Cisco Expo 2009

Designing Solution with Cisco Intrusion Prevention Systems

Petr Růžička, CSE

CCIE #20166

Session Abstract

IPS technology could be placed in many different places in the network and as such it has to be flexible enough to be positioned wherever we want and need. The session will cover possible deployment options of Cisco IPS, from the basic setups and concepts to very complex DC scenarios.

We will cover typical solutions and also potential problems. We will not cover basics of security, Cisco IPS technology or terminology.

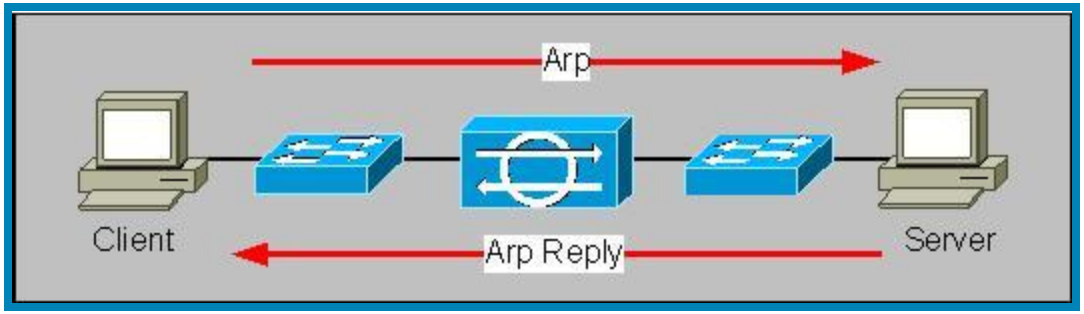
We expect advanced knowledge of networking, design and security concepts.

Agenda

- Design Considerations
- IPS Virtualization
- HA
- EtherChannel
- VSS
- DC 3.0
- Q & A

What is Intrusion Prevention ?

1. IPS closely resembles a Layer 2 bridge or repeater
2. “Identical to a wire” is the closest analogy
3. Inline interfaces have no MAC or IP and cannot be detected directly
4. Network IPS passes all packets without directly participating in any communications including spanning tree (but spanning tree packets are passed)
5. Default Behavior is to pass all packets even if unknown, (ie IPX, Appletalk, etc) unless specifically denied by policy or detection



High Level Considerations

Planning Points for IPS

- General Location Decisions (perimeter, internal, zones of trust, etc) Similar considerations as used for IDS deployments
- Response actions used
- Specific Location Decisions (Between Router and Firewall, Between two switches, etc) - Different considerations than those used for IDS deployments
- Re-cabling and other physical requirements
- Inline Performance Requirements
- Control and Responsibility Issues for an inline device

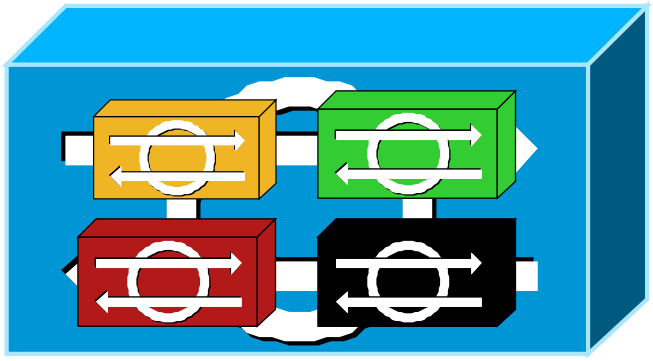
Planning Points for IPS II

- IPS is IDS deployed into the packet stream.
- IPS vs IDS
  - Pros
    - TCP/IP Traffic Normalization
    - Inline Response Actions (Deny Packet)
  - Cons
    - Packet Effects (latency, etc)
    - Network Effects (bandwidth, connection rate, etc)
- There is little point in deploying inline if you don't take advantage of the situation

IPS Virtualization

IPS Virtualization

1. From version 6.0 IPS sensor has a ability to create virtual instances of sensors a.k.a. contexts
2. Physical sensor performance is divided between contexts
3. Up to 4 virtual sensors could be created on one physical hardware
4. For AIP-SSM ASA has to run 8.0 or higher software



IPS Virtualization Advantage

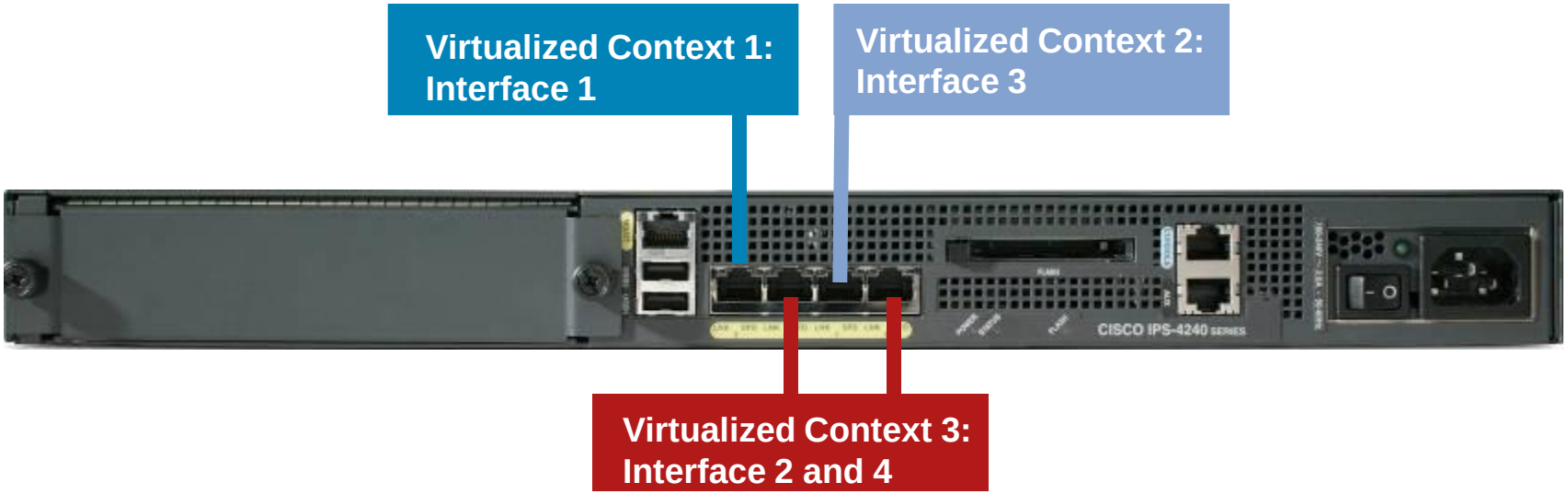
1. Each context could have it’s own
    1. Interfaces or VLAN Pairs
    2. Signature definition
    3. Event Action Rule Policy (filters and overrides)
    4. Anomaly Detection Policy
    5. Anomaly Detection Operation Mode
    6. TCP Session Tracking Mode
2. Some of above points could be shared between contexts

Following Combinations Could be Attached to Context

1. Physical Interface
2. VLAN Groups
3. Inline Interface pairs
4. Inline VLAN pairs

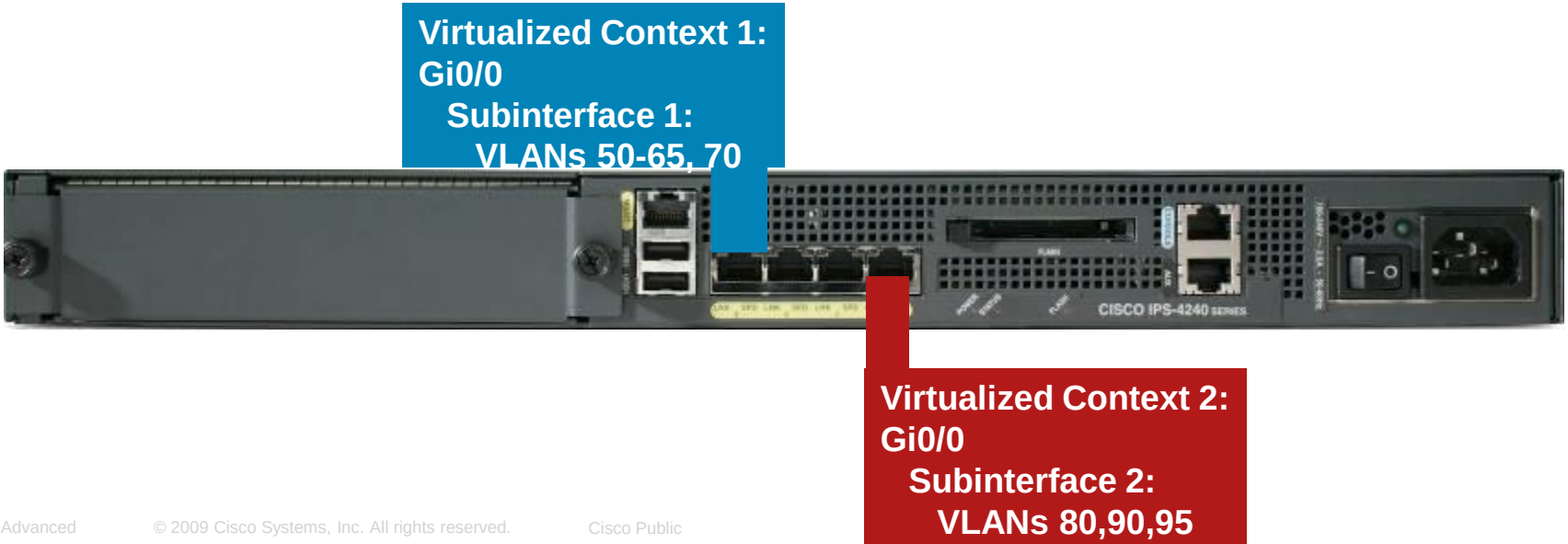
Physical Interface

1. Single physical interface attached to sensor would be in **promiscuous** mode
2. You could attach more than one physical interface to the sensor



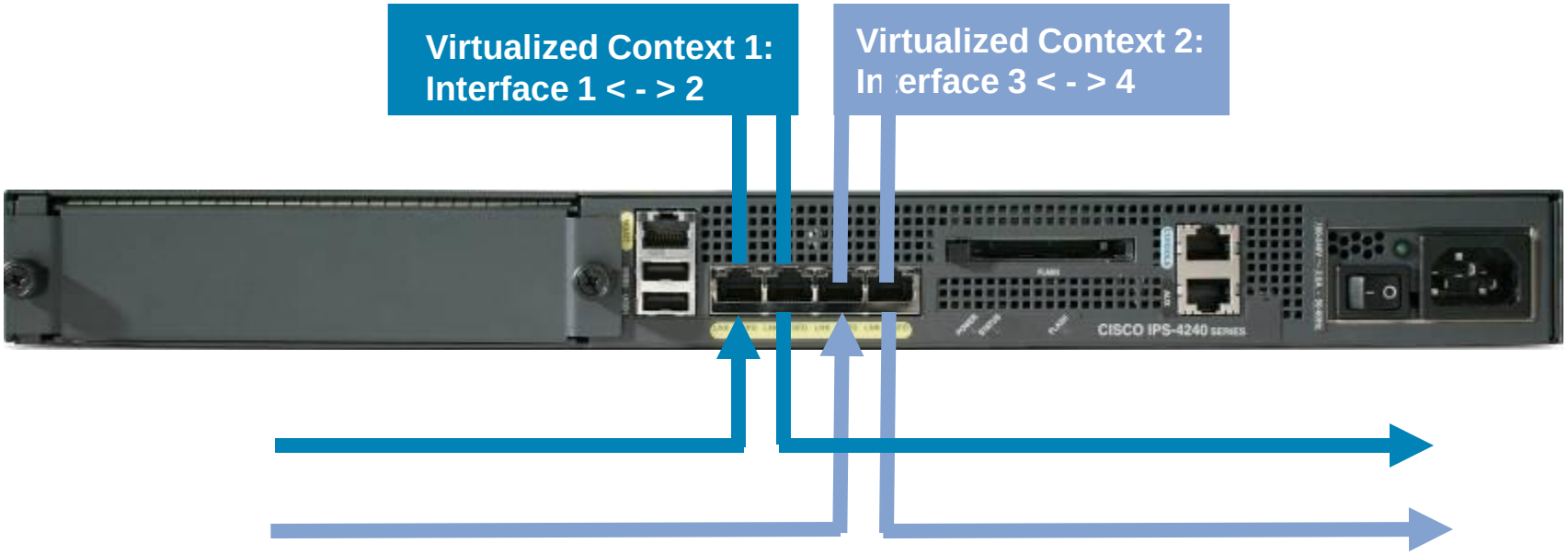
VLAN Groups

1. VLAN Groups mode are like multiple interfaces on one physical interface
2. Group of VLANs are attached to subinterface created on physical interface
3. Up to 255 of subinterfaces (VLAN Groups) can be created

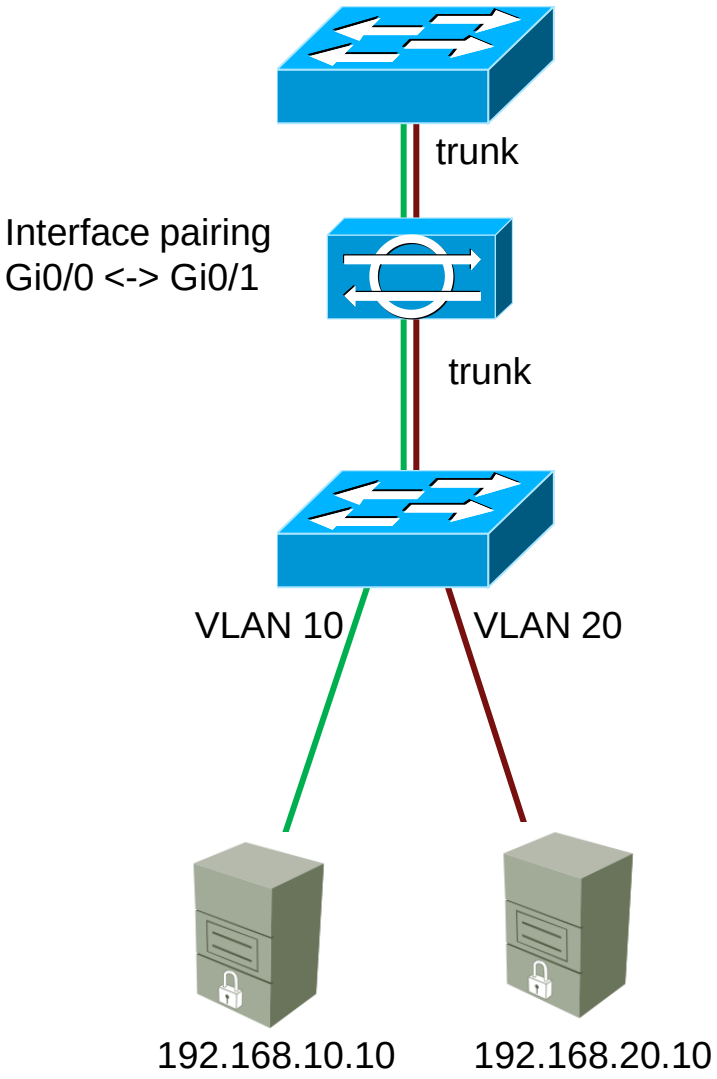


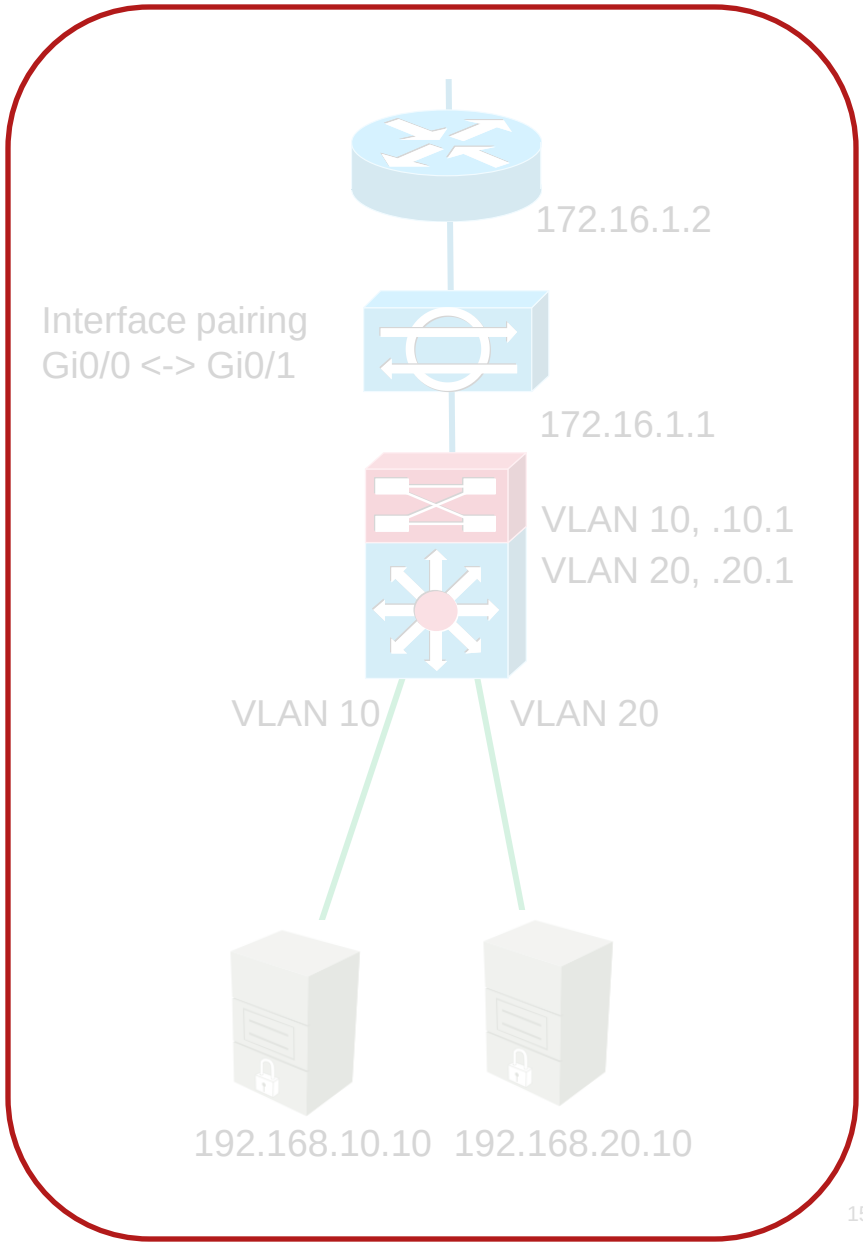
Inline Interfaces

1. Traffic flows from one physical interface to the other
2. On 4260 and 4270 we could take advantage of hardware bypass when supported ports are tight together



Inline Interfaces Example



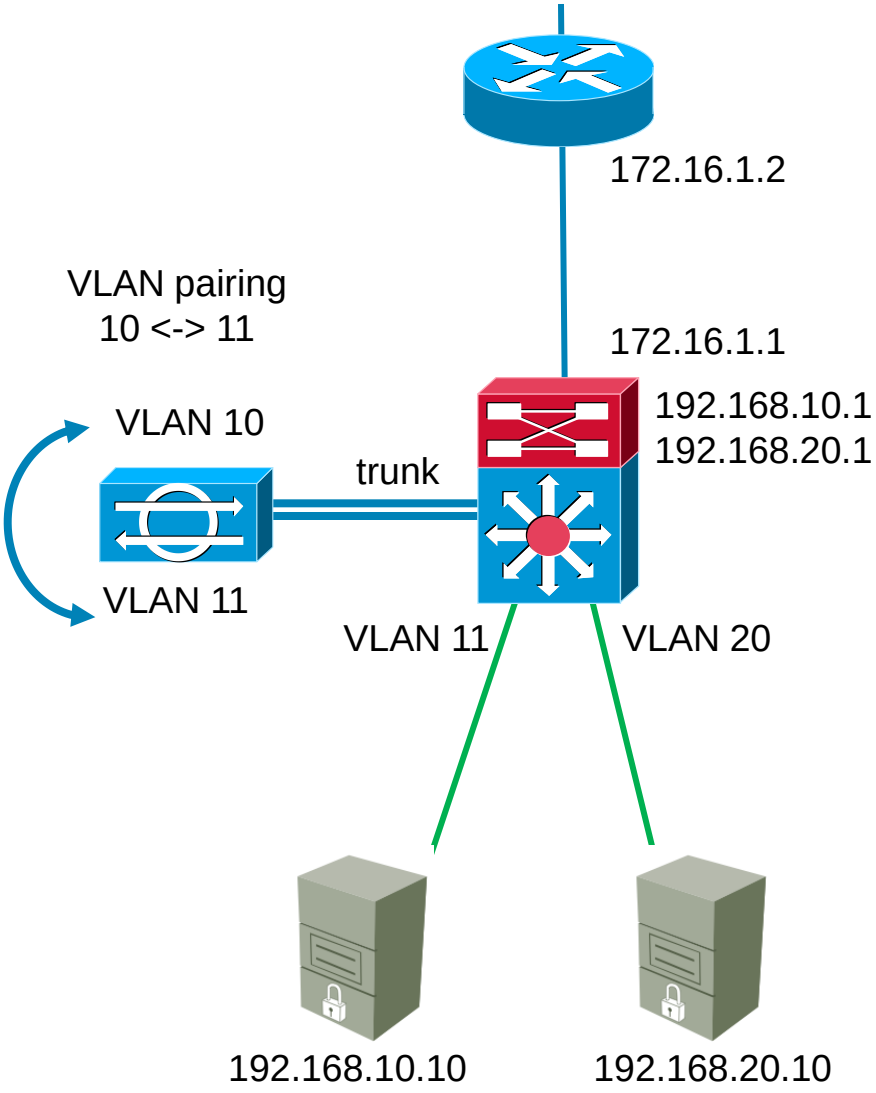


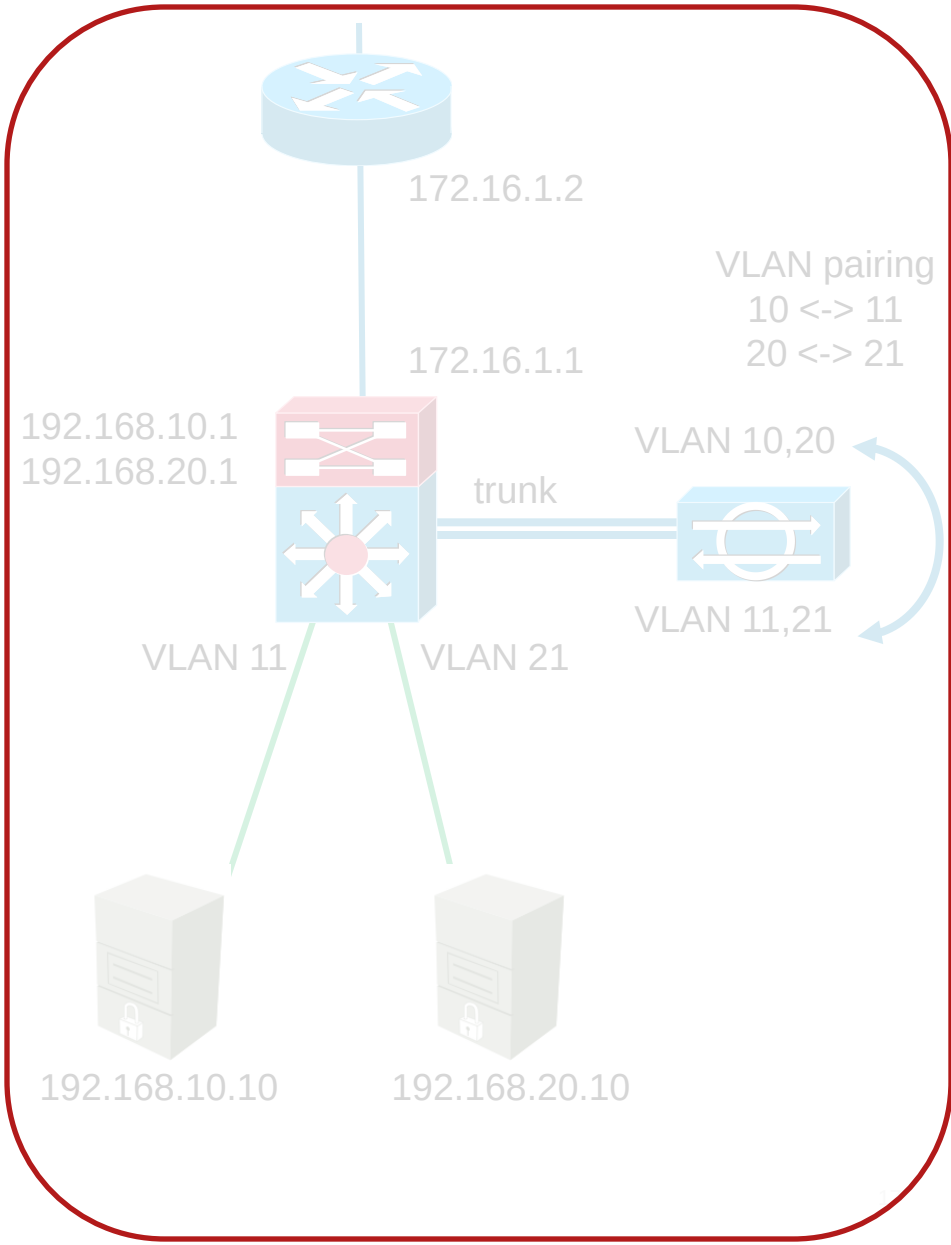
Inline VLAN Pairs

1. Sensor would bridge between two VLANs
2. Up to 255 VLAN pairs could be bridged on one physical interface which acts as trunk port

Virtualized Context 1:
Gi0/0
Subinterface 1:
VLAN Pair 50 < - > 51
Subinterface 2:
VLAN Pair 60 < - > 61

VLAN Pairing Example





What is the “Normalizer” in Cisco IPS ?

1. There are easy evasions available to the determined attacker at both the IP and TCP layers
2. First version of Normalizer was designed to prevent the evasions discussed in *Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection* by Newsham and Ptacek and all other evasions that we could think of that were related to or inspired by the paper.
3. Two general categories:

   IP Normalizer (12xx sigs)

   TCP Normalizer (13xx sigs)

High Availability

High Availability for IPS is Important...

1. Deploying an IPS sensor into the traffic stream introduces a new device to possibly fail and prevent traffic from flowing (It will be the first thing blamed for any problems).
2. High Availability is defined as building into the network, the ability to cope with the loss of a component of that network to ensure that network functionality is preserved

HA Solution

1. Fail-open techniques: Hardware or software that functions to detect problems and pass packets through the device without inspection when required
2. Failover: One or more paths through the network to allow packets, in the event of a device failure, to either go through a backup IPS sensor or through a plain wire
3. Load Balancing: Using devices or software features to split a traffic load up across multiple devices. This can achieve both higher data rates and redundant paths in case of failure

Reliance on fail-open strategies leaves your network with no protection !!!

Inline (Software) Bypass

1. Ability to go „around“ inspection engines
2. Three modes of operation, default is “Auto”

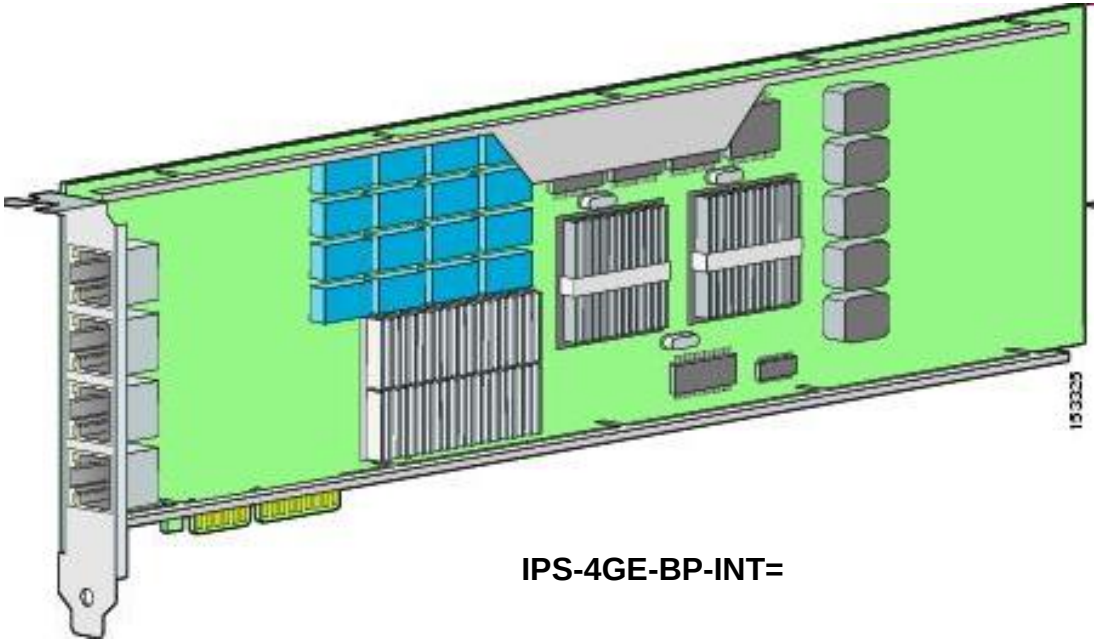
   Auto - if analysis engine fails, traffic continues to flow without interruption (but also without any inspection) through sensor

   Off - if analysis engine is down, traffic stops flowing through sensor

   On - traffic bypasses analysis engine and is not inspected
3. Useful for failover as well as for troubleshooting

Hardware Bypass

1. Both Cisco IPS 4260 and 4270 support HW bypass using 4-port GigabitEthernet cards
2. Bypass is supported only between 0 and 1 and between 2 and 3



IPS-4GE-BP-INT=

HW Bypass Check

```
sensor# sh interfaces gigabitEthernet0/0
MAC statistics from interface GigabitEthernet0/0
  Interface function = Sensing interface
  Description =
  Media Type = TX
  Default Vlan = 0
  Inline Mode = Paired with interface GigabitEthernet0/1
  Pair Status = Down
  Hardware Bypass Capable = No
  Hardware Bypass Paired = N/A
  Link Status = Down
  Admin Enabled Status = Enabled
```


Way to Disable HW Bypass

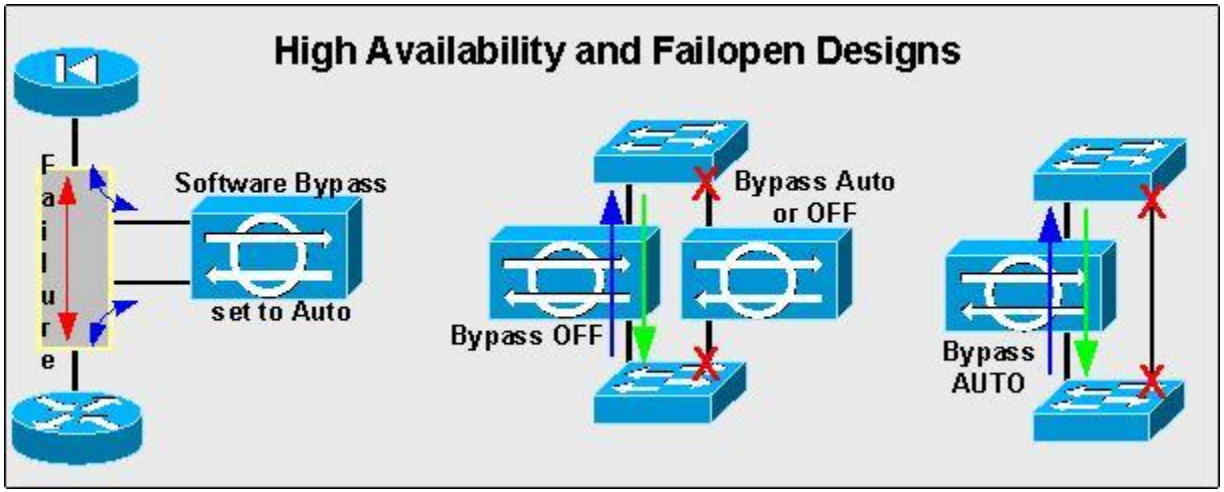
1. Pair unsupported ports together to disable HW bypass

```
ips4270(config)# service interface
ips4270(config-int)# inline-interfaces Inside
ips4270(config-int-inl)# interface1 GigabitEthernet3/0
ips4270(config-int-inl)# interface2 GigabitEthernet3/3
ips4270(config-int-inl)# exit
ips4270(config-int)# exit
Apply Changes?[yes]: yes
Warning: Hardware bypass functionality is not available
    on inline-interface Inside because
    GigabitEthernet3/0 is only capable of hardware-
    bypass when paired with GigabitEthernet3/1
```

Fail-open and Failover Deployments

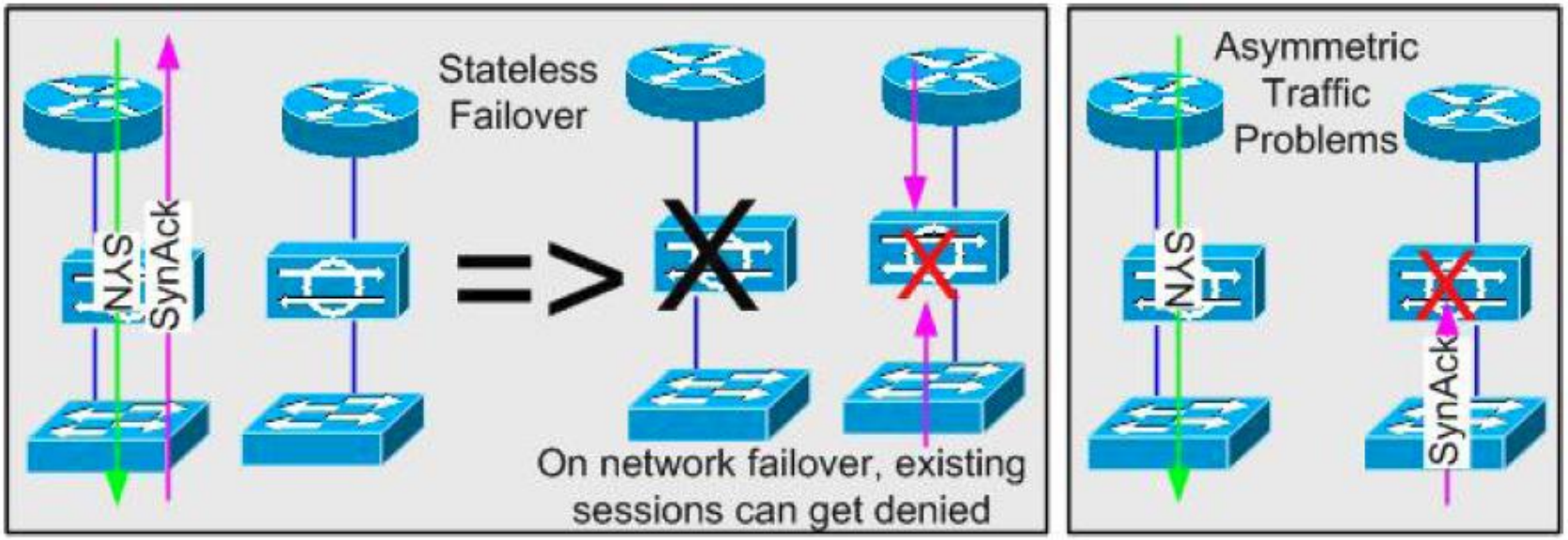
IPS Appliance Sensor Solutions:

1. Standalone Sensor in Hardware Bypass Deployment
2. Redundant Deployment using Spanning Tree for Active/Passive Failover
3. Redundant Deployment using Spanning Tree for High Availability (along with plain wire)

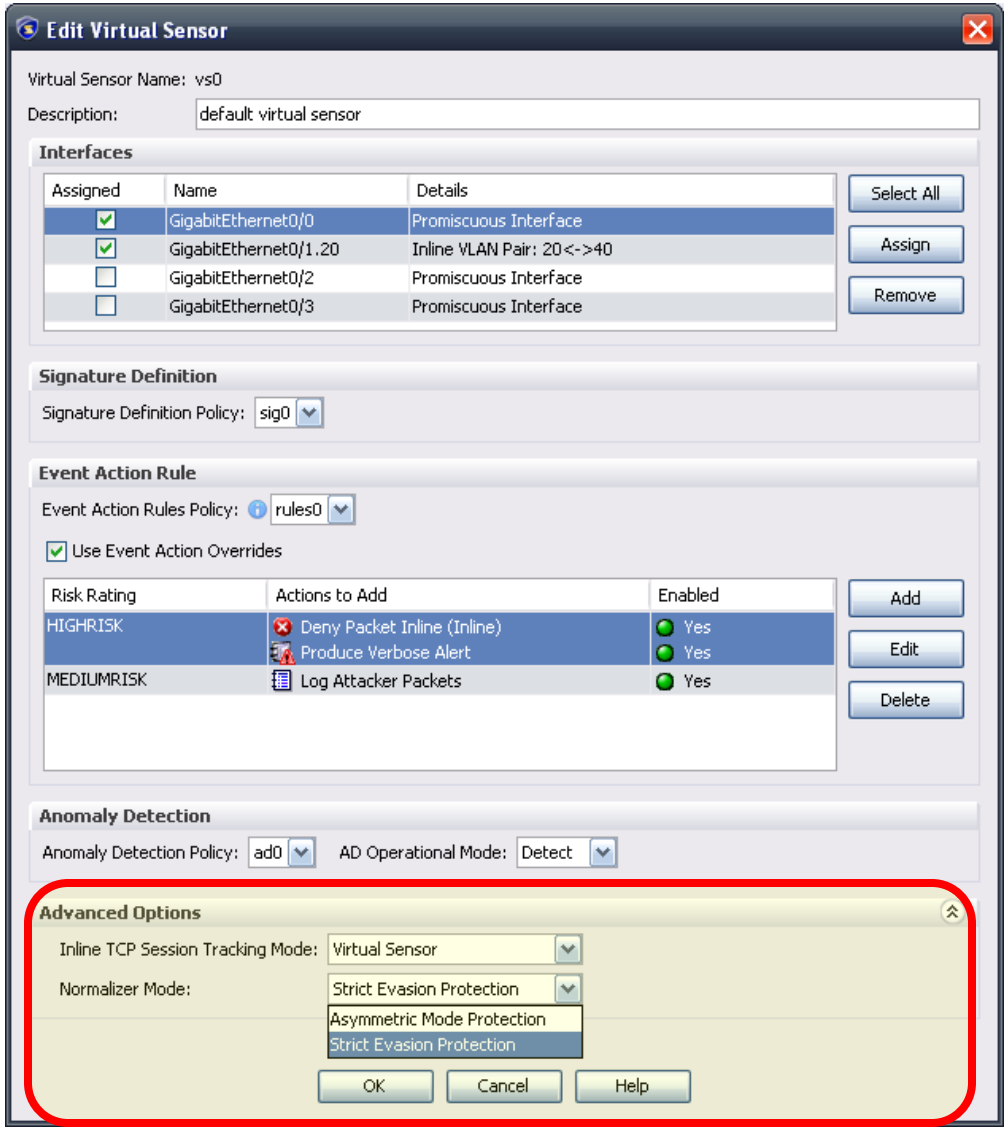


Asymmetric Support for IPS

1. Cisco IPS does not support HA natively (yet)
2. There could be problems with asymmetric flows
   - Check TCP Reassembly Modes
   - Check Normalizer settings



Normalizer Mode



TCP Reassembly Mode

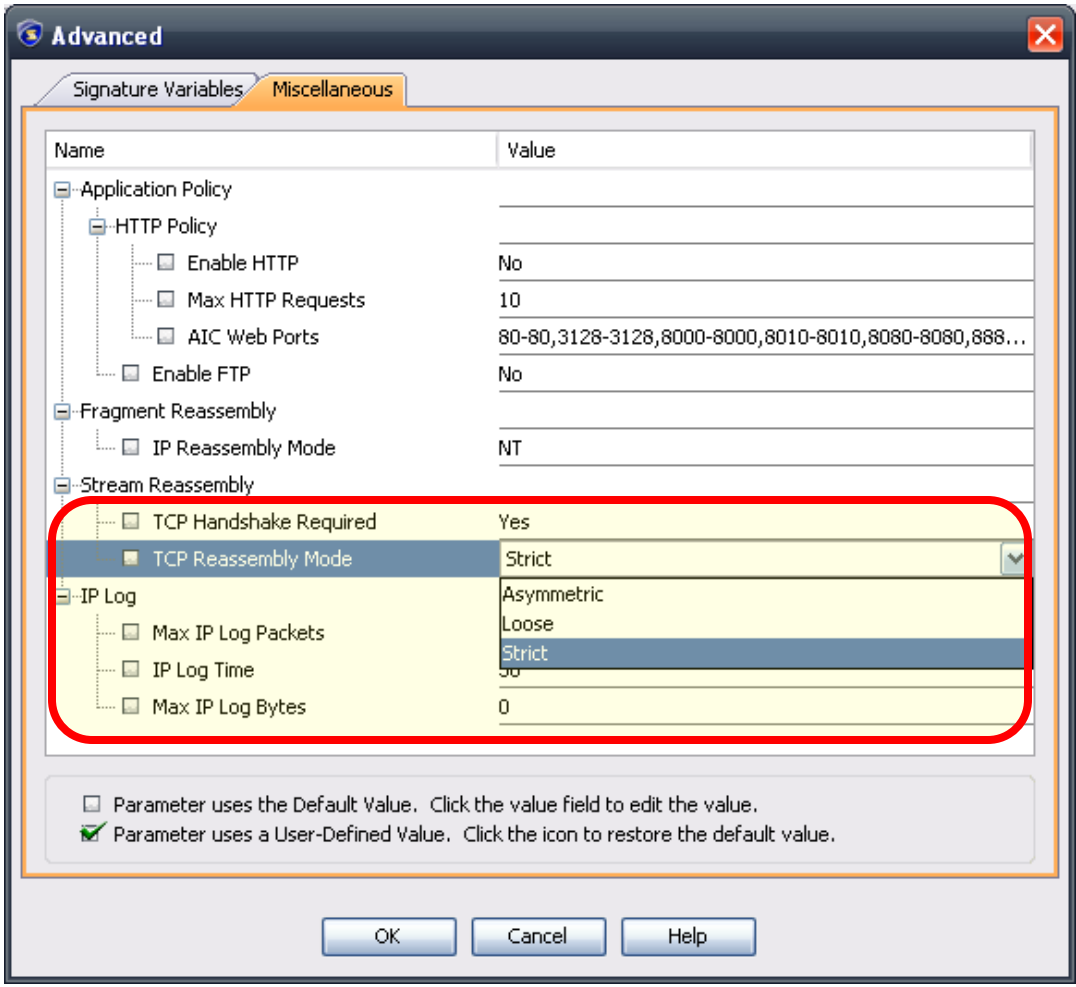
Using IME

Configuration ->

Signature Definitions –>

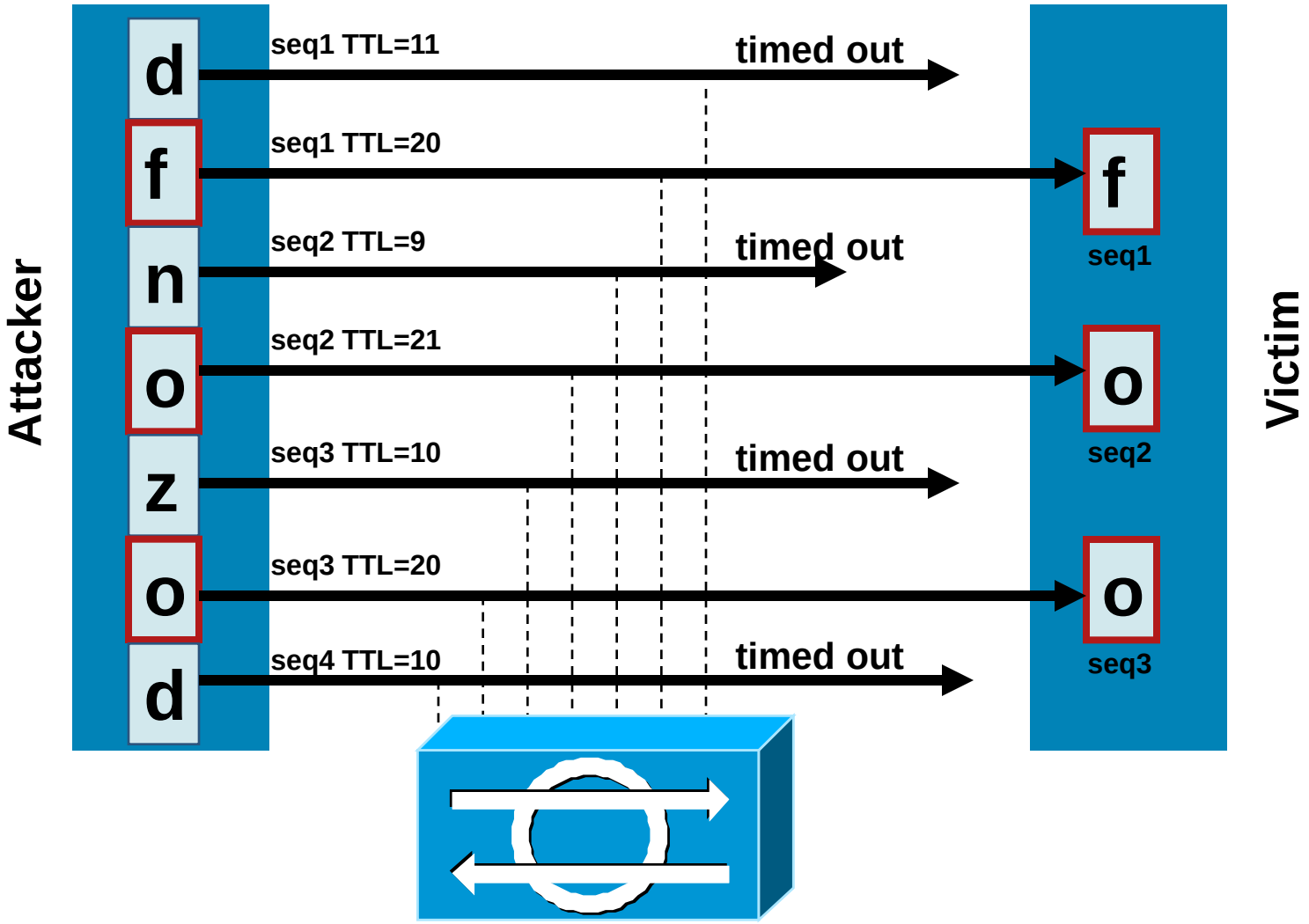
All signatures –>

Advanced…



How could you evade IPS sensor using TTL manipulation ?

How to Evade IPS (Without Normalizer) I



d or f?; n or o?; z or o?

EtherChannel

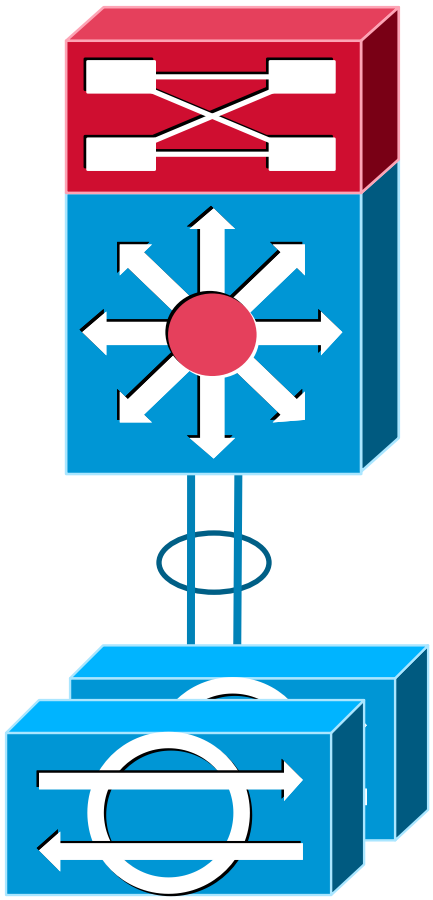
EtherChannel Load Balancing

- Fault tolerant architecture that dynamically reconfigures the cluster on a HW or SW failure
- Scalable Performance Allows up to 8 sensors deployed inspecting the same data set
- Relies on EC algorithm to split flows amongst the different blades

EtherChannel Load Balancing

1. Can only maximize performance based on specific powers of 2: 2, 4 or 8 devices
2. Total Bandwidth (capacity of IPS) multiplied by (2, 4 or 8) is the max amount you can balance (“split”)
3. Performance will only be maximized with 2, 4 or 8 IPS devices
4. 3, 5, 6, 7 IPS will NOT improve performance – only provides (additional) failover

ECLB Scenarios:Performance Design



2x4270

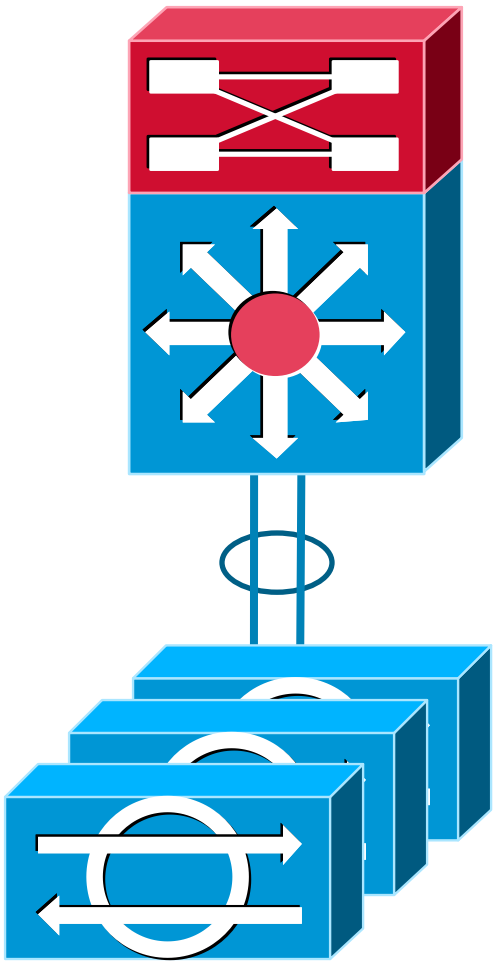
8G Traffic

4G & 4G

Total capacity

- 8G
- No failover !

ECLB Scenarios: Redundant Design



3x4270

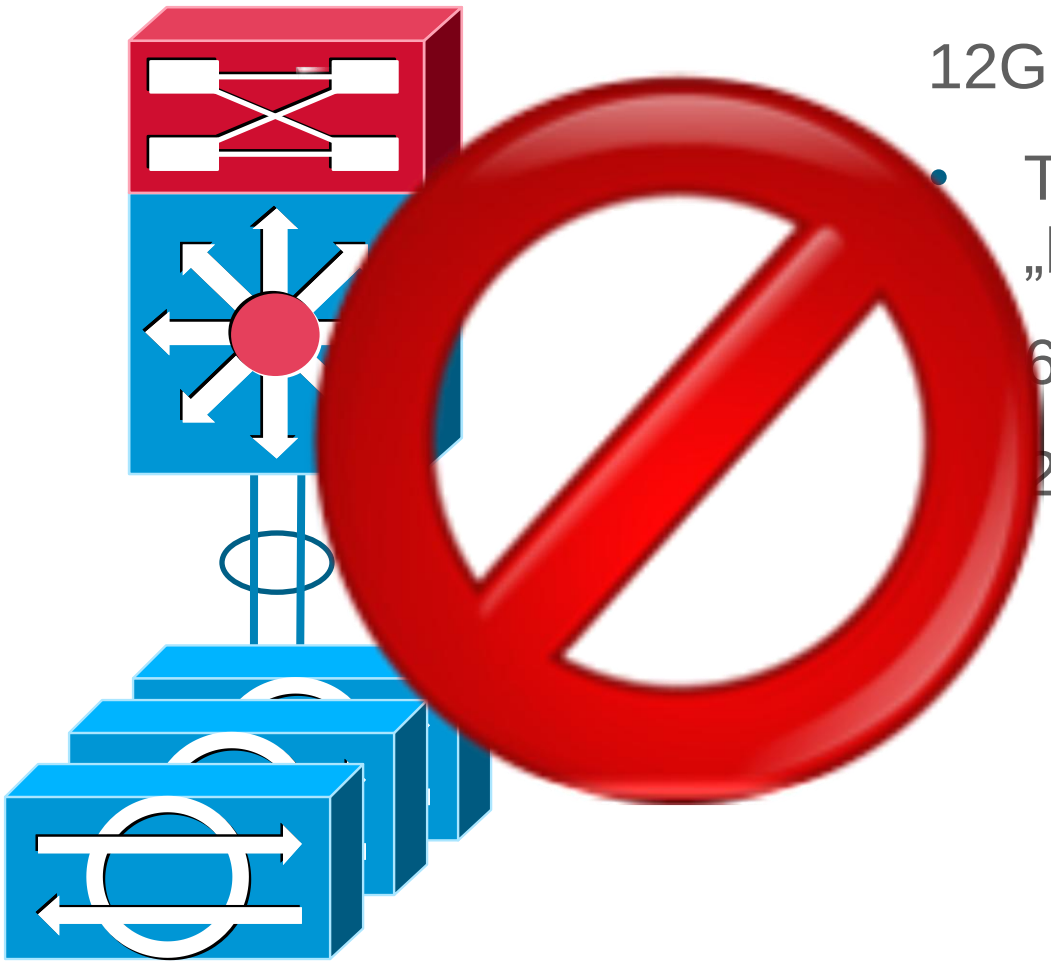
8G Traffic

4G & 2G & 2G

Total capacity

- 8 G
- If any one fails, traffic balances across remaining
- Each of the remaining gets rest

ECLB Scenarios: BAD Design



3x4270

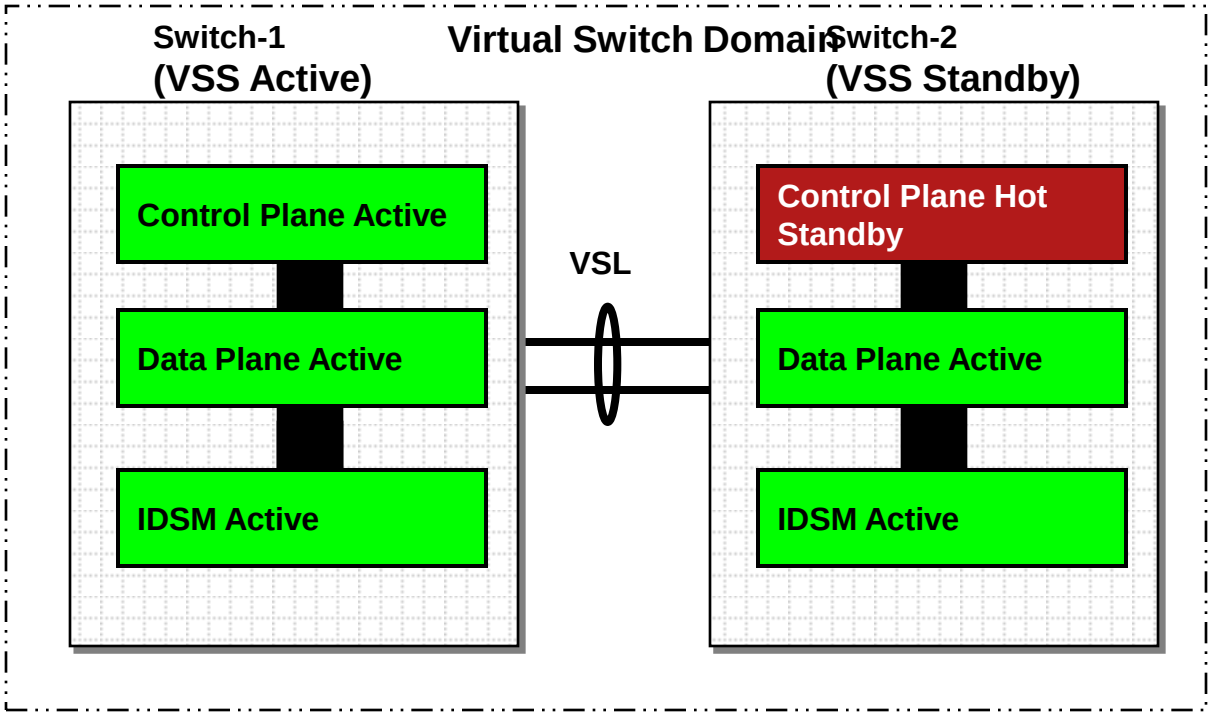
12G Traffic (3 IPSx4G)

- Traffic goes to 4 „buckets“
- 6G & 3G & 3G
- 2G gets lost

VSS

VSS Service Module Integration
IDSM2 Service Module High Availability

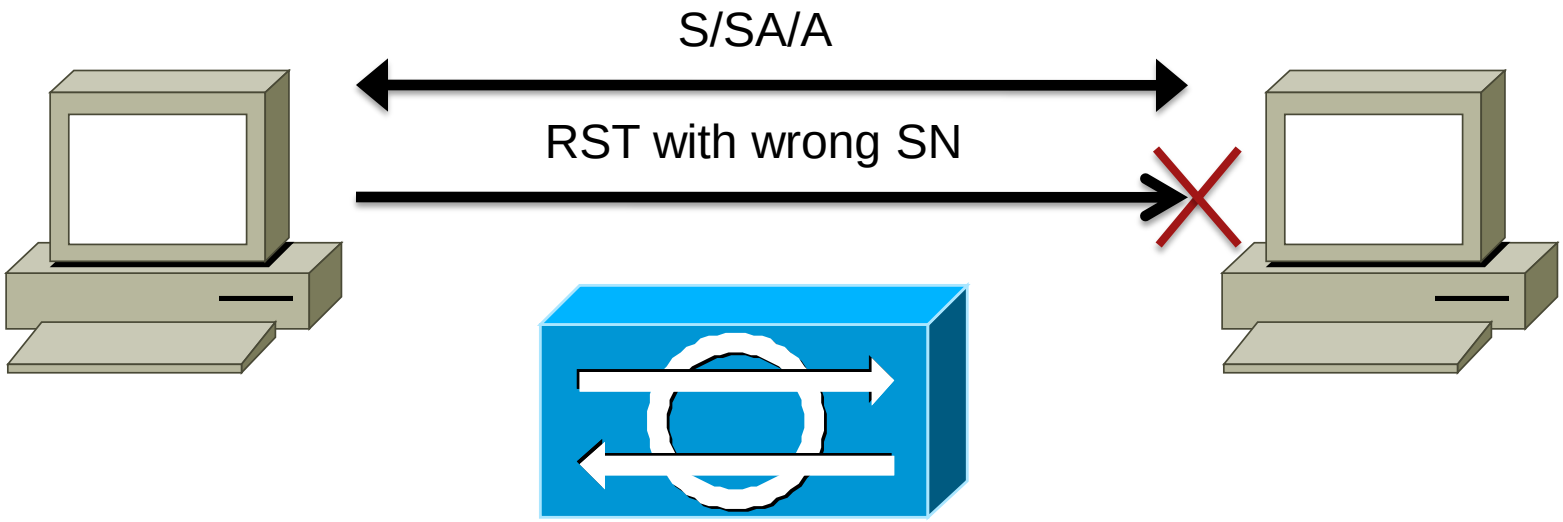
IDSM2 does not support session failover mechanisms, however more than one active IDSM2 is supported in a Virtual Switching System. Traffic Load-balancing in VSS is similar to standalone containing multiple IDSMs in a single chassis, it is achieved using Etherchannel configuration*



How could you evade sensor using RST/FIN sequence numbers?

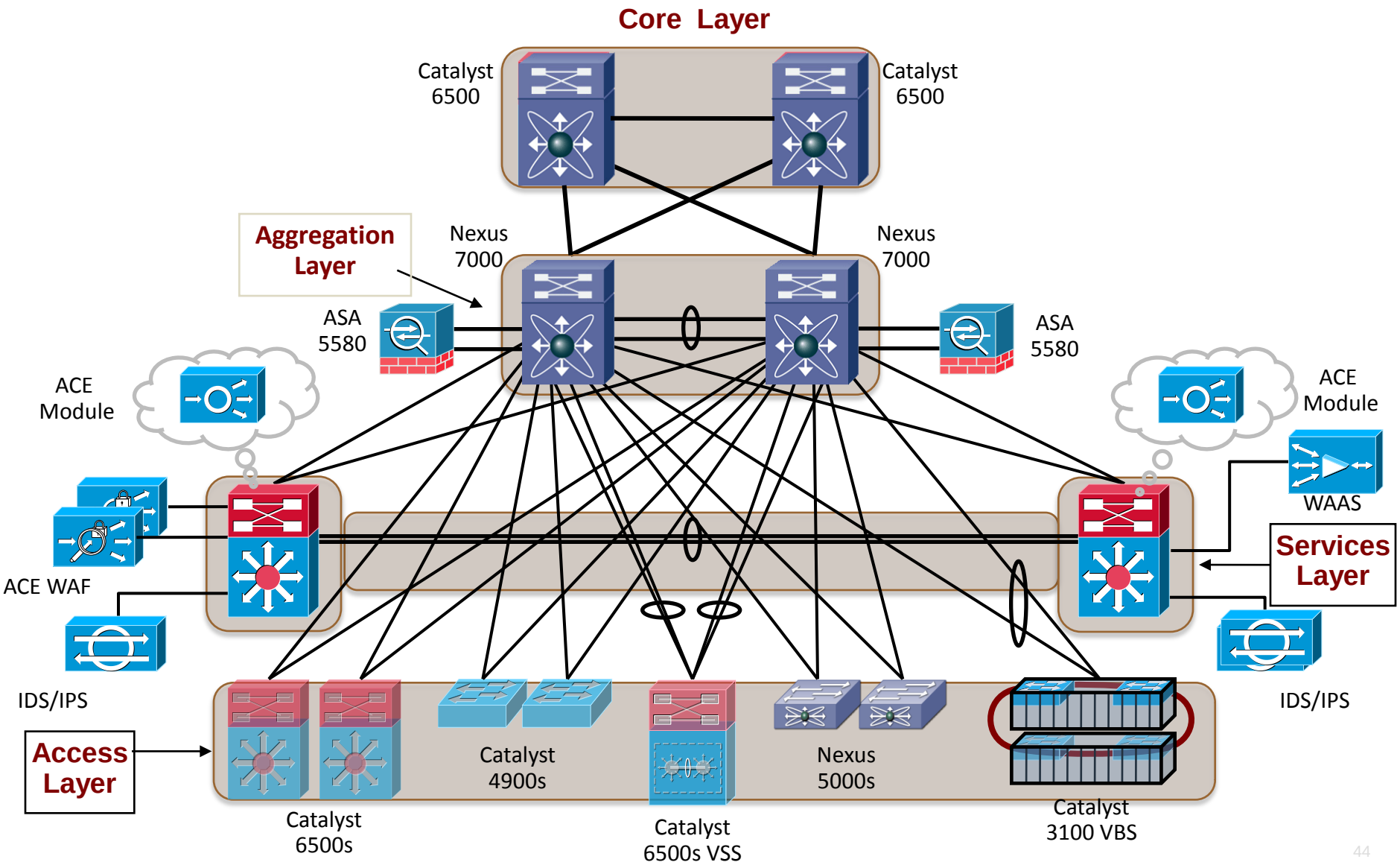
How to Evade IPS (Without Normalizer) II

1. Establish TCP connection across IPS
2. Torn connection with FIN or RST packet but use wrong sequence numbers (SN)
3. If IPS doesn't check SN…

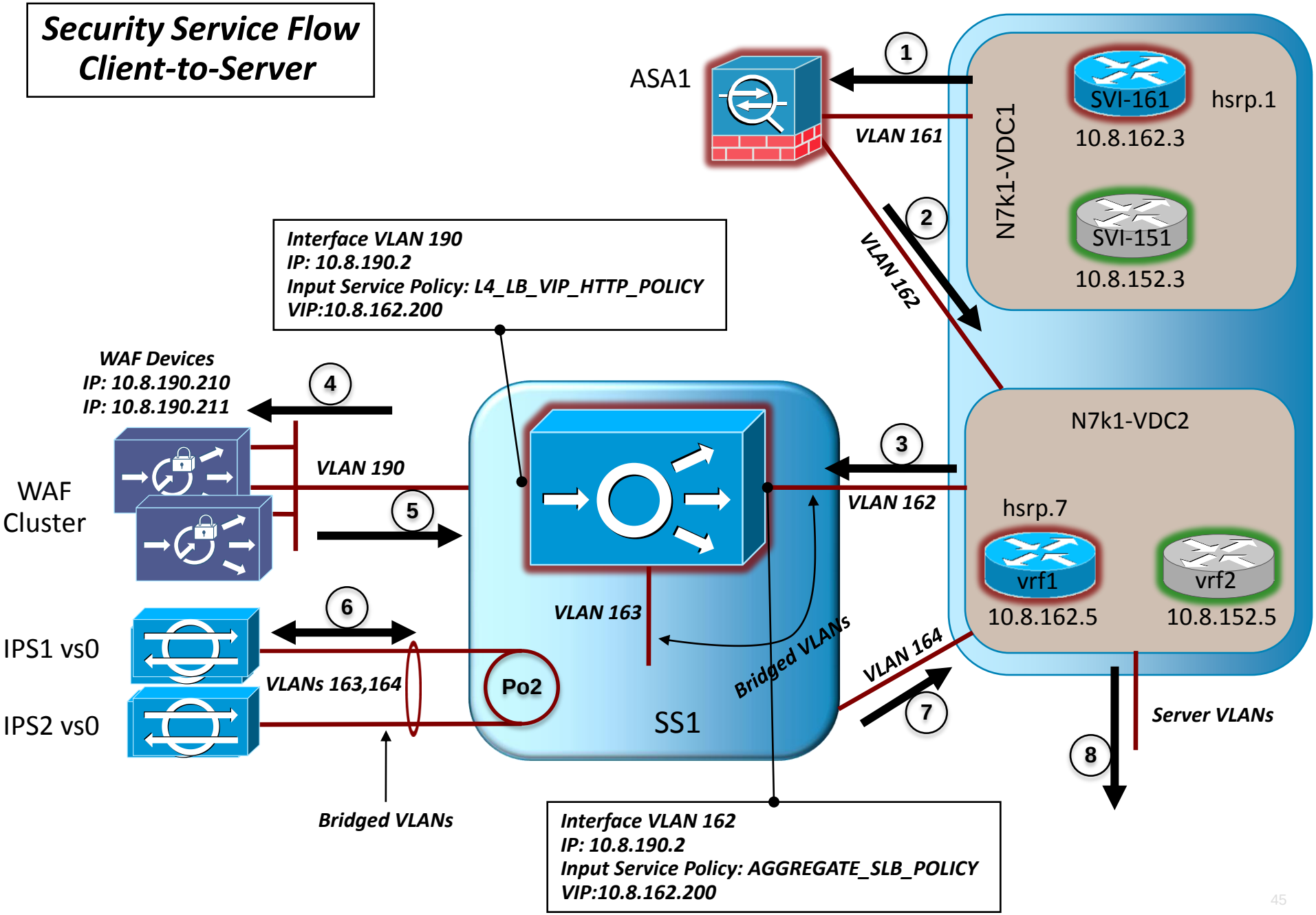


DC 3.0

Physical Solution Topology



Security Service Flow Client-to-Server



Global Correlation

Cisco IPS Global Correlation

Network IPS to Global IPS

- **Coverage**

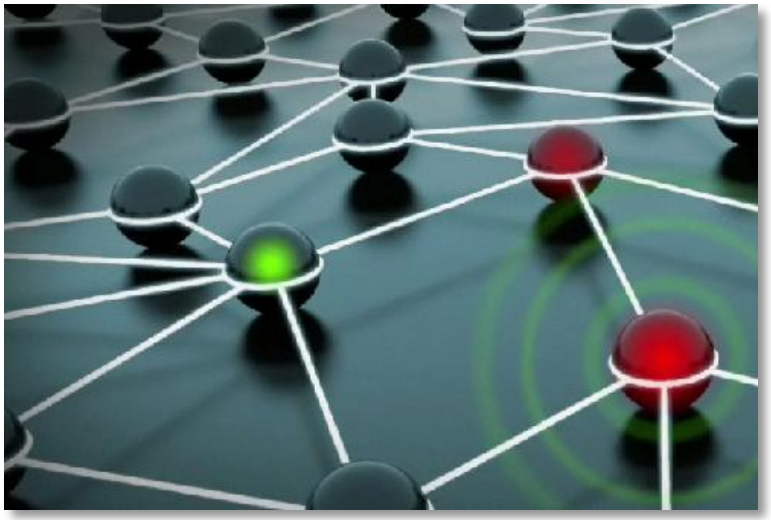
  Twice the effectiveness of traditional IPS

- **Accuracy**

  Reputation analysis decreases false positives

- **Timeliness**

  100x faster than traditional signature-only methods



IPS Reputation Filtering powered by Global Correlation

Agenda

- Design Consideration
- IPS Virtualization
- HA
- Etherchannel
- VSS
- DC 3.0
- Q & A

Interesting Links

Security Inteligence Operations

http://www.cisco.com/security/

Cisco SAFE Reference Guide

http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg.html

Enterprise Campus 3.0 Architecture: Overview and Framework

http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/campover.html#wp709388

Design Zone

http://www.cisco.com/go/designzone

Insertion, Evasion , and Denial of Service: Eluding Nework Intrusion Detection

http://insecure.org/stf/secnet_ids/secnet_ids.pdf

Registrujte se za Cisco Networkers
25-28. januar 2010. Barselona
28-31. mart 2010. Bahrein