



Cisco Expo
2008

Cisco ASR 1000 Series Routers

Securing Enterprise Network



Lei Chen
Product Marketing
Cisco Systems, Inc

Agenda

- **ASR 1000 Series Security Services**
- ASR 1000 Series IPSec Implementation
- ASR 1000 Series Firewall Implementation
- ASR 1000 Series Firewall Logging
- ASR 1000 Series Security Software Packages
- Summary – Key Differentiators

Introducing the Cisco ASR 1000 Series High Performance Firewall and VPN



Industry-leading Router-Based VPN Performance

- Up to 4 Gbps IPsec throughput
- Superior QoS and IP Multicast Handling
- In-box HA for Firewall, NAT and IPsec

Unmatched IOS Zone-Based Firewall scale

- Up to 10Gbps Firewall throughput
- Up to 20,000 connections/sec
- Ultra low latency, and sub-50 ms Failover

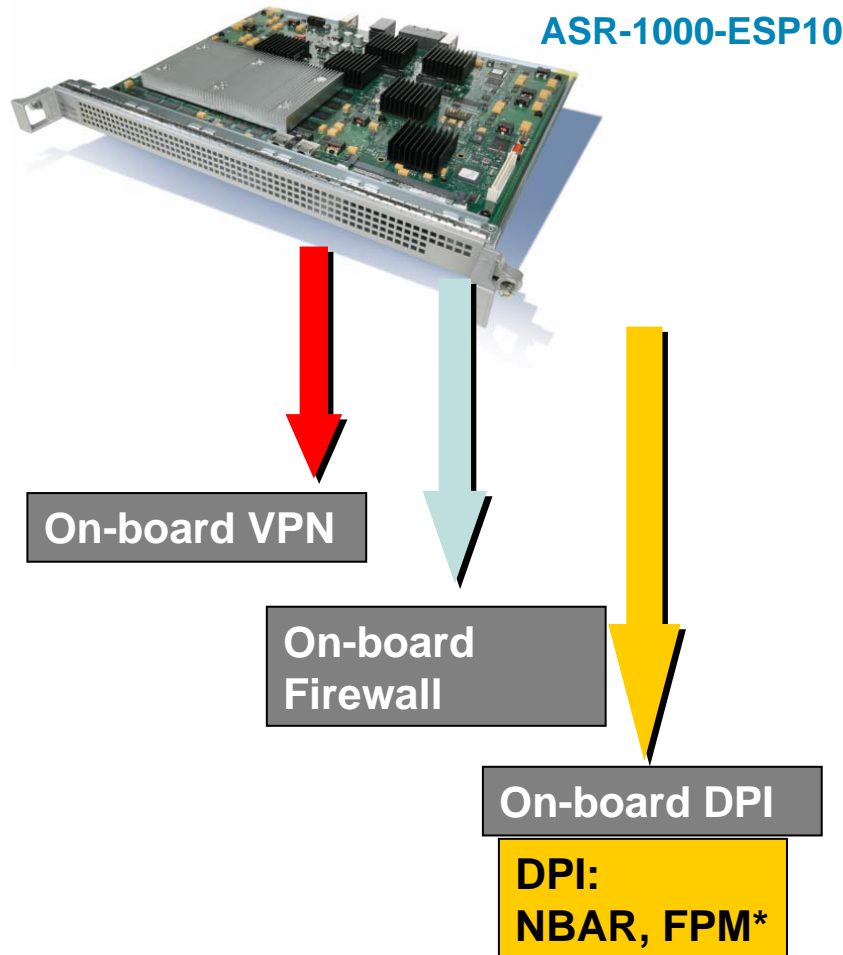
Scalable Event Logging and Data Monitoring

- High speed NetFlow Security Event Logging
- Highly scalable NetFlow Data Export
- Hardware-based Control Plane Policing

Raising the bar for Integrated Firewall and VPN capabilities

Embedded Services Processor

Built-In Security Acceleration

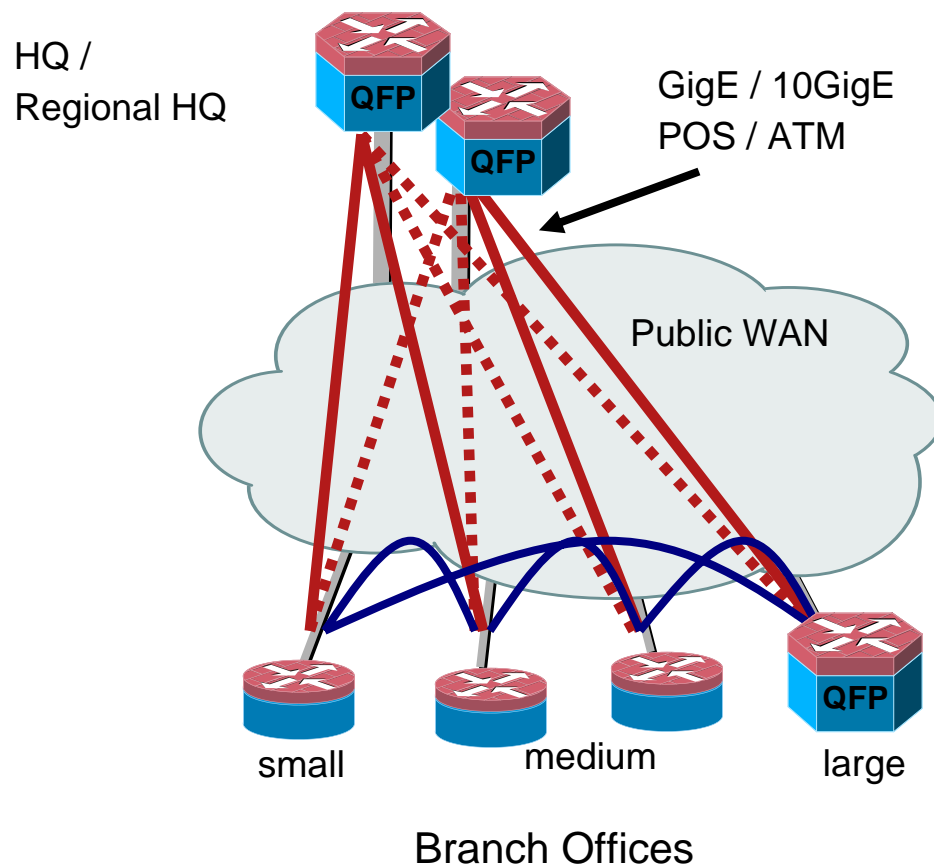


- Up to 4.4 Gbps 3DES and AES
- Up to 10 Gbps Firewall Acceleration with NetFlow v9 Logging
- Deep Packet Inspection (DPI) Acceleration (NBAR, FPM*)
- NetFlow Acceleration
- Superior IP Multicast Encryption
 - Full-circle back pressure mechanisms between Crypto and Forwarding Engine
- Hardware QoS at up to 10 Gbps
 - 128K CBWFQs
 - Off-loads Shaping, Policing, and Queuing

Performance with Investment Protection

Industry-leading VPN Performance

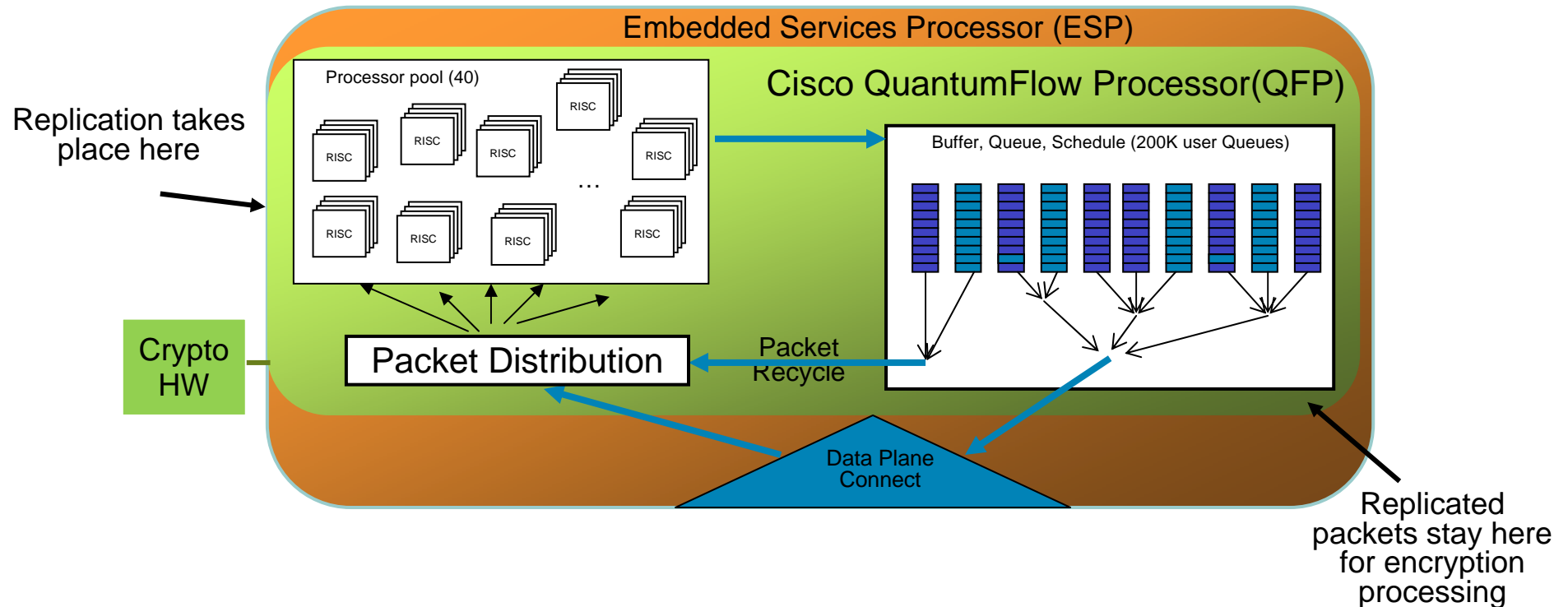
Multi-Gigabit Integrated, Secure VPN Head-end



- Offer a full service IPsec VPN Aggregation Router which scales to meet new BW demands
- Supports industry-leading site-to-site and RA VPN: DMVPN, Enhanced Easy VPN
- No service SPA required
- Optimized for QOS & Encrypting IP Multicast
- Up to 4Gbps Crypto throughput
- Up to 10K tunnels
- Up to 50 Tunnels Per Second
- In-box IPsec HA

Industry-leading VPN Performance

Hardware-Accelerated QoS and IP Multicast

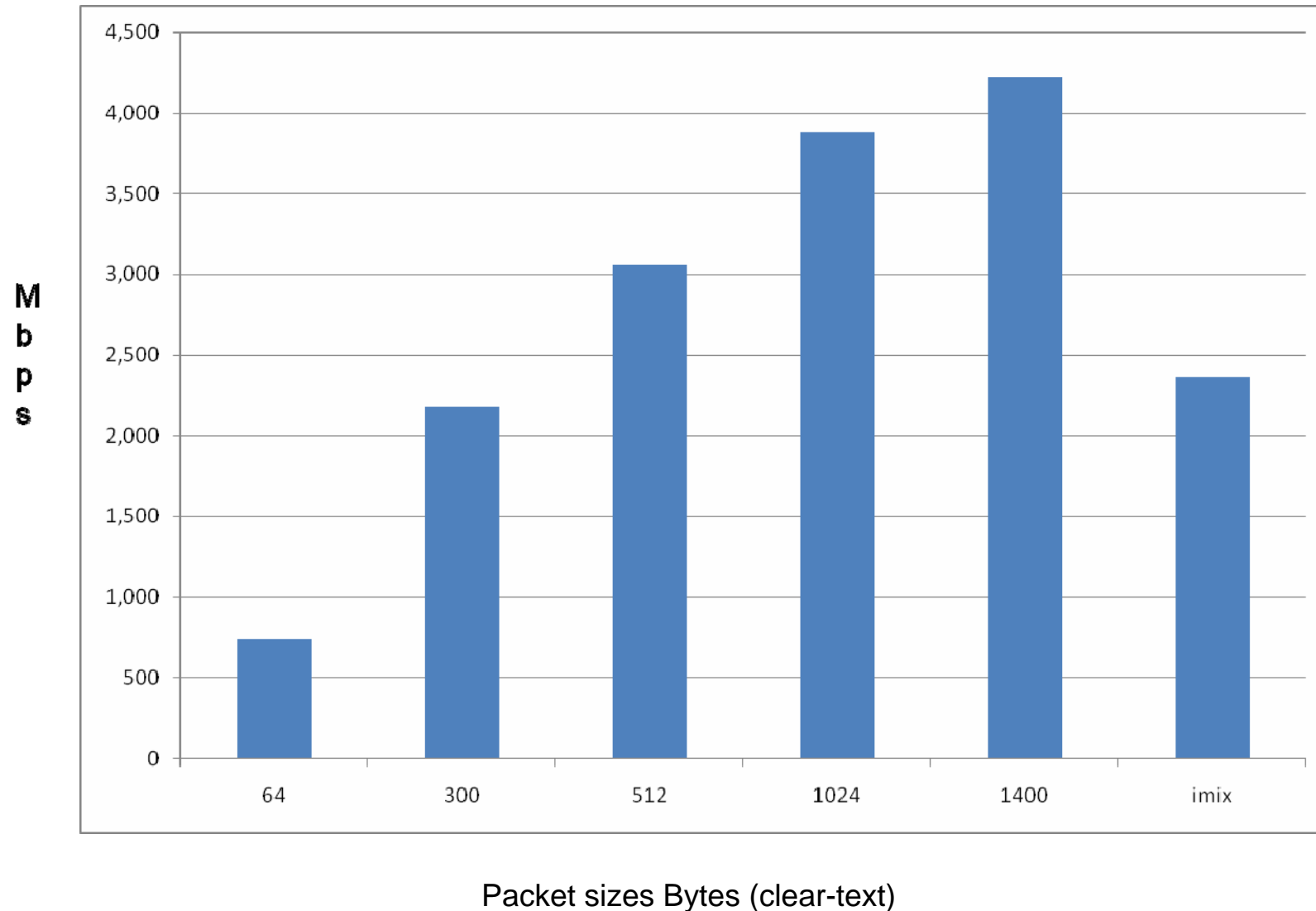


Traffic Manager off-loads all QoS functions including marking, queuing, shaping, and policing at wire rates

- Multicast encryption has the tendency of causing drops at Rx Ring of Crypto Engine
- ASR 1000 minimizes chances of this happening by way of a full circle of back pressure mechanism between Traffic Manager and Crypto Engine

Industry-leading VPN Performance

Multi-Gigabit IPsec Throughput (ESP-10G)

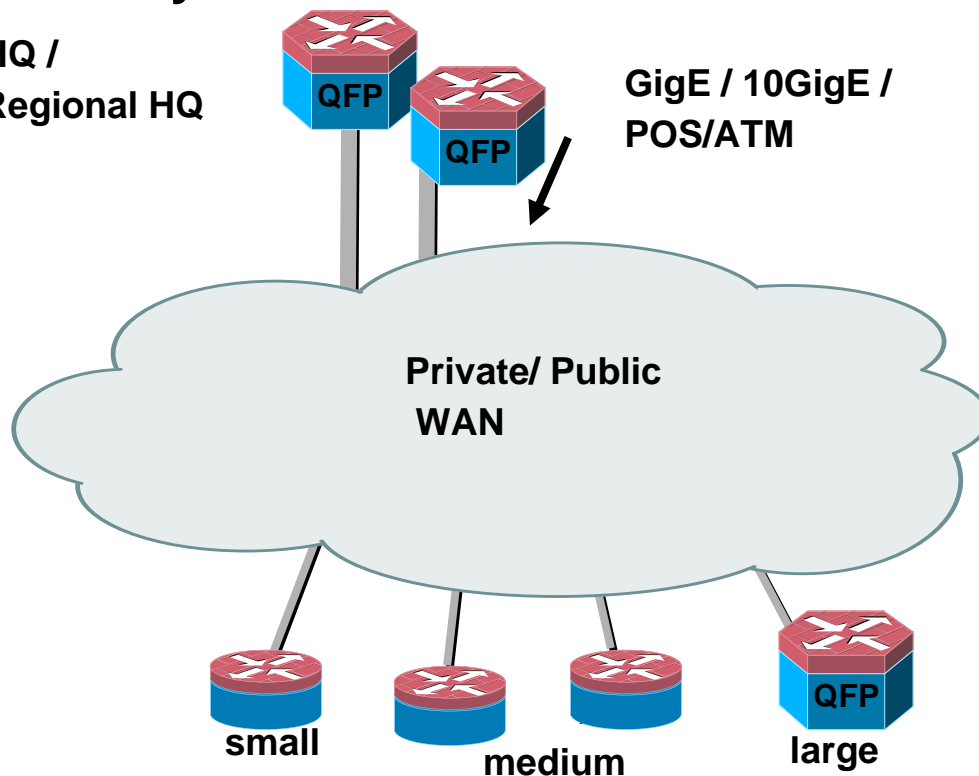


Unmatched IOS Zone-Based Firewall scale

10 Gigabit Firewall in a Router

WAN Aggregation or Internet Gateway

HQ /
Regional HQ



Branch Offices

Full T1's w/ satellite, DSL etc. backup

Going to multiples of
Ethernet/DSL/Wireless...

- Being able to use IOS Zone-Based FW up to Multi-Gigabit BW

- In-box stateful HA

- Firewalling supported on all interfaces in the router

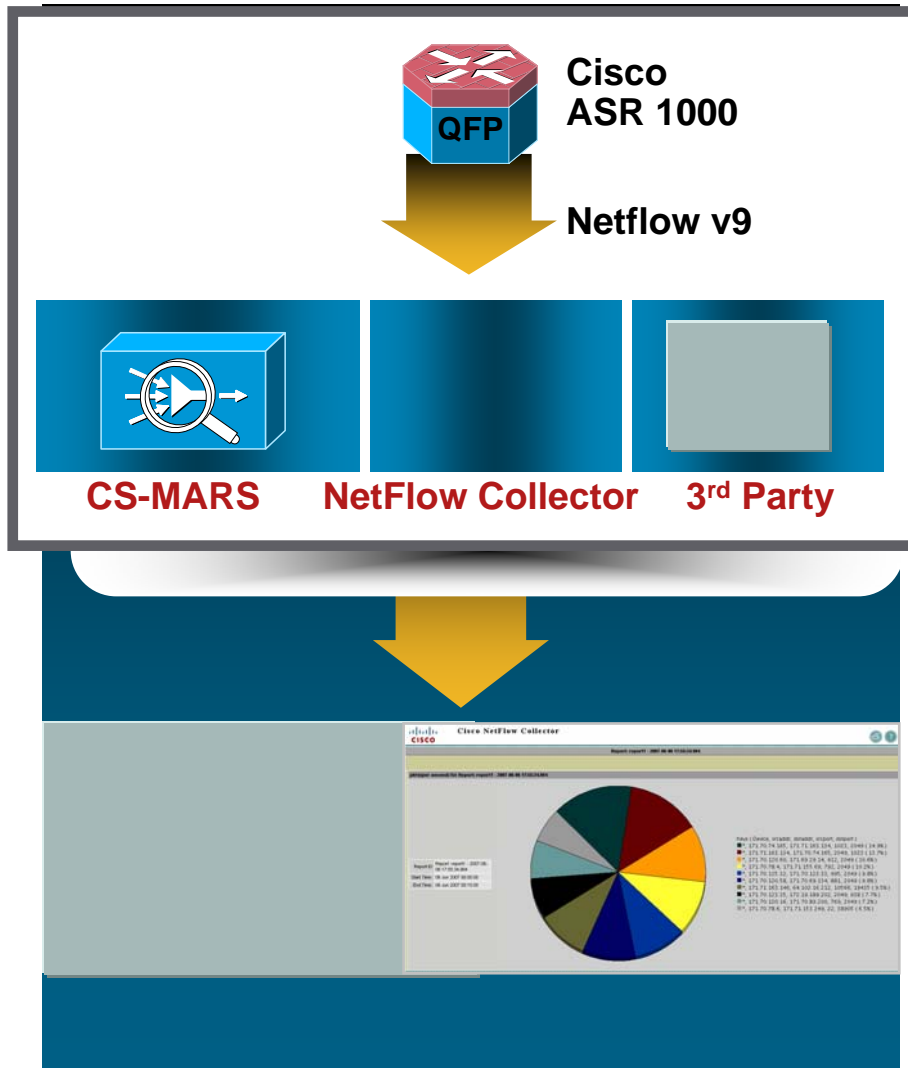
- No service blades required

- Full Firewalling is done within QFP (including ALGs)

- High-Speed Security Event Logging available via NetFlow v9

Scalable Event Logging and Data Monitoring

NetFlow Security Event Logging in a Router

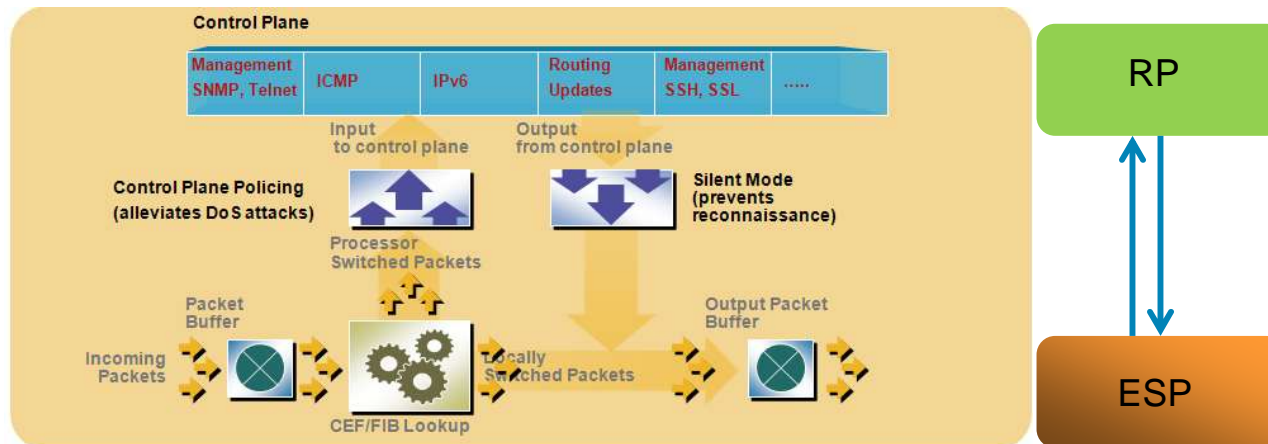


- Security Event correlation and reduction for multi-gigabit traffic
- Enables Compliance Auditing
- Reduces bandwidth consumption due to binary format
- Identifying rogue devices, mis-configured hosts, unauthorized applications and other policy violations
- Up to 40K events per second
- NetFlow export directly from Cisco QFP, hence no Routing Plane Impact
- FW and NAT events, using NetFlow v9 templates

Scalable Event Logging and Data Monitoring

Best-In-Class DDoS Detection and Mitigation

- Cisco NetFlow v9 instrumentation and telemetry export for rapid detection, classification, and traceback of DDoS traffic across the entire network topology.
- Hardware-based Control Plane Policing (CoPP) for built-in protection of the ASR1000 routing and management functions
- Hardware-based Access Control Lists (ACLs) which can be used to enforce policy, protect network infrastructure devices from attack, and as a DDoS reaction tool.
- Strict- and Loose-Mode Unicast Reverse Path Forwarding (uRPF) anti-spoofing capabilities.
- Source-based Remotely-Triggered Blackhole (S/RTBH) functionality which allows rapid blackholing of DDoS traffic at network edges serviced by the ASR1000.



Various HW-offload

IOS Feature	HW Resource	Benefits
Access Lists (v4/v6)	TCAM, and ACL Range Lookup	Faster look-up, with no degradation
uRPF	Pointer Lookup Unit	Minimal degradation with uRPF turned on
NAT/FW Session Lookup	Hash Mod Read	Holding performance with large # of sessions
Policing	QFP	No degradation for turning on CoPP to protect against DDoS
IPSec	Nitrox-II 24XX Crypto Engine	Multi-core chip for high throughput and minimal latency crypto offload

Agenda

- ASR 1000 Series Security Services
- **ASR 1000 Series IPSec Implementation**
- ASR 1000 Series Firewall Implementation
- ASR 1000 Series Firewall Logging
- ASR 1000 Series Security Software Packages
- Summary – Key Differentiators

IPSec Introduction

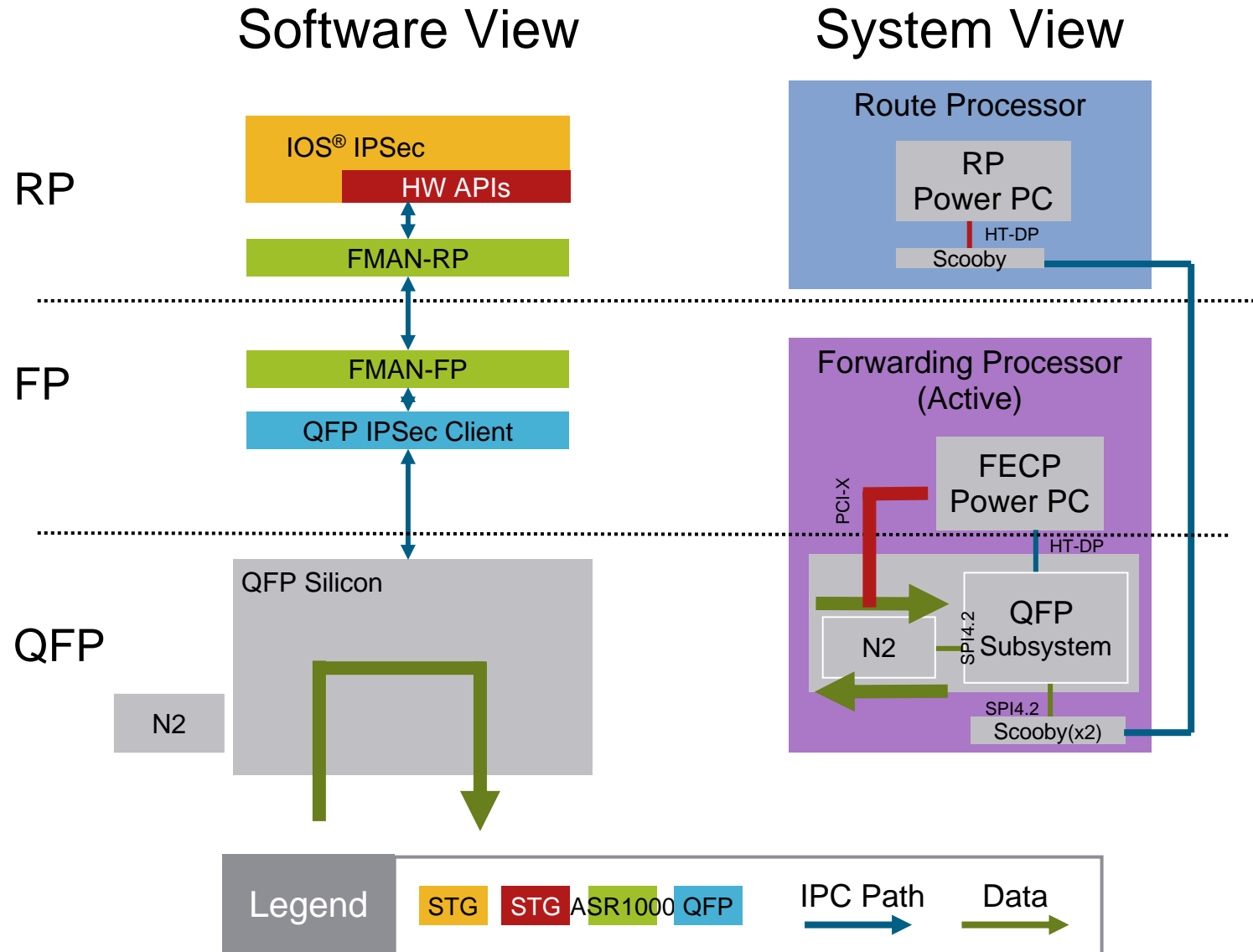
- Number of IPSec tunnels:
 - ESP-10G: 10,000 (configurable, constraints are N2, SA DRAM)
 - ESP-20G: 10,000 (configurable, constraints are N2, SA DRAM)
- Throughput: ESP-10G 2.5 Gbps (IMIX), ESP-20G 8 Gbps with 300 byte packets
- IKE session setup rate target: ~50/sec (ESP-10G)
- In-Box High Availability (HA) 6 RU configuration:
 - ESP to ESP - stateful
 - RP to RP – stateless
- Box to Box HA is post-FCS

IPSec Introduction (contd.)

- ASR 1000 IOS IPSec components are based on the 12.4(4)T feature set (rowboat*)
- Follows general Macedon/Zamboni schema
- IKE implementation resides in IOSd
- IPSec protocol is implemented in the data path (ASR)
- IOS IPSec components communicate with the data path components via a messaging protocol called “Host API” (HAPI)

Note: It is assumed that the reader is familiar with ASR 1000 system basics

Software/System Stack for IPsec on ASR 1000 Series QFP



HW Crypto Engine : Nitrox II

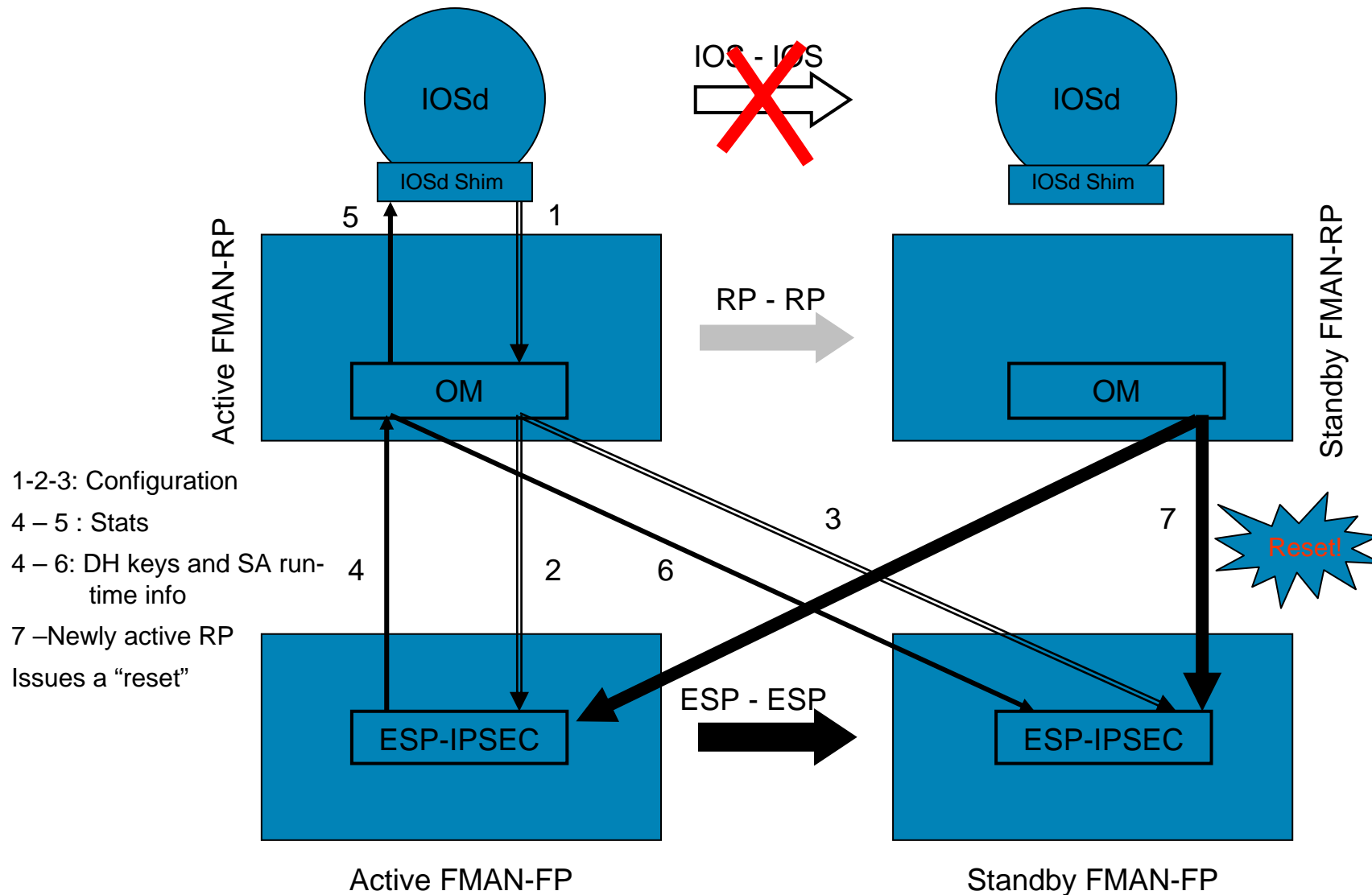
- Cavium Nitrox II CN24XX crypto coprocessor (8 core silicon) – ESP10G
- Cavium Nitrox II CN24XX crypto coprocessor (18 core silicon) – ESP20G
- Supports up to 500 IKE sessions setups per second
- Supports up to 2^{22} IPsec SA with full IPsec packet processing
- QFP accesses N2 via SPI4.2 for IPsec packet processing
- Each Nitrox core provides around 0.475-0.5 Gbps of encryption throughput
- One core is going to be used for GP_OP, and others will be used for regular IPsec processing
- ASR IPSEC-MGR (running on FECF) accesses N2 via PCI-X for IKE support
- Max. MTU size supported is 10KB on Nitrox II

IPSec Functional details

Following is the summary of the distribution of tasks done by QFP and Nitrox II (IPSec data plane)

QFP	Nitrox II
Outbound Packet Classification and context lookup	Anti Replay Check
Ingress Context Lookup (based on SPI)	Encryption/Decryption, DH
Formatting packets for Tx to Nitrox	NAT-Traversal (UDP 4500)
Receiving packets from Nitrox and reformatting them as normal IP packets	Traffic based lifetime expiry
Recovering packet state from packets when encrypted/decrypted packets return from Nitrox	
Re-assembly of fragmented IPSec packets	

ASR 1000 IPSec In-box HA

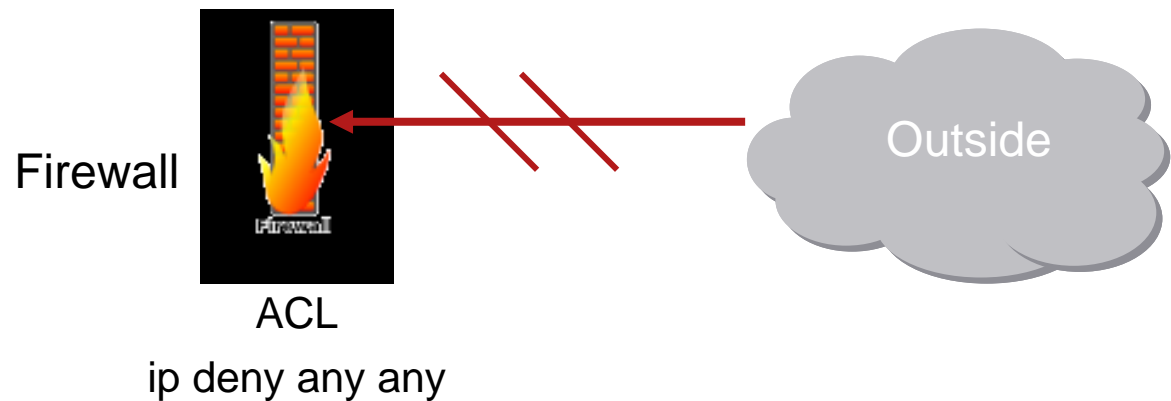
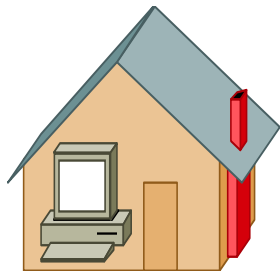


Agenda

- ASR 1000 Series Security Services
- ASR 1000 Series IPSec Implementation
- **ASR 1000 Series Firewall Implementation**
- ASR 1000 Series Firewall Logging
- ASR 1000 Series Security Software Packages
- Summary – Key Differentiators

Traditional Firewall

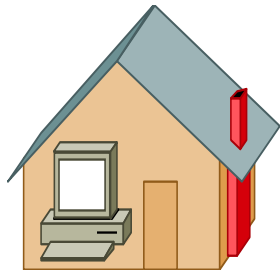
Access from outside is denied



Traditional Firewall

Traffic initiated from inside firewall creates a 'pin hole'

telnet 198.133.219.25



da 198.133.219.25 dp 23 sa 192.168.1.1 sp 2453

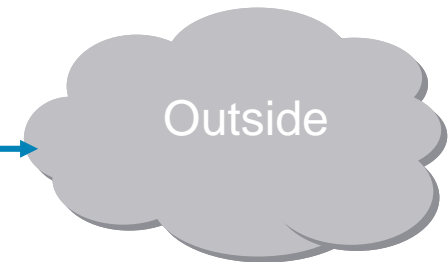


Firewall



ACL

ip deny any any

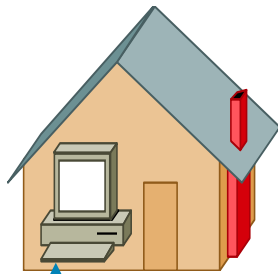


tcp permit 192.168.1.1 eq 2453 198.133.219.25 eq 23

Traditional Firewall

The return traffic of users telnet session is permitted

telnet 198.133.219.25



da 198.133.219.25 dp 23 sa 192.168.1.1 sp 2453

Firewall



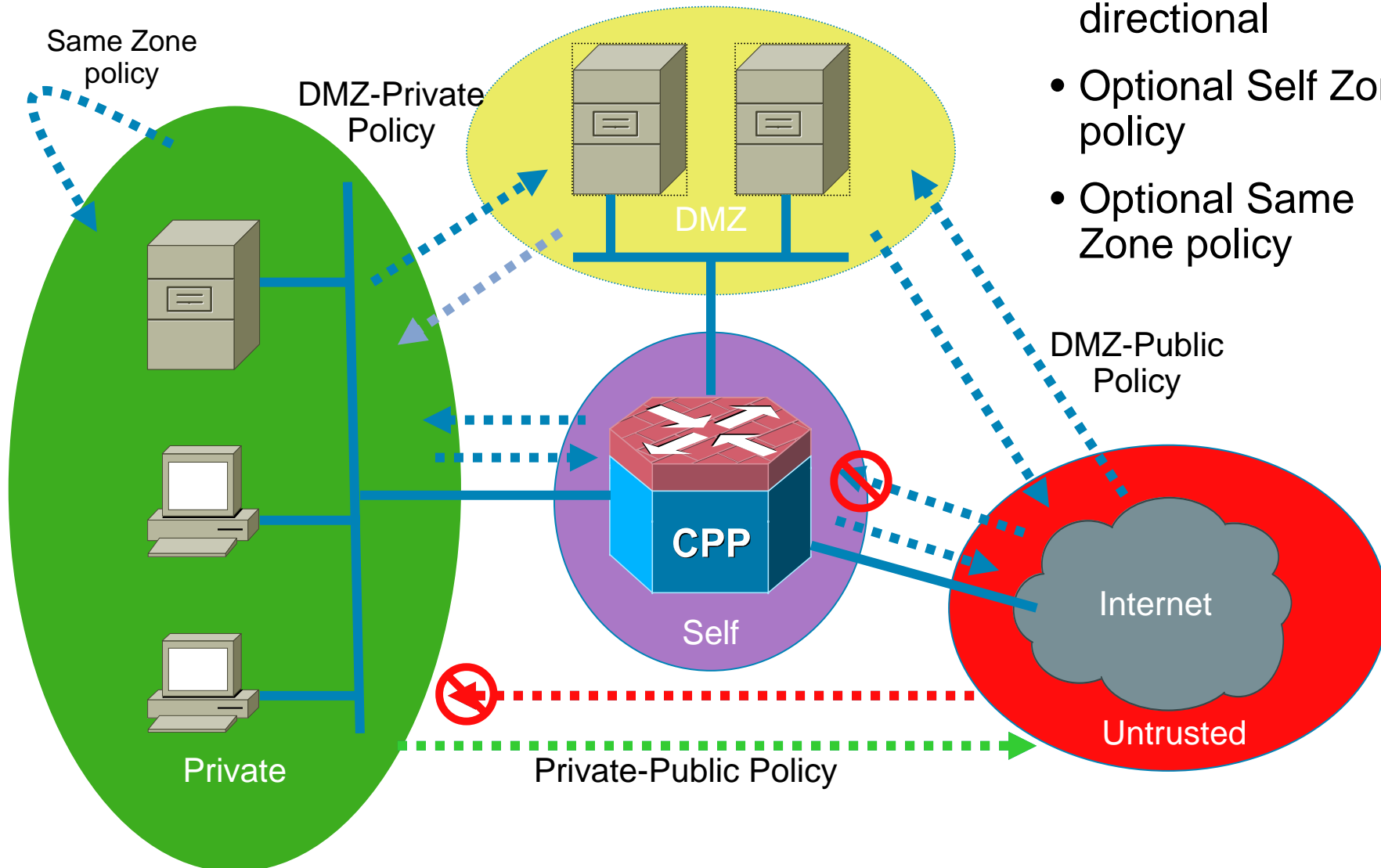
ACL

ip deny any any

tcp permit 192.168.1.1 eq 2453 198.133.219.25 eq 23



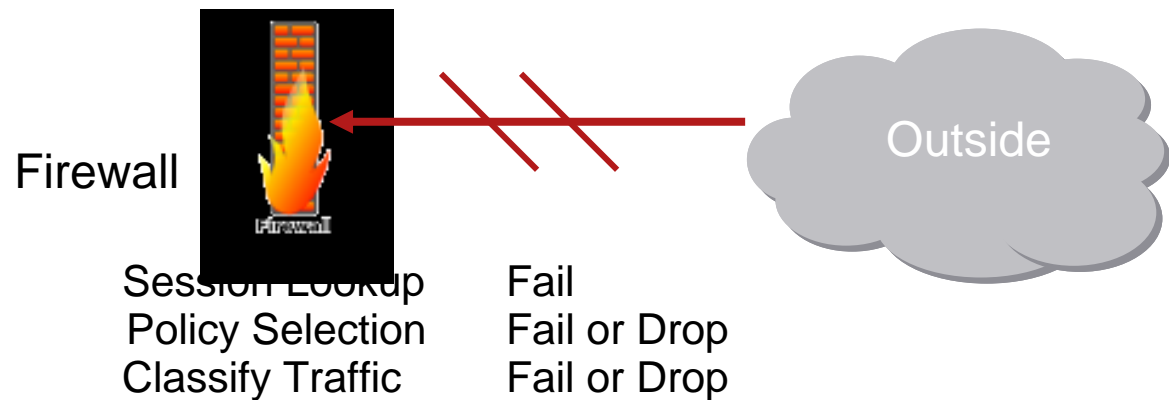
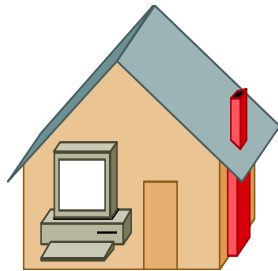
Zone Based Firewall



- Zone pairs are directional
- Optional Self Zone policy
- Optional Same Zone policy

Zone Based Firewall

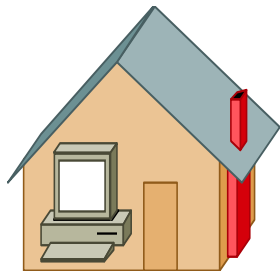
Access from outside is denied



Zone Based Firewall

Traffic initiated from inside firewall creates a session

telnet 198.133.219.25



da 198.133.219.25 dp 23 sa 192.168.1.1 sp 2453



Firewall



Session Lookup
Policy Selection
Classify Traffic
Session Create
L4 Inspect

Fail
Success
Success
Success
Success



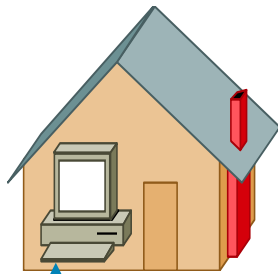
Outside

Session
192.168.1.1:2453
198.133.219.25:23

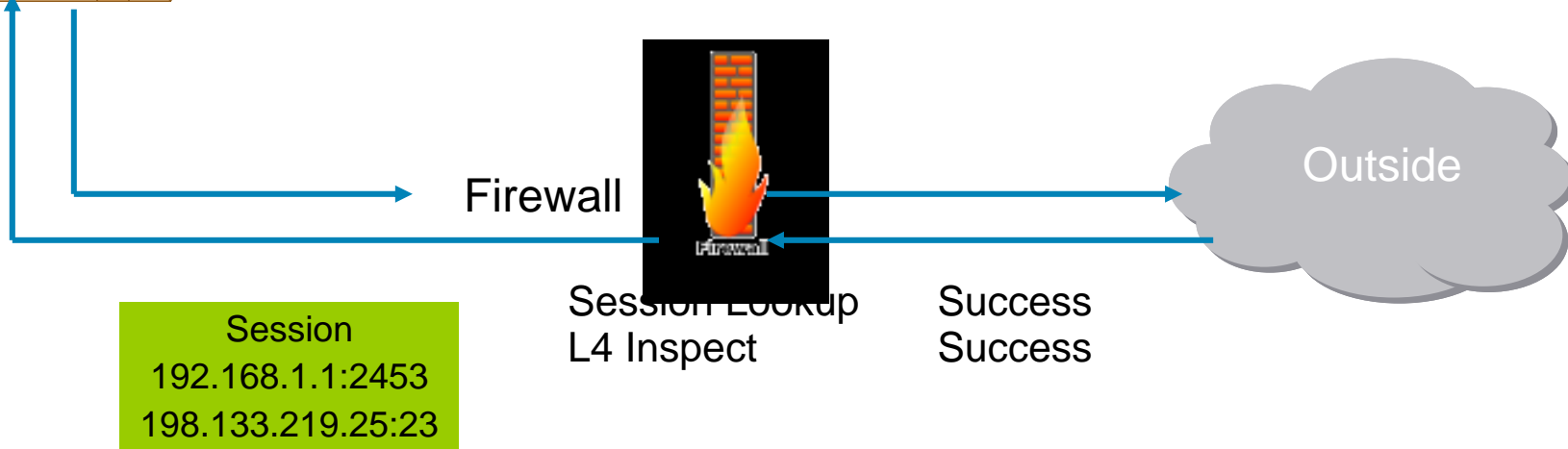
Zone Based Firewall

The return traffic of users telnet session is permitted

telnet 198.133.219.25



da 198.133.219.25 dp 23 sa 192.168.1.1 sp 2453



Zone Based Firewall Configuration

```
parameter-map type inspect pmap_tcp  
audit-trail on  
alert on  
one-minute high 10000  
tcp max-incomplete host 100
```

Parameter maps allow per class customization

```
class-map type inspect match-all c_ftp_tcp  
match protocol ftp  
match access-group 101
```

Class maps define the matching criteria

```
policy-map type inspect p1  
class type inspect c_ftp_tcp  
inspect pmap_tcp  
class class-default  
drop log
```

Policy maps group classes and define actions
Parameter map is tied to inspect action.

```
zone security z_client  
zone security z_internet
```

```
zone-pair security hi2int source z_internet destination z_client  
service-policy type inspect p1
```

Zone pairs define packet direction and identify the policy

```
interface POS0/3/0  
zone-member security z_internet
```

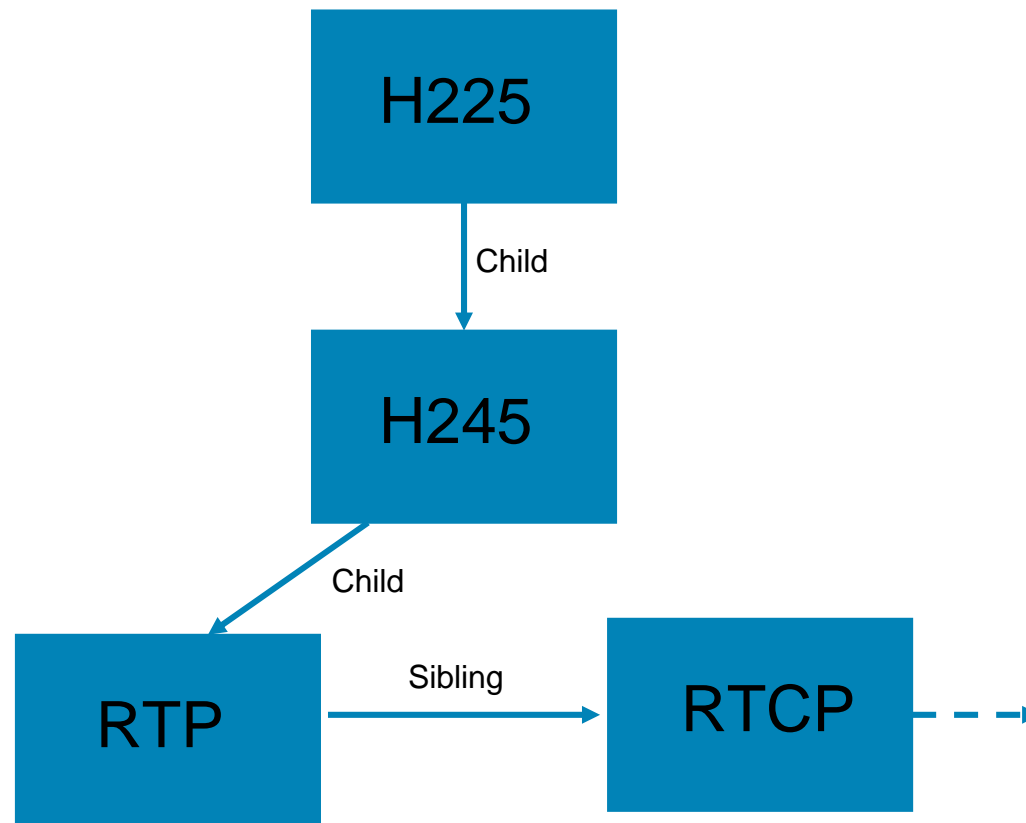
Interfaces are associated with zones.

```
interface POS0/3/1  
zone-member security z_client
```

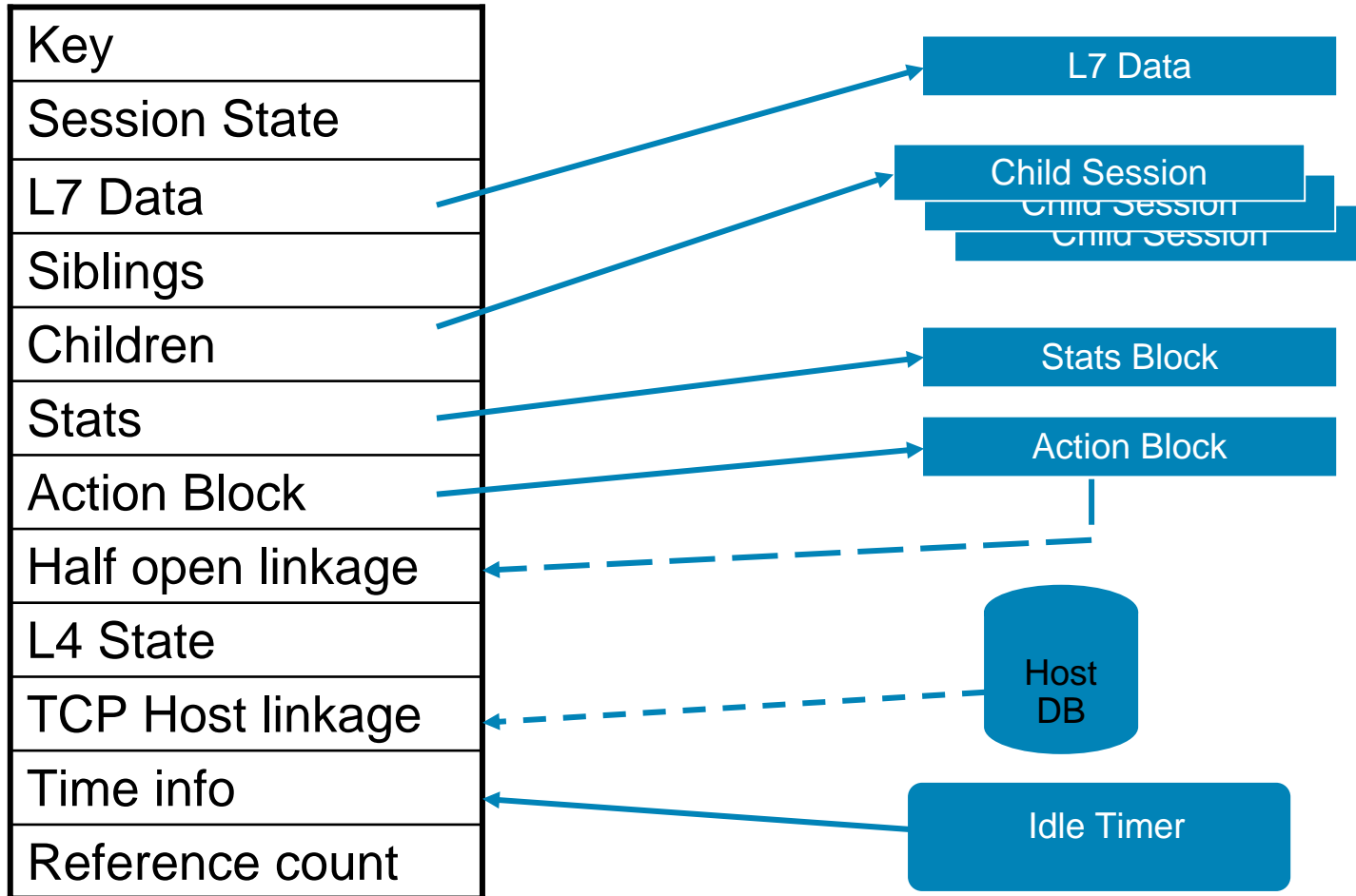
Firewall Session DB

- Two session databases
 - Normal Session (5 tuple)
 - Imprecise session (4 tuple)
- Hierarchical
- Two different type of sessions
 - L7 Inspectable (session control)
 - No L7 Inspection
- Addresses in key are normalized (numerically ordered)
- Key (ntuple)
 - Initiator Address and port
 - Responder Address and port
 - Protocol
 - Zonepair id
- Protocols
 - TCP
 - UDP
 - ICMP

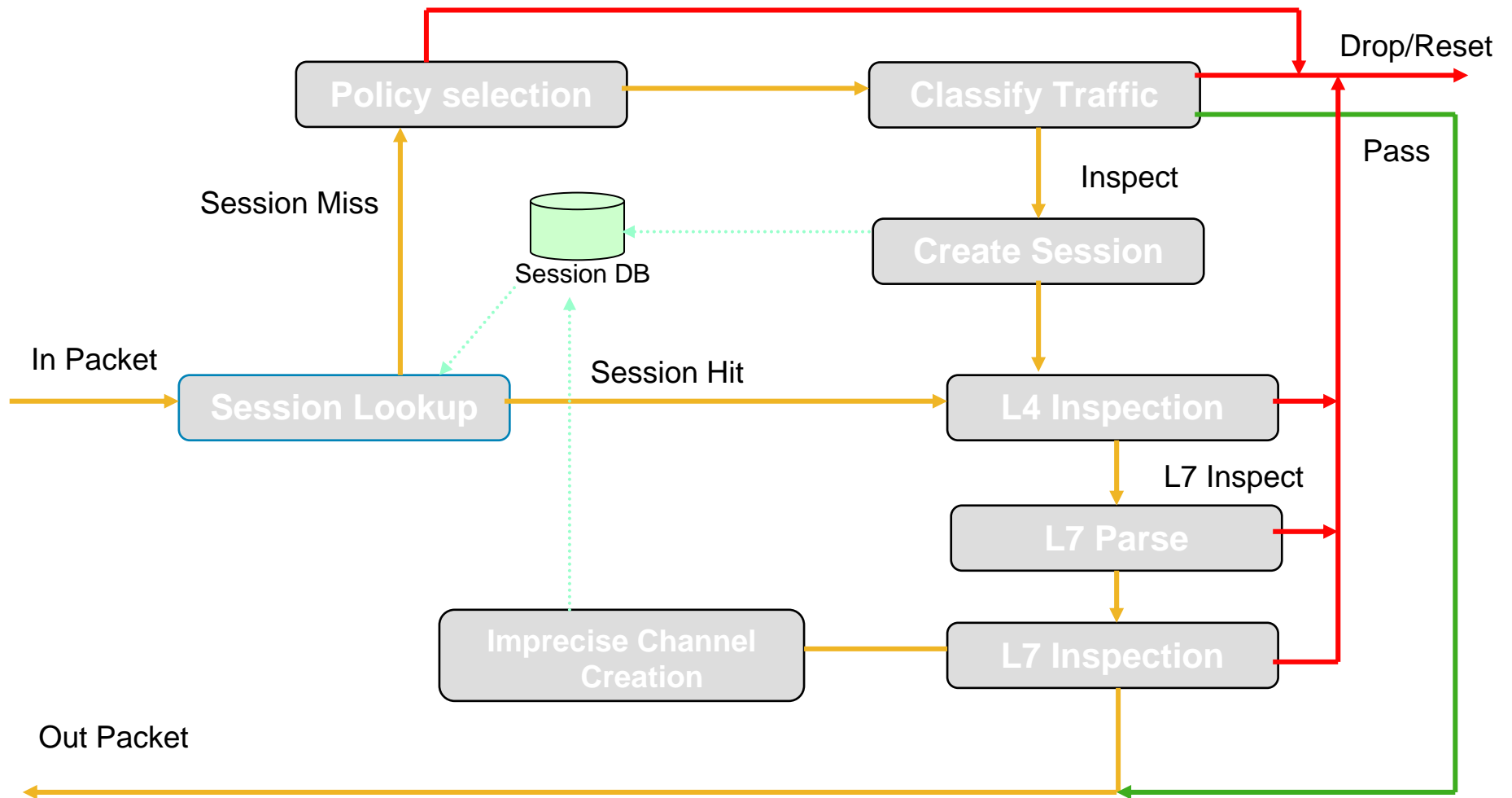
Firewall Session Hierarchy



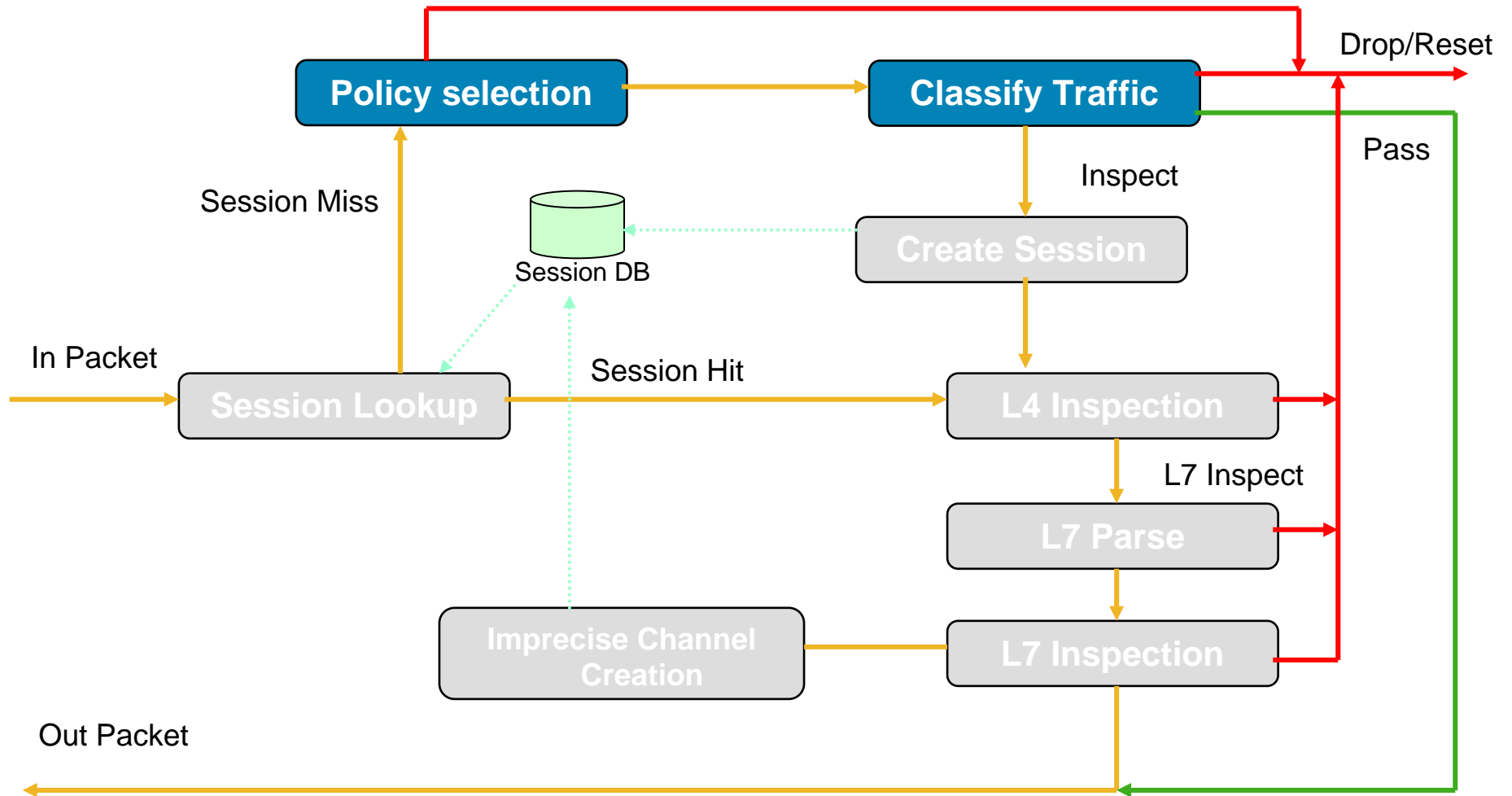
Firewall Session Entry



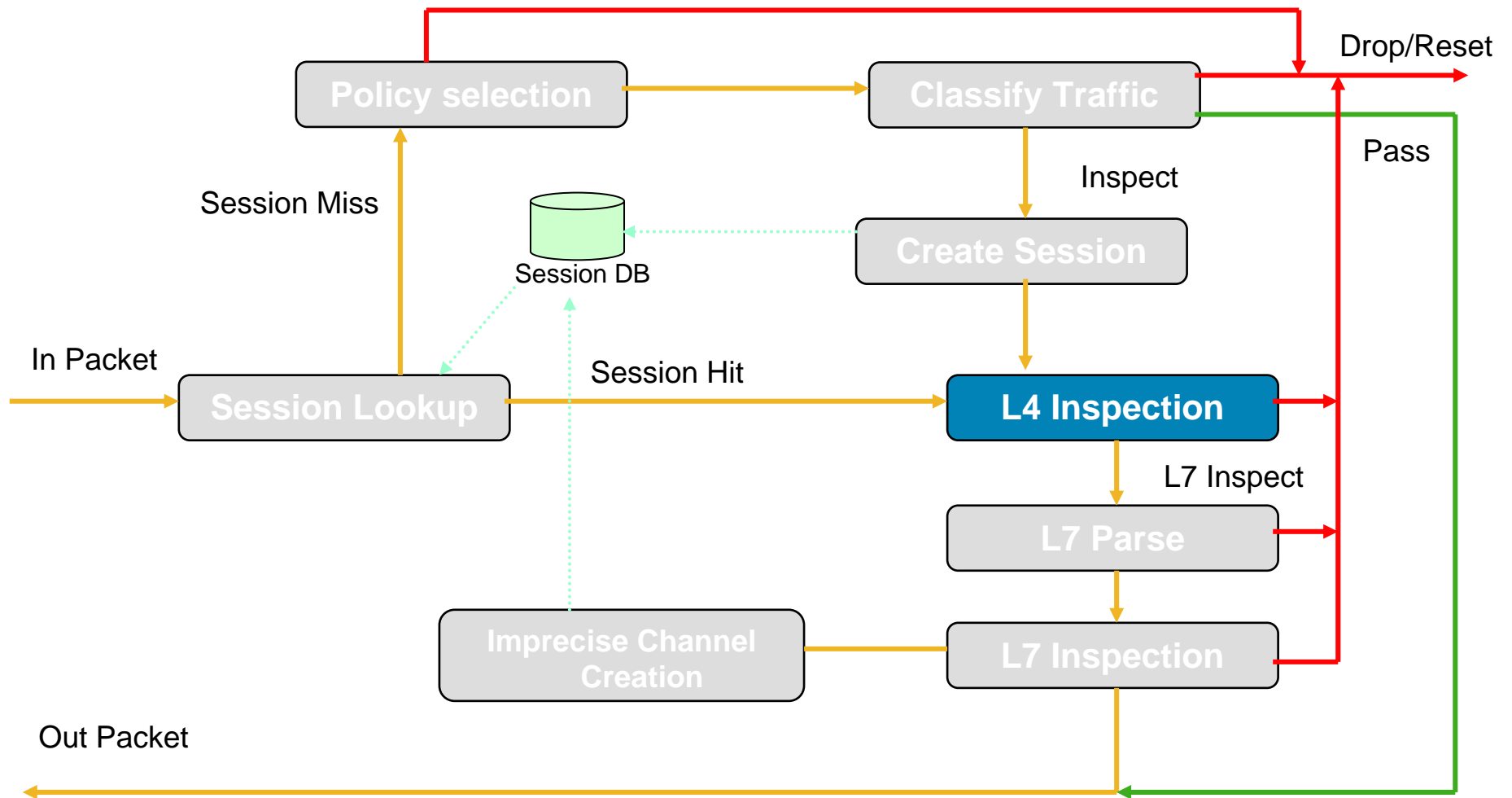
Basic Zone Based Firewall Flow



Basic Zone Based Firewall Flow



Basic Zone Based Firewall Flow



Agenda

- ASR 1000 Series Security Services
- ASR 1000 Series IPSec Implementation
- ASR 1000 Series Firewall Implementation
- **ASR 1000 Series Firewall Logging**
- ASR 1000 Series Security Software Packages
- Summary – Key Differentiators

Logging

- Firewall Logs Different type of events
 - Audit – session creation and deletion
 - Alert – Halfopen, max open or host black holing
 - Drop – Packets drop (multiple reasons)
 - Pass – Packet pass do to policy
 - Summary – Policy drop and pass summary

Logging (cont)

- Syslog

- Supported, but limited to low number of sessions per second.
 - High overhead to format records and transport records to RP.

- Netflow Event Logger

- Based on Netflow V9 UDP

- High performance

- Multiple records packet into one packet

- Raw data records.

- Option records allow compact data records

- For example class id is sent in normal record. Option record contains class id and class name.

Logging (cont)

- Netflow Event Logger

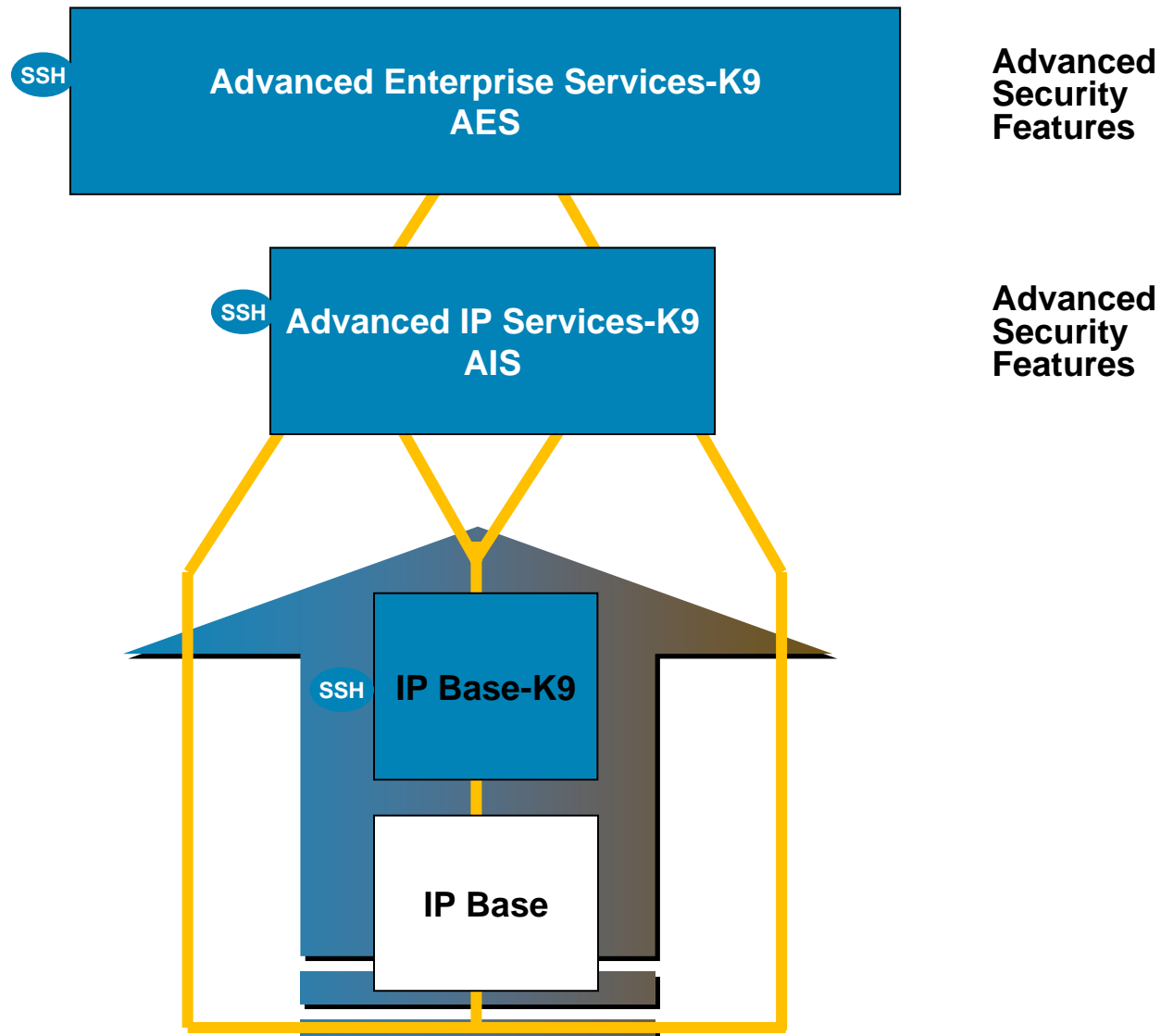
- Firewall Netflow records use standardized fields and published record formats
- Third party vendors support Netflow collectors
- Future CPP implementations may include support for
 - IPFIX – next generation netflow
 - Reliable protocol such as TCP or SCTP

Agenda

- ASR 1000 Series Security Services
- ASR 1000 Series IPSec Implementation
- ASR 1000 Series Firewall Implementation
- ASR 1000 Series Firewall Logging
- **ASR 1000 Series Security Software Packages**
- Summary – Key Differentiators

Cisco IOS Software in ASR 1000

Simplified Image Selection



Agenda

- ASR 1000 Series Security Services
- ASR 1000 Series IPSec Implementation
- ASR 1000 Series Firewall Implementation
- ASR 1000 Series Firewall Logging
- ASR 1000 Series Security Software Packages
- **Summary – Key Differentiators**

Platform Differentiators for Security

- Cisco ASR 1000 is the first router ever in Cisco routing portfolio to introduce truly embedded multi-gigabit rate NAT, Firewall, and IPsec
- Cisco ASR 1000 is the first router to have true In-box stateful HA for NAT, Firewall and IPsec at FCS
- Cisco ASR 1000 is the first router to have all L3-L7 NAT and Firewall processing done inside Forwarding Processor
- Cisco ASR 1000 is the first router to have an option for NetFlow v9 based high speed logging export for NAT and Firewall
- Cisco ASR 1000 is the first router to have In-box stateful NAT and Firewall switchover times of less than 50ms

