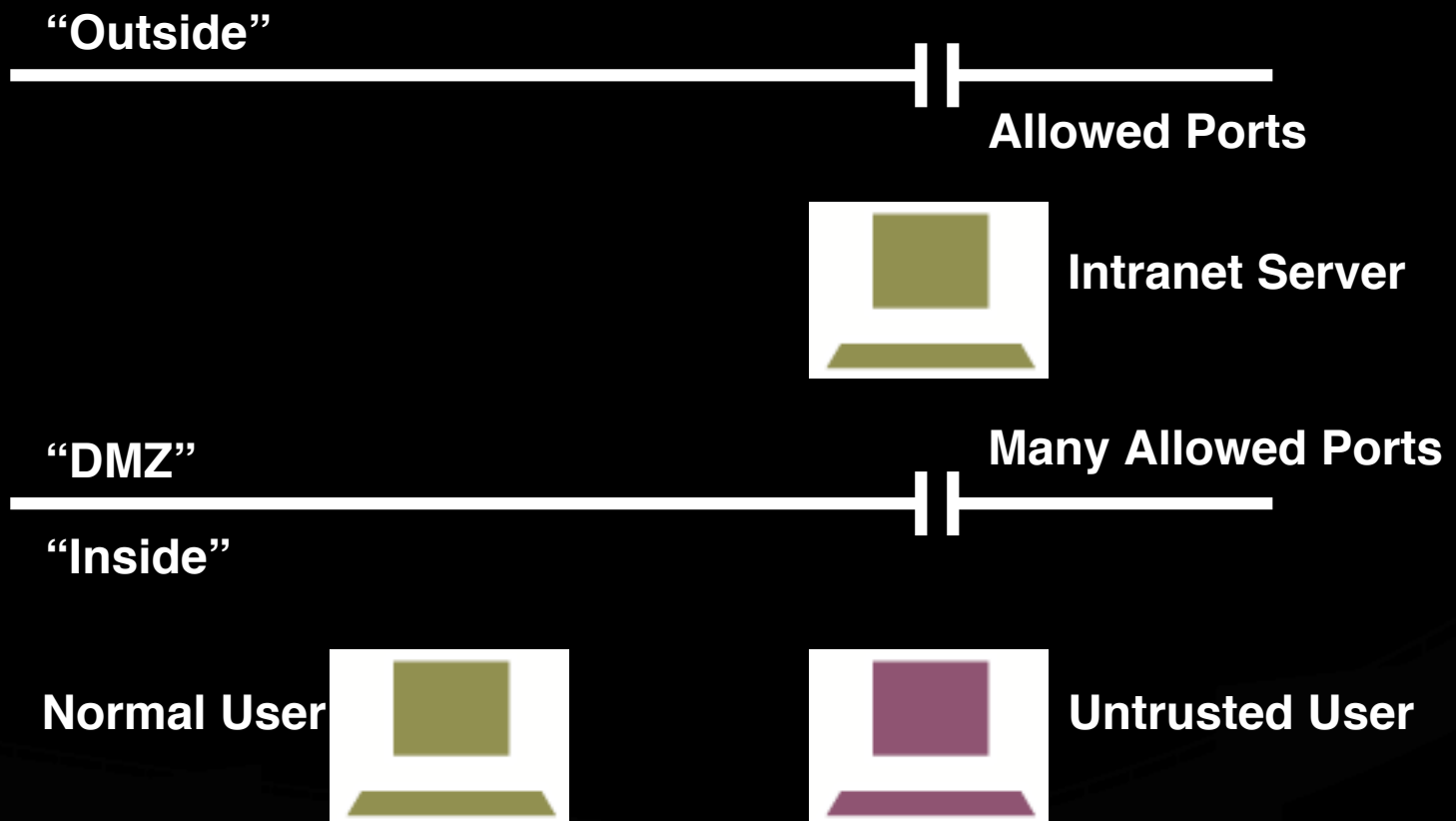




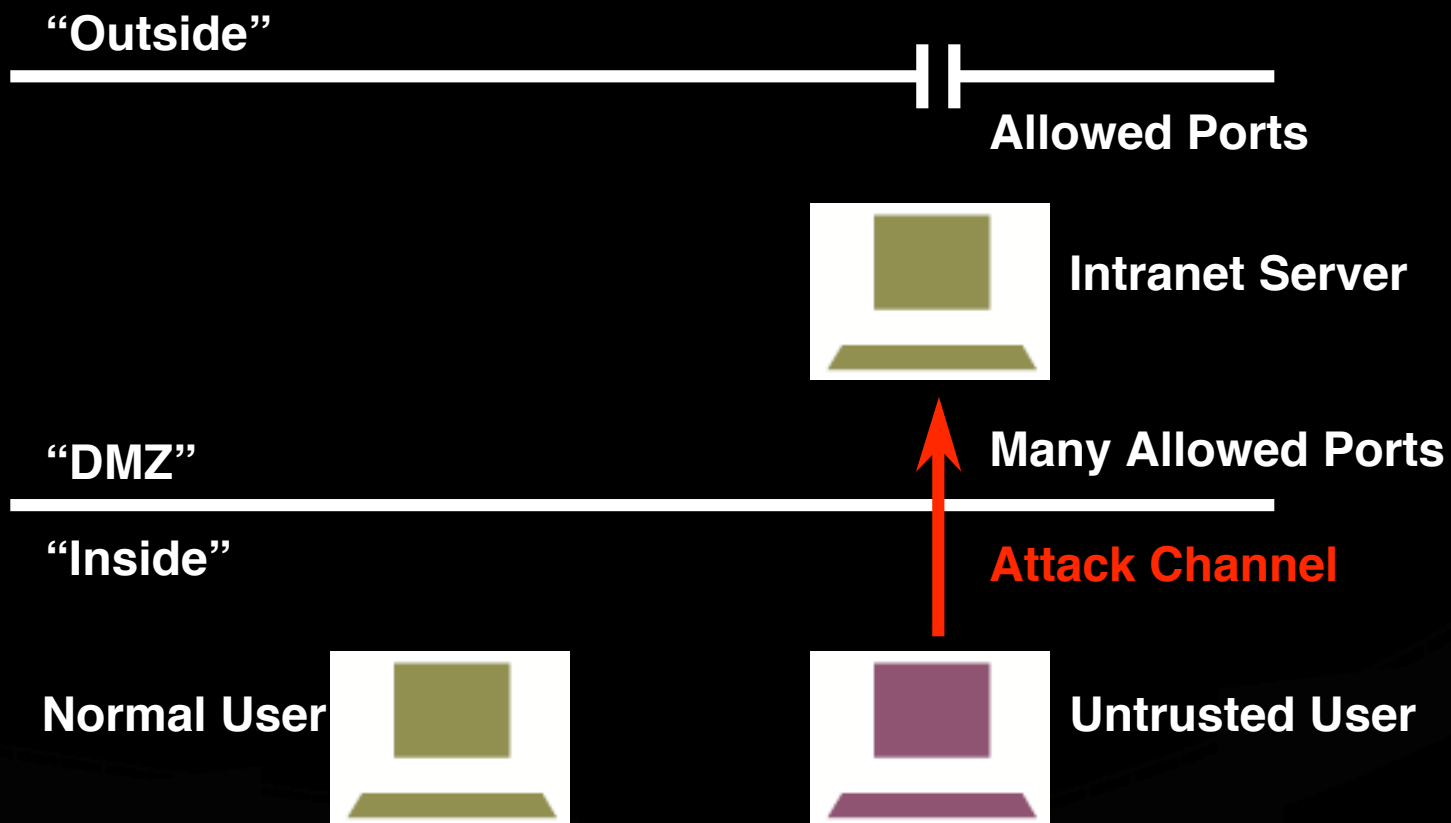
# Stepping-Stone Attack



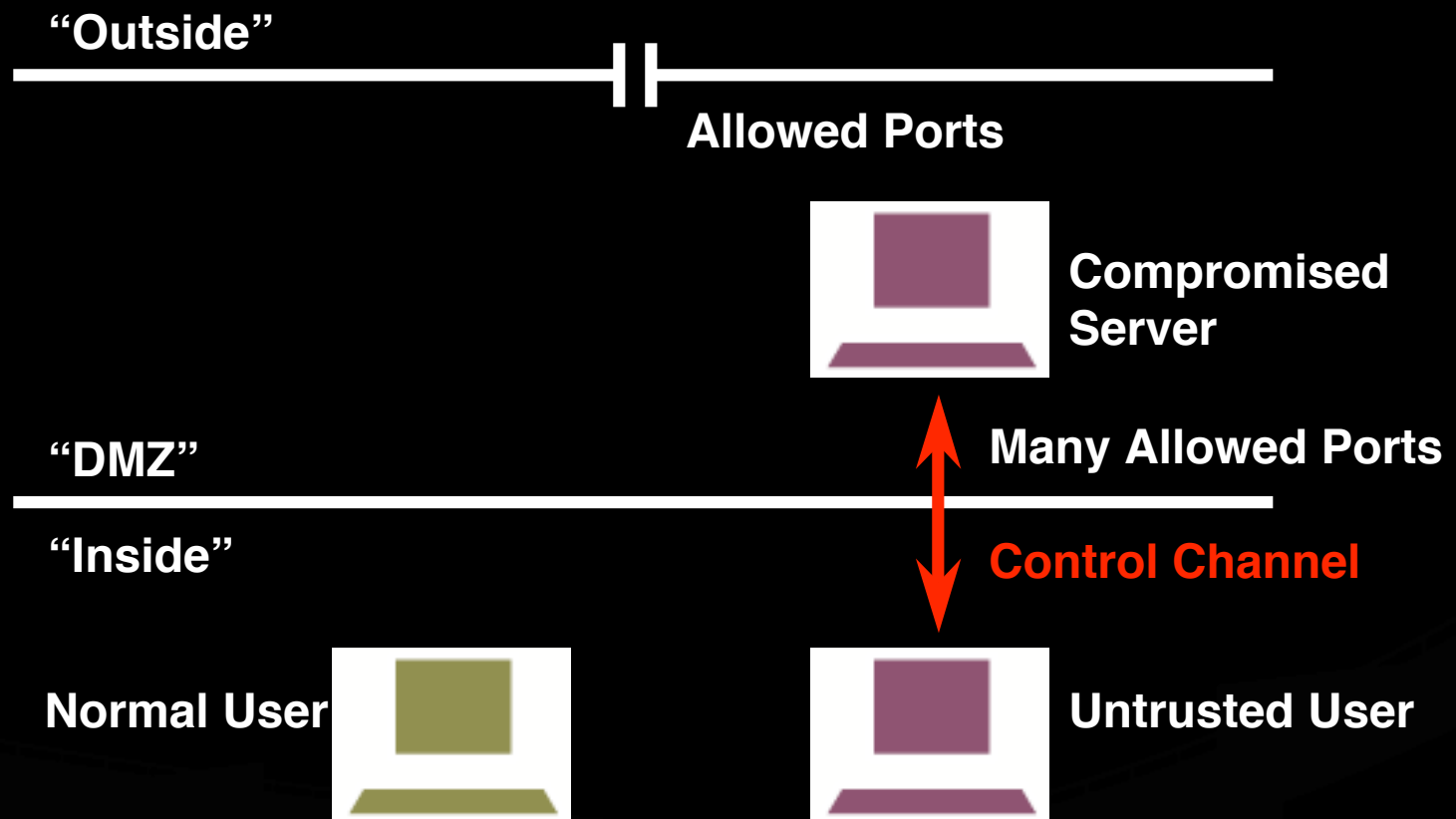
# Untrusted User Attack



# Untrusted User Attack



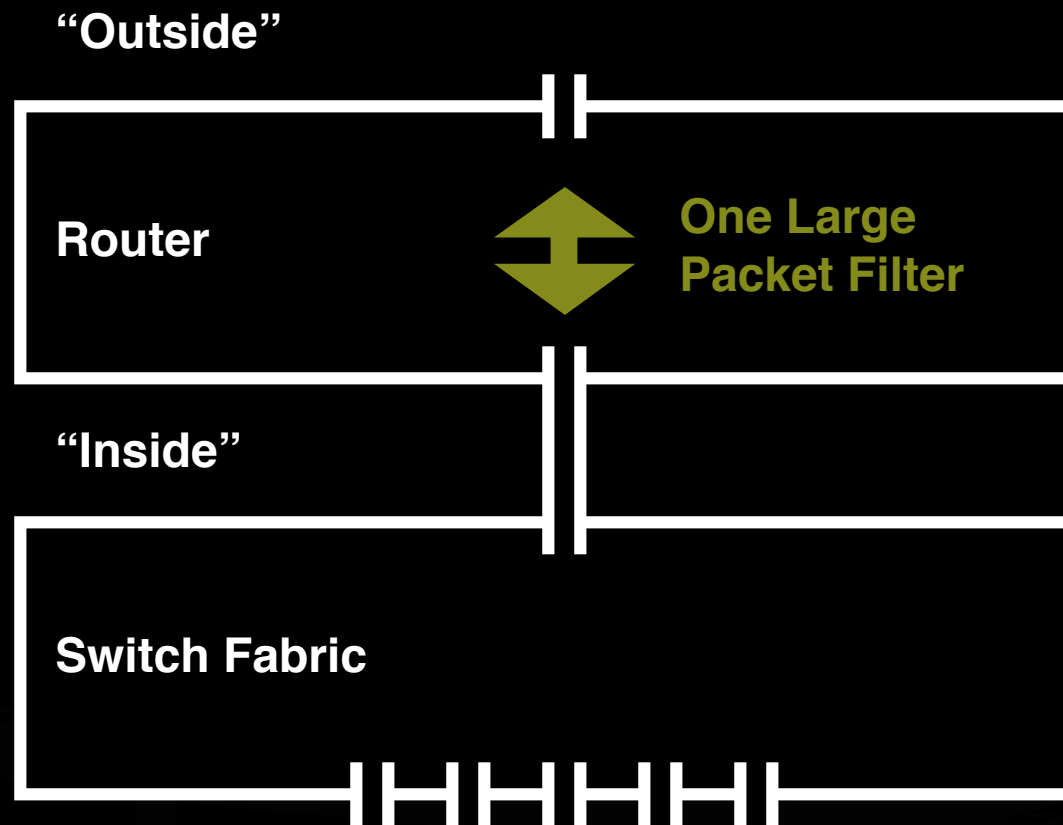
# Untrusted User Attack



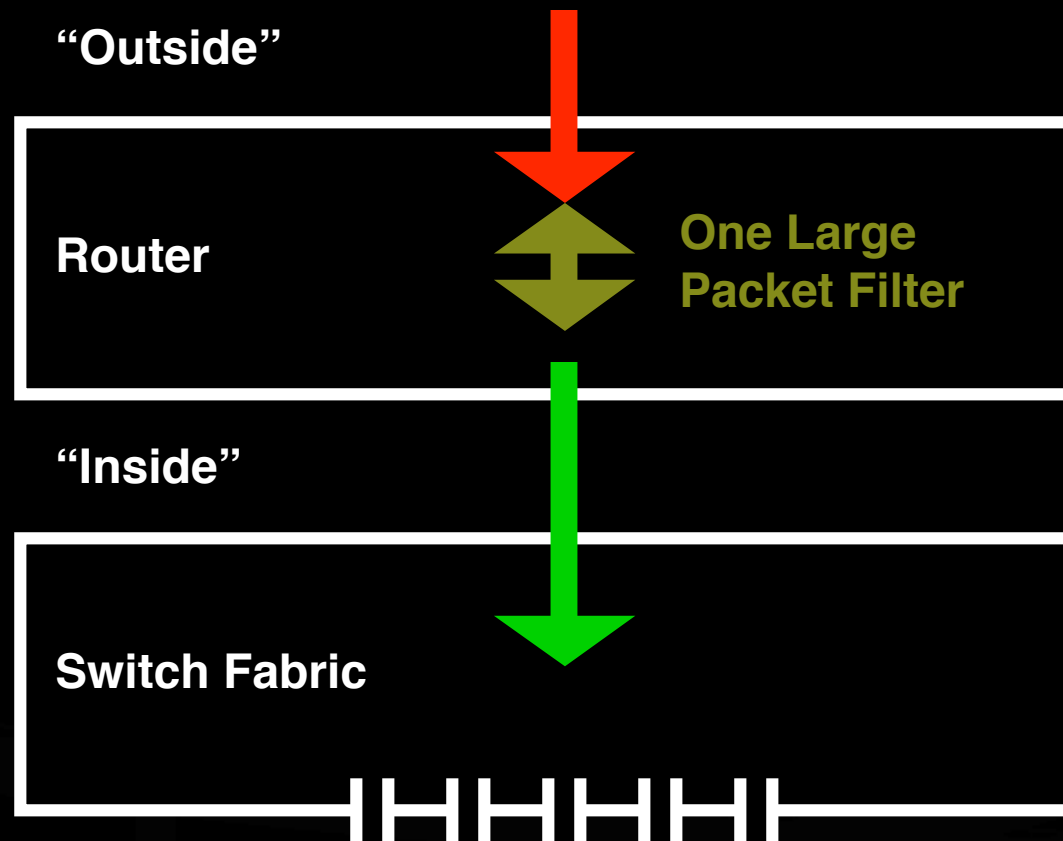
# Modern Firewalling

- 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.

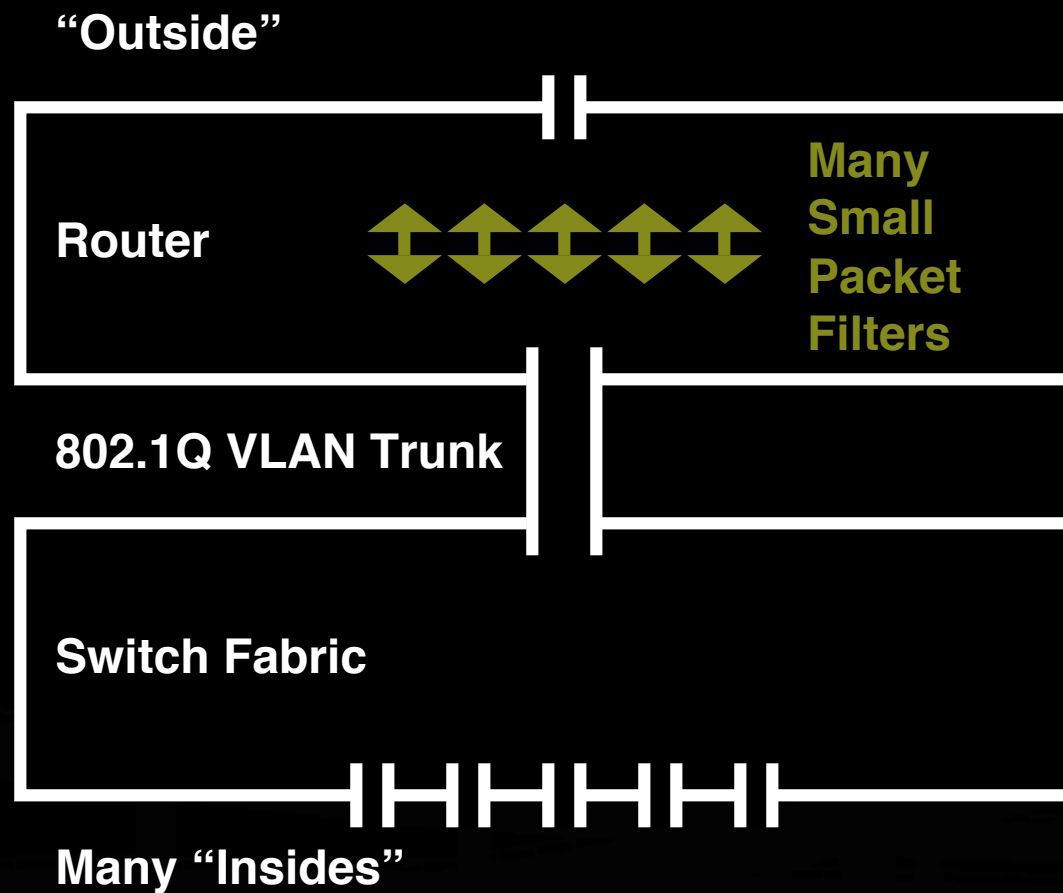
# Simple Packet Filter



# Simple Packet Filter

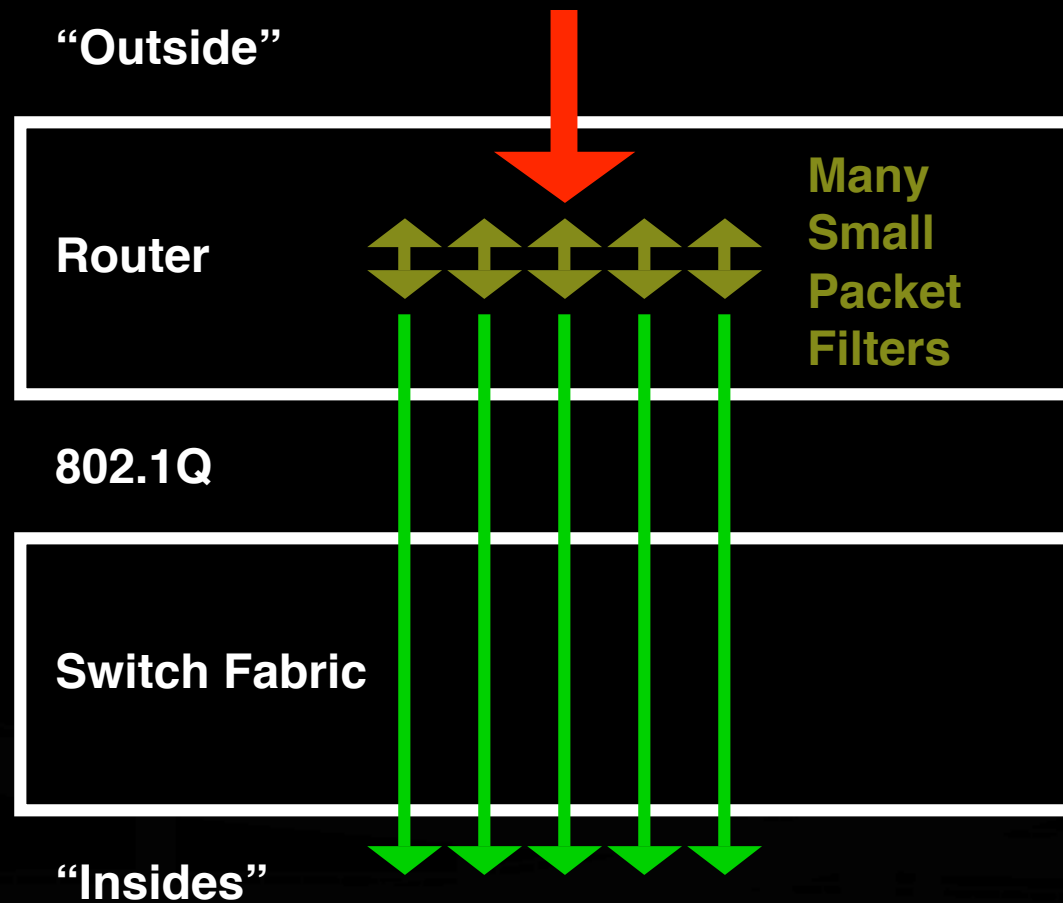


# VLAN-Based Firewalling

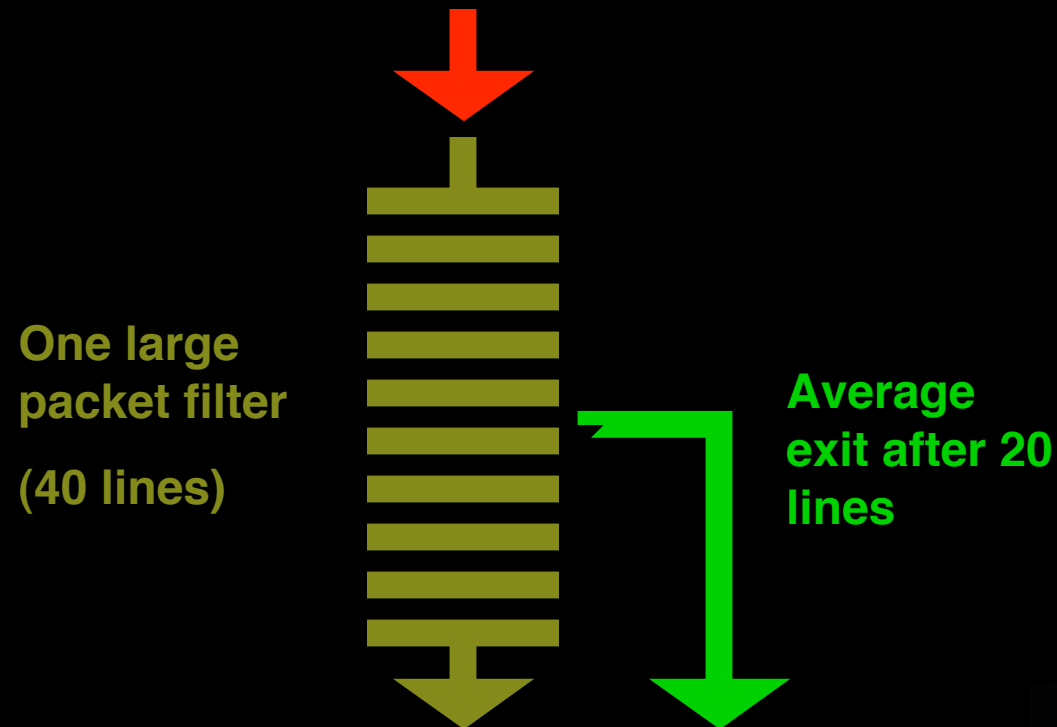




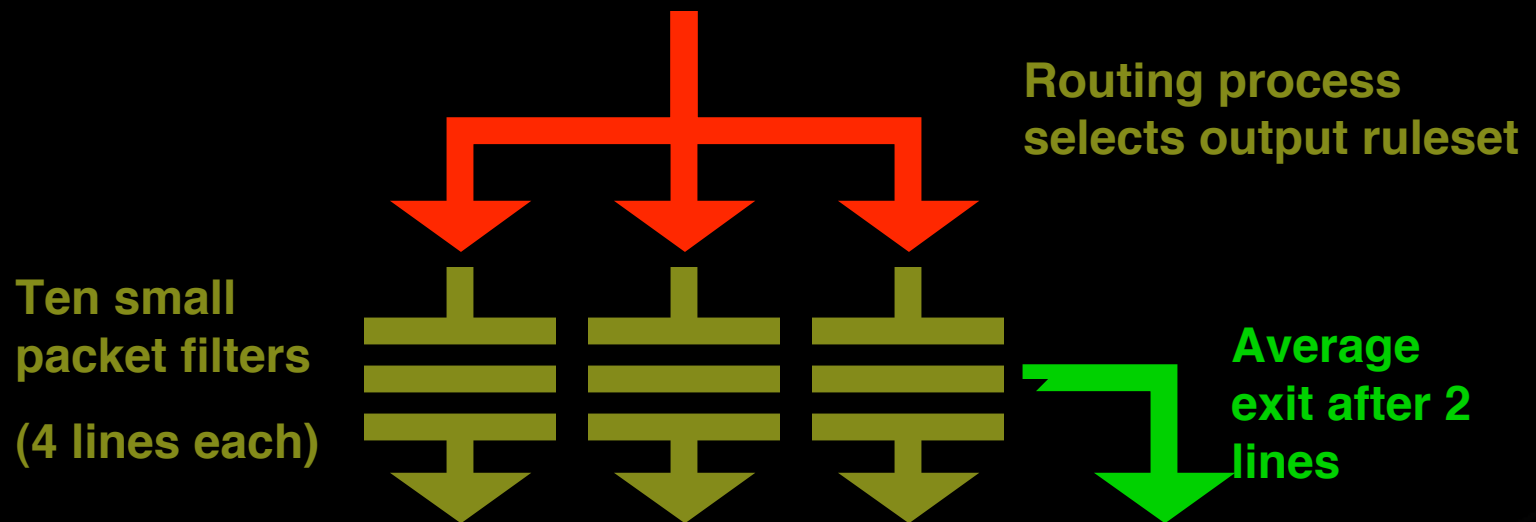
# VLAN-Based Firewalling



# Relative Processing Speed



# Relative Processing Speed



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

# What This Looks Like: Switch

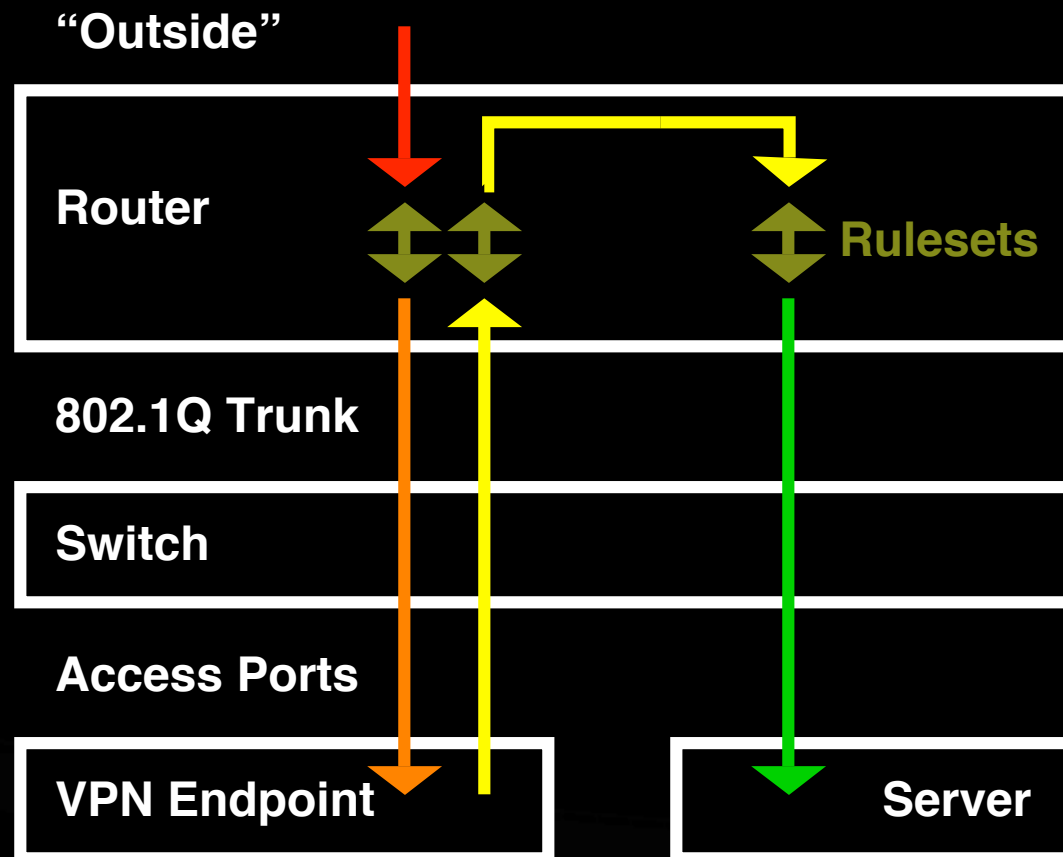
```
hostname OAK-Switch-3
!  
interface FastEthernet0/41  
  description VLAN_341-OAK_DNS-131.161.2.0/30  
  switchport access vlan 341  
  speed 100  
  full-duplex
```

```
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....
```

# What This Looks Like: Router

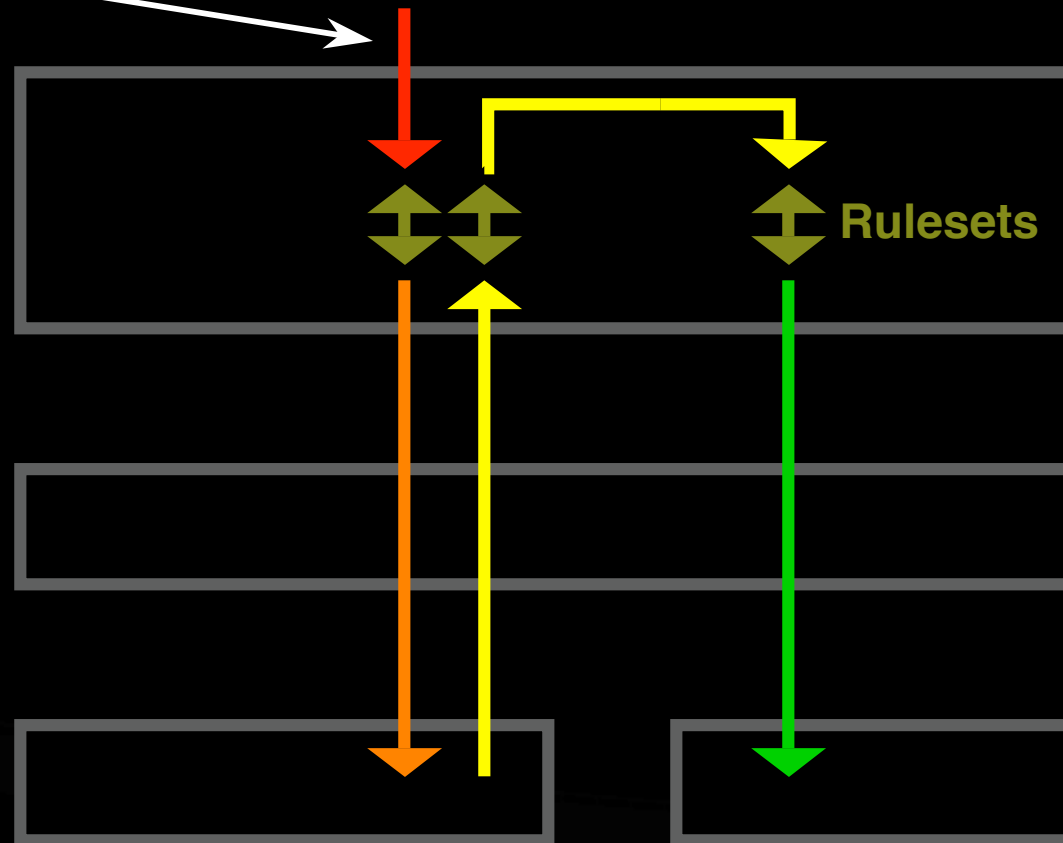
```
hostname OAK-Firewall
!
interface FastEthernet0/0
  description 802.1Q VLAN Trunk to OAK-Switch-1
  no ip address
  speed 100
  full-duplex
!
interface FastEthernet0/0.341
  description VLAN_341-OAK_DNS-131.161.2.0/30
  encapsulation dot1Q 341
  ip address 131.161.2.2 255.255.255.252
  ip access-group 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
```

# Example With VPN Endpoint

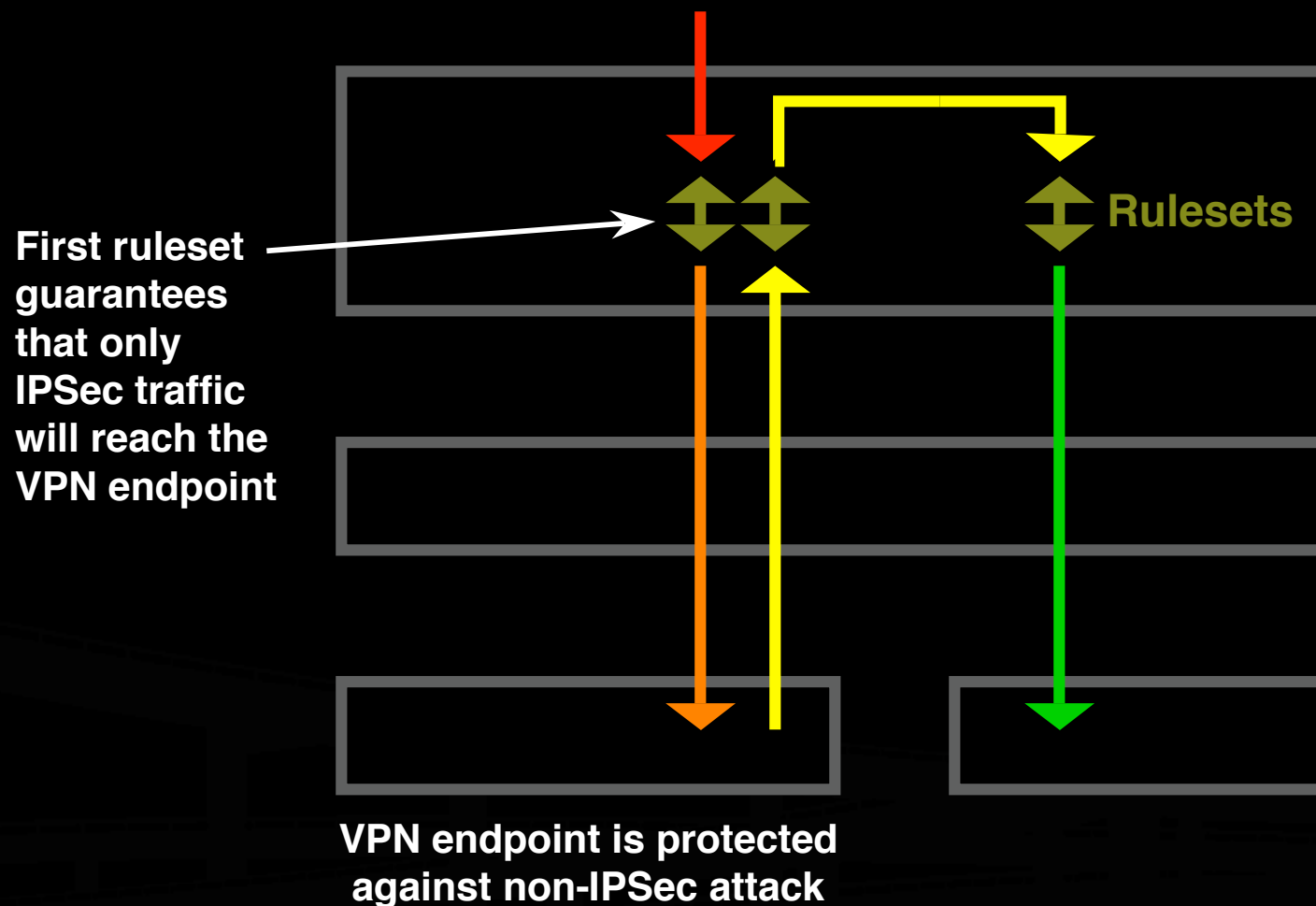


# Example With VPN Endpoint

Traffic enters  
network from  
the  
commodity  
network

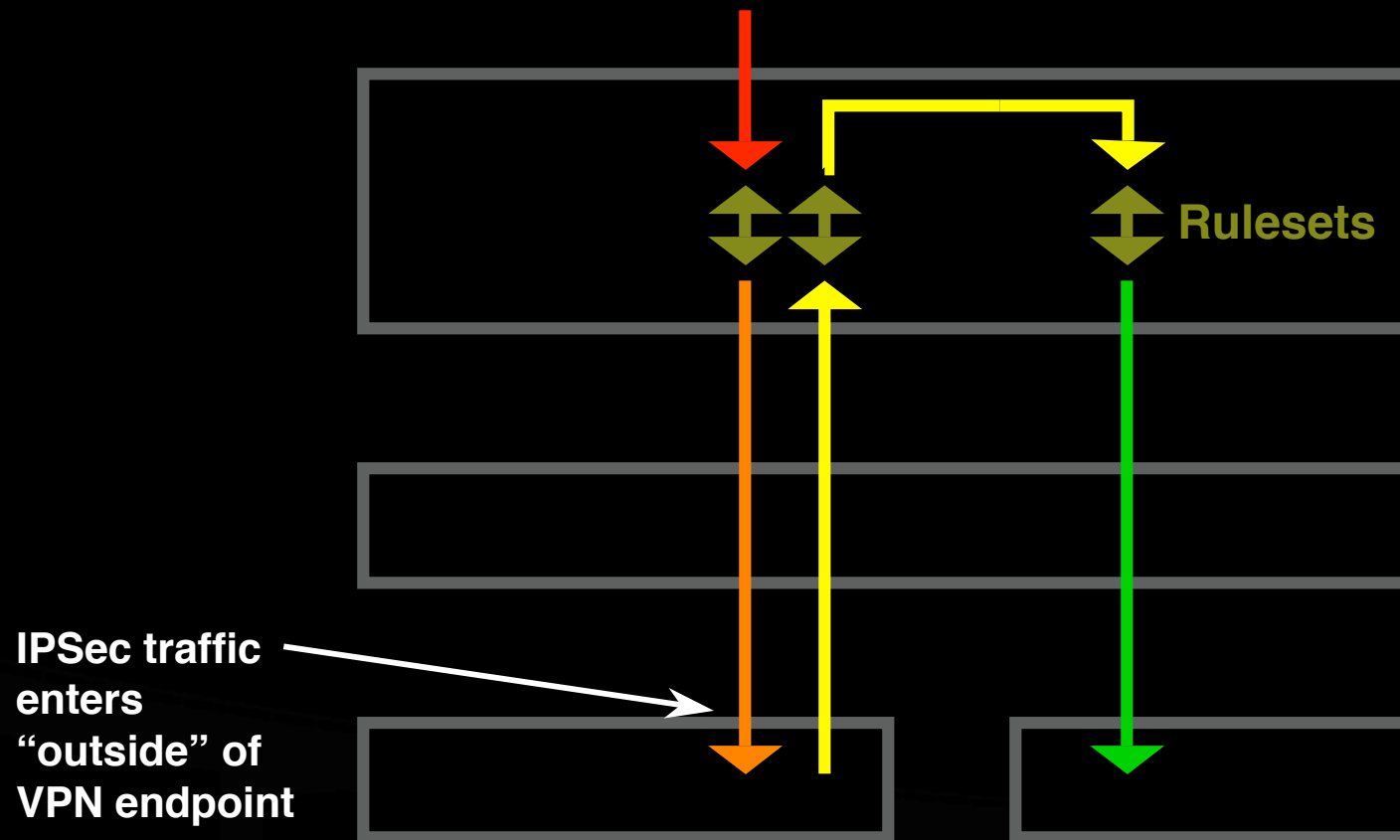


# Example With VPN Endpoint

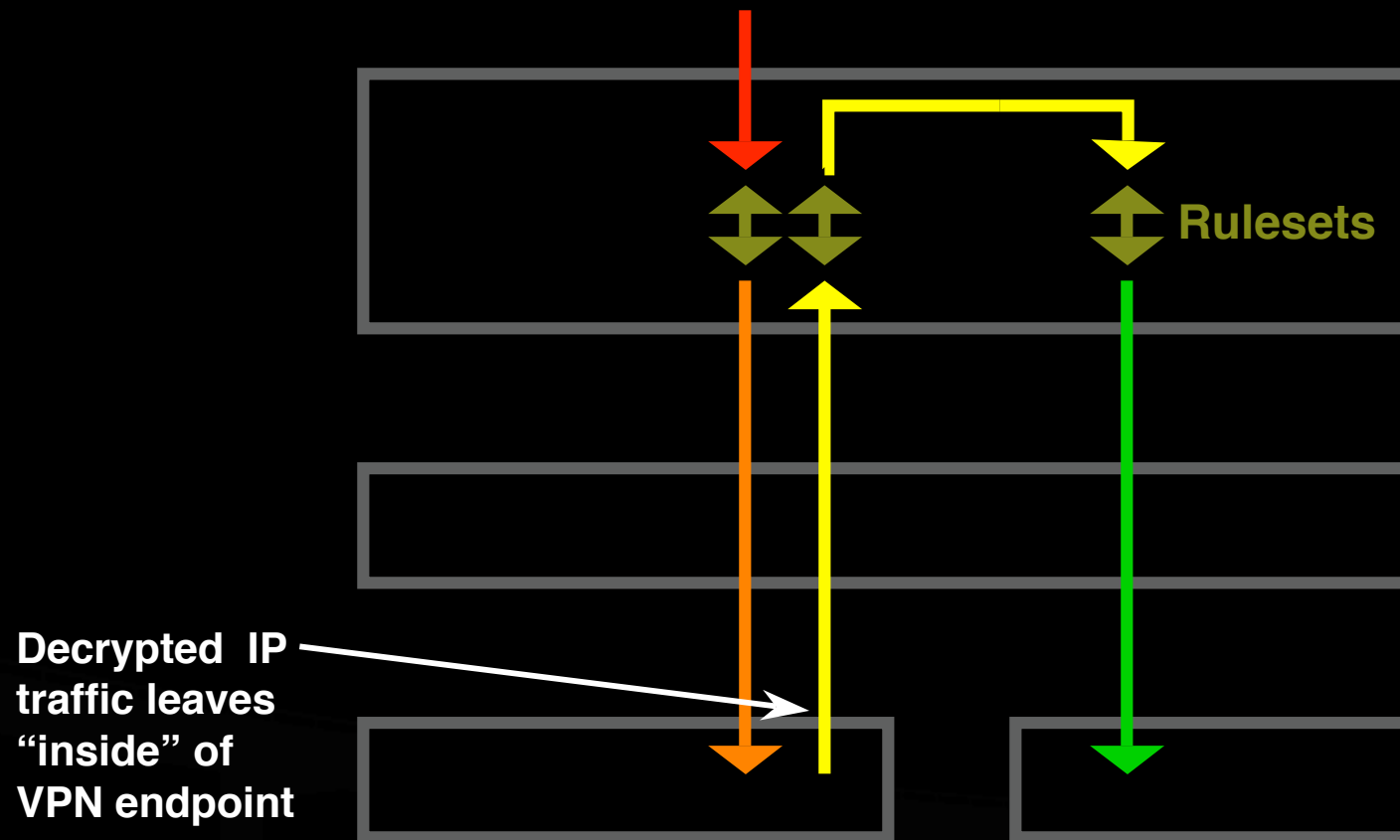




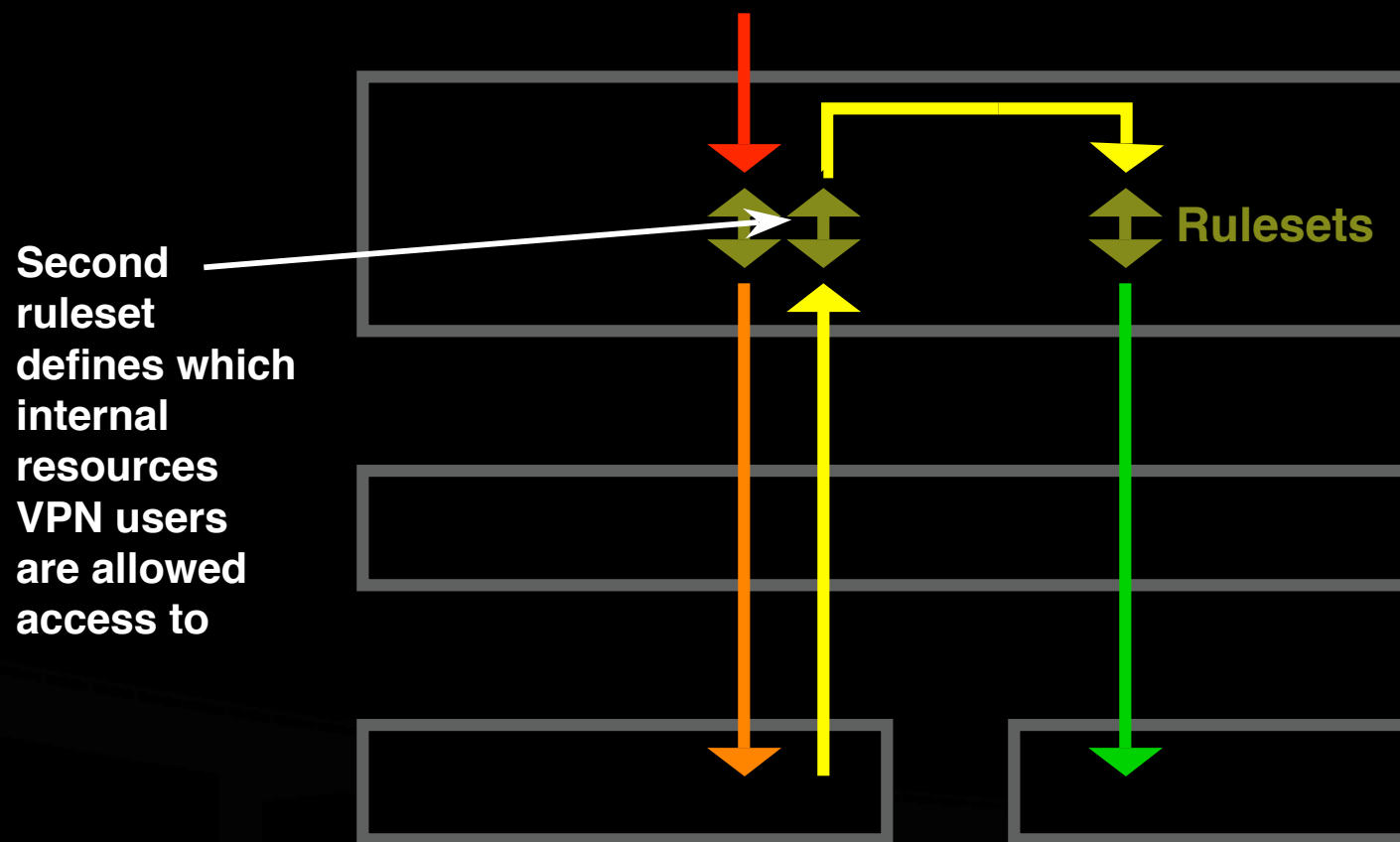
# Example With VPN Endpoint



# Example With VPN Endpoint



# Example With VPN Endpoint



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

# Example With VPN Endpoint

