

Securing Layer-2 Networks with Cisco Switches

Steve Birnbaum

KSAJ Inc.

Network and Security Consultant

www.PENETRATIONTEST.com

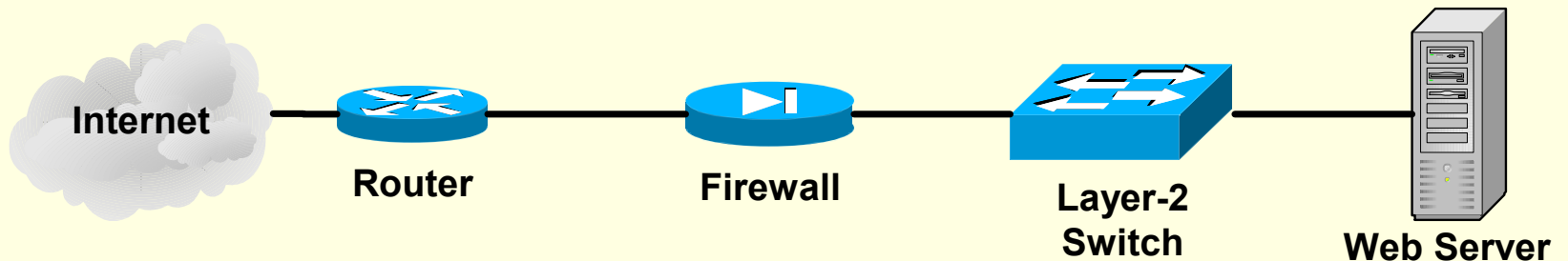
Agenda

- Common service network security issues
- Private VLANs
- VACL security solutions
- Other VACL ideas

Disclaimer : we don't work for Cisco and we don't have Cisco stock :-)

Insecure Practices Still Common

- Many service networks (DMZ) still based on simple design
- “Hard crunchy outside, soft chewy inside!”



Evolution of Current Practices

- Slow adoption of new technologies
- Firewall evolutions
 - Performance over security
- Intrusion Detection

Protection Inside the Perimeter

- Limited options to date
 - Port Security (MAC filtering)
 - Host-based packet filtering

MAC Address Filtering

```
set port security <mod/port> enable 01-02-03-04-05-06 shutdown
```

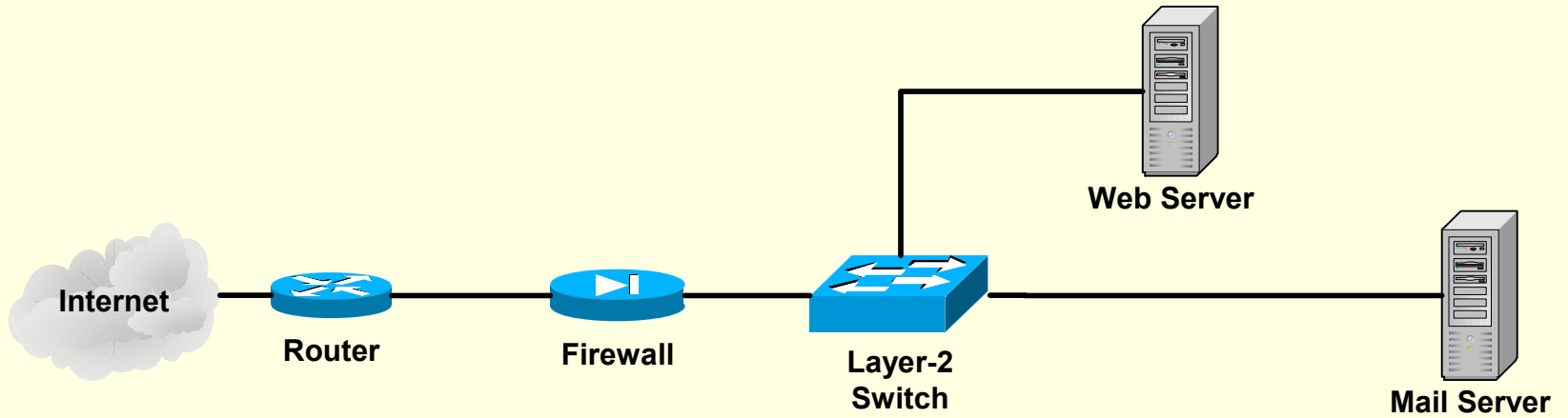
Limitations:

- Only secures which devices can connect
- No control of traffic
- Problems with High Availability solutions
- Requires network reconfiguration for hardware changes
- Potential for input errors on MAC addresses

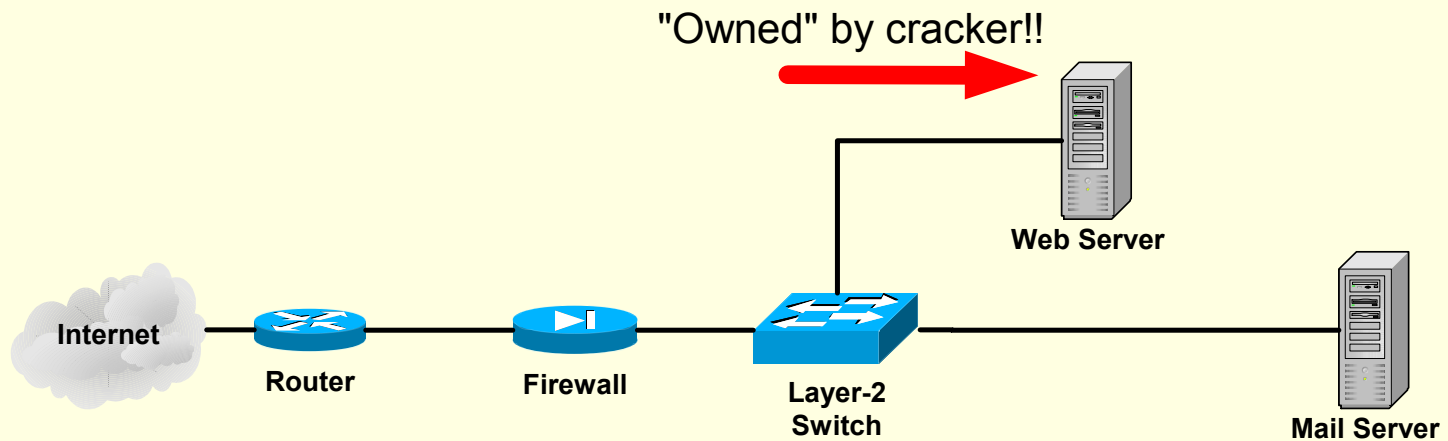
Host-based Packet Filtering

- Each OS has its own method or syntax
- Hard to maintain; certainly not scalable
- No central management
- Bugs, vulnerabilities, features...all different

Problems With Soft Networks

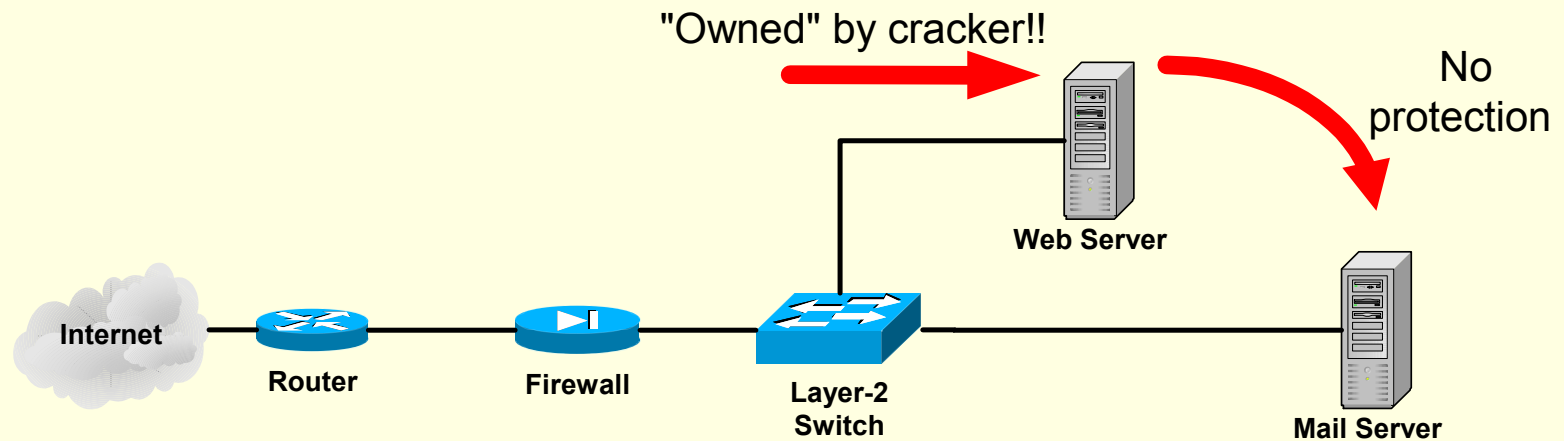


Problems With Soft Networks



- Intruder has found a vulnerability in the web server
- ...Hard work is now done!

Problems With Soft Networks



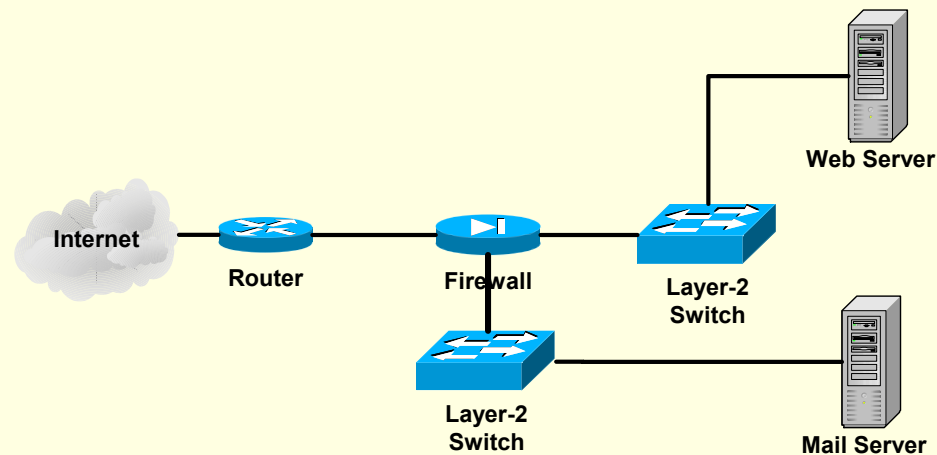
- Intruder can now move from system to system

Fundamentally, what is the goal?

A proper level of security is achieved when it is at least as difficult to break into the subsequent systems as the first.

Additional Segmentation

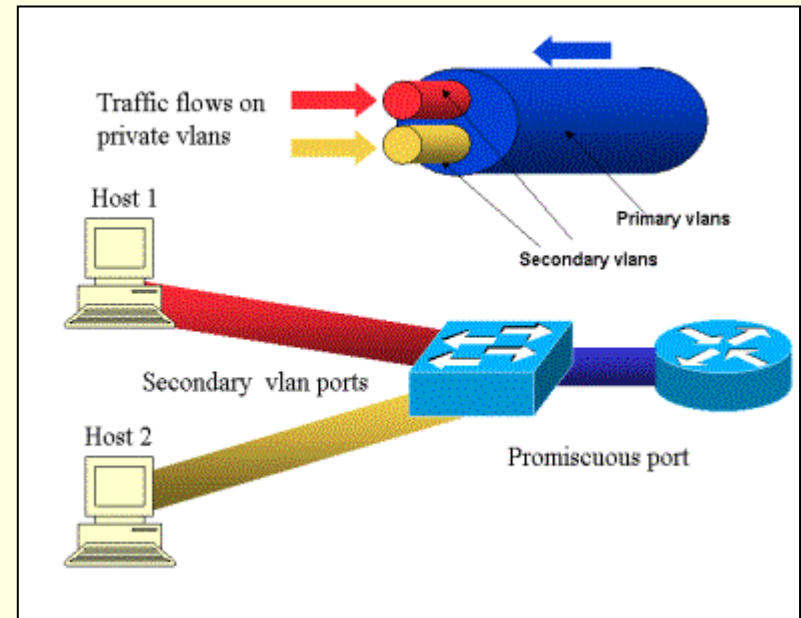
- Add new firewall interfaces for each system or zone
 - Does not scale well
 - Difficult to manage policy
 - No logical policy



Private VLANs

- Keep a logical separation of networks
- Administratively easy to design
- Keeps traffic isolated
- Very scalable
 - Limited only by maximum available VLANs (macreduction)

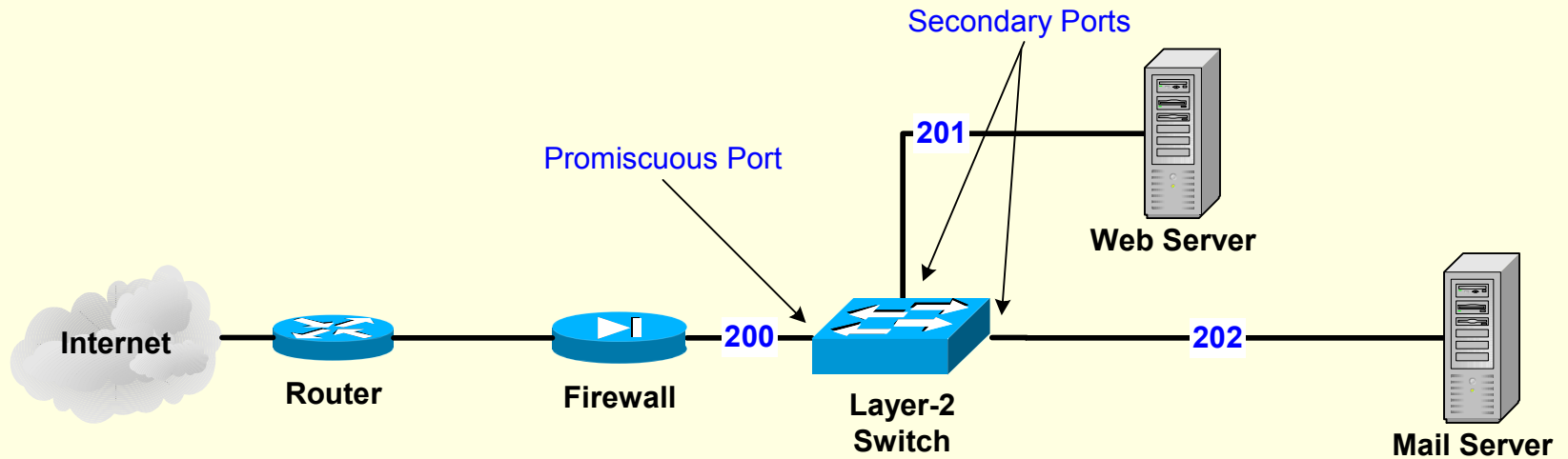
```
set spantree macreduction enable
```



Configuring Private VLANs

- Isolated:
 - Can only talk to promiscuous ports
- Community:
 - Similar to isolated, but systems on ports within the PVLAN can communicate with each other
 - Suggested use: HA systems, highly dependant servers
- Promiscuous:
 - Can communicate with hosts on mapped community and isolated ports
 - Suggested use: routers, firewalls

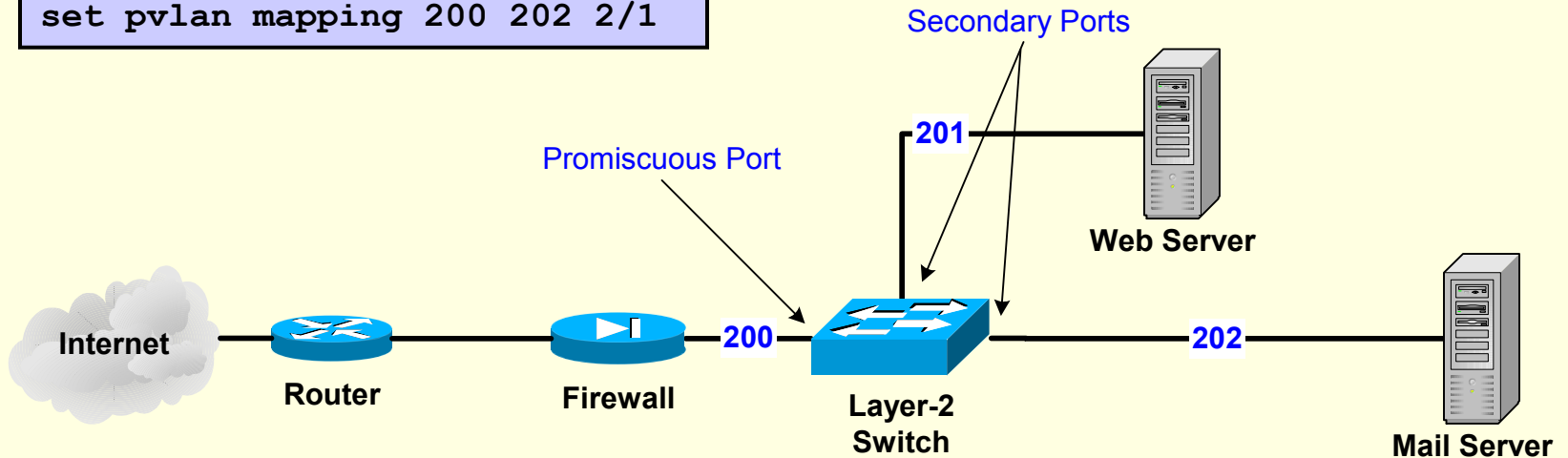
Configuring Private VLANs



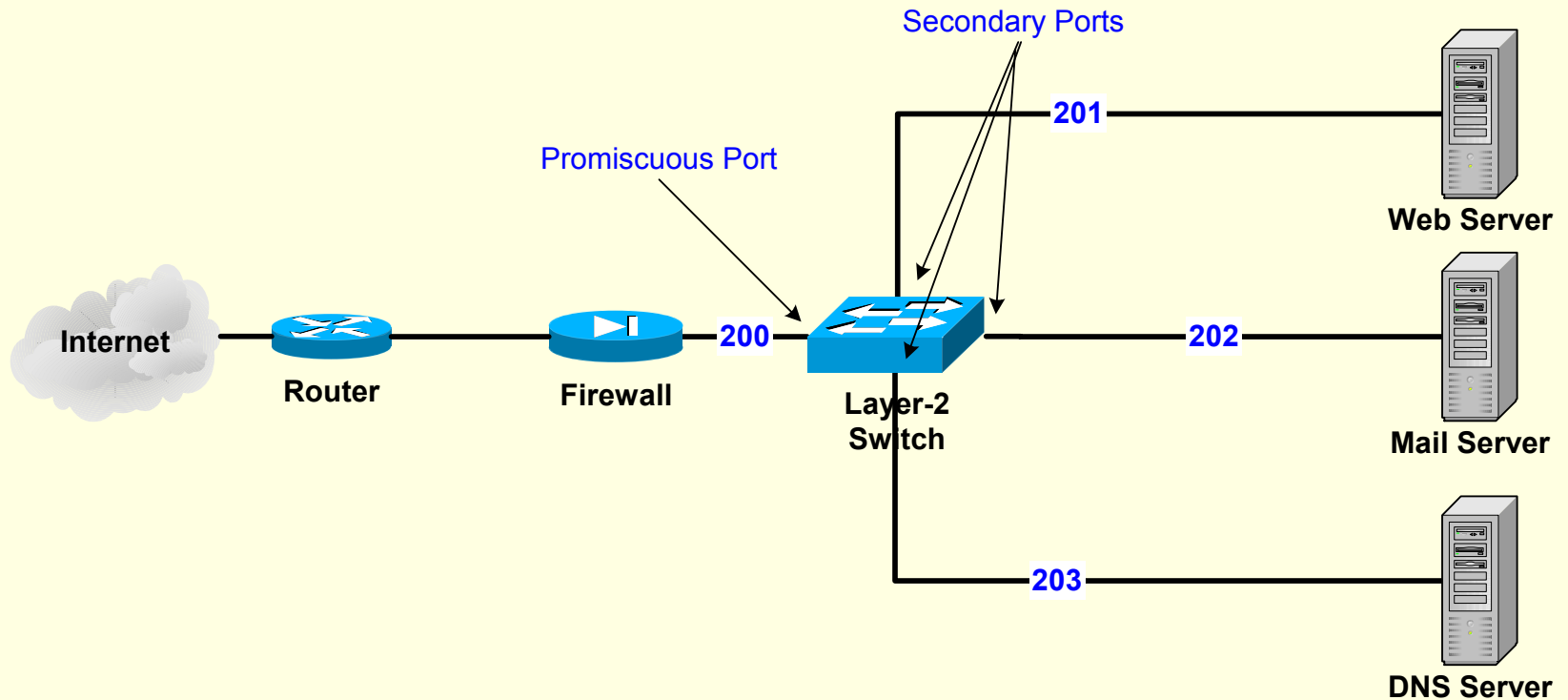
Configuring Private VLANs

```
set pvlan 200 201 3/1
set pvlan 200 202 3/2

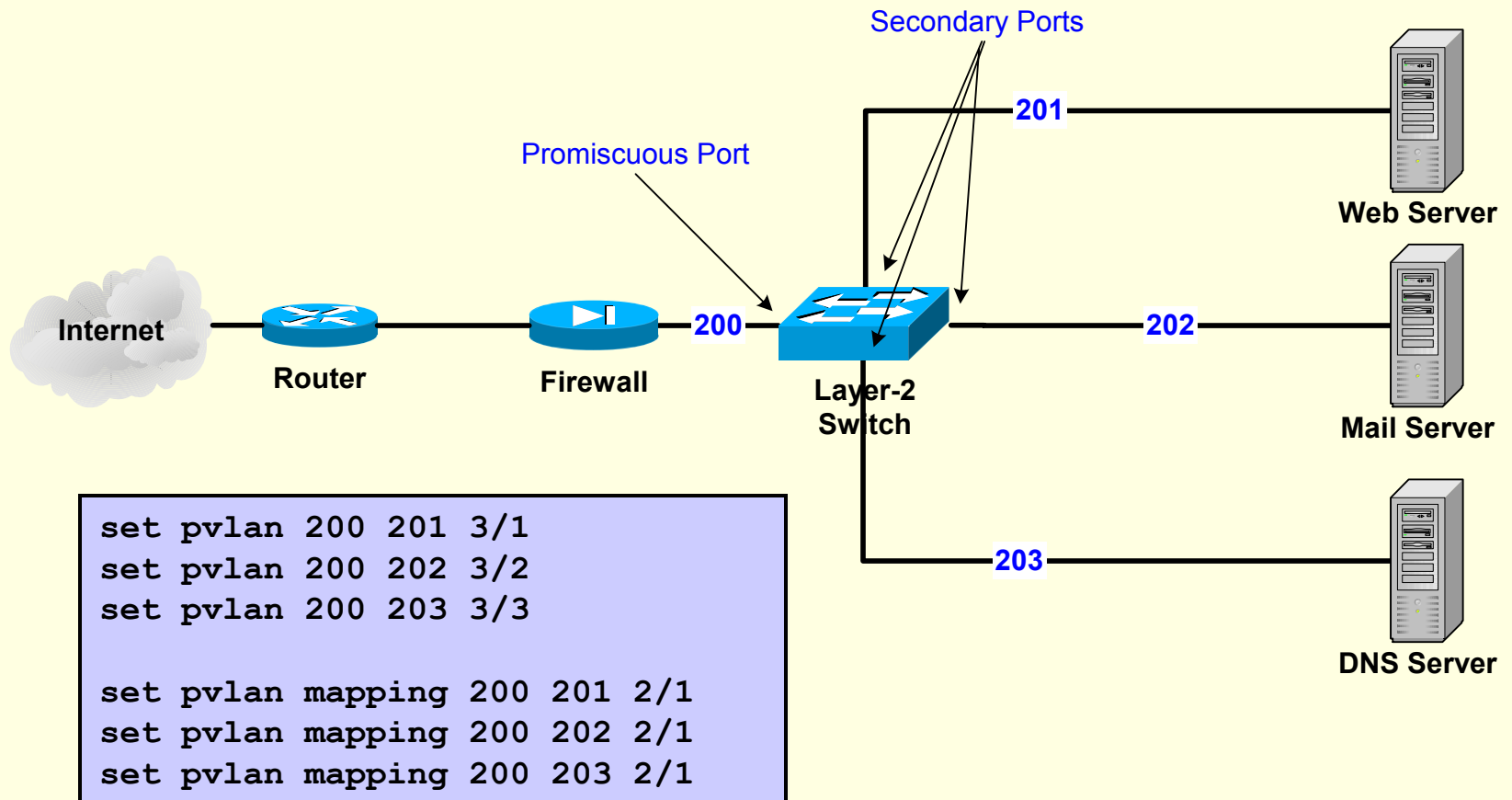
set pvlan mapping 200 201 2/1
set pvlan mapping 200 202 2/1
```



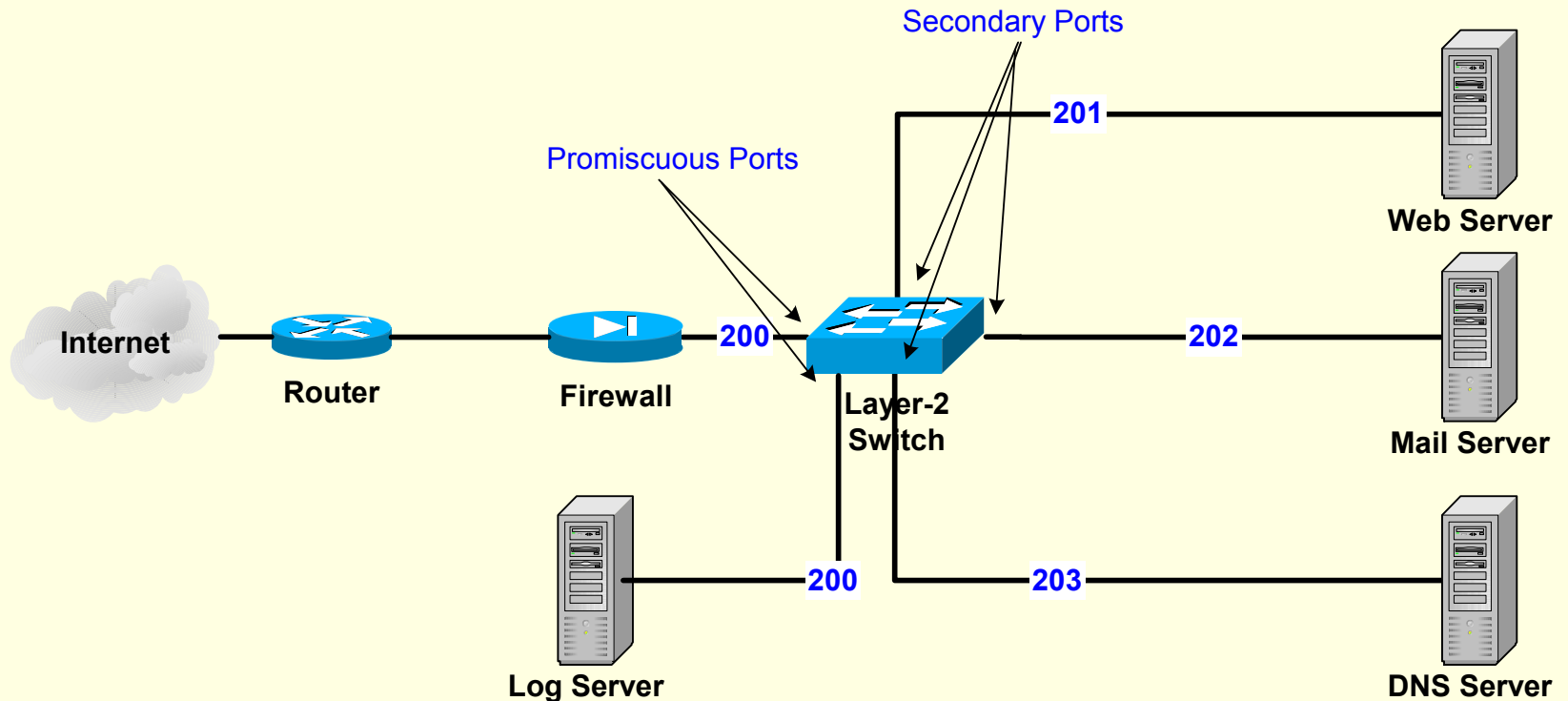
Possible Scenarios: Adding a public DNS server



Possible Scenarios: Adding a public DNS server



Possible Scenarios: Adding a log server



Possible Scenarios: Adding a log server

- Multiple promiscuous ports
- Log server now vulnerable to attack from community & isolated systems
- Minimize the connectivity
 - Do not have to map all PVLANS to all promiscuous ports

Possible Scenarios: Adding a log server

- Multiple promiscuous ports
- Log server now vulnerable to attack from community & isolated systems
- Minimize the connectivity
 - Do not have to map all PVLANS to all promiscuous ports

```
set pvlan 200 201 3/1
set pvlan 200 202 3/2
set pvlan 200 203 3/3

set pvlan mapping 200 201 2/1
set pvlan mapping 200 202 2/1
set pvlan mapping 200 203 2/1

set pvlan mapping 200 202 2/2
set pvlan mapping 200 203 2/2
```

Multiple Promiscuous Ports

- Not limited to one promiscuous port for a primary VLAN
- Promiscuous status defined per-port
- Some hardware limitations

Vulnerabilities

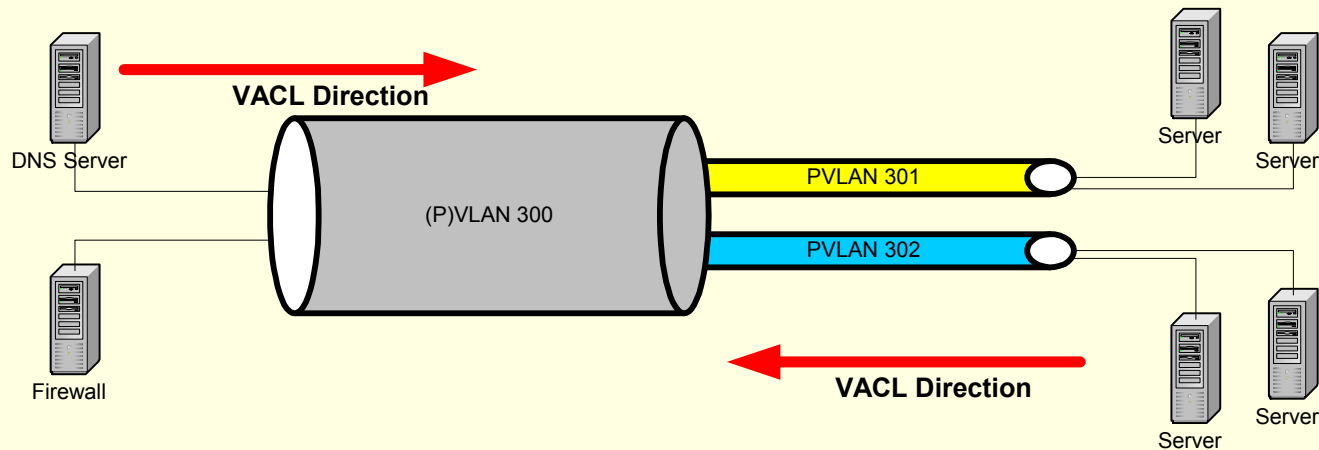
- By moving the log server to a promiscuous port, it is now vulnerable to devices connected to mapped community ports
- The firewall is also vulnerable, but its own security policy protects it better than most hosts
- Host-based packet filtering still not a solution
- Must resolve with a central solution!

VLAN ACLs (VACLs)

- Configured and managed on the L2 switch
- *Hardware-based*; wire speed
- Provide filtering capabilities up to layer 4
- Logging of denied packets
- Uses beyond traffic filtering for security

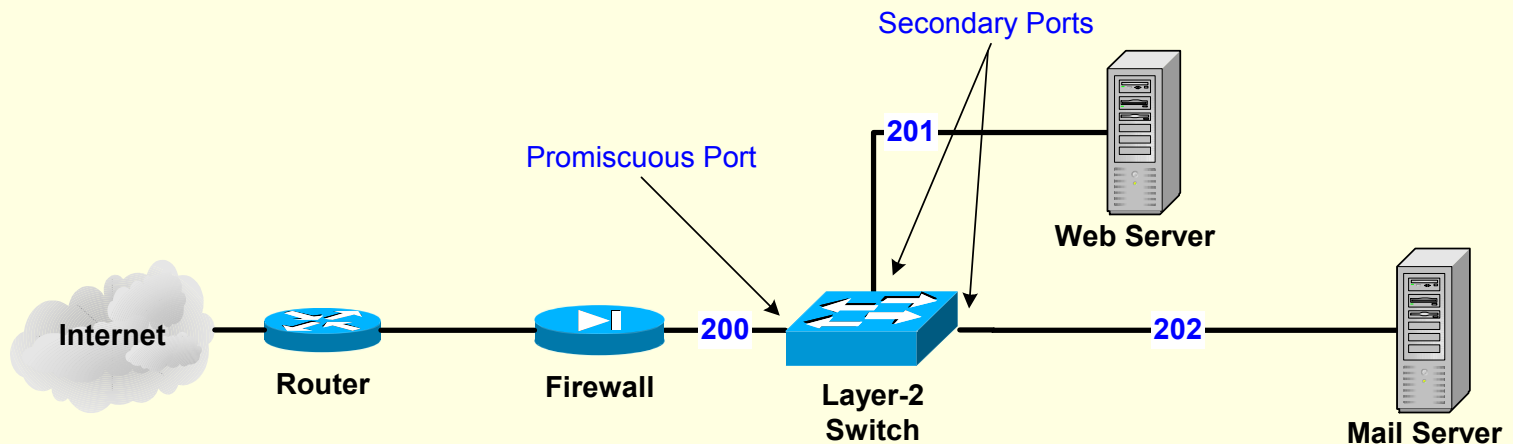
VACL Concepts

- Applied to a VLAN or PVLAN
- Can be applied to isolated, community and primary PVLAN types
- Always operate on traffic “inbound” to the switch

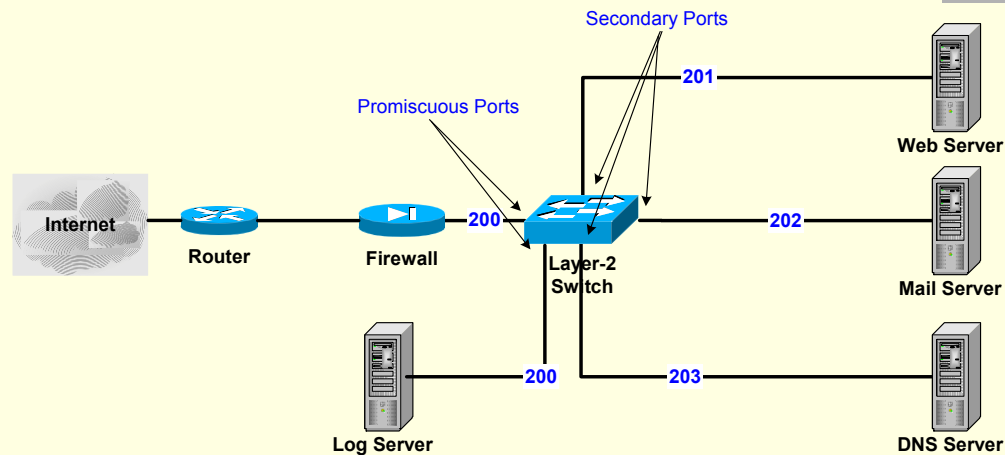


Designing VACLs

- Three possible VACLs:
 - PVLAN 200: Traffic in from firewall to servers
 - PVLAN 201, 202: Traffic from servers to other networks
 - Response traffic (ACK bit) to inbound queries



Designing VACLs

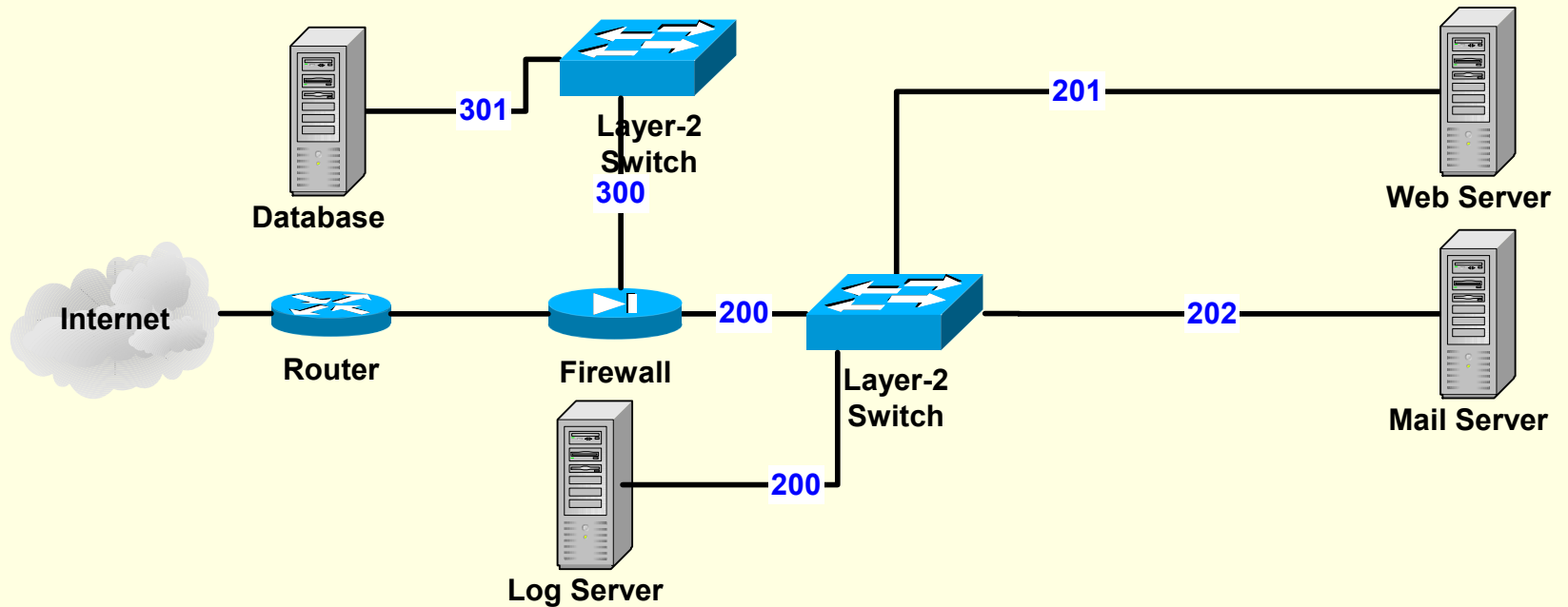


- PVLAN 200's VACLs now handle traffic inbound from the *Internet to hosts* **AND** traffic from the *log server to other PVLANS or to the Internet*
 - The opposite direction of traffic from VACLs on the other PVLANS

VACL Confusion

- VACL design can become very confusing
- If the network is complex, wrap your mind around the concepts first, such as:
 - Hosts on promiscuous ports
 - Simultaneous VACLs on multiple subnets with traffic destined from one to another

VACL Confusion



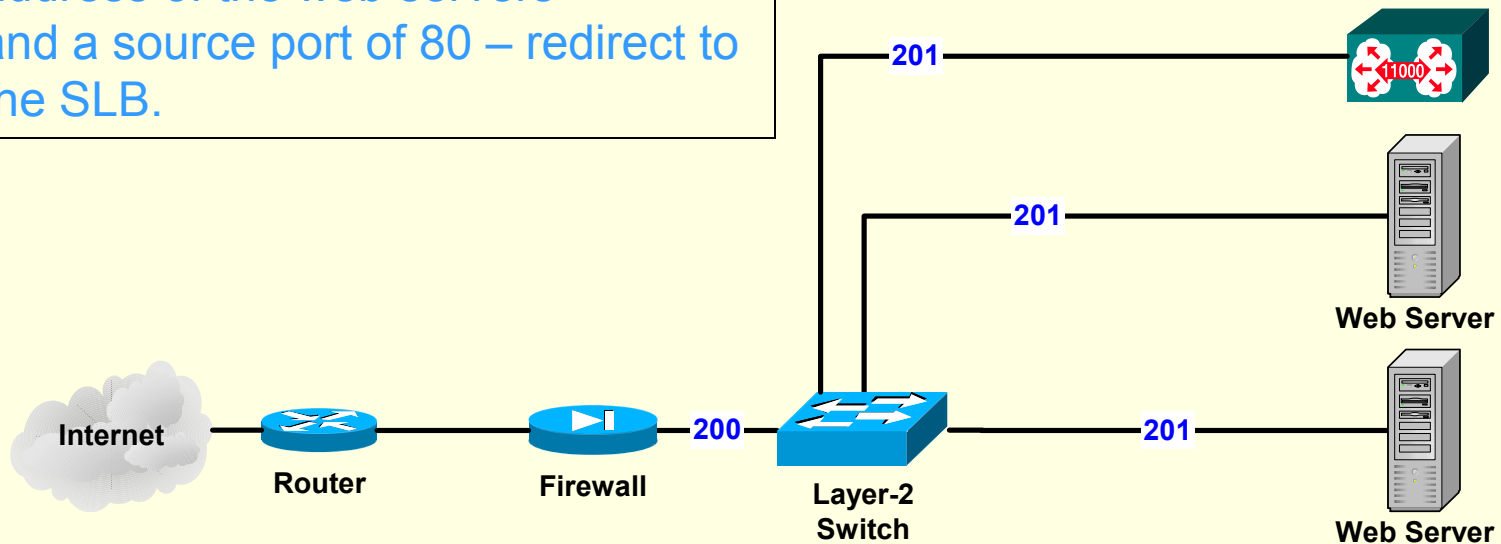
Other VACL Uses: Traffic Redirection

- Using the “redirect” keyword, match traffic and redirect to a different physical port

- Possible Uses:
 - Security systems
 - SLB return-path

Using VACL Redirect with SLB

Match packets with a source IP address of the web servers and a source port of 80 – redirect to the SLB.



Do not have to change the default gateway for a flat network to use the SLB.

Summary

- Centrally harden your layer-2 network
- Do not rely on perimeter security
- Use Private VLANs to **isolate servers** based on administrative policy
- Use VACLs to **enforce** the security policy

Questions

Any questions?

Steve Birnbaum

sbirn@security.org.il

www.PENETRATIONTEST.com