WELCOME

PROVIDING SECURE INTERNET SERVICES

ARBOR TMS INTEGRATION

HANNU AHOLA, ALCATEL-LUCENT

SReXperts
Warsaw 2011

September 16th, 2011

AT THE SPEED OF IDEAS™

Alcatel·Lucent

AGENDA

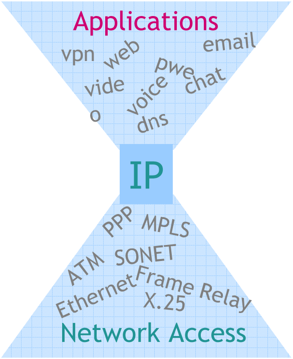
1. Introduction
2. Arbor solution overview
3. Integrated threat mitigation
4. Use cases
5. Deployment models
6. Conclusions

AGENDA

1. Introduction
2. Arbor solution overview
3. Integrated threat mitigation
4. Use cases
5. Deployment models
6. Conclusions

MARKET TRENDS IMPACTING SERVICE PROVIDERS

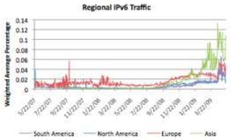
Everything over IP



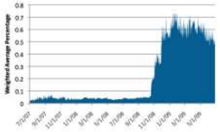
Common IP Network Layer:
Cost savings, more flexible

Massive explosion in traffic

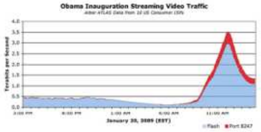
IPv6 growth



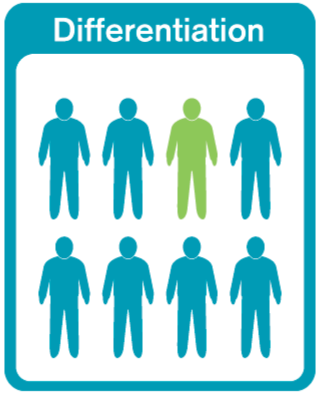
Changing apps



Video explosion



Unique services for customers



Managed Security Services, MPLS VPN Security Services, etc.

Bigger & Smarter Network Threats

Availability

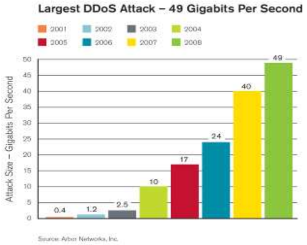
99.9%

99.95%

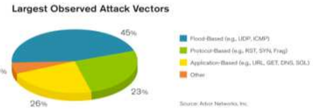
99.99%

99.999%

Bigger



&



Smarter

DDOS IS A GROWING & EVOLVING TREND

The *convergence* of more attack motivations and the increased availability of botnets equals more attacks

More Attack Motivations

- *Geopolitical* "Burma taken offline by DDOS attack"
- *Protests* "Visa, PayPal, and MasterCard attacked"
- *Extortion* "Techwatch weathers DDoS extortion attack"

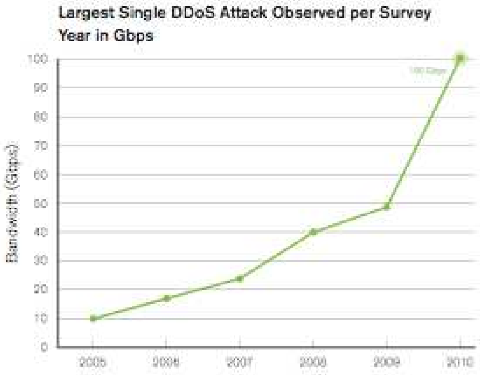
+

Greater Availability of Botnets

- *Better Bots* More infected PCs with faster connections
- *Easy Access* Using web 2.0 tools to control botnets
- *Commoditized* Cloud-based botnets, cheaper

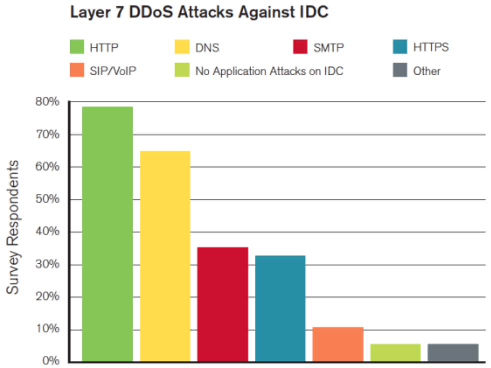
Increased Volume

Largest *volumetric DDoS has* grown from 9 to 100 Gbps in 5 years



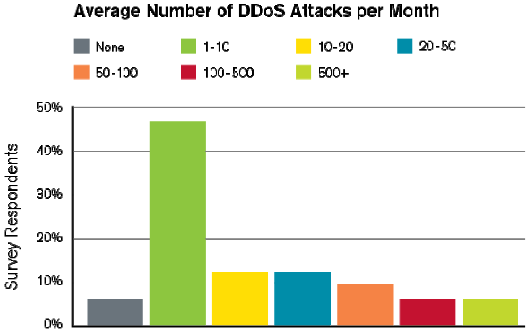
Increased Complexity

Over quarter of attacks are now *application-based DDoS mostly targeting HTTP, DNS, SMTP*



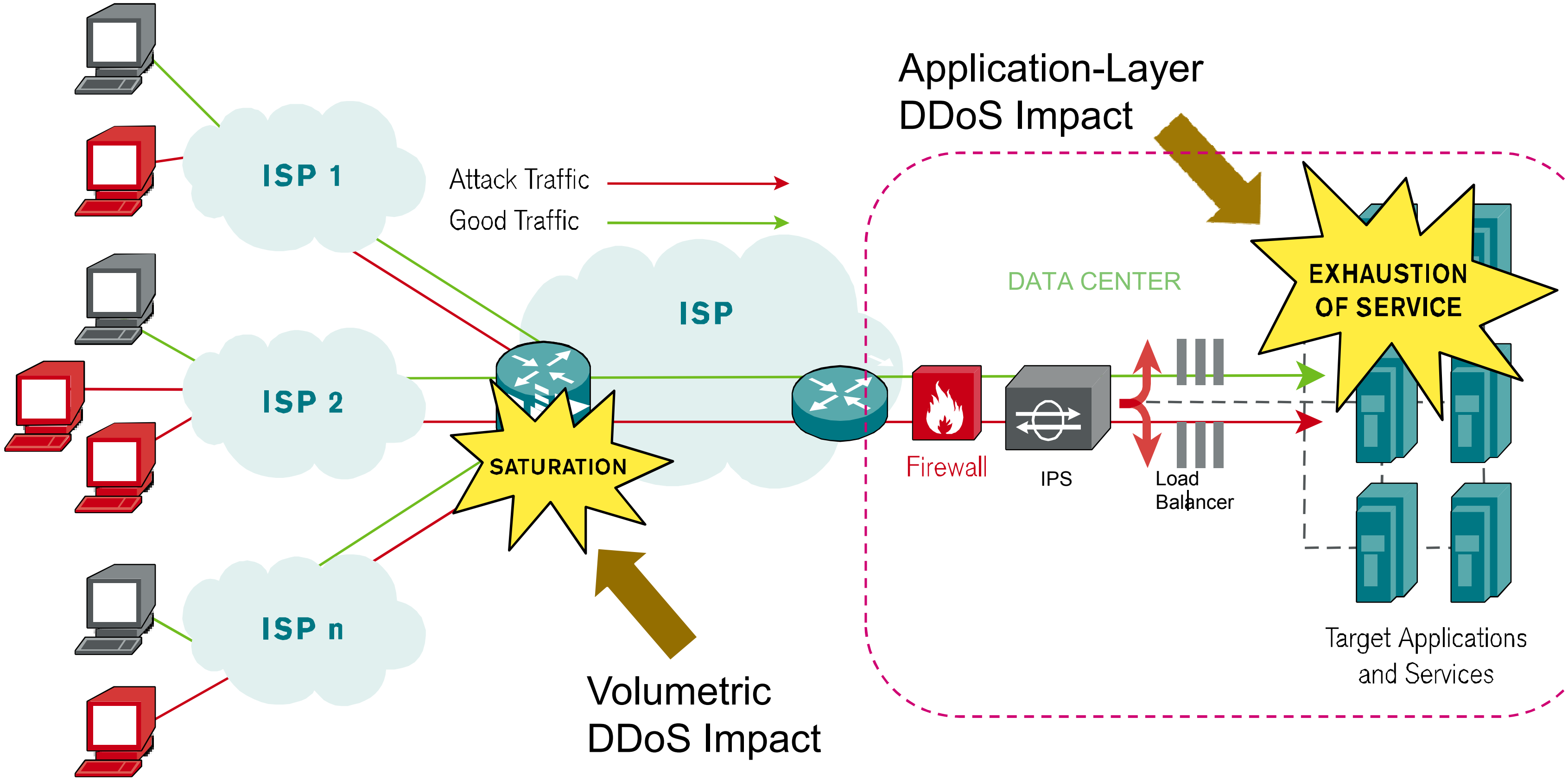
Increased Frequency

More than 50% of data center operators are seeing more than 10 attacks per month



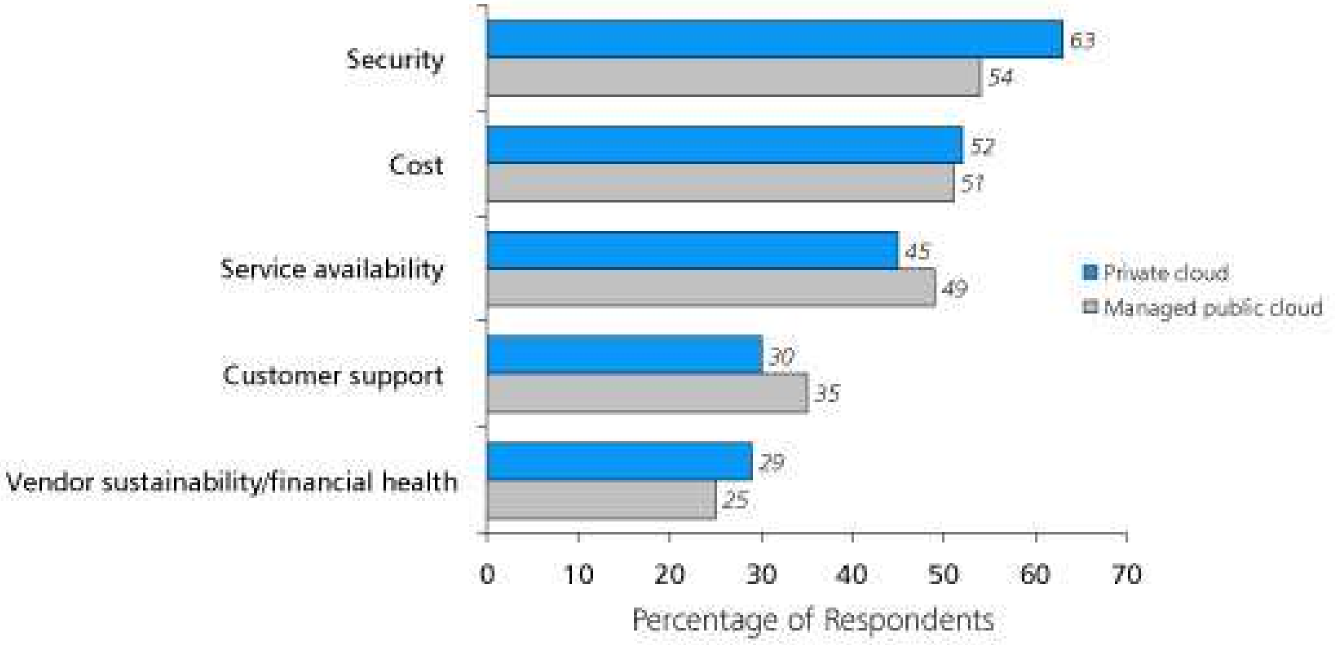
THE EVOLVING THREAT AGAINST DATA CENTERS

Both *volumetric* and *application-layer* DDoS attacks can bring down critical data center services



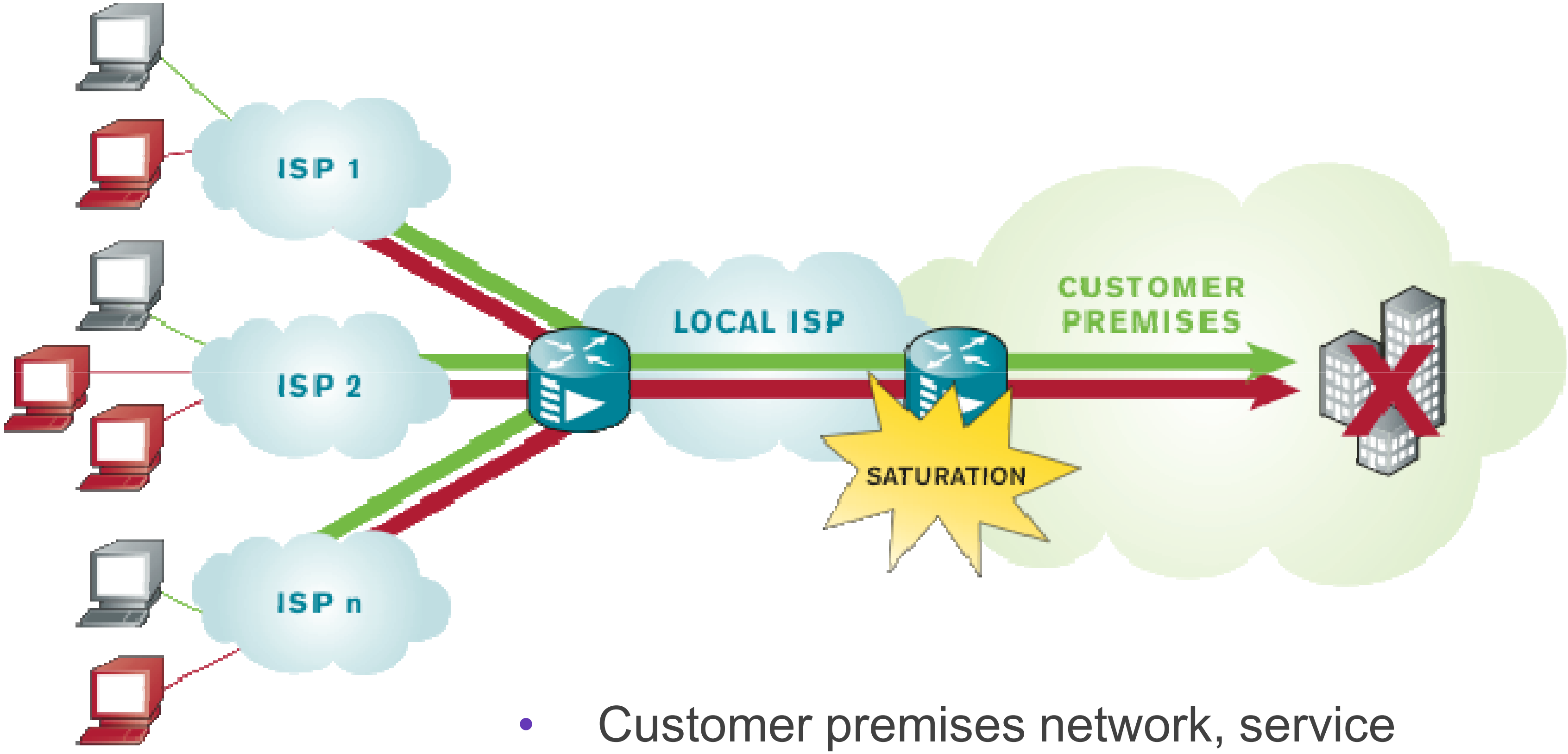
CLOUD SECURITY TOP CONCERN FOR ENTERPRISES

- Enterprises seek five main attributes when choosing a cloud service provider or partner (Yankee: Anywhere Enterprise - Large: 2009 U.S. Transforming Infrastructure and Transforming Applications Survey, Wave 1-12)



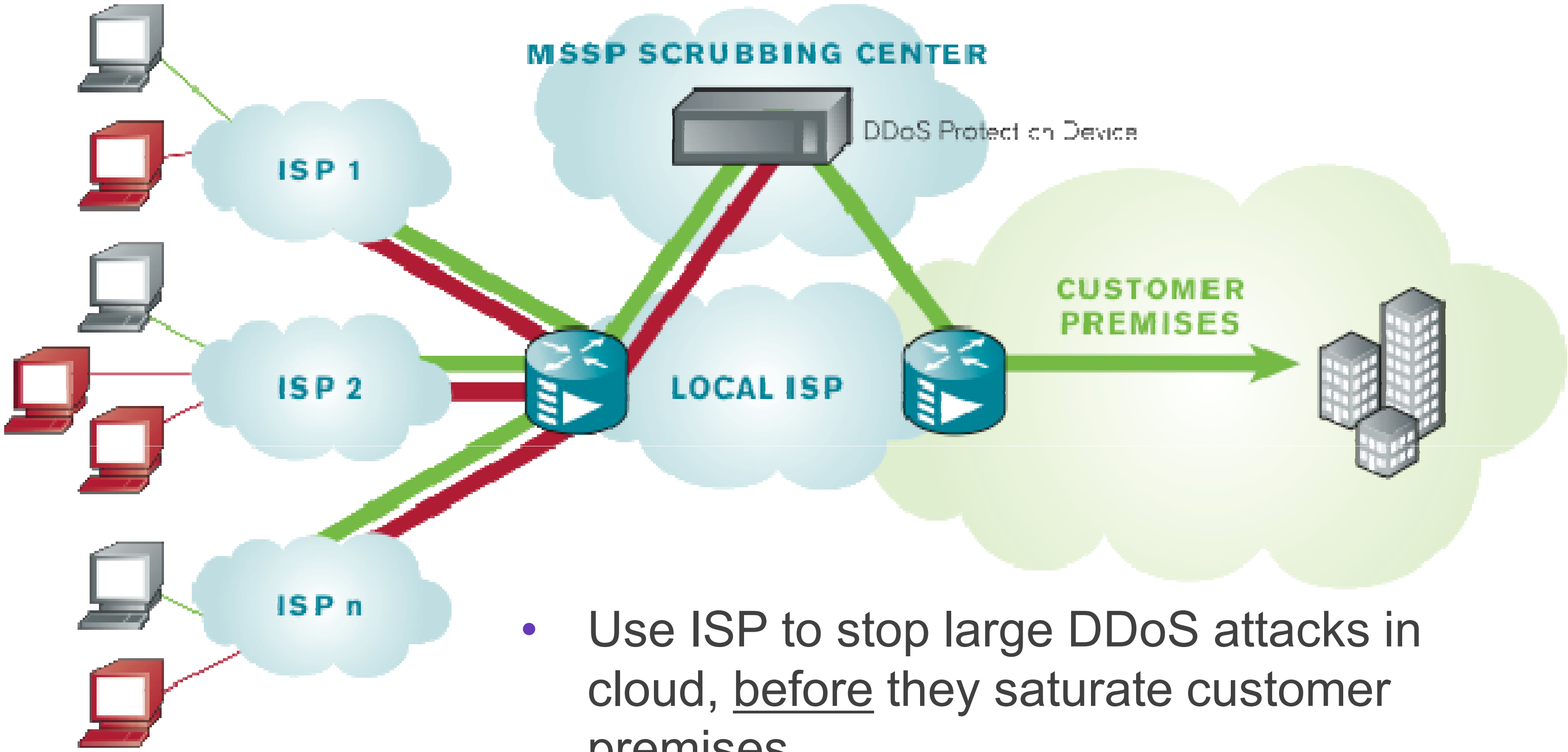
- Enterprises hesitant to move to cloud computing because cloud providers offer less-than-adequate security
  - If providers embrace “clean clouds”, which use the cloud’s key attributes to provide far better security than what’s considered enterprise-grade today, they can spur adoption

A VOLUMETRIC DDOS ATTACK..



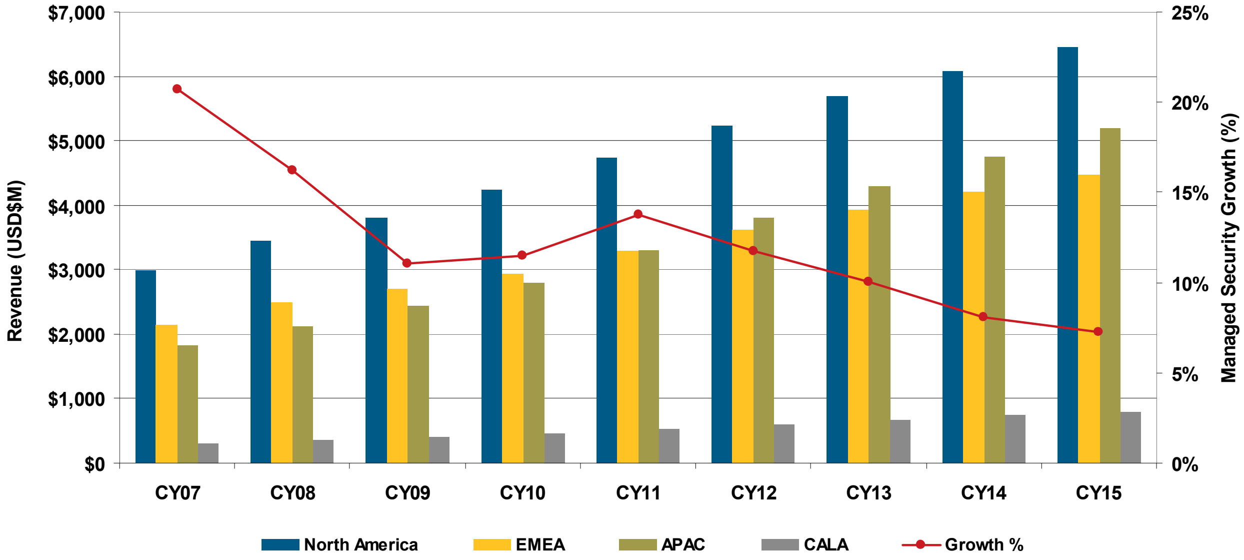
- Customer premises network, service and security infrastructure is overwhelmed

…IS BEST STOPPED IN AN ISPs CLOUD



- Use ISP to stop large DDoS attacks in cloud, before they saturate customer premises
- ISPs work with other ISPs to stop “distributed” DOS attacks at peering/transit points

MANAGED SECURITY SERVICES
MARKET AND OPPORTUNITIES



~10% YoY growth

Infonetics - Managed Security Services and SaaS
Biannual Market Size and Forecasts - 2011

- Integrated Security services – Service Provider opportunities
  - Generate new revenue – E.g. CleanPipe Service
  - Differentiate your network & IDC service offerings
  - Protect your networks & services from DDoS attacks
  - Lower security related support costs
  - Increase customer loyalty

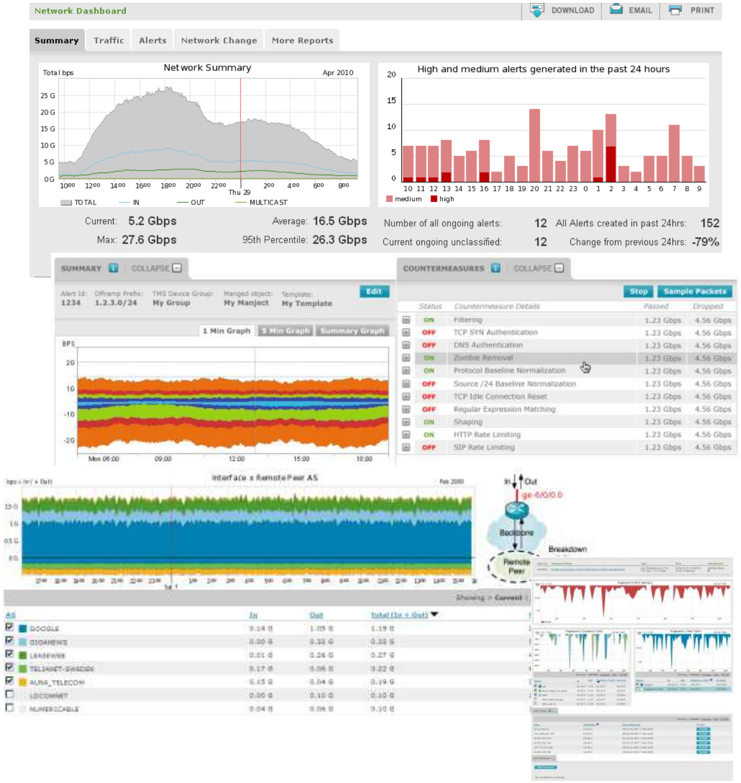
AGENDA

1. Introduction
2. Arbor solution overview
3. Integrated Threat Mitigation
4. Use cases
5. Deployment models
6. Conclusions

THE PEAKFLOW SP SOLUTION

ARBOR® NETWORKS
How networks grow™

- Providing pervasive network visibility and deep insight into services
  - Leverage "IP flow" technology for broad network visibility,
- Protecting network and service availability via comprehensive threat management
  - Detection, surgical mitigation and reporting of DDoS and application-layer attacks that threaten business services
- Enabling in-cloud services
  - A platform which offers the ability to deliver new, profitable, revenue-generating services (i.e., DDoS protection and MPLS VPN visibility)



Current: 5.2 Gbps
Max: 27.6 Gbps
Average: 16.5 Gbps
95th Percentile: 26.3 Gbps

Number of all ongoing alerts: 12
Current ongoing unclassified: 12
All Alerts created in past 24hrs: 152
Change from previous 24hrs: -79%

Alert Id: 1234
Offramp Prefix: 1.2.3.0/24
TMS Device Group: My Group
Manged object: My Manject
Template: My Template

	Status	Countermeasure Details	Passed	Dropped
⊞	ON	Filtering	1.23 Gbps	4.56 Gbps
⊞	OFF	TCP SYN Authentication	1.23 Gbps	4.56 Gbps
⊞	OFF	DNS Authentication	1.23 Gbps	4.56 Gbps
⊞	ON	Zombie Removal	1.23 Gbps	4.56 Gbps
⊞	ON	Protocol Baseline Normalization	1.23 Gbps	4.56 Gbps
⊞	OFF	Source /24 Baseline Normalization	1.23 Gbps	4.56 Gbps
⊞	OFF	TCP Idle Connection Reset	1.23 Gbps	4.56 Gbps
⊞	OFF	Regular Expression Matching	1.23 Gbps	4.56 Gbps
⊞	ON	Shaping	1.23 Gbps	4.56 Gbps
⊞	ON	HTTP Rate Limiting	1.23 Gbps	4.56 Gbps
⊞	OFF	SIP Rate Limiting	1.23 Gbps	4.56 Gbps

All	In	Out	Total (In + Out)
☑ GOOGLE	0.14 G	1.05 G	1.19 G
☑ GIGANEWS	0.00 G	0.32 G	0.33 G
☑ LEASEWEB	0.01 G	0.26 G	0.27 G
☑ TELIANET-SWEDEN	0.17 G	0.06 G	0.22 G
☑ AUNA_TELECOM	0.15 G	0.04 G	0.19 G
□ LDCOMNET	0.00 G	0.10 G	0.10 G
□ NUMERICABLE	0.04 G	0.06 G	0.10 G

Alcatel·Lucent

THE PEAKFLOW SP SOLUTION

KEY SOLUTION COMPONENTS

Arbor Peakflow SP CP

Model: CP-5500

Collector Platform (CP collects IP Flow data and manages other Peakflow SP devices (e.g. PI, TMS)

Arbor Peakflow SP TMS

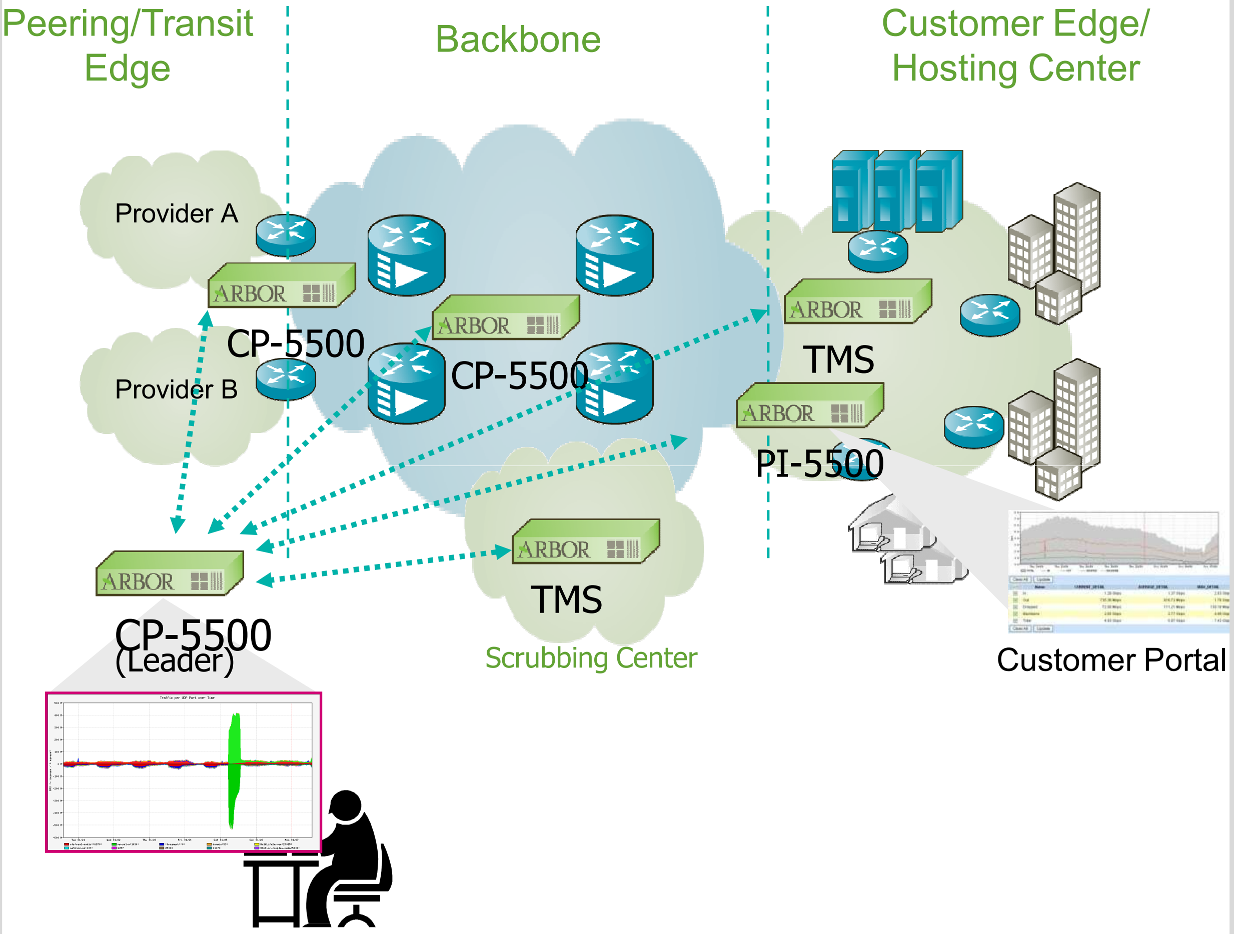
Models: TMS-1200/2x00/3x00/4x00

Threat Management System (TMS) used for surgical mitigation of attacks, service visibility and protection.

Arbor Peakflow SP PI

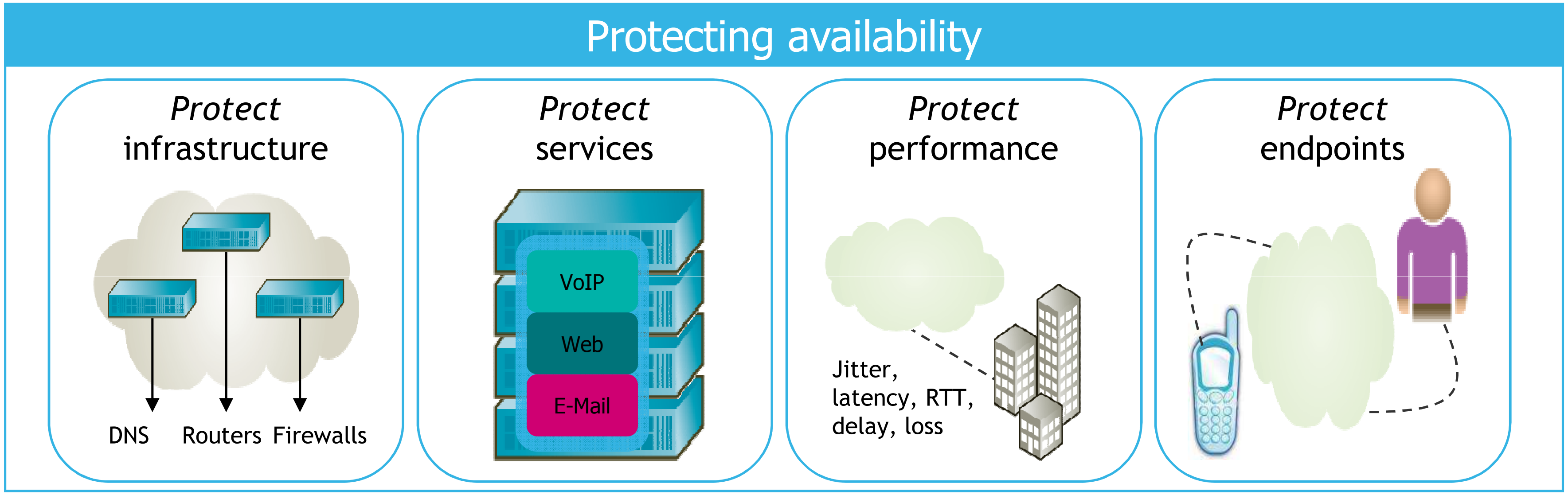
Model:PI-5500

Portal Interface (PI) provides user interface for customer portal, increases scalability and adds redundancy for Peakflow SP based managed services.



Central Console for Network Visibility and Threat Management

THE PEAKFLOW SP SOLUTION



Visibility is the foundation for security and thus protecting availability

ARBOR – ALCATEL-LUCENT RELATIONSHIP

RESELLER

- ALU can resell Arbor’s Peakflow SP and TMS products

OEM

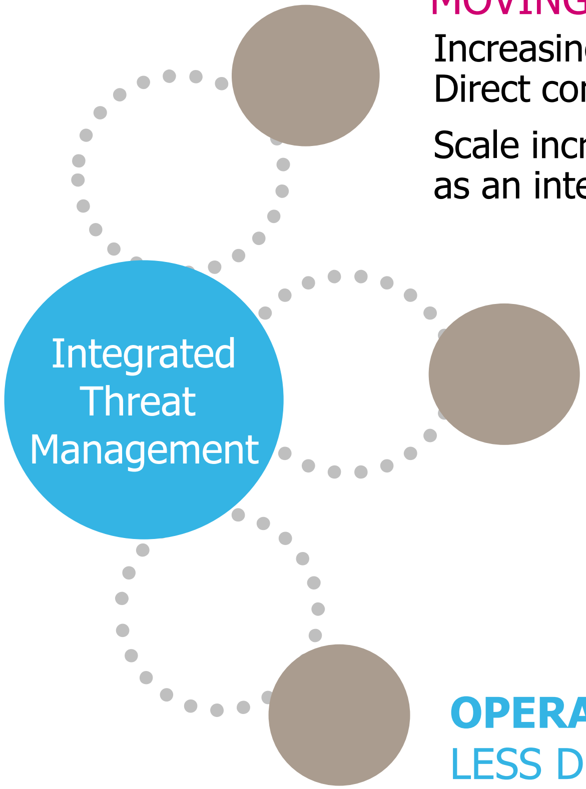
- Arbor’s TMS technology embedded into ALU 7750 SR
- Pre-sales - Arbor will provide assistance
- Post Sales - ALU provides Tier 1, Arbor provides Tier 2

Leverage 7750 SR for in-cloud DDoS mitigation

AGENDA

1. Introduction
2. Arbor solution overview
3. Integrated threat mitigation
4. Use cases
5. Deployment models
6. Conclusions

DRIVERS FOR INTEGRATED THREAT MANAGEMENT



MARKET ADOPTION

MOVING FROM NICHE TO MAINSTREAM

Increasing enterprise dependency on online service availability. Direct commercial impact, reputation damage, etc.

Scale increase makes it feasible to consider threat management as an integral part of the PE functionality

ENABLER FOR DISTRIBUTED DEPLOYMENT

DROP ATTACK TRAFFIC SOONER

Integration allows simpler and more cost-effective distributed deployment, e.g., no interconnect ports needed.

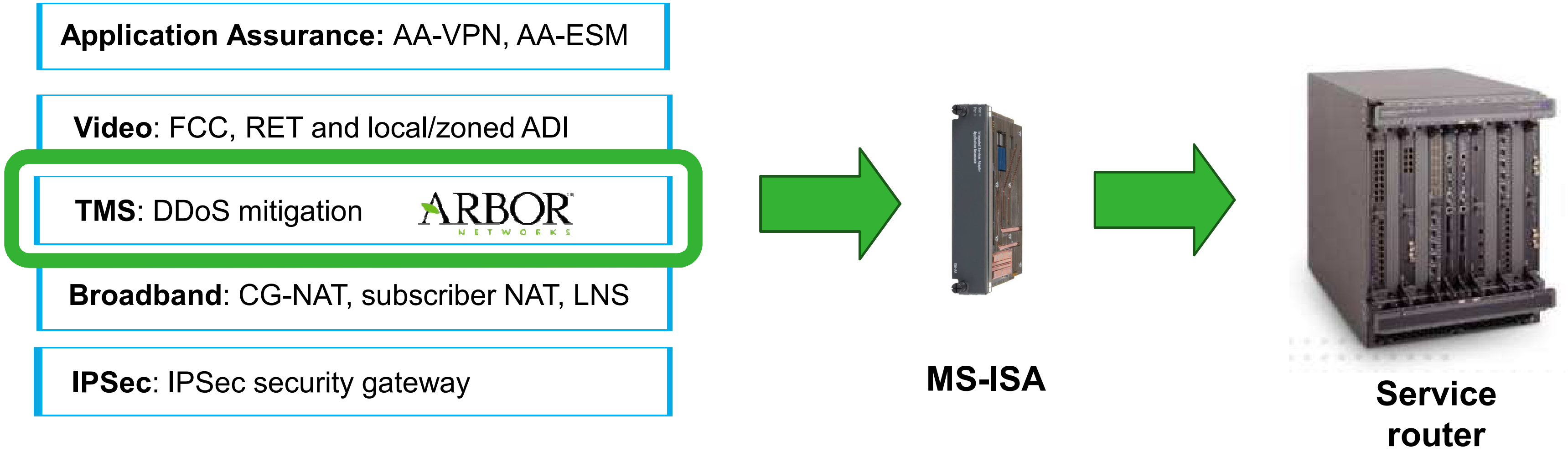
A distributed architecture allows service providers to drop attack traffic sooner, preventing overload on their infrastructure.

OPERATIONAL SIMPLICATION

LESS DEVICES TO MANAGE/OPERATE

Less devices to manage (configure, operate, install). Less devices to provide spares for. Single routing control plane to validate.

7750 SR AND MS-ISA TMS



Application Assurance: AA-VPN, AA-ESM

Video: FCC, RET and local/zoned ADI

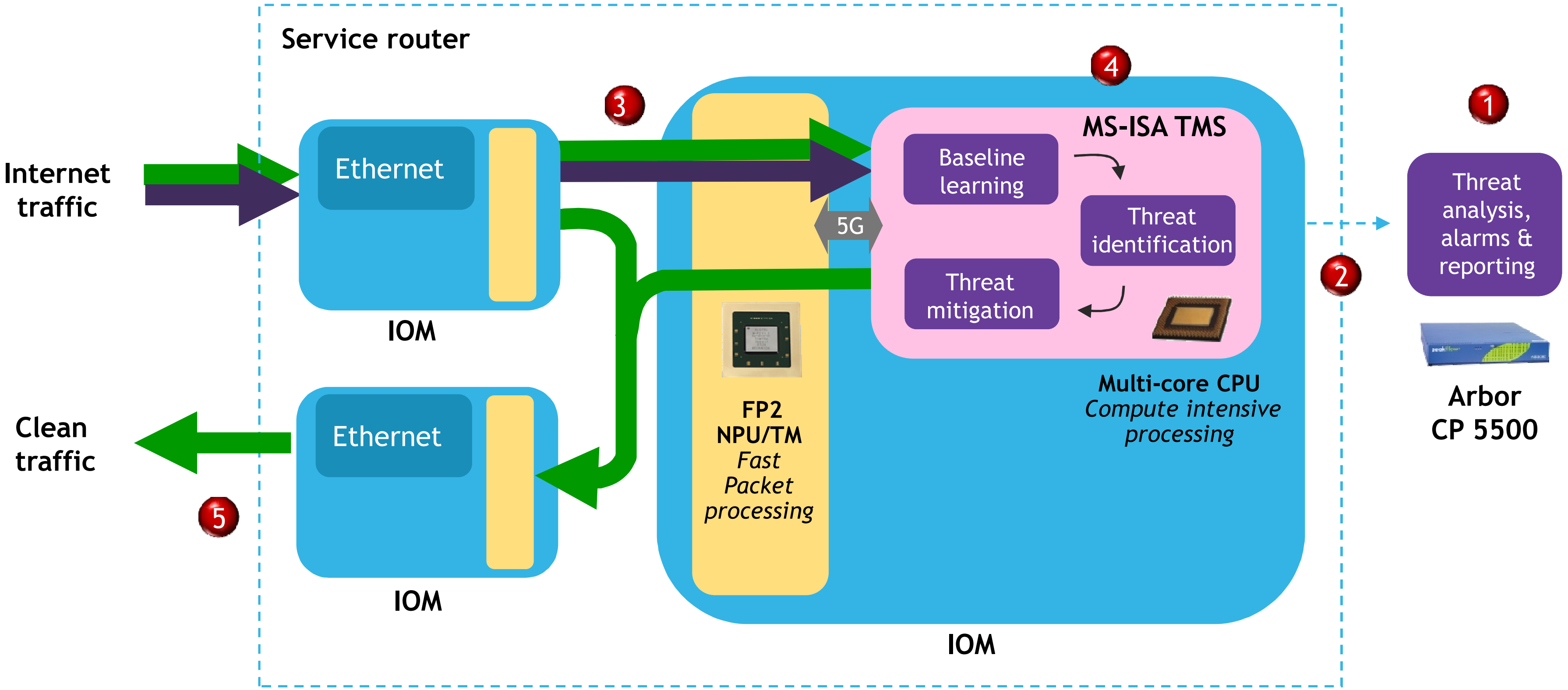
TMS: DDoS mitigation

Broadband: CG-NAT, subscriber NAT, LNS

IPSec: IPSec security gateway

- Multi-core server card for high-touch services on 7750 SR
- MDA form-factor (1/2 slot)
- Scalable multicore processing architecture
  - 5+ Gb/s DDoS and threat mitigation per MS-ISA (60+ Gb/s DDoS processing per node)
  - 50+ DDoS mitigations per MS-ISA
- Up to 12 active MS-ISA cards for threat management per 7750 SR
- Seamless hardware and software integration

MS-ISA TMS: HIGH-LEVEL VIEW

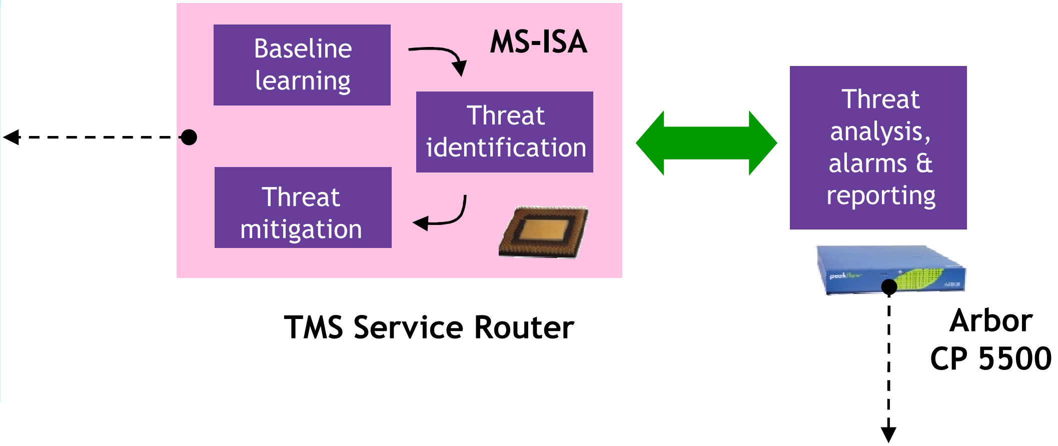


1. CP-5500 analyzes network behavior and uncovers potential attacks
2. CP-5500 signals service router
3. Traffic for destinations under attack diverted to MS-ISA TMS blades
4. MS-ISA TMS performs surgical threat mitigation
5. Clean traffic passed to destination

MS-ISA TMS: HIGH-LEVEL VIEW (2)

Surgical mitigation

- Baseline enforcement
- Black & white Lists
- Payload filtering
- HTTP, DNS, VOIP specific
- Rate limiting
- Network “fingerprints”

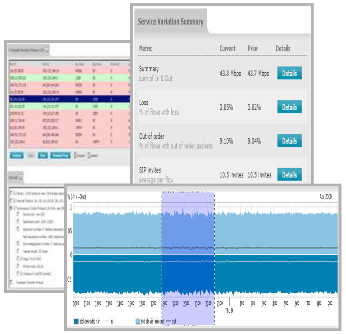


Threat landscape

- TCP stack / generic flood attacks
- Fragmentation attacks
- Application-Layer attacks
- Connection attacks
- Vulnerability exploit attacks
- Malware pipes

Threat analysis, alarms & reporting

- Set baseline service-level characteristics
- Identify potential attacks & send alerts to operators & MS-ISA TMS
- Fine-tune mitigation tools on MS-ISA TMS
- View what is being blocked



Operator & enterprise consoles

AGENDA

1. Introduction
2. Arbor solution overview
3. Integrated threat mitigation
4. Use cases
5. Deployment models
6. Conclusions

CLOUD-BASED TMS: ENTERPRISE SERVICES

OFFERING

CLEAN INTERNET SERVICE

- Filter attacks: Prevent connectivity overload to the enterprise
- Allow legitimate traffic through
- Protect enterprise IPS/IDS/firewall defenses from overload

CUSTOMER BENEFITS

DIRECT VALUE TO THE ENTERPRISE

- Reduces risk of customer portal disruptions
- Reduces risk of business process disruptions
- Protects reputation & bottom line

OPERATIONS

OPERATIONAL BENEFITS

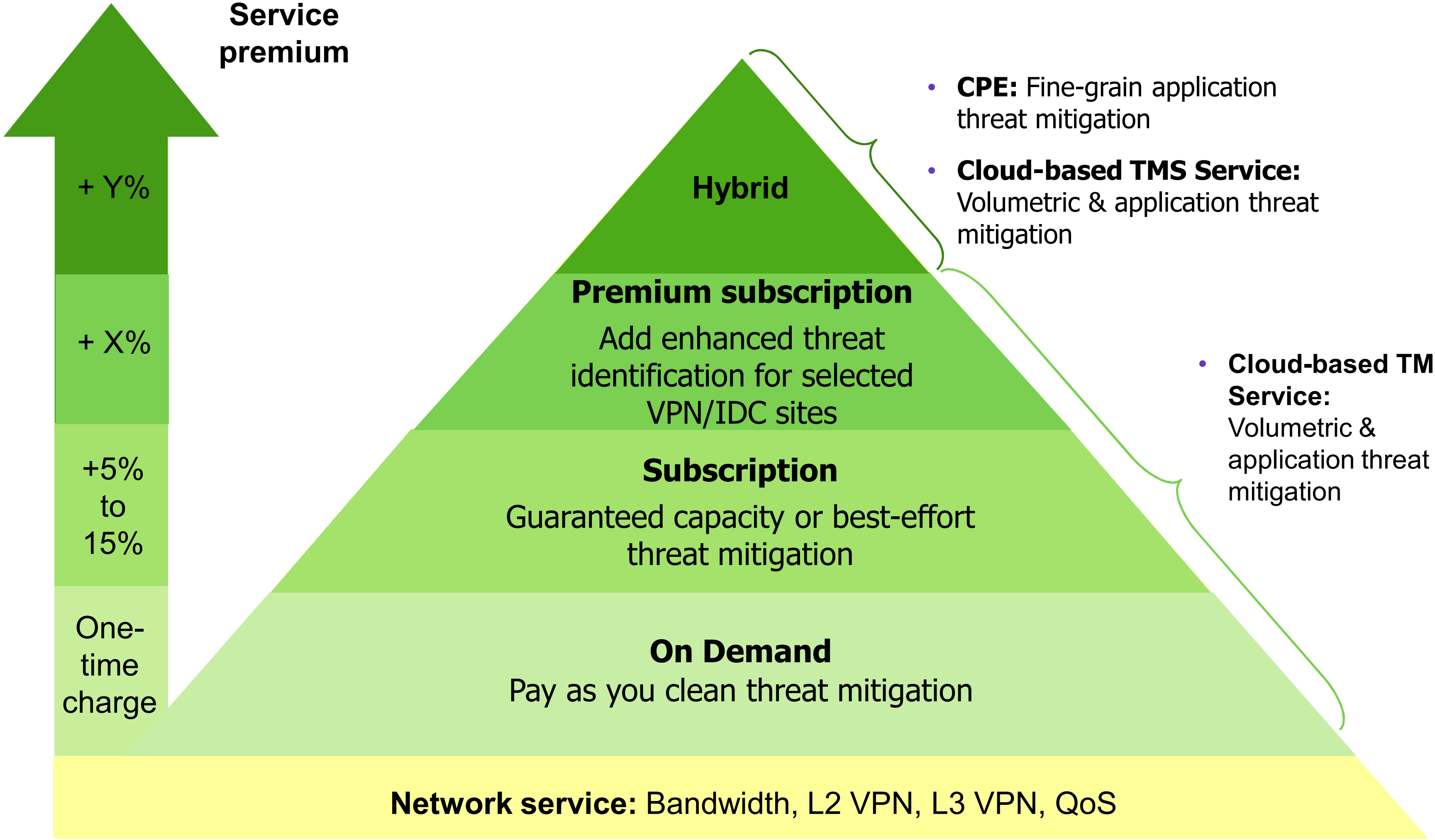
- DDoS protection outsourced to the service provider
- No need to train staff, have 24x7 coverage,..
- Flexibility to buy the required protection level

OPERATOR BENEFITS

SERVICE PROVIDER BENEFITS

- Additional revenue for value-add services
- Differentiated services
- Increase customer loyalty

THREAT MANAGEMENT AS A BUSINESS SERVICE



Hybrid

Premium subscription
Add enhanced threat identification for selected VPN/IDC sites

Subscription
Guaranteed capacity or best-effort threat mitigation

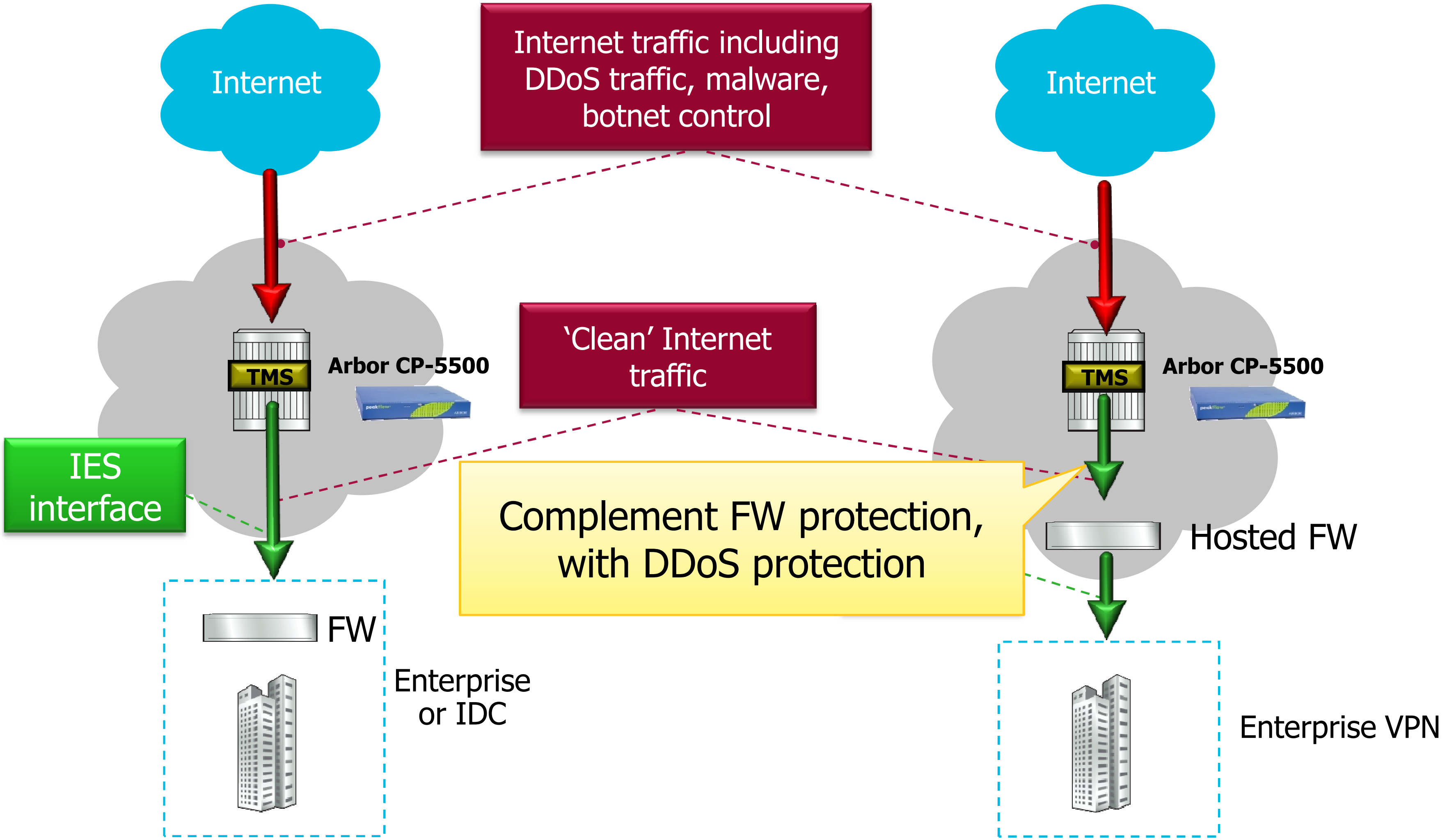
On Demand
Pay as you clean threat mitigation

Network service: Bandwidth, L2 VPN, L3 VPN, QoS

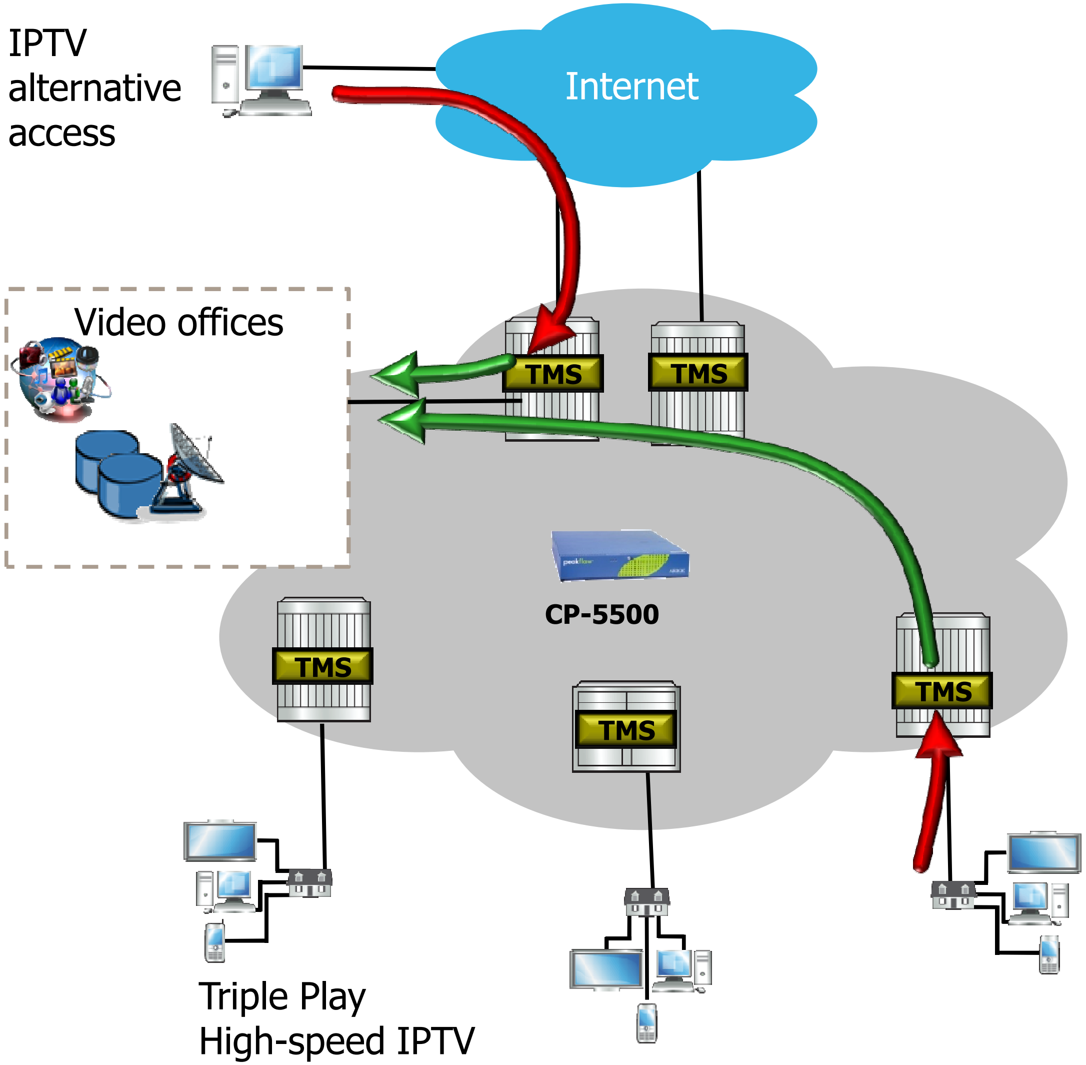
- **CPE:** Fine-grain application threat mitigation
- **Cloud-based TMS Service:** Volumetric & application threat mitigation

- **Cloud-based TMS Service:** Volumetric & application threat mitigation

CLOUD-BASED TMS ENTERPRISE SERVICES

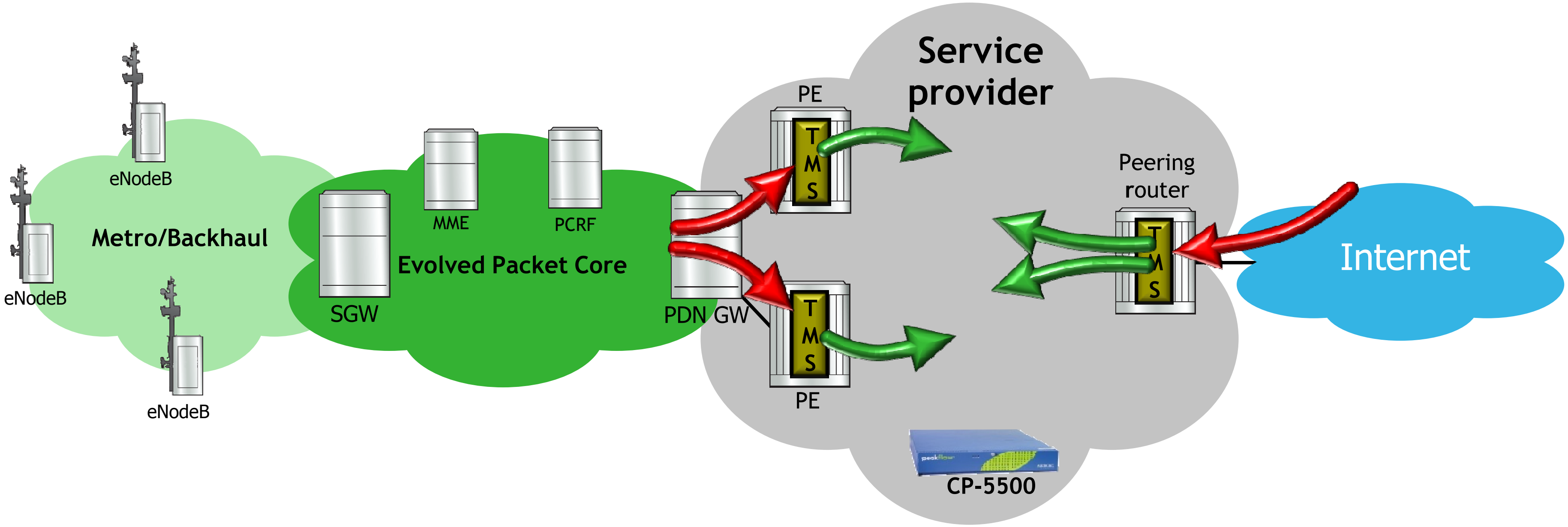


PROTECTING TRIPLE PLAY INFRASTRUCTURE



- Emerging residential threats
  - Internet capability in high-speed set-top boxes
  - Alternative access to IPTV content
  - Infected subscribers launching internal & external attacks
- Integrated protection for:
  - Video & network infrastructure from internet attacks
  - Video & network infrastructure from infected subscribers
  - Reputation as source of attack traffic

PROTECTING THE MOBILE INFRASTRUCTURE

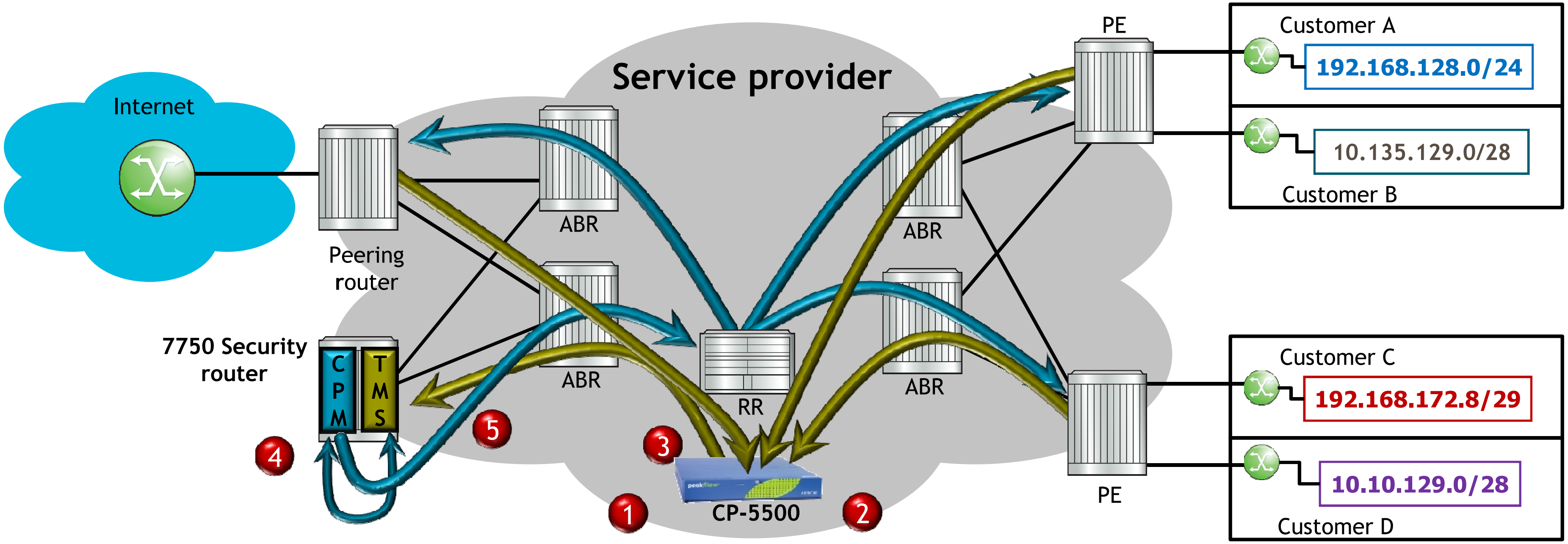


- Integrated protection from inbound threats
  - Protect mobile infrastructure from Internet attacks
  - Protect mobile services from Internet attacks
- Integrated protection from Outbound threats
  - Protect mobile infrastructure from infected smartphone attacks
  - Reputation as source of attack traffic

AGENDA

1. Introduction
2. Arbor solution overview
3. Integrated threat mitigation
4. Use cases
5. Deployment models
6. Conclusions

SECURITY ROUTER SOLUTION WITH OFF-RAMPING
REDIRECTION OF DDOS

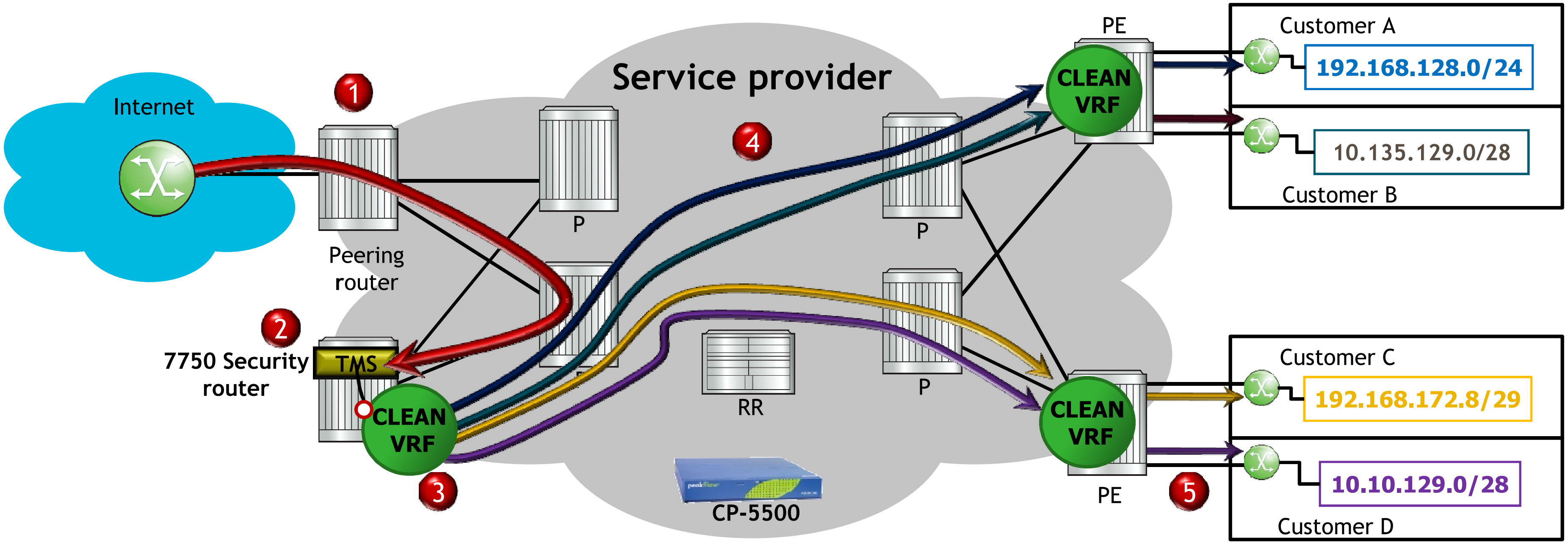


Off-ramp solution – Learning

1. 7750 SR at the edge exports Cflowd that is collected by Arbor CP
2. Arbor collects and analyzes the flows, and determines and classifies attacks
3. Arbor communicates to the TMS that reside on the 7750 MS-ISA blades of the prefixes under attack and instructs it to scrub the listed prefixes
4. 7750 SR CPM to TMS communication learns of specific prefixes of interest and dynamically originates the routes in BGP setting next hop to “Self”
5. 7750 SR advertises the BGP updates to the RR, which in turns advertises to all iBGP peers

SECURITY ROUTER SOLUTION WITH OFF-RAMPING

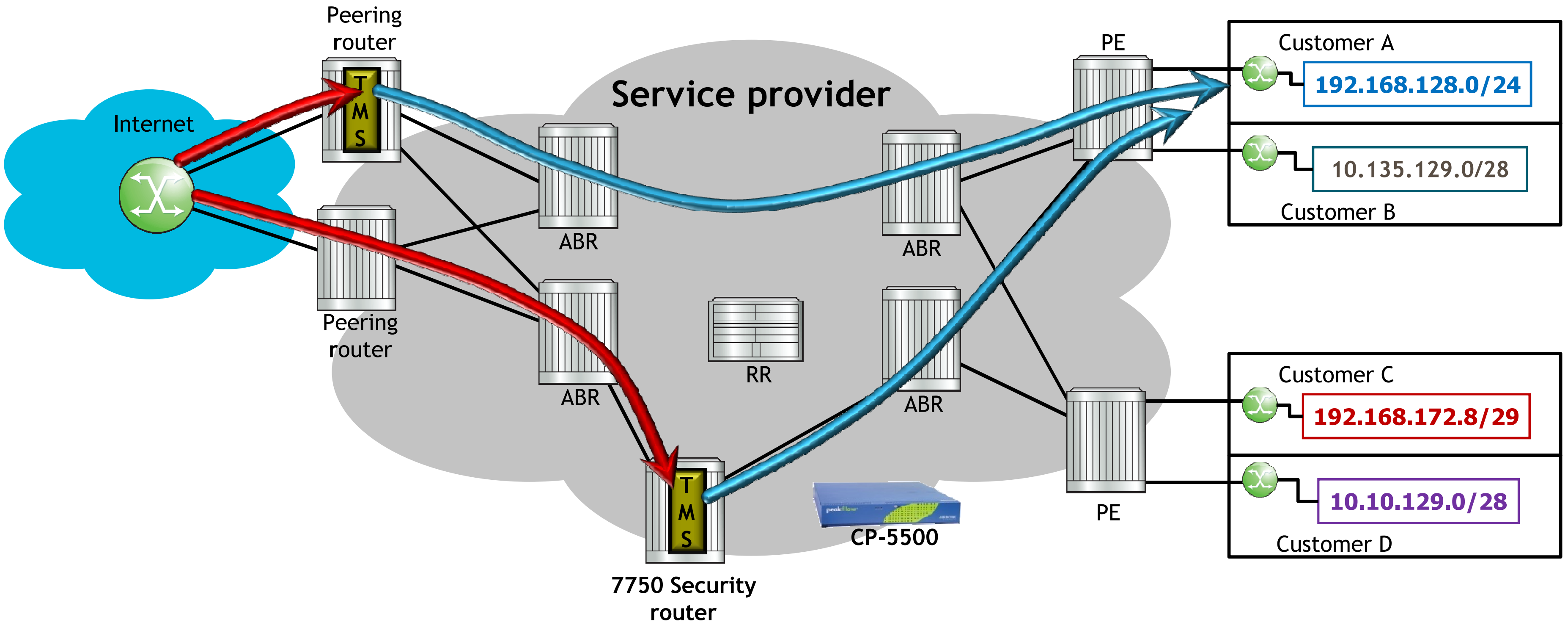
SCRUBBING AND CLEANED PACKETS



Off-ramp solution – Redirection and scrubbing

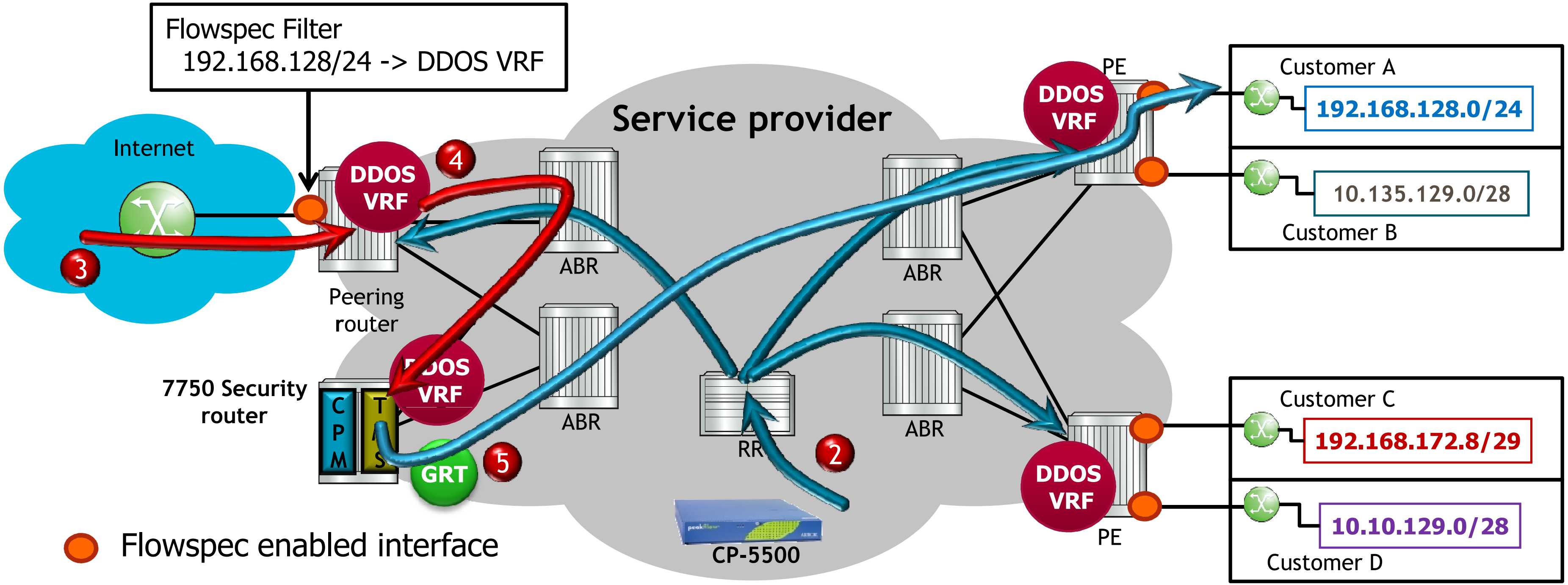
1. Inbound DDOS suspected traffic is now routed to the 7750 Security Router (SR)
2. 7750 SR will forward inbound packets to the Arbor TMS-ISA blade for scrubbing; DDoS packets are dropped and recorded, while cleaned packets are forwarded to the outbound I/O card
3. Logical SAP Interfaces provide access for cleaned packets egress TMS-ISA & into the pre-configured VPRN
4. Transport tunnels (LDP, RSVP or GRE) and MP-BGP are used to deliver cleaned packets to PE
5. Traffic from the VRF will take a default route to the Global Routing Table and are forwarded out of the PE-CE link

FLEXIBLE DEPLOYMENT OPTIONS



- Local-redirect combined with standalone security router deployment
  - Full flexibility, driven by business case and operational parameters
  - Smooth migration from (semi-) centralized to distributed

EVOLUTION: FLOWSPEC OFF-RAMPING
BASED ON VRF-ACTION



● Flowspec enabled interface

Off-ramp using Flowspec

1. 7750 SR exports flow records; Arbor CP analyzes flows and detects attacks
2. Flowspec routes originated for prefix(es) under attack: redirect to DDOS VRF
3. Traffic on flowspec interface subject to filtering and redirection
4. DDOS VRF contains 0/0 routes pointing to TMS instance(s)
5. Clean traffic routed through the GRT towards the destination

Additional enhancement: Allow ‘internet in a VRF’ instead of in GRT

MOST COMPREHENSIVE MITIGATION SOLUTION

Benefits of stand-alone TMS	Benefits of embedded TMS-ISA
Router independence • TMS does not rely upon a 7750 SR • TMS could be installed in areas of the network where 7750 SRs are not deployed, or the opportunity cost of an 7750 slot is high (slot can be used for other purposes)	**Router integration** • Leverage 7750 SR installed base to extend reach of DDoS scrubbing service • Potential TCO improvements via reduced backhaul of DDoS attack traffic and integrated BGP routing • Integration with other SR services such as L2/L3 VPNs and Application Assurance

DDoS mitigation form factor flexibility & investment protection

AGENDA

1. Introduction
2. Arbor solution overview
3. Integrated threat mitigation
4. Use cases
5. Deployment models
6. Conclusions

CONCLUSIONS

- Integrated TMS security offering provides service providers with scalable and operationally simplified means to protect the network & services from DDoS attacks
- Incorporating Arbor's industry-leading DDoS detection & mitigation solution
- Generate new revenue via expanded threat management services
- Differentiate your network and IDC service offerings
- Lower threat mitigation and related support costs

ARBOR NETWORKS
TMS Software
Carrier-grade service router

AT
THE
SPEED
OF
IDEAS™

Alcatel·Lucent

AT
THE
SPEED
OF
IDEAS™

Alcatel·Lucent

www.alcatel-lucent.com