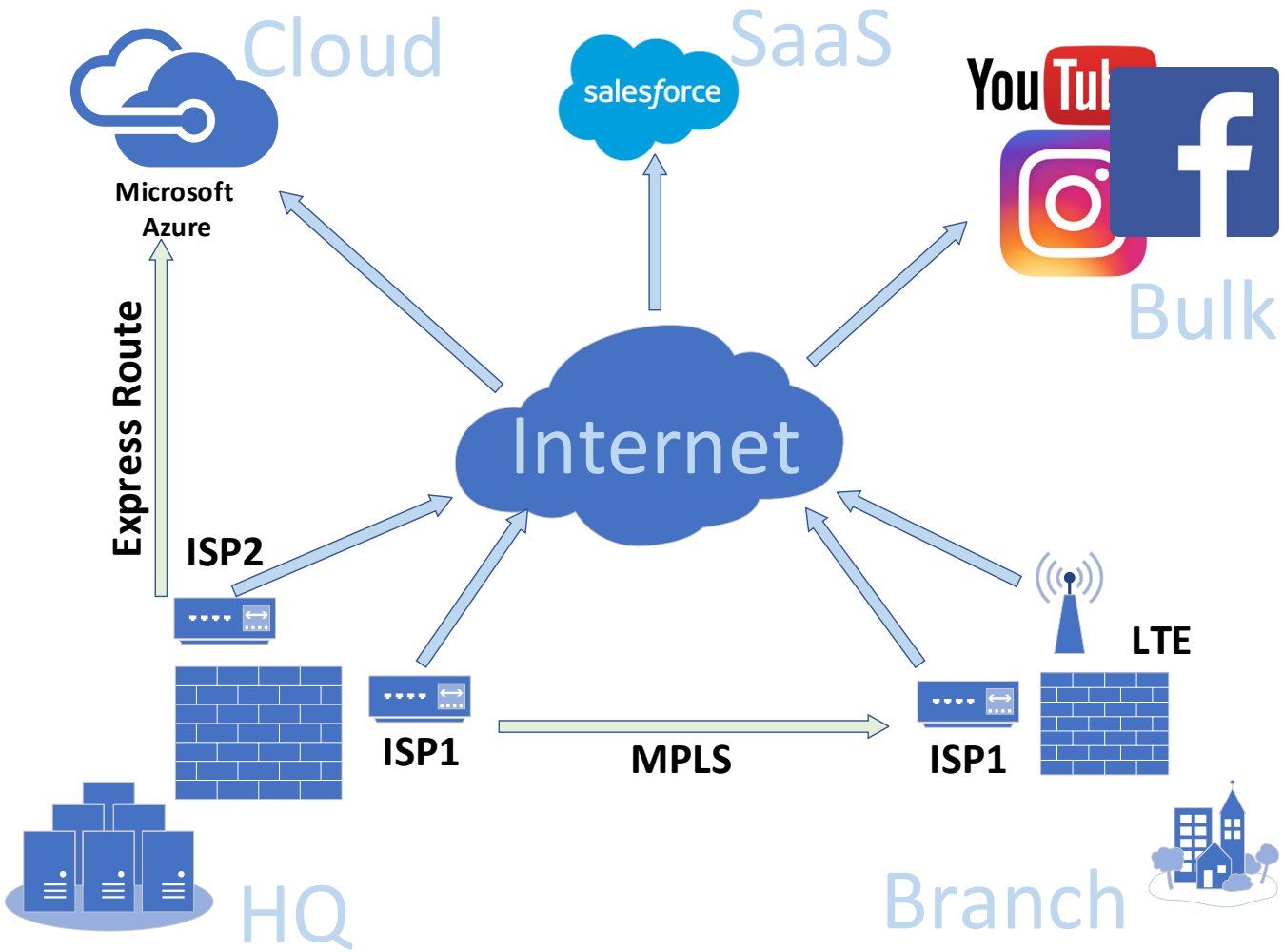

Barracuda
TECHSUMMIT19
BARRACUDA TECHNICAL SUMMIT
SD-WAN in CloudGen Firewall

SD-WAN objectives

- Application delivery
  - LAN to LAN (ERP, voice, etc)
  - LAN to Internet (SaaS, fe. Office365, Salesforce, etc.)
  - LAN to Cloud (cloud based internal applications)
- Orchestrate available internet access resources
  - Multiple ISP, LTE, ExpressRoute
- Secure Data
  - Encryption, Content control


Cloud
SaaS
Microsoft
Azure
salesforce
Bulk
Express Route
Internet
ISP2
LTE
ISP1
MPLS
ISP1
HQ
Branch

Expectations

Internet/VPN resources are shared between business critical applications and bulk traffic.

Internet breakout traffic may coexist with VPN traffic

Protect business critical applications.

Compensate for ISP outage (redundancy)

Optimize ISP (smart path selection)

Load balance accross multiple ISPs

Adapt to changes in network performance

The 4 corner stones of SD-WAN

Multi transport VPN / Multi provider internet breakout

VPN tunnel provides routing from Net A to Net B
Each tunnel has multiple transports using the available resources

Network parameter measurement

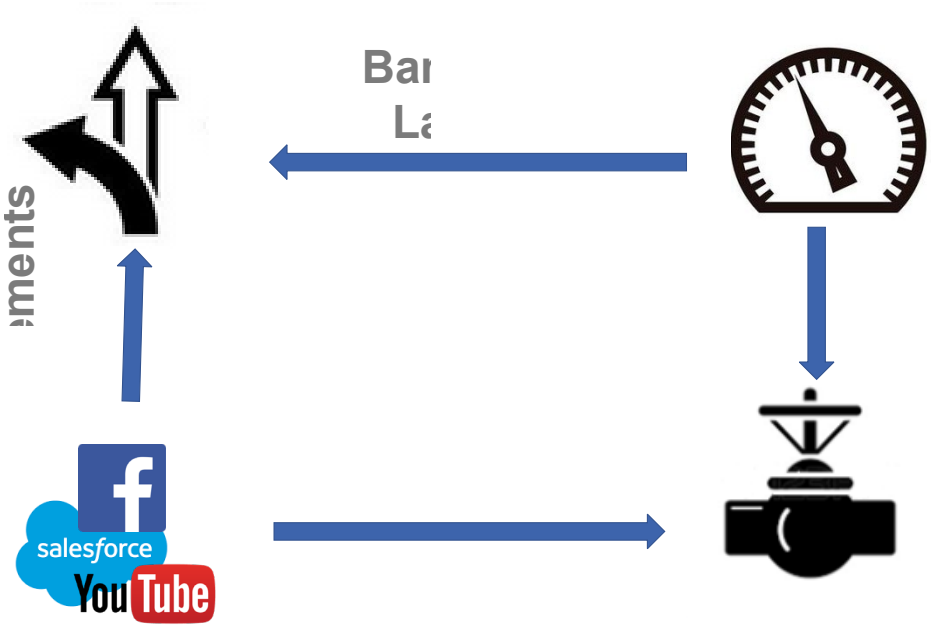
Detect up and down stream bandwidth
Detect latency
Detect loss

Traffic shaping

Consolidated out- and ingress shaping
„pre encapsulation“ shaping

Traffic categorization

Applications, protocols, etc.


ments
Bar
La
salesforce
YouTube

Acquiring information

VPN partners exchange information

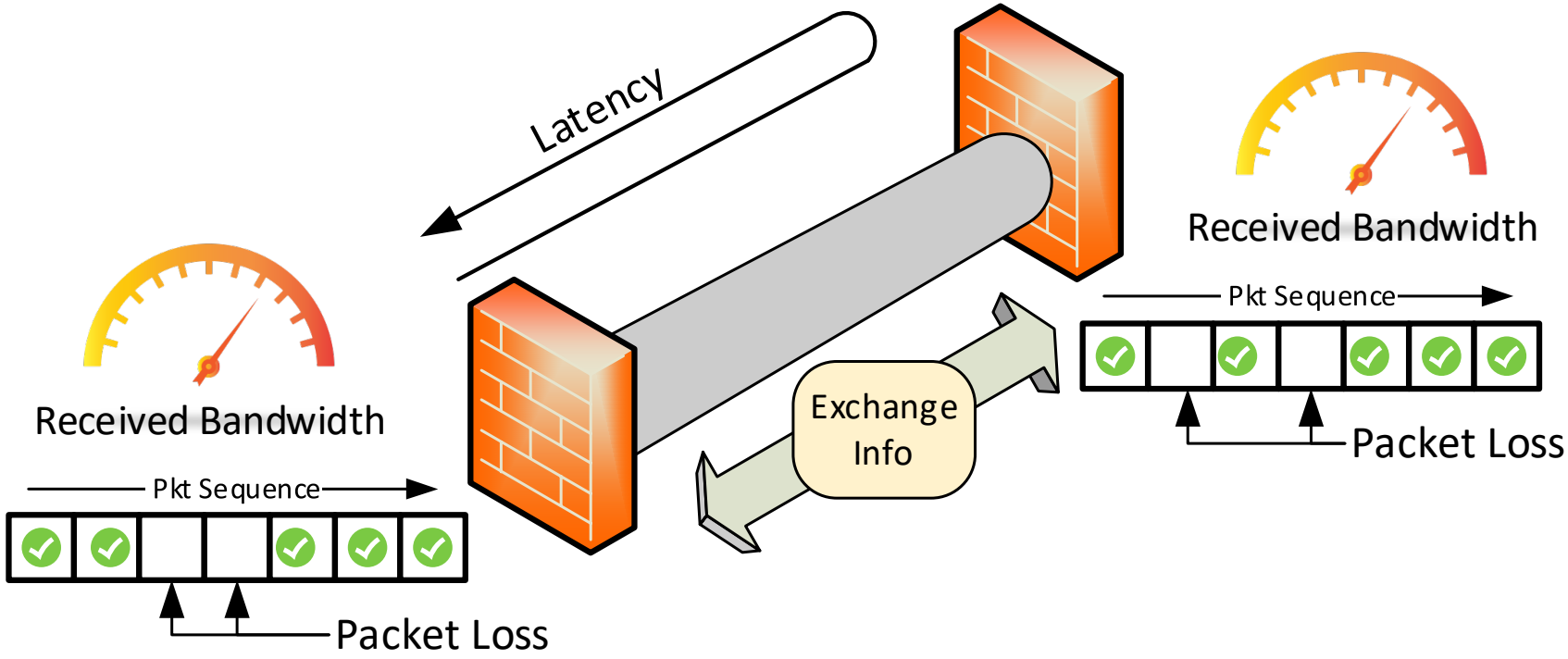
Make use of the fact that VPN endpoints can talk to each other using „meta“ packets.
Use VPN sequence number and replay protection to detect loss.
Gain information about „actual received“ bandwidth.
Use „heartbeat“ packets to measure latency.

Measured values are shared between partners

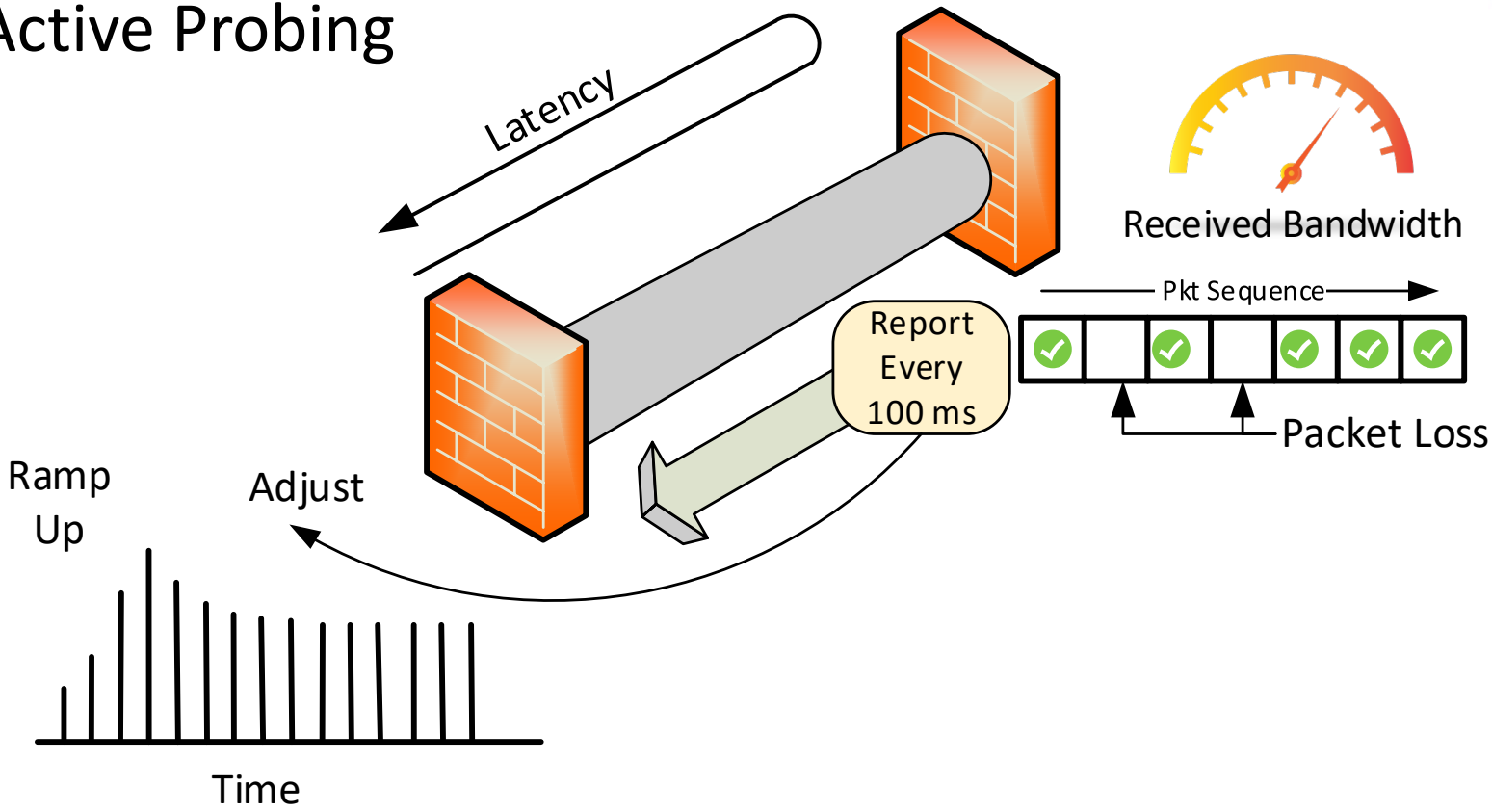
Use „active probing“ to test available bandwidths

Internet breakout: „Syn Race“ to detect best provider for a specific application.

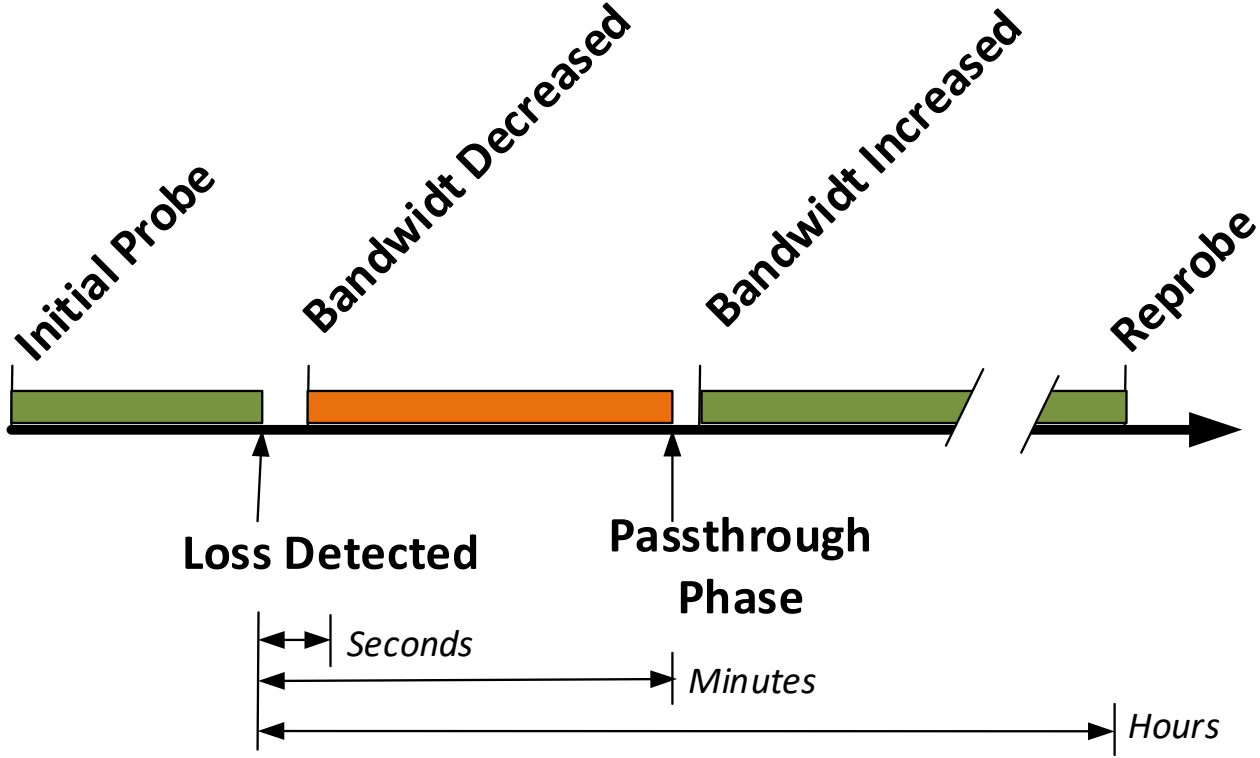
Passive Monitoring



Active Probing



Probing Lifecycle



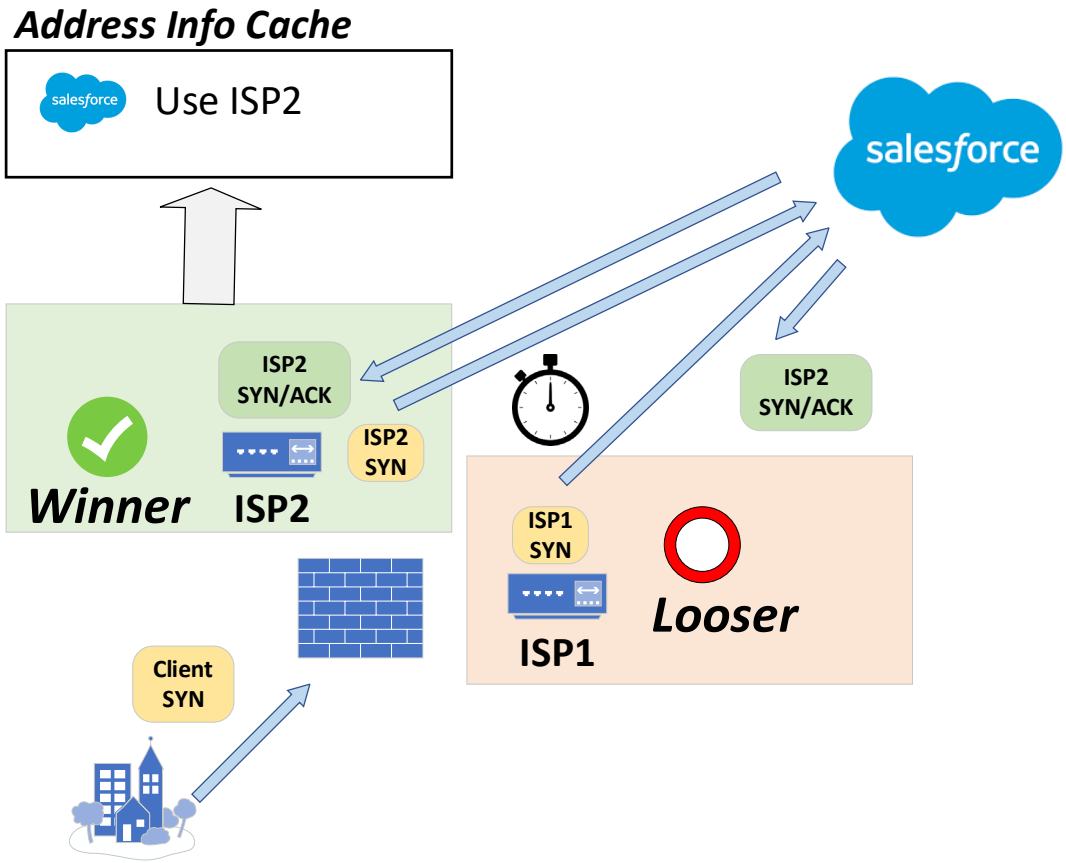
„SYN Race“ or find the best ISP for a SaaS

Unlike to a VPN endpoint SaaS endpoints do not provide performance information.

Try all possible ISPs and keep the one with the quickest response.
„SYN Race“

Use initial client sessions as probes.

Store the result for future sessions (address info cache).


Address Info Cache
Use ISP2
salesforce
ISP2
SYN/ACK
ISP2
SYN
Winner
ISP2
ISP2
SYN/ACK
ISP1
SYN
ISP1
Looser
Client
SYN

Acquired information

For each VPN transport (ISP)

- Effecive up/downstream bandwidth
- Latency
- Current loss

For internet/cloud applications (SaaS)

- Most reactive ISP
- Derive ISP bandwidth from VPN bandwidth

Advanced VPN routing

Separate VPN Routing from VPN Transport

A VPN tunnel is used for routing between WAN networks
A VPN transport is used to deliver the encapsulated traffic

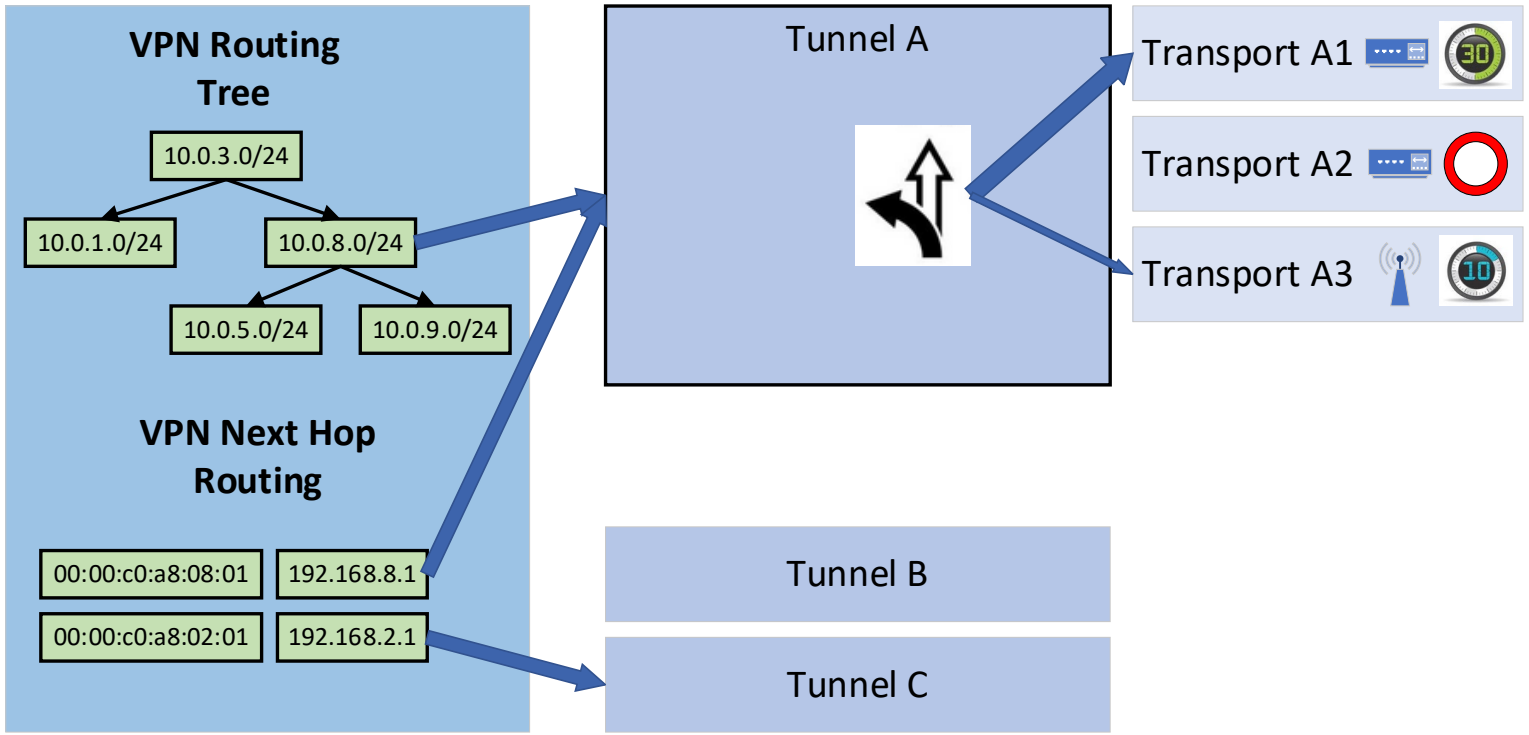
Explicit VPN Routing

Source and destination network are part of the tunnel configuration

„Routed" VPN

Behaves like a „real" network device
Next Hop to tunnel association
Integrates witn dynamic routing protocols (BGP, OSPF, etc.)

Separate VPN Routing from VPN Transport



ISP selection

Transport status provides input for „decisions“

- Availabilty (functional or disfunctional)
- Current available up/down stream bandwidth
- Current latency
- Current number of long term sessions

„Address Info Cache“ provides latency for accessing SaaS

SD-WAN profile uses to above information to select an ISP

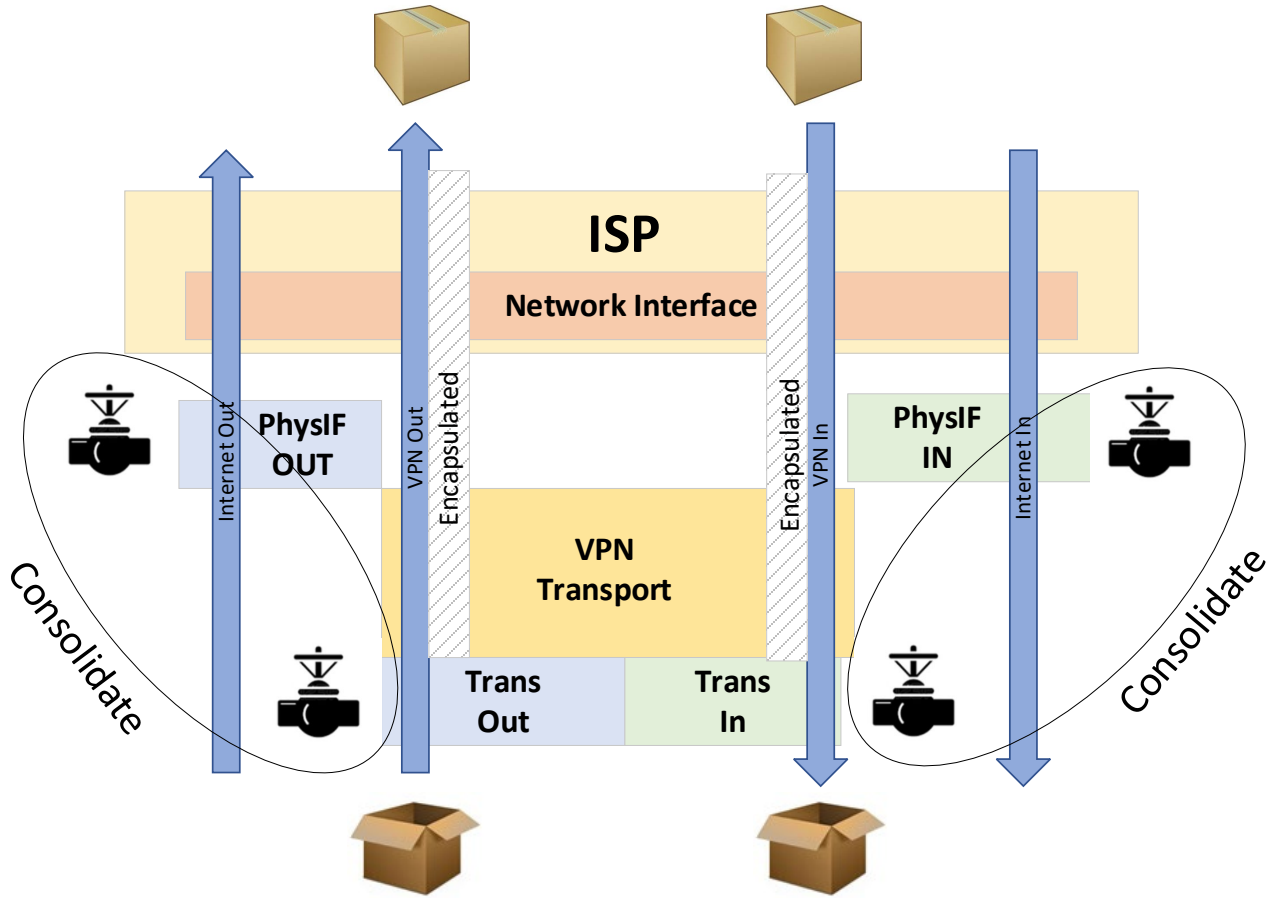
SD-WAN traffic shaping

Consolidate VPN and breakout shaping
VPN and breakout traffic must coexist
VPN and SaaS traffic must be protected from bulk internet traffic.

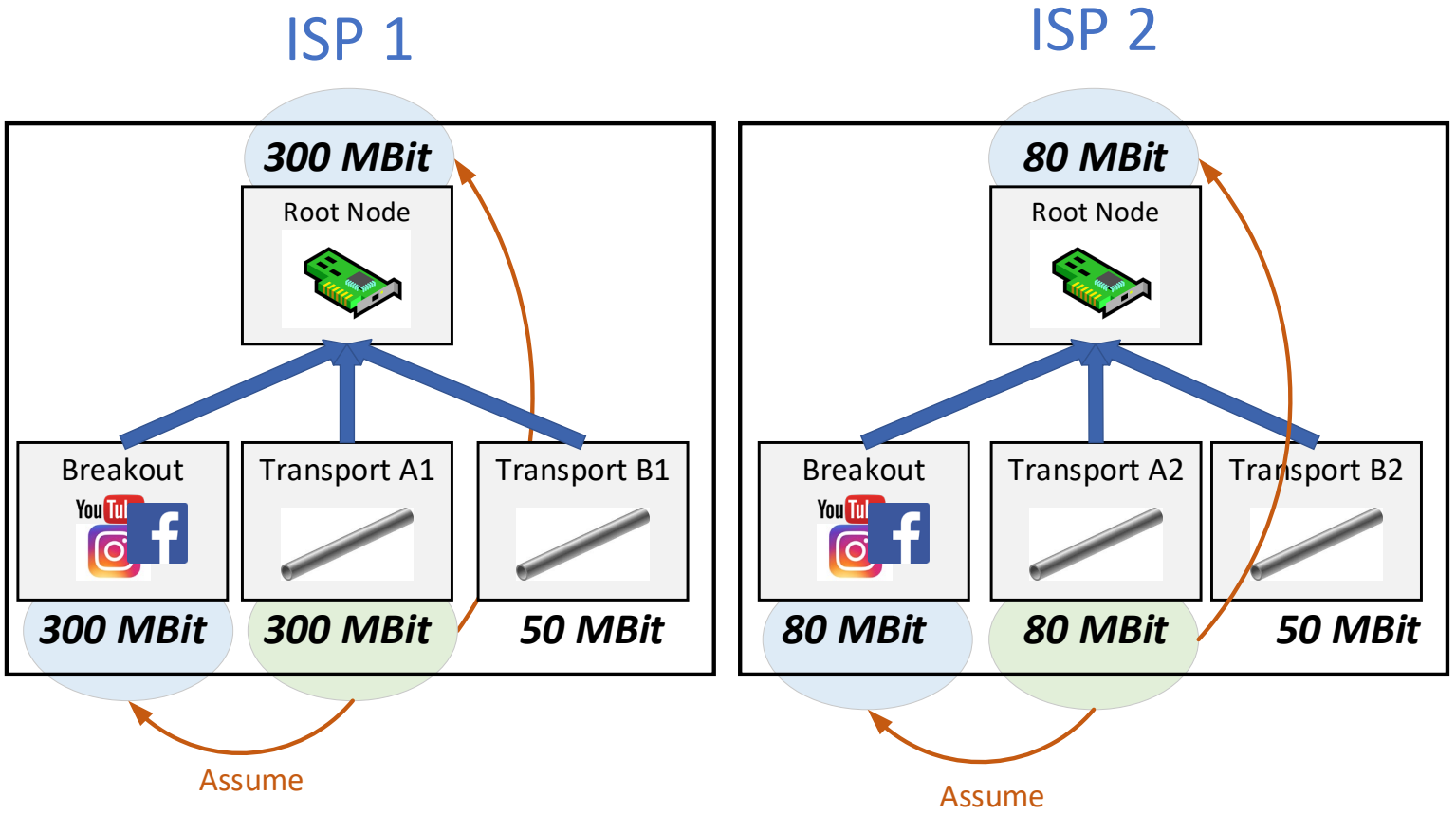
Need „pre encapsulation shaping“
Application information would be lost otherwise.

Need „ingress shaping“ to protect inbound VPN or SaaS
Only way to „stop“ inbound bulk internet traffic.
No control over endpoint.

Consolidated VPN and breakout shaping



SD-WAN shaping tree



SD-WAN requires a new type of policies

Access/Application rule set not suitable anymore
Focus was on access limitation
Provider selection and prioritization along with access policy

7 different types of decisions in 2 rule sets

- Access policy
- Provider selection and shaping
- Application policy
- URLCat policy
- Virus policy
- TLS interception policy
- Content policy

Old Firewall Rule Set

Access Rule Set

✓	10.0.4.0/24	Internet	TCP 80/443	Use: 213.4.5.6	Prio Medium	
✓	10.0.0.0/8	Internet	Any	Use: 81.2.2.3	Prio Low	
✓	10.0.0.0/8	SAP-Network	Any	Use: Orig. Src	Prio ND	VPN ISP1

Application Rule Set

✓	10.0.0.0/8	Salesforce		Prio High	
✓	10.0.0.0/8	ANY			URLCat Policy

+

Exception List (Hostnames,…)

Disadvantages of the old rule set

Structure for conditions in rules are not suitable for all policies
Fe. URLCat and shaping policy have different but overlapping conditions.

Need for „multiplication“ of rules.

Adjustment of one policy affects other policy.

Some conditions are covered using exception lists
Fe. TLS hostname exception.

No „working“ default rule set. Build from scratch !

Independent policies

- Clear focus on policy when configuring
- Separation of operational/optimizing and security settings
- Multiple match possible for some policies
- Default policy „good enough“ for most cases
- Exceptions cover special cases

SD-Wan Policy 

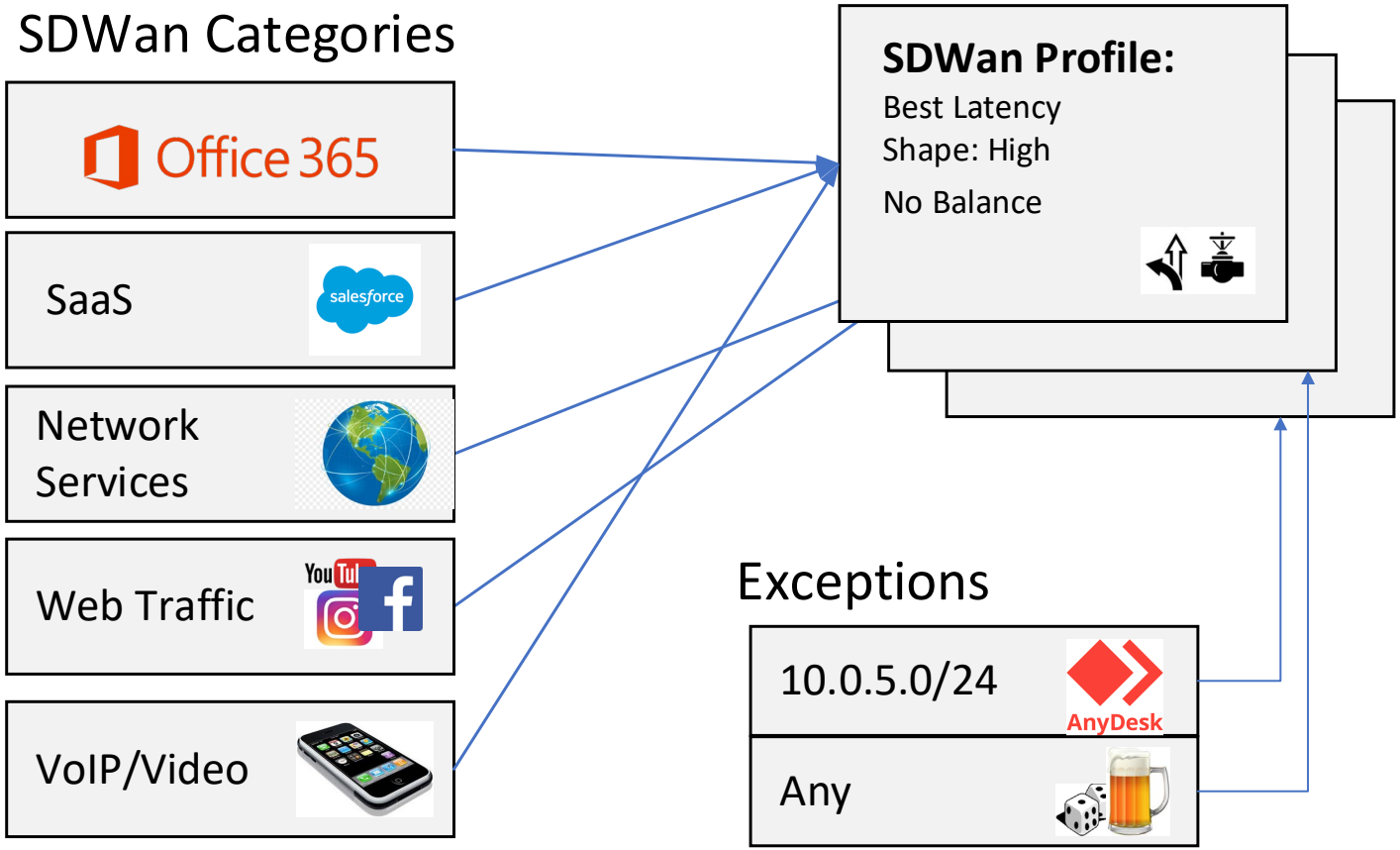
App Policy 

URLCat Policy 

Virus Policy 

TLS Policy 

SD-WAN policy



URLCat policy

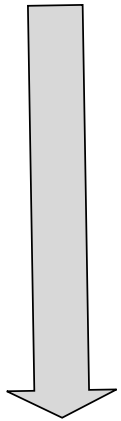
Default Policy (Editable)
Based on „Super Categories“

Deny

Allow

Exceptions:

Marketing 	Add 
	
	



Virus scanning policy

Overall settings for default behaviour

Exceptions based on:

Source networks
Application
URL category
Hostname
Content

Parameterization of:

Archive policy
Maximum file sizes
Fail Open/Close

Putting it all together

Intelligent SD-WAN routing/VPN engine

Handle an intrinsically complex problem with smart defaults

Pre-assignment of SD-WAN profiles to applications (let us do the work)

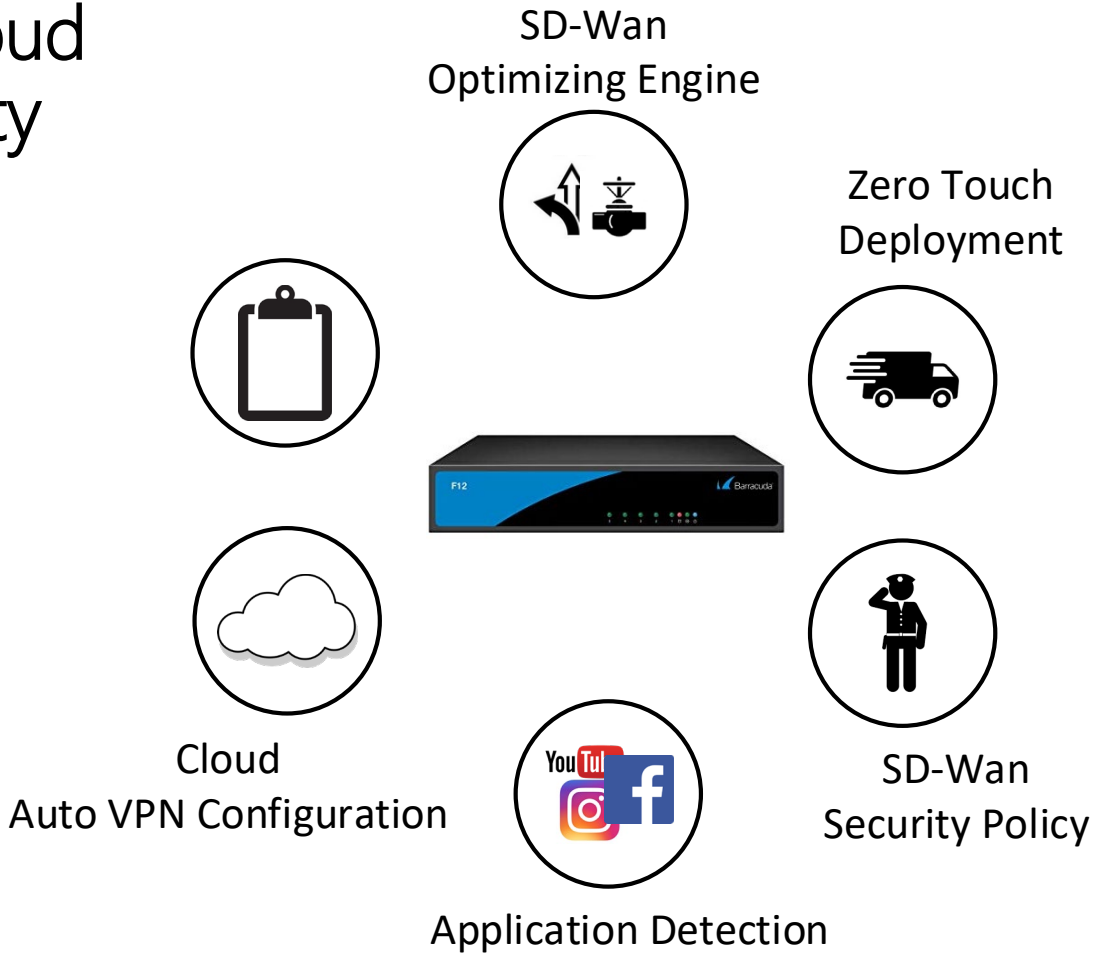
Default allows optimized operation

Cover specific needs with simple exceptions

Complete „Zero Config“ with auto VPN configuration

Deploy using „Zero Touch“

Branch/Cloud Connectivity Box




Thank you
Barracuda
TECHSUMMIT19
BARRACUDA TECHNICAL SUMMIT