



Architectural issues of Grid Security

3rd TERENA NREN-Grids Workshop

Paris, April 28th 2006

Dirk Schroetter

Cisco Systems EMEA

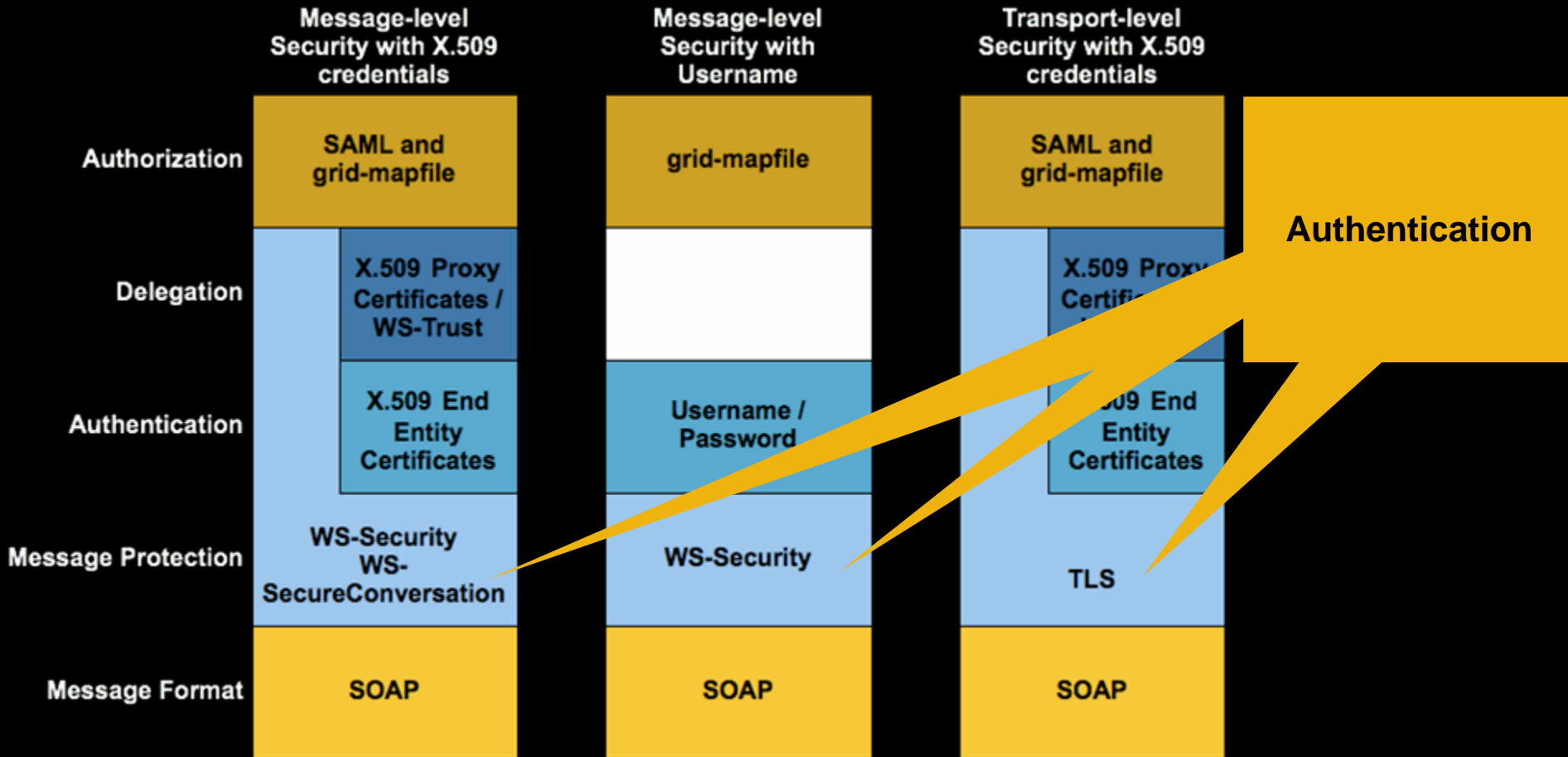
Consulting System Engineer

dschroet@cisco.com

Security Consideration fro Grid Middleware



GLOBUS 4.0 Security architecture



Security considerations of GLOBUS 4.0

- All the security elements are there

Authentication

Confidentiality

- But are they used?

Quote from “Globus Toolkit Version 4 Grid Security Infrastructure: A Standards Perspective“:

“GT4.0's support for message-level security is important as it allows us to comply with the WS-Interoperability Basic Security Profile. However, because current message-level security implementations have relatively **poor performance**, GT4.0 services use transport- level security by default. This choice is driven by user performance demands.“

Specialized Processors?

- **NEs exist that offload SSL/TLS/X.509 processing**
- **These could be used to minimize the performance hit of message-based authentication/confidentiality**
- **Architectural impact**
 - **Certificates would be associated with the NEs**
- **XML-Processors could implement „application firewall“ through content filtering**
- **Feasible from NW perspective, also for users?**

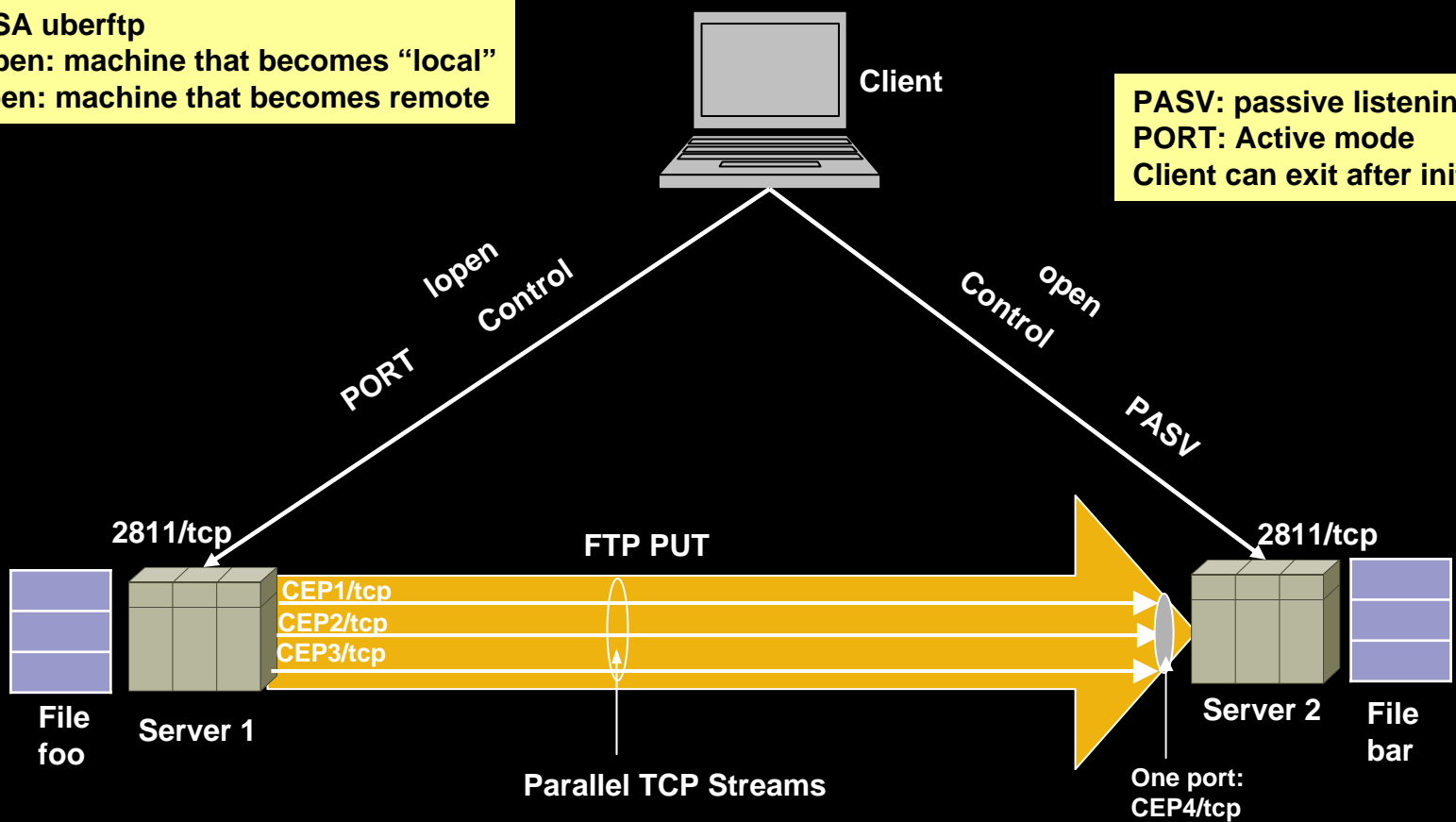
Security considerations for GridFTP

2

GridFTP – 3rd Party Transfer

NCSA uferftp
 lopen: machine that becomes “local”
 open: machine that becomes remote

PASV: passive listening mode
PORT: Active mode
 Client can exit after initiating

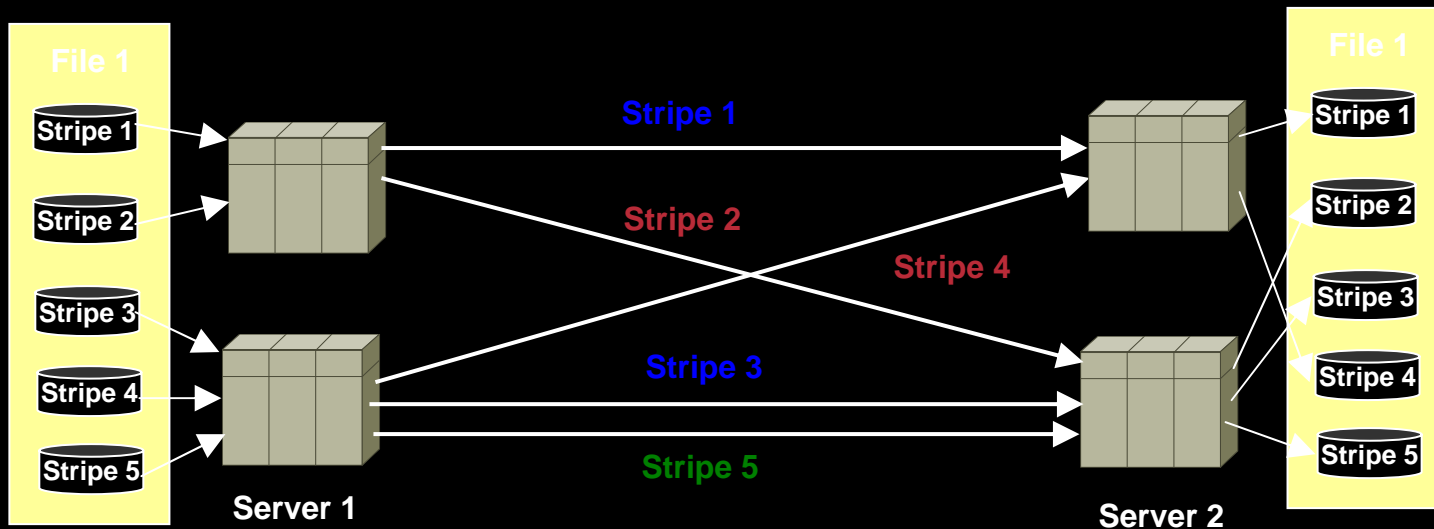


GT4 3rd party FTP: `globus-url-copy -vb -tcp-bs 2097152 -p 4 gsiftp://other.machine.my.edu/tmp/foo gsiftp://remote.machine.my.edu/tmp/bar`

CEP: Controlled Ephemeral Ports by setting `$export GLOBUS_TCP_PORT_RANGE = 45000, 45100`, for example

GridFTP – Striped Transfer

- A file is striped and “owned” by a node (in a cluster, for example)
- Perform interleaved transfers, thus increasing throughput (specially network throughput)



Problems with GridFTP

- **Control channel well behaved**

But (commercial) stateful firewalls don't support the protocol extensions

- **Data Channel operation problematic**

For passive operation of target server, the Firewall needs to be open on the complete range of Ephemeral ports

May be protected with ACLs

Striped transfers have no footprint in the data channel that indicate the addition or removal of a data connection

- **From Security perspective, one would wish for a different protocol**

Firewall issues



Current commercial firewalls ...

- **Scale to throughput of about 5 Gbit/s**
 - Good, but still not enough for single flows of 10Gbit/s**
 - Clustering possible, but load-balancing requires distinct 5-tuples**
- **Stateful firewalls usually only support “standard” protocols**
 - Special ASIC development for a relatively small market**
 - Typical ASIC development time 12-18 months**
- **Can be augmented by “application-aware” appliances that offload processing**
- **But is that really what the community wants?**

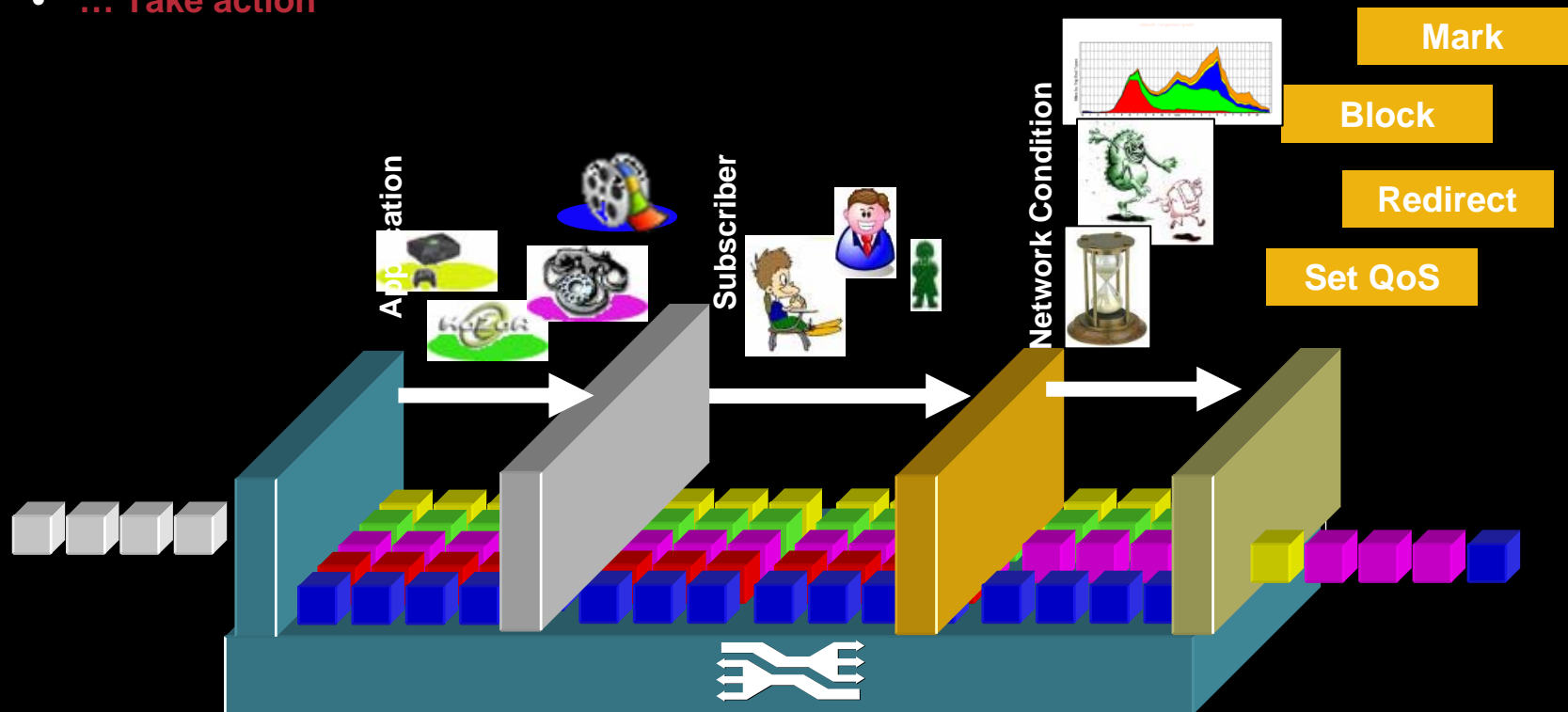
Service Control to the rescue?

4

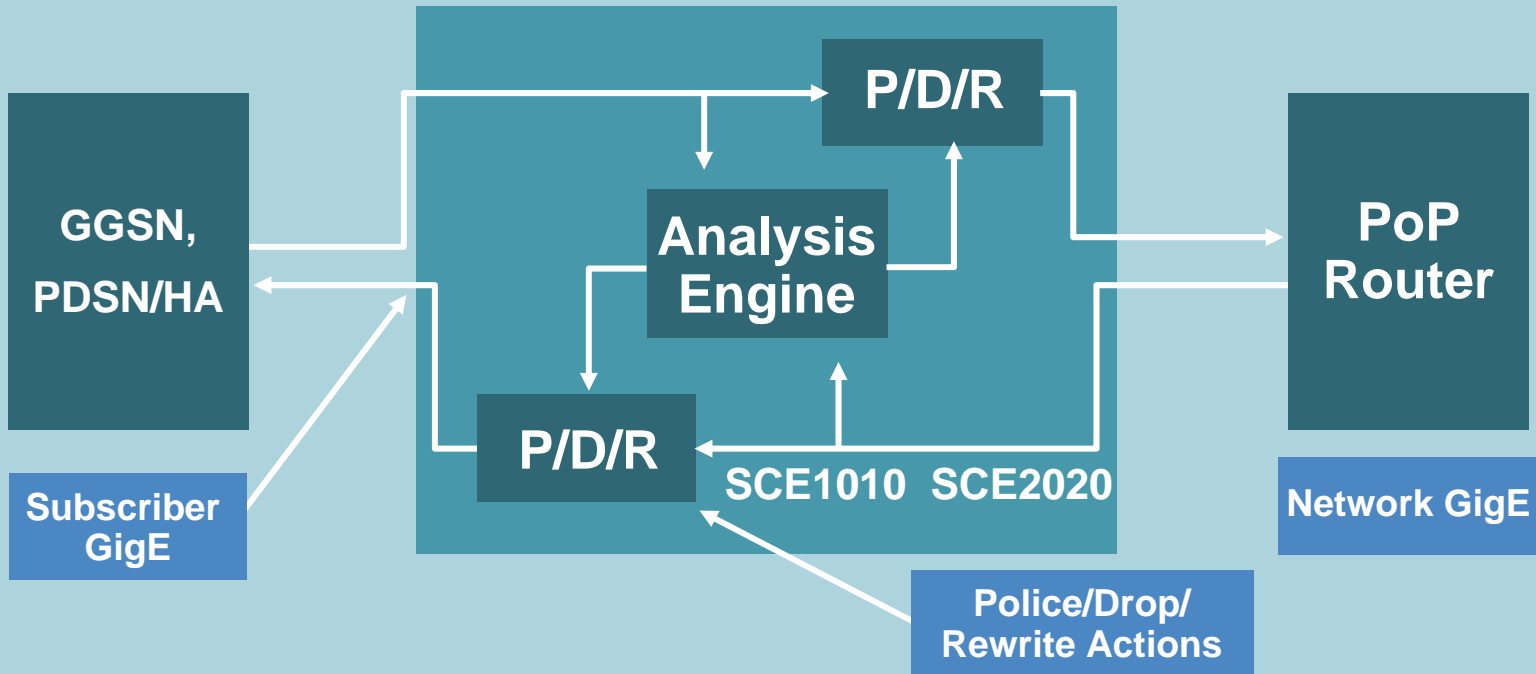
Basic Idea

Intelligent Inspection and Control of IP Packets

- ... Classify to end-user application; determine application semantics
- ... Map to subscriber identity, policy and state
- ... Select action based on network condition—time of day, congestion, other concurrent activities
- ... Take action



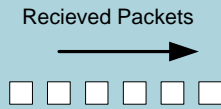
Product Concept “Bump-on-a-Wire”



- **Stateful Analysis Engine with application awareness**—sees all packets in both directions
- Analysis Engine implements **Business Rules** via **Dynamic Control Policy** on a **subscriber basis** (ex. rate policing, packet drop or header rewrite actions)
- **Packets are not routed or switched**; packets from a subscriber interface always go to the corresponding network interface, and vice-versa

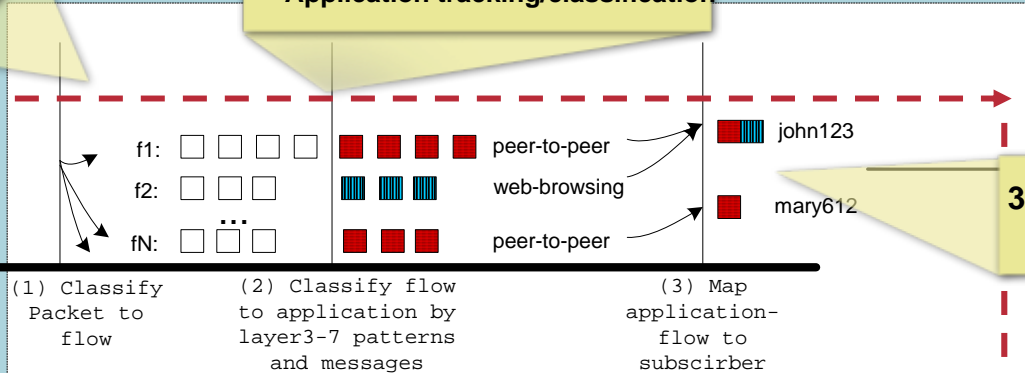
Logical Flow

1. Packets classified into bi-directional flows

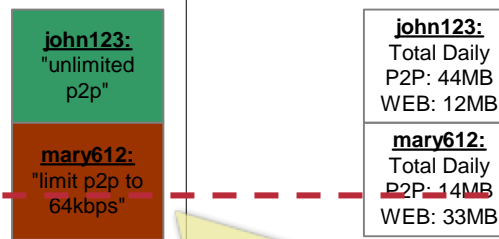
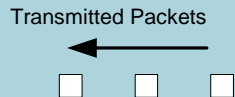


2. Flows classified by application/content:

- TCP state machine,
- Signature detection,
- Application tracking/classification



3. Flow mapped to subscriber-context



4. Subscriber state:

- Policy Package
- Usage/Quota

6. Packet level enforcement

(6) Perform Bandwidth Shaping & Control

(5) Select Enforcement Policy

(4) Maintain Subscriber State & Quota

5. Rule/action selected:
Block, redirect, BW control, queue, mark, report

What Service Control can do ...

- **Scale to throughput of about 10 Gbit/s**
- **Can police/drop/rewrite on based on any information in the packet (deep packet inspection)**
- **Allows for “external” classifiers**
- **... but it is not a classical firewall where ports are opened and closed. The intelligence is in the packet classifier.**

Q and A



CISCO SYSTEMS

