Barracuda

TECHSUMMIT19

BARRACUDA TECHNICAL SUMMIT

Best Practice "SD-WAN"

Real-life experiences from the field

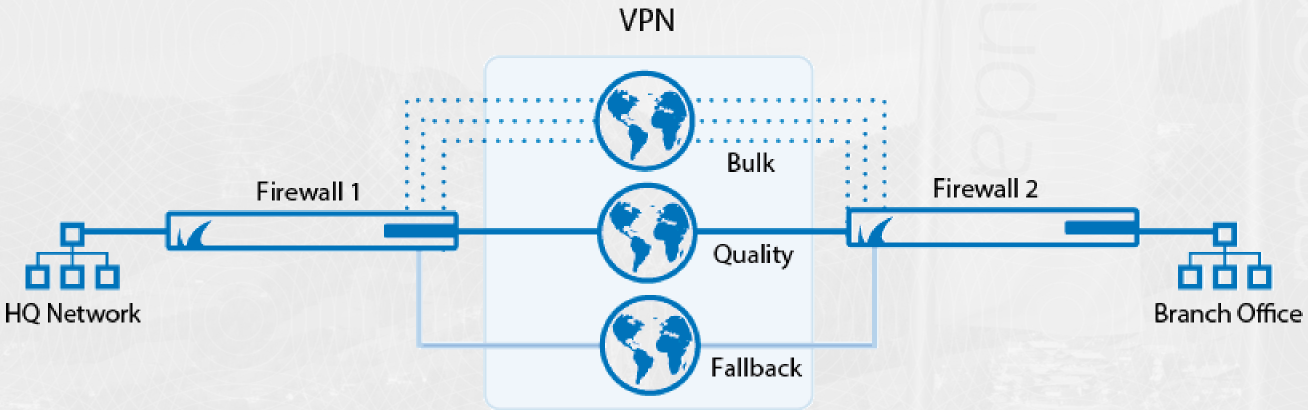
Agenda

- SD WAN Overview
- Customer Expectations & Recommendations
- Complexity Reduction
- Sizing & Performance Tuning
- SD-WAN & VRF
- ZTD
- SD-WAN & The Public Cloud

SD-WAN – only one feature to switch on?

SD WAN - Multi-Transport VPN

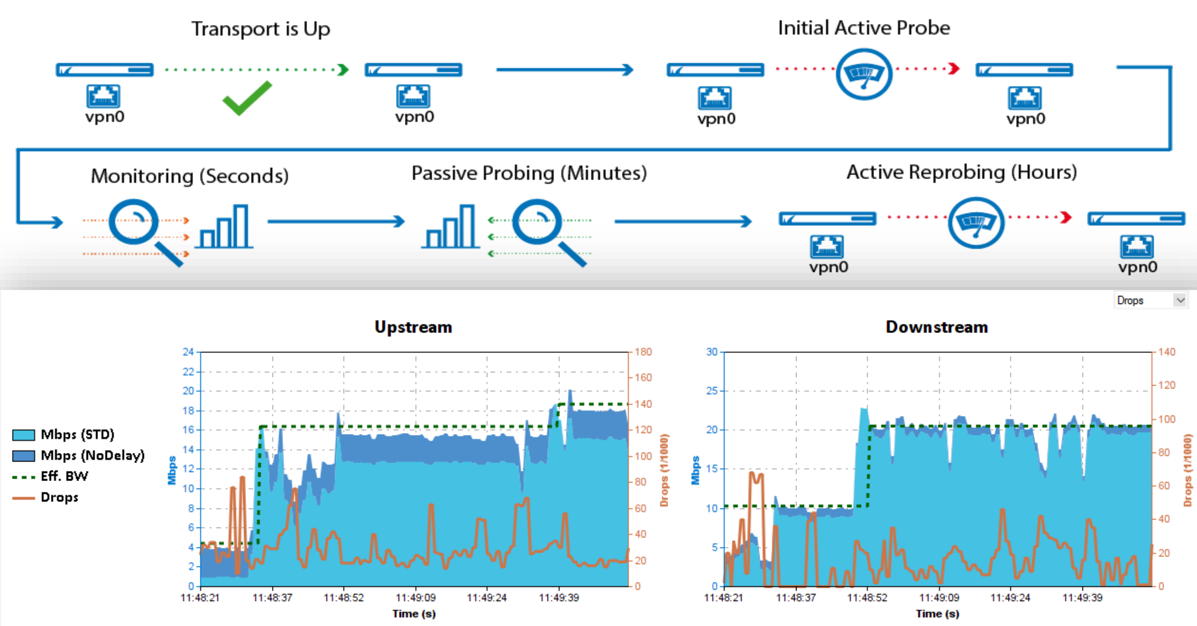
Multi-Provider Internet Breakout



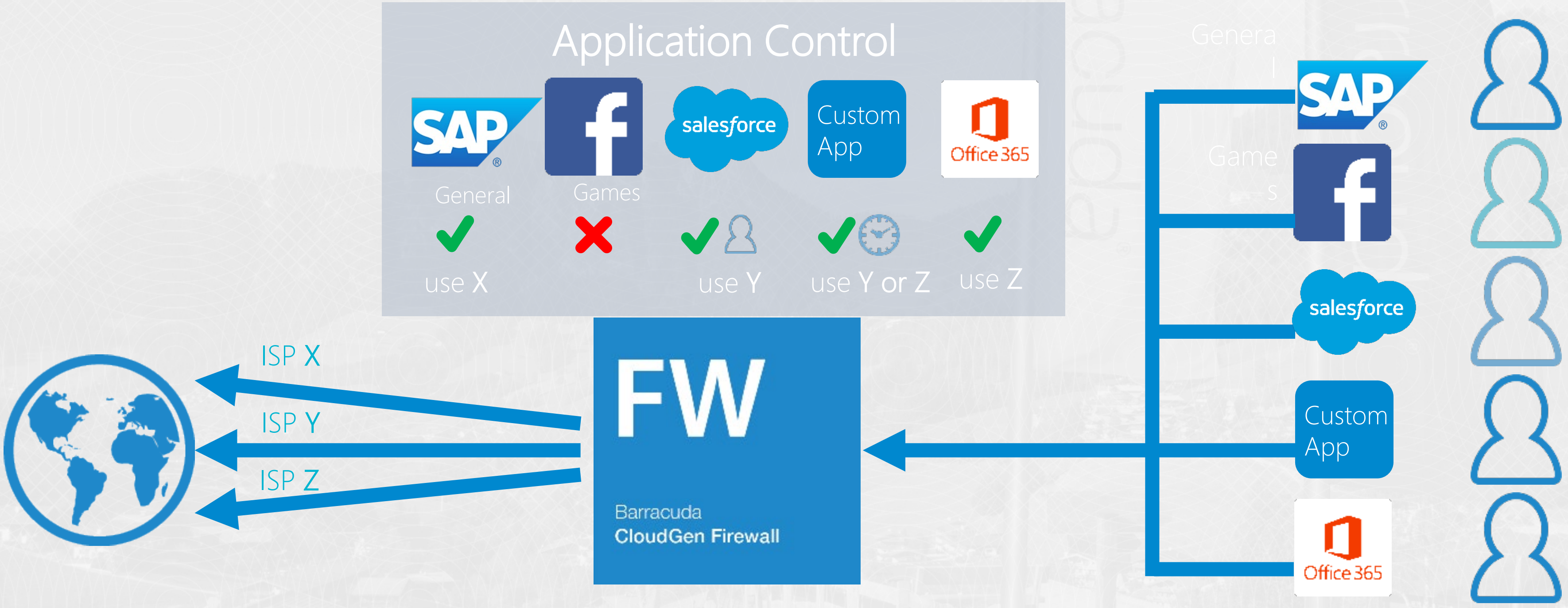
Multiple Transports in VPN

SD-WAN – Network Parameter Measurement

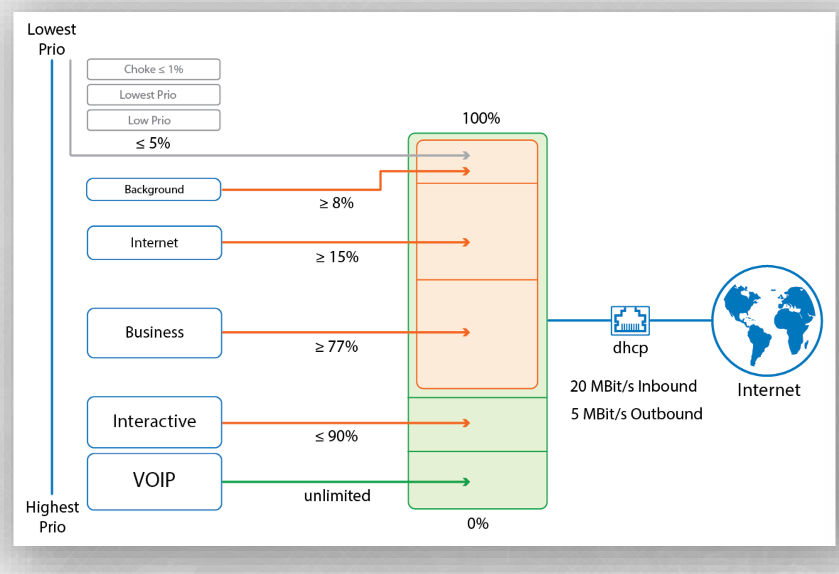
Bandwidth (up & down) – Latency – Packet Loss

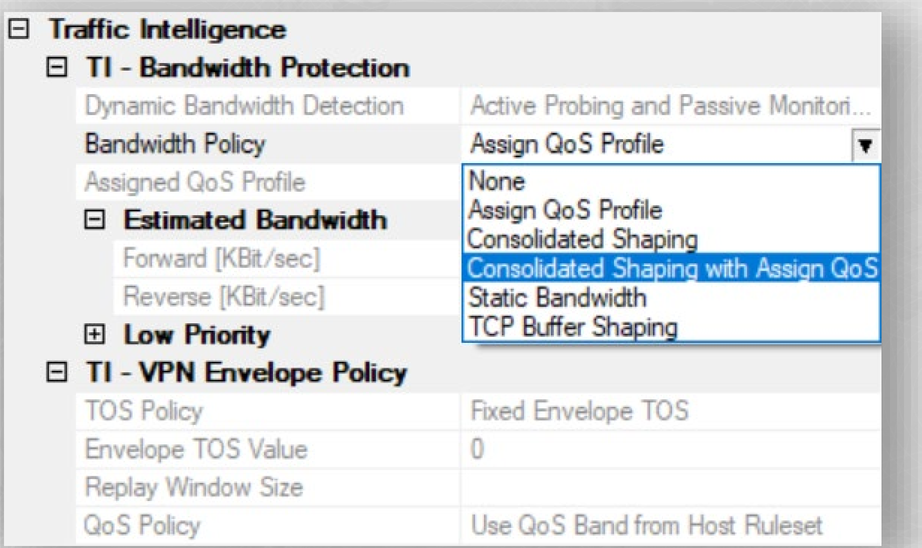


SD-WAN - Traffic Categorization



SD-WAN - Traffic Shaping





⊟ Traffic Intelligence

⊟ TI - Bandwidth Protection

Dynamic Bandwidth Detection	Active Probing and Passive Monitori...
Bandwidth Policy	Assign QoS Profile
Assigned QoS Profile	

⊟ Estimated Bandwidth

Forward [KBit/sec]	
Reverse [KBit/sec]	

⊞ Low Priority

⊟ TI - VPN Envelope Policy

TOS Policy	Fixed Envelope TOS
Envelope TOS Value	0
Replay Window Size	
QoS Policy	Use QoS Band from Host Ruleset

Customer expectations

- Reduction of WAN costs
- Performance improvements
- Flexibility & speed when rolling out new branches / offices
- Complexity reduction
  - hardware, software, management, licensing
- Provider SLA measurement

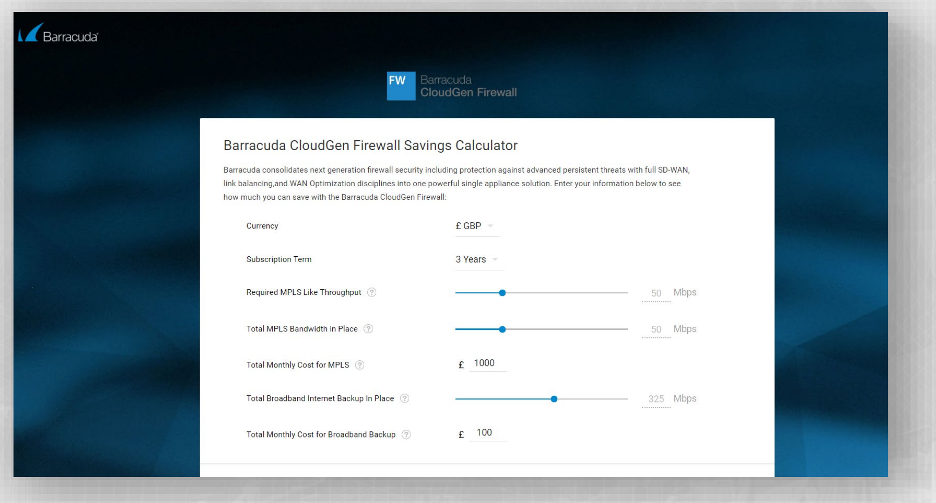
GET MORE – PAY LESS

Line Cost Reduction

MPLS replacement

Barracuda Savings Calculator

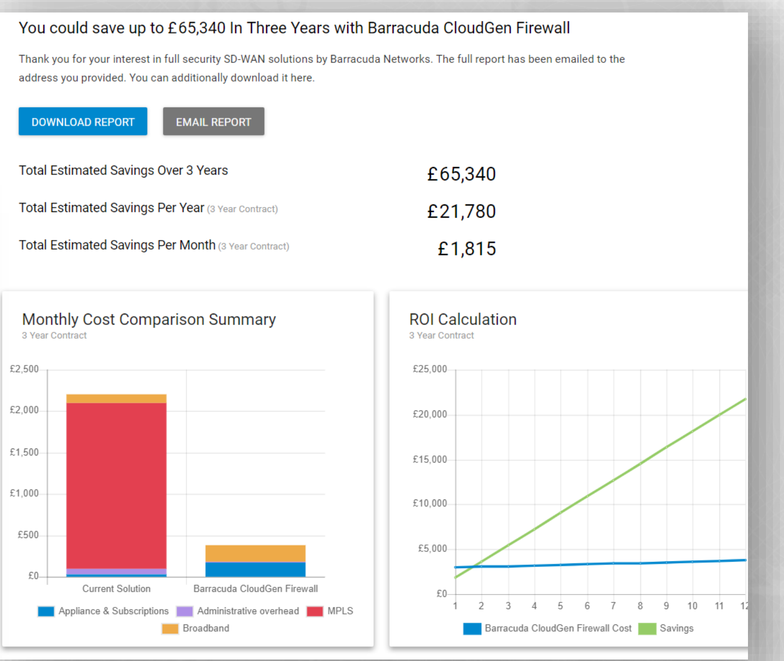
https://savings.barracuda.com



Barracuda CloudGen Firewall Savings Calculator

Barracuda consolidates next generation firewall security including protection against advanced persistent threats with full SD-WAN, link balancing,and WAN Optimization disciplines into one powerful single appliance solution. Enter your information below to see how much you can save with the Barracuda CloudGen Firewall:

Currency	£ GBP
Subscription Term	3 Years
Required MPLS Like Throughput ?	50 Mbps
Total MPLS Bandwidth in Place ?	50 Mbps
Total Monthly Cost for MPLS ?	£ 1000
Total Broadband Internet Backup In Place ?	325 Mbps
Total Monthly Cost for Broadband Backup ?	£ 100



You could save up to £65,340 In Three Years with Barracuda CloudGen Firewall

Thank you for your interest in full security SD-WAN solutions by Barracuda Networks. The full report has been emailed to the address you provided. You can additionally download it here.

Total Estimated Savings Over 3 Years	£65,340
Total Estimated Savings Per Year (3 Year Contract)	£21,780
Total Estimated Savings Per Month (3 Year Contract)	£1,815

Monthly Cost Comparison Summary

3 Year Contract

ROI Calculation

3 Year Contract

MPLS replacement

Points to consider and discuss with your customer before you migrate from MPLS to commercial-grade internet lines:

- Guaranteed SLAs
- No or only little overbooking (defined by product)
- Guaranteed bandwidth & QoS
- Fully managed - end-to-end
- Network not reachable from public internet

4G - LTE / 5G – The solution for all problems?

High-speed internet at low costs

but …… bandwidth is not the only thing that counts

4G - LTE / 5G & cable – Things to consider

High-speed Internet at low costs

- Best effort media - overbooked by provider
- Smartphones get priority over internet routers
- High bandwidth & latency fluctuation throughout the day
- Packet loss rate?
- SLAs? Read the footnotes & fine print in your contract!
- Network is reachable from public internet

Shared Internet Access

Hybrid solutions

Most providers call it "hybrid internet" or "hybrid technology"

Combination of broadband & 4G - LTE within the providers internet router/modem

Not recommended for SD WAN

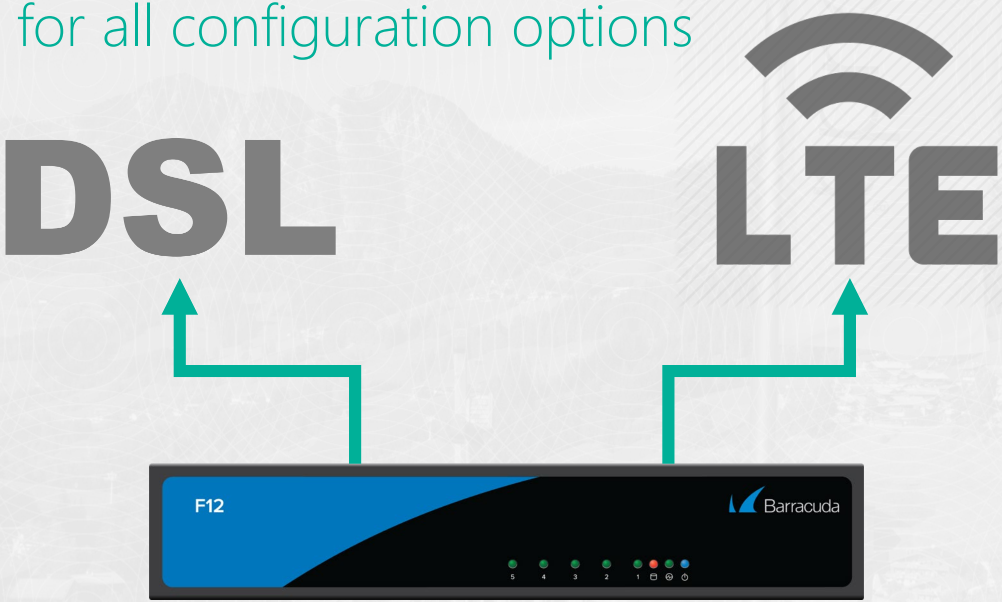
- will lead to unexpected behavior
- TINA tunnel is only one session!

SD WAN Deployment Options

SD-WAN „light“

Transport behaviour is very different

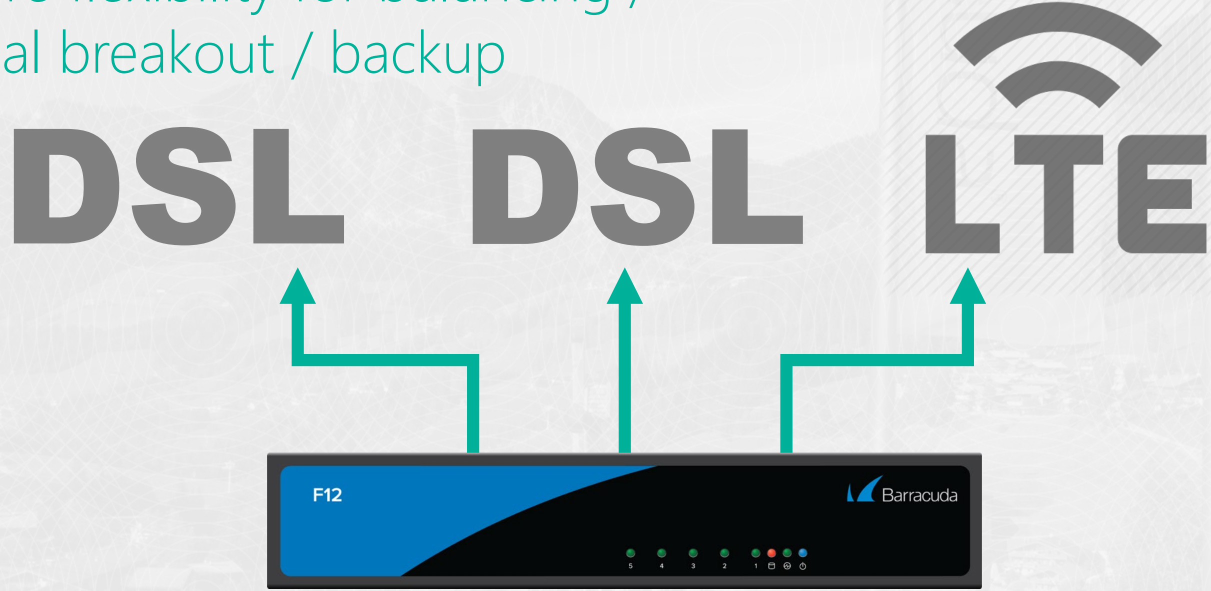
- Not optimal for all configuration options



SD-WAN

Consider more than 2 uplinks / ISPs

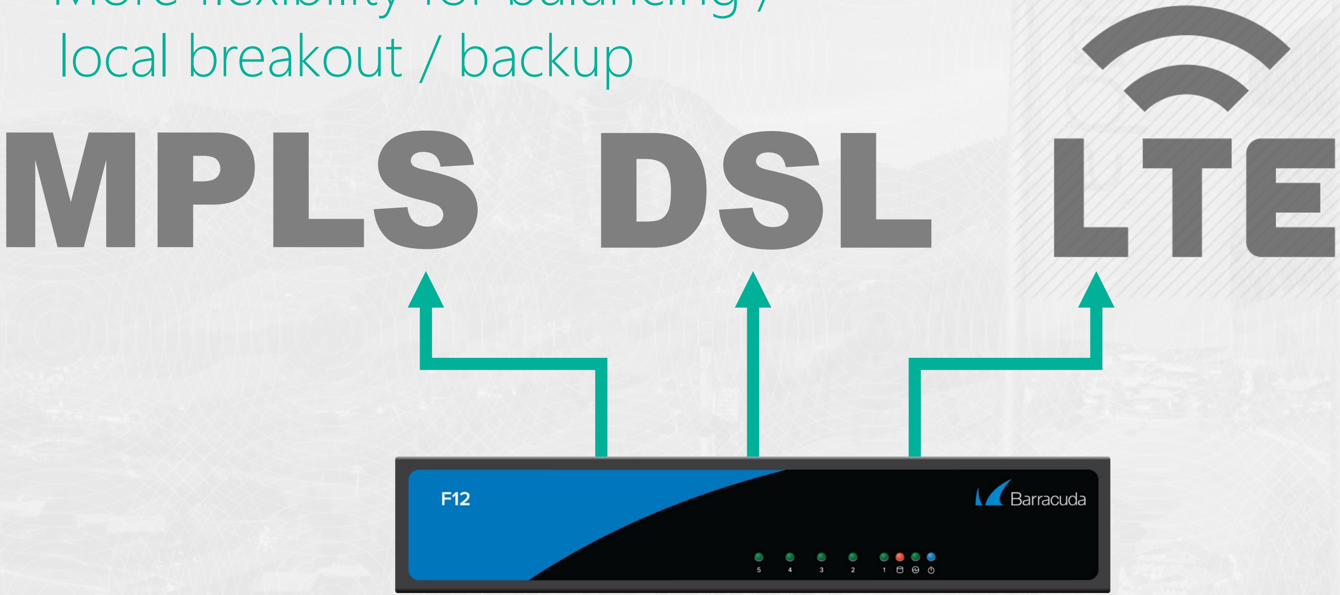
- More flexibility for balancing / local breakout / backup



SD-WAN

Consider more than 2 uplinks / ISPs

- More flexibility for balancing / local breakout / backup

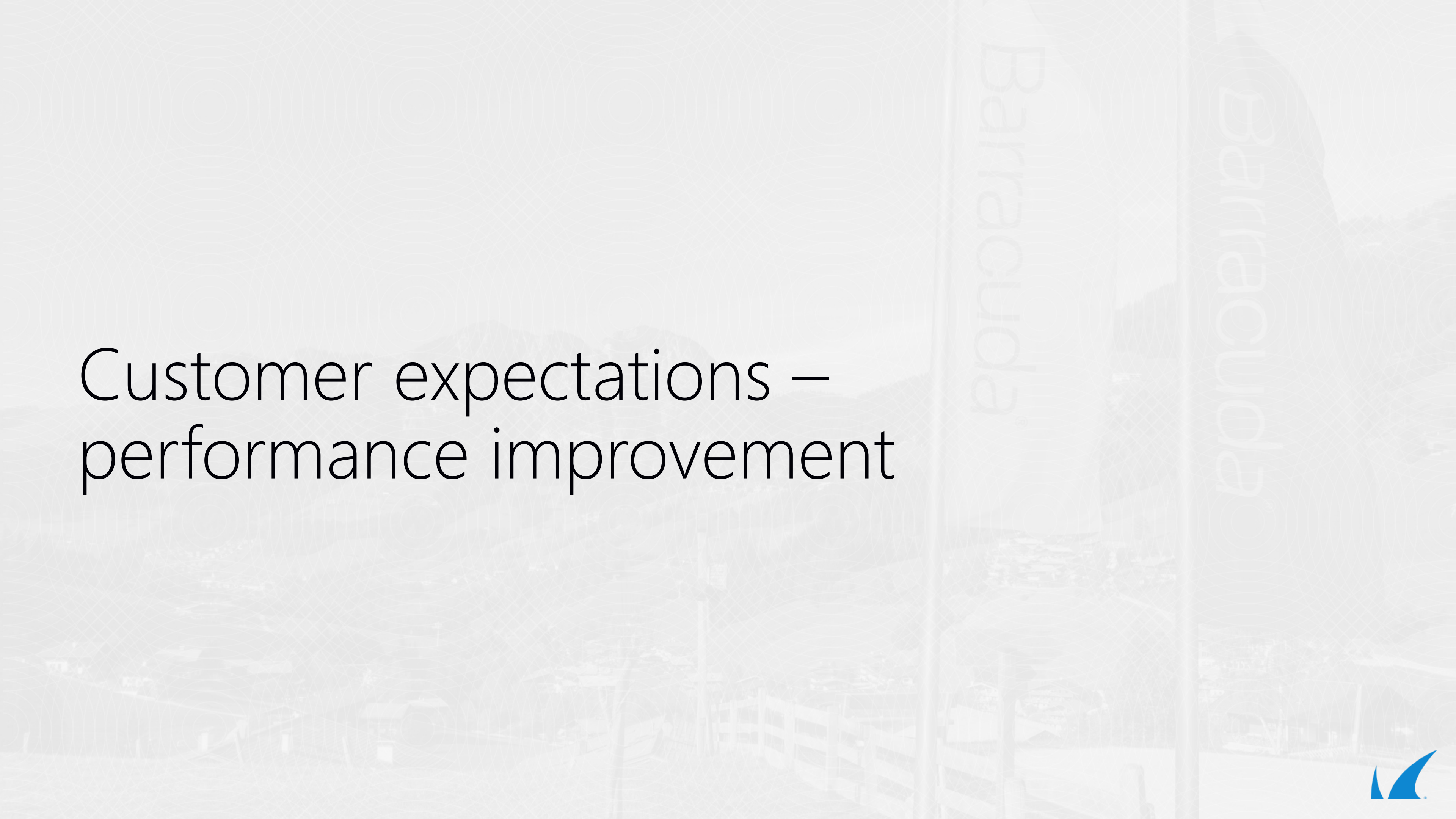


MPLS DSL LTE

You must choose wisely…

Maximum Reliability

Maximum Performance



Customer expectations – performance improvement

Performance improvements

Performance problems & customer expectations

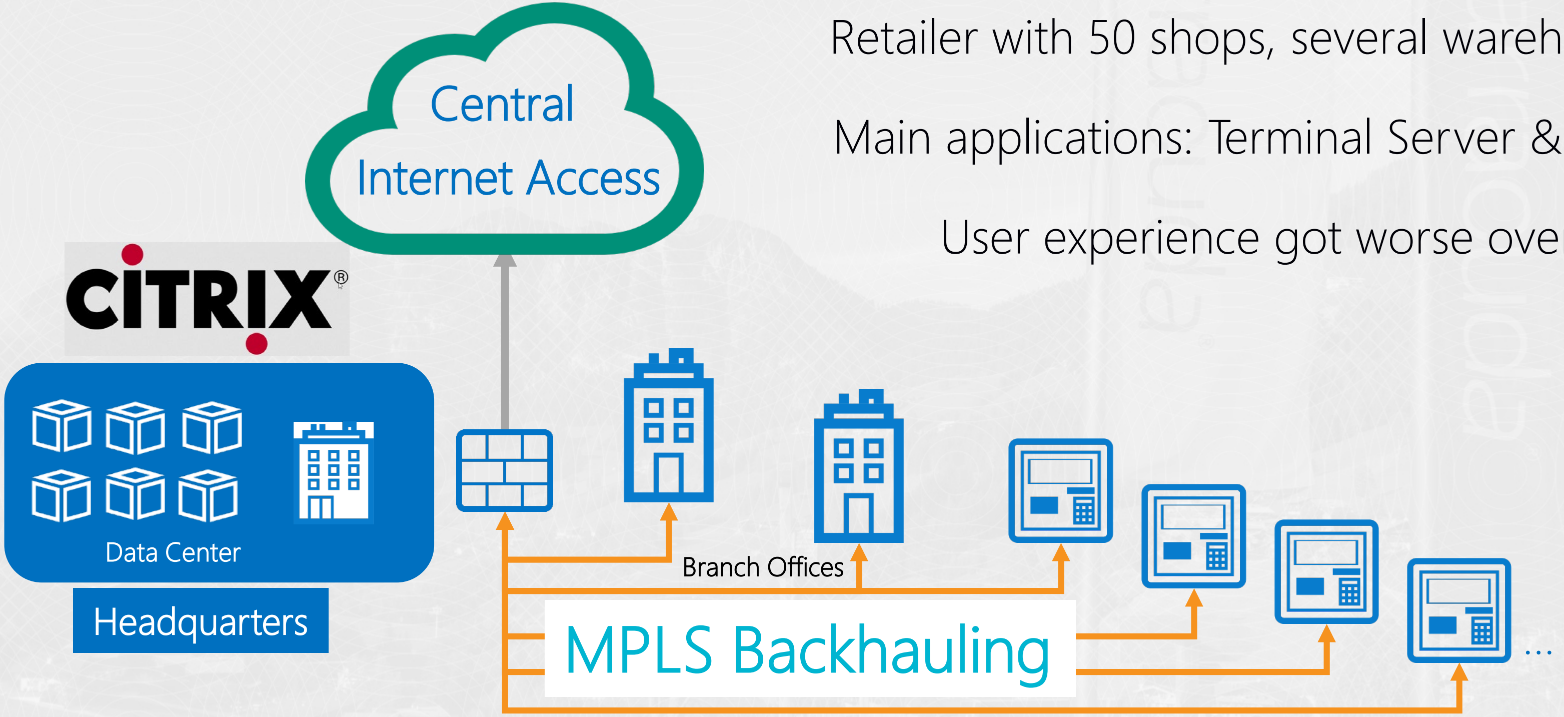
- The users complain about bad performance
- Other factors like usage peak, application, storage, hypervisors
- It‘s not only about the network

End-to-end application performance

- Questions to ask
  - which application, which users/groups, when, what happens,….

End user experience

Customer example – retailer with 50+ shops

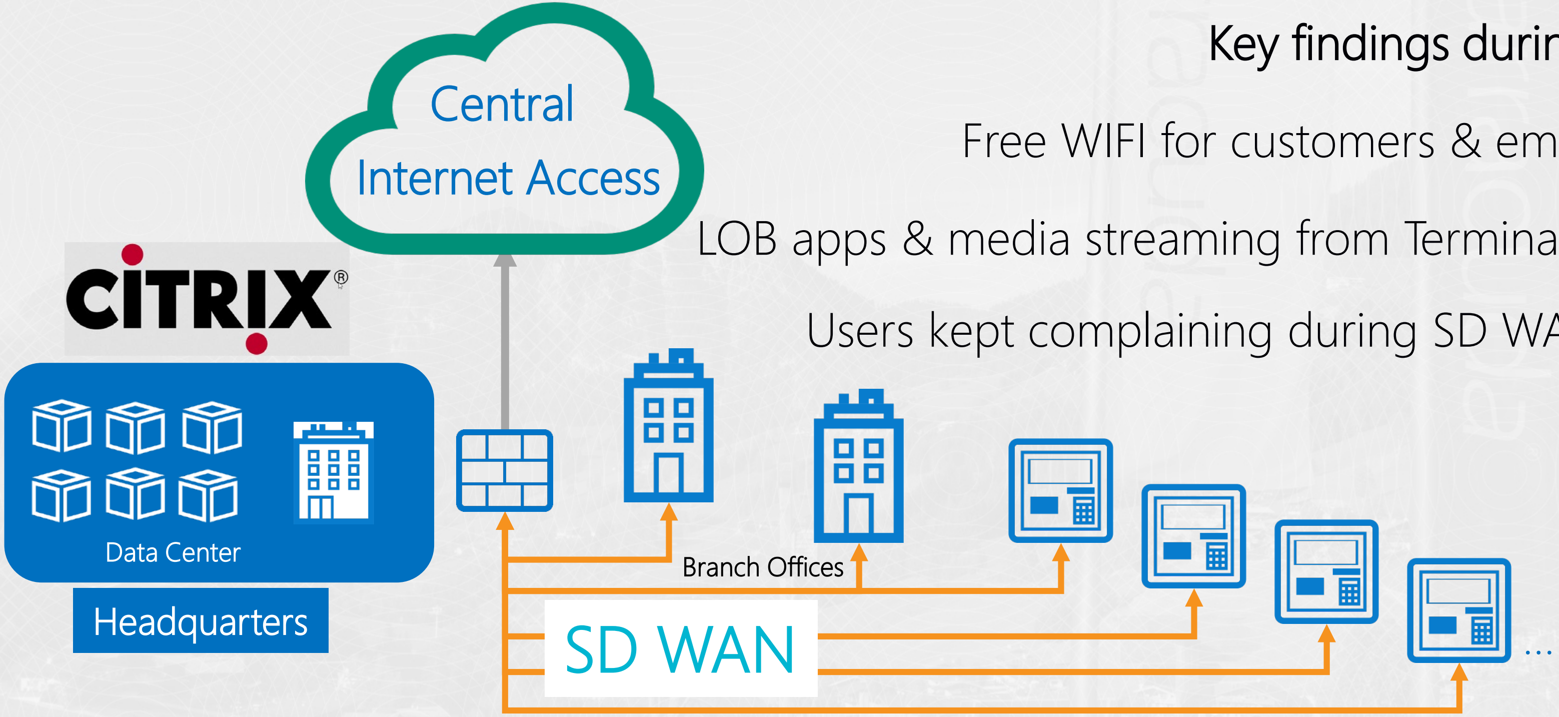


Retailer with 50 shops, several warehouses

Main applications: Terminal Server & VOIP

User experience got worse over time

Customer example – Retailer with 50+ shops



Key findings during POC:

Free WIFI for customers & employees

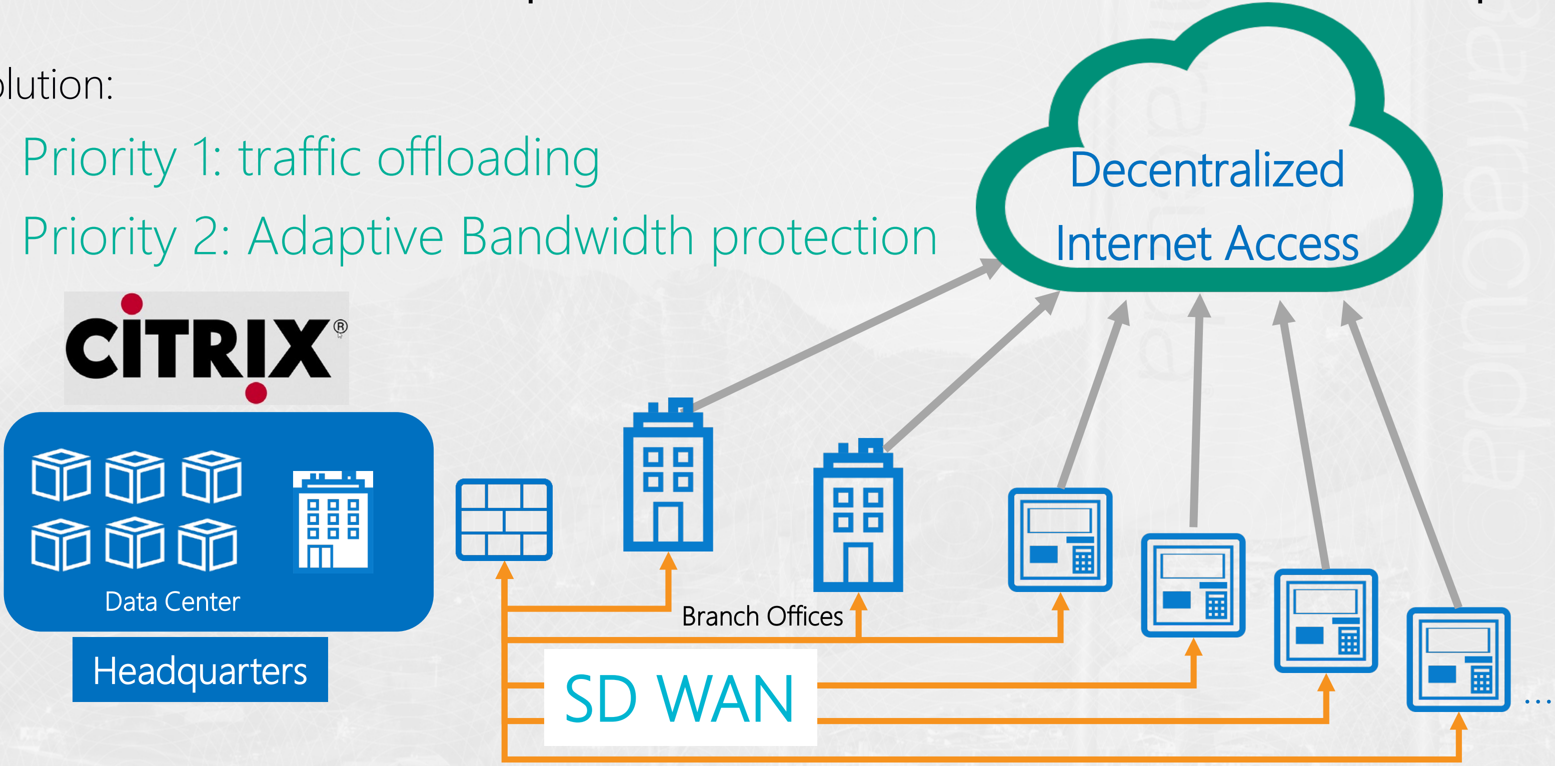
LOB apps & media streaming from Terminal Server

Users kept complaining during SD WAN POC

Customer example – Retailer with 50+ shops

Solution:

- Priority 1: traffic offloading
- Priority 2: Adaptive Bandwidth protection



End-user experience

End user experience – important advices:

- Define KPIs – objective metrics
- Do not change more than one thing at a time

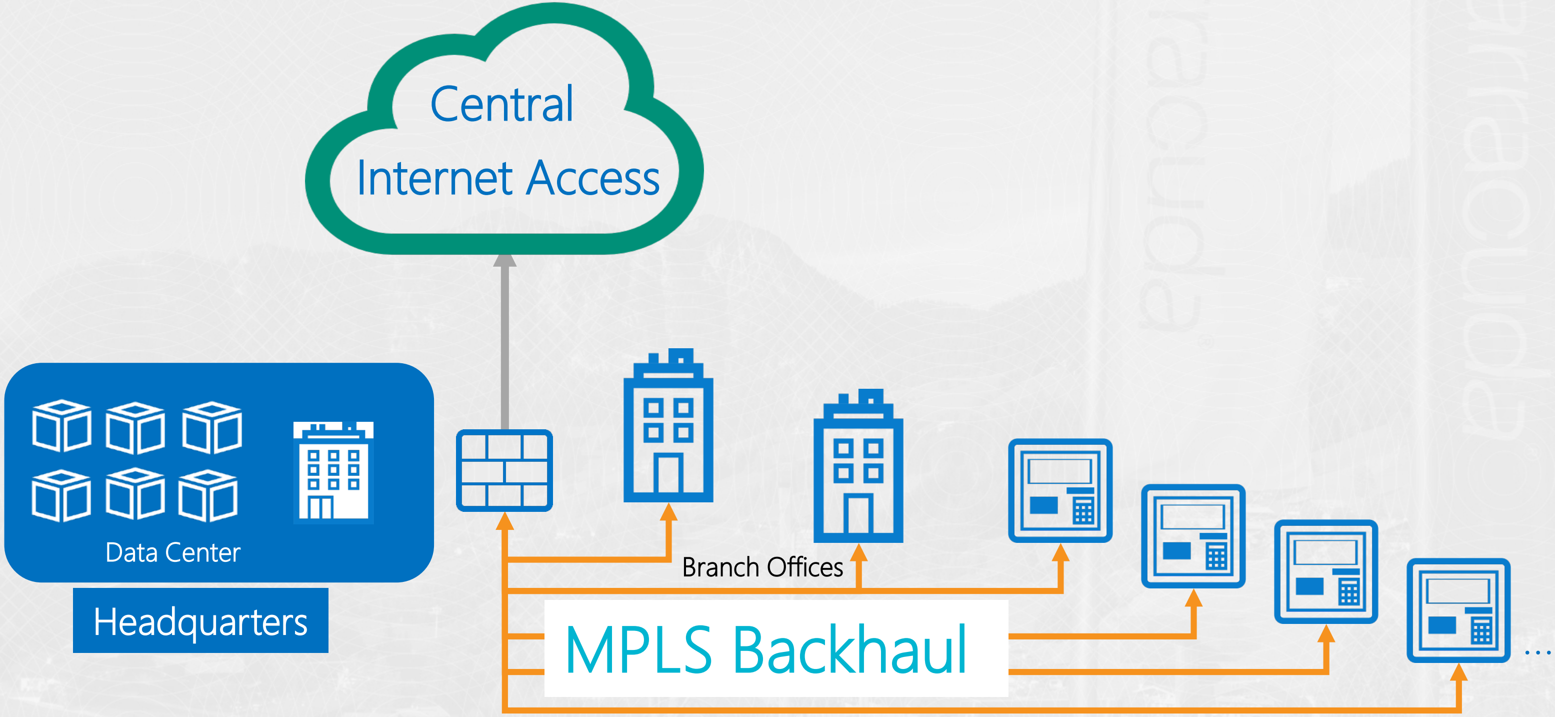
End-user experience monitoring – use 3rd party tools like:

- Lakeside *https://www.lakesidesoftware.com*
- Nexthink *https://www.nexthink.com*

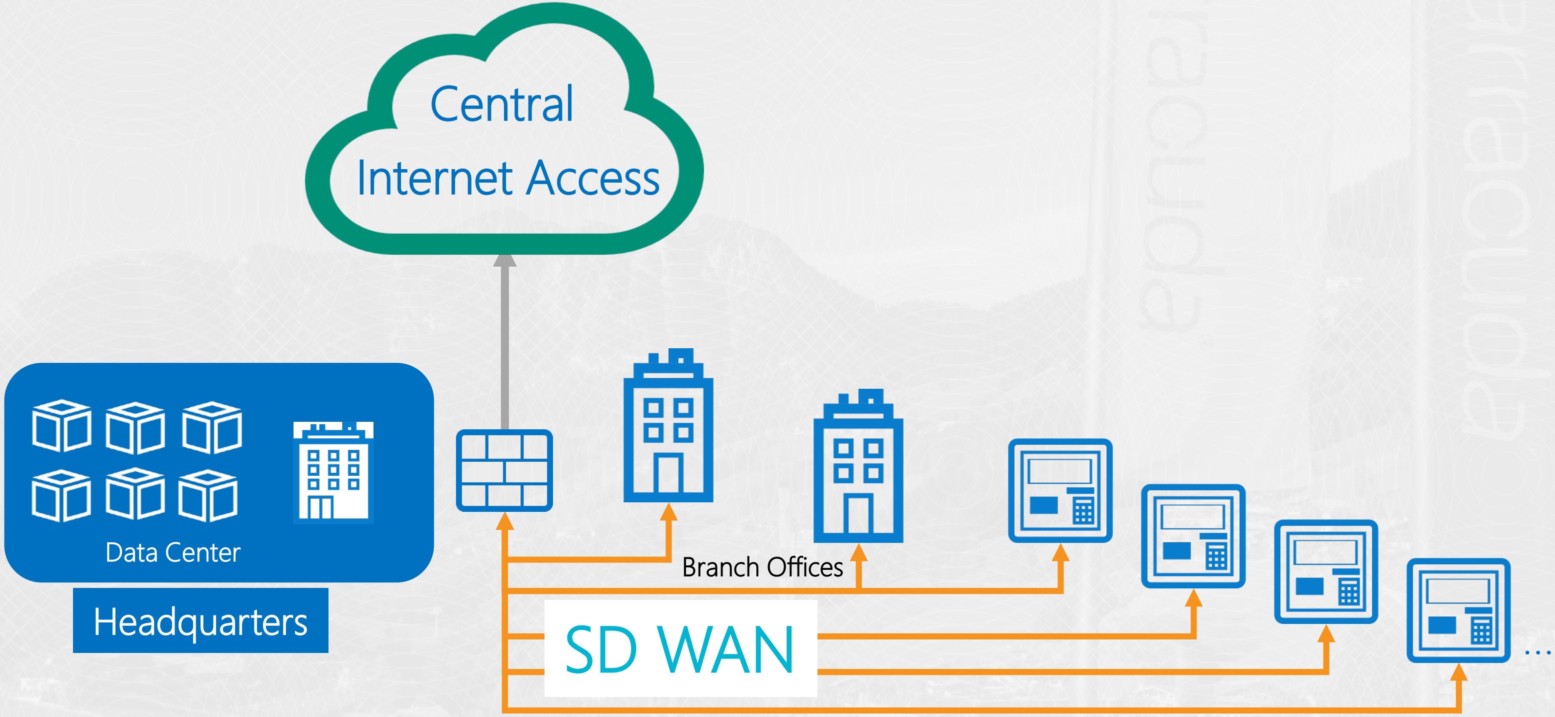
.....

Traffic offloading

Do not simply replace MPLS by SD-WAN



Do not simply replace MPLS by SD-WAN



Traffic offloading – Local internet breakout

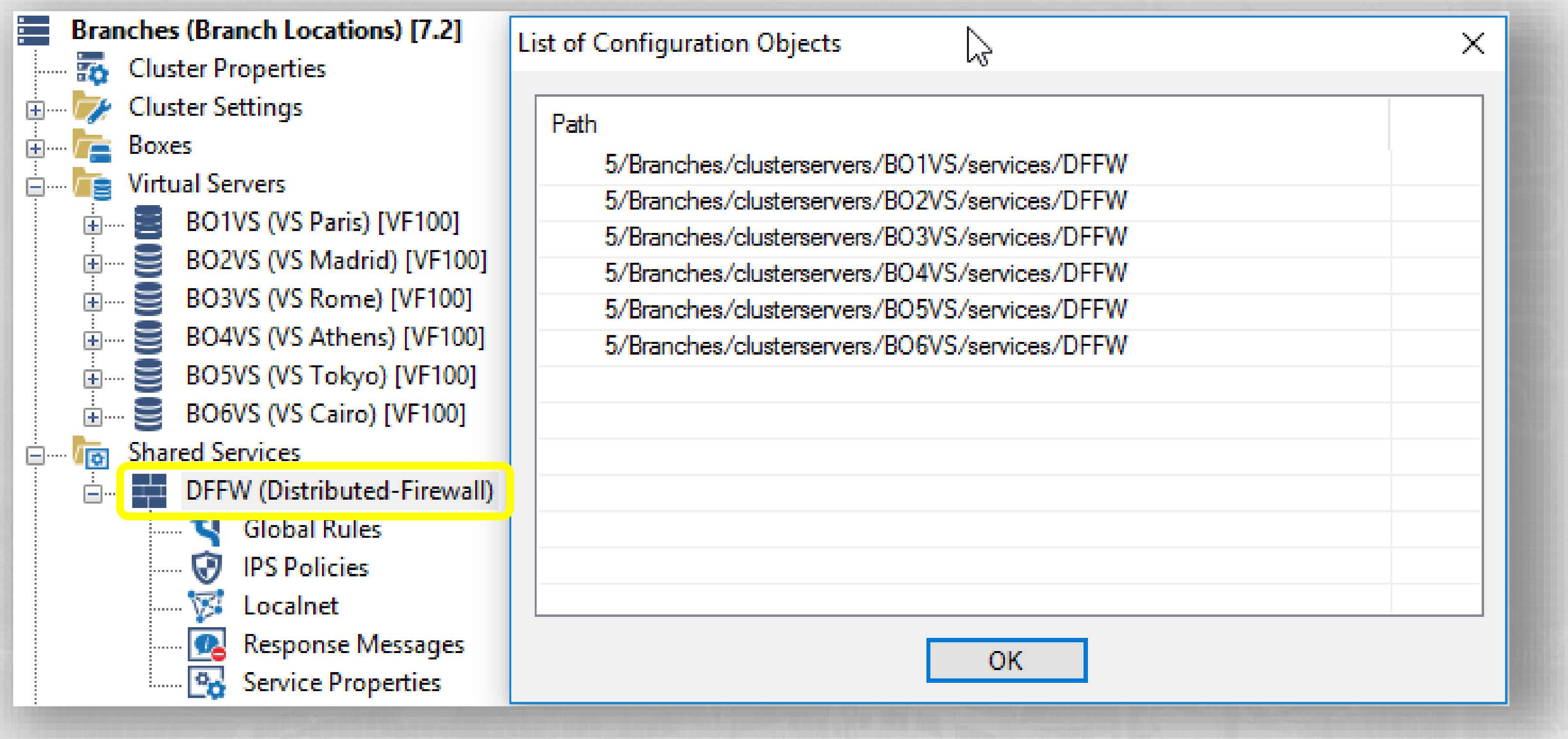
It is not an option – it is a must!

How to manage:

- Distributed firewall
- Application based policies & provider selection
- QoS per application
- Repositories for firewall, traffic shaping,.....

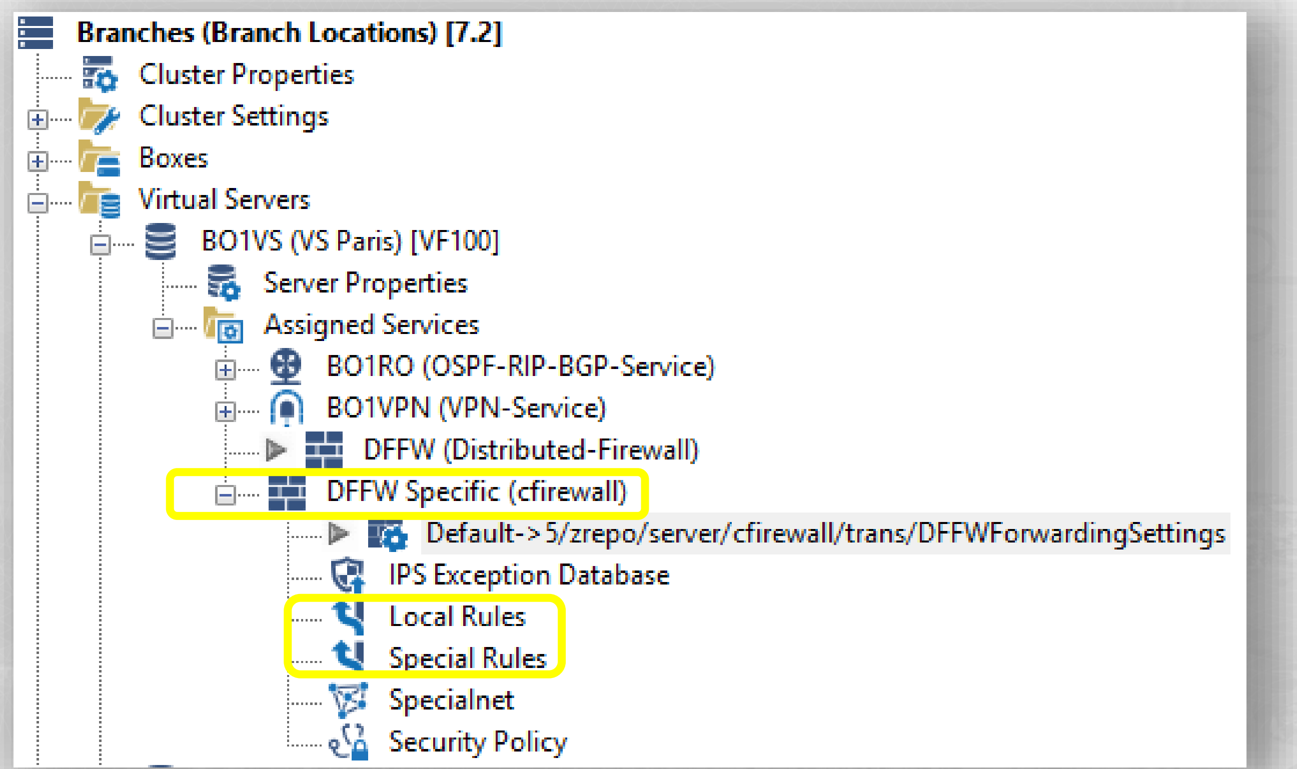
BARRACUDA NETWORKS
CloudGen Firewall F800.CCE v7.2.3
NEXT GENERATION FIREWALL
NSS LABS
RECOMMENDED
JULY
2019

Traffic Offloading - Distributed Firewall



Path
5/Branches/clusterservers/BO1VS/services/DFFW
5/Branches/clusterservers/BO2VS/services/DFFW
5/Branches/clusterservers/BO3VS/services/DFFW
5/Branches/clusterservers/BO4VS/services/DFFW
5/Branches/clusterservers/BO5VS/services/DFFW
5/Branches/clusterservers/BO6VS/services/DFFW

Traffic Offloading - Distributed Firewall

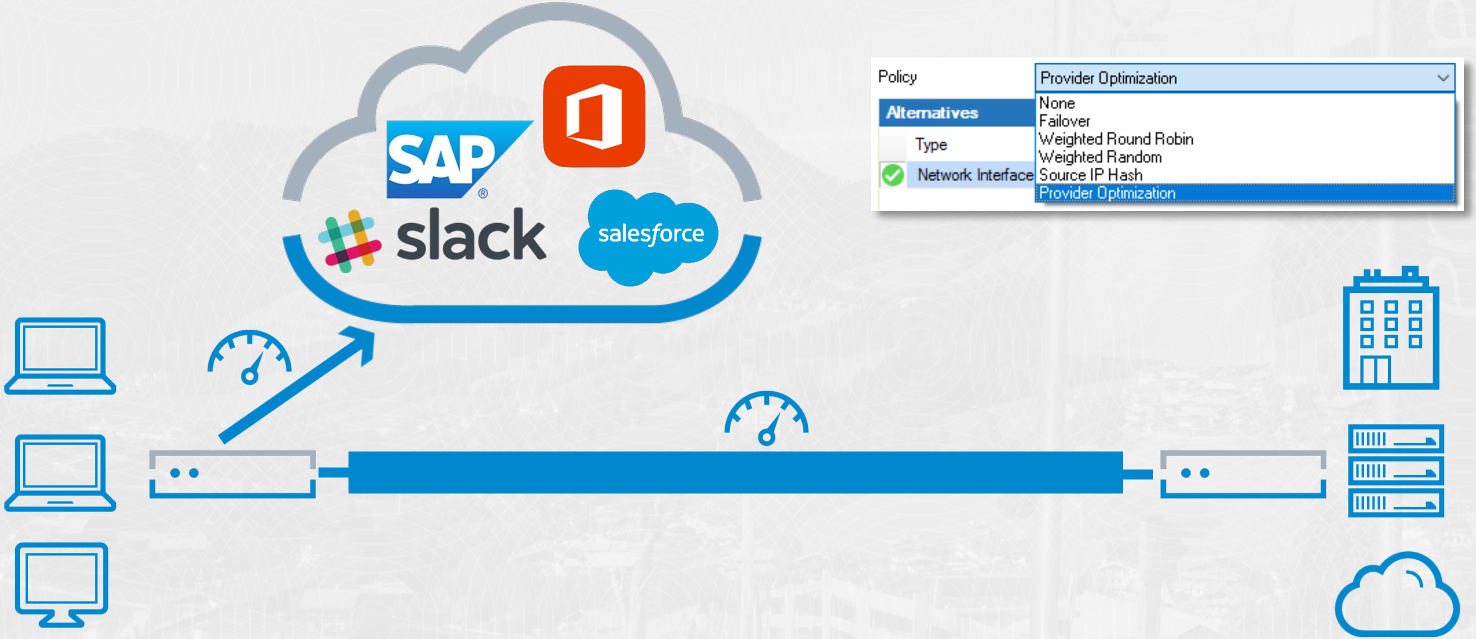


Branches (Branch Locations) [7.2]

- Cluster Properties
- Cluster Settings
- Boxes
- Virtual Servers
  - BO1VS (VS Paris) [VF100]
    - Server Properties
    - Assigned Services
      - BO1RO (OSPF-RIP-BGP-Service)
      - BO1VPN (VPN-Service)
      - DFFW (Distributed-Firewall)
    - DFFW Specific (cfirewall)
      - Default-> 5/zrepo/server/cfirewall/trans/DFFWForwardingSettings
      - IPS Exception Database
      - Local Rules
      - Special Rules
      - Specialnet
      - Security Policy

SD-WAN – Local Breakout

O365 Detection – App Detection – Provider Optimization (8.0.1)



Policy: Provider Optimization

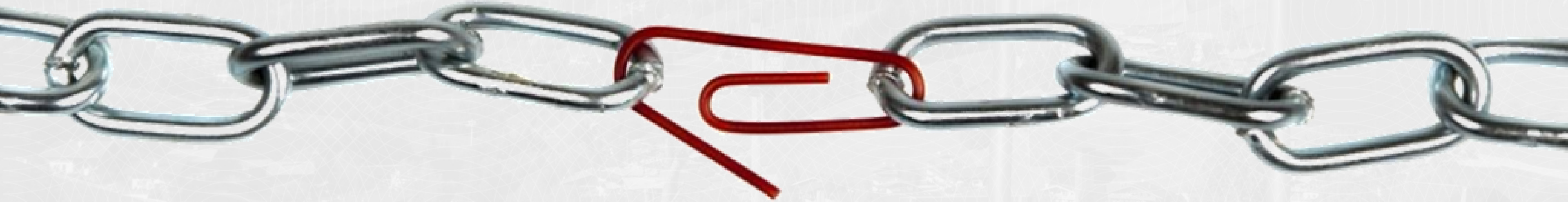
Alternatives

Type

Network Interface

Traffic offloading - Distributed firewall

- Don‘t let one branch office become the weakest link that infects the whole network
- Use the same subscriptions and rules in headquarters and branch offices (Malware Protection & ATP)



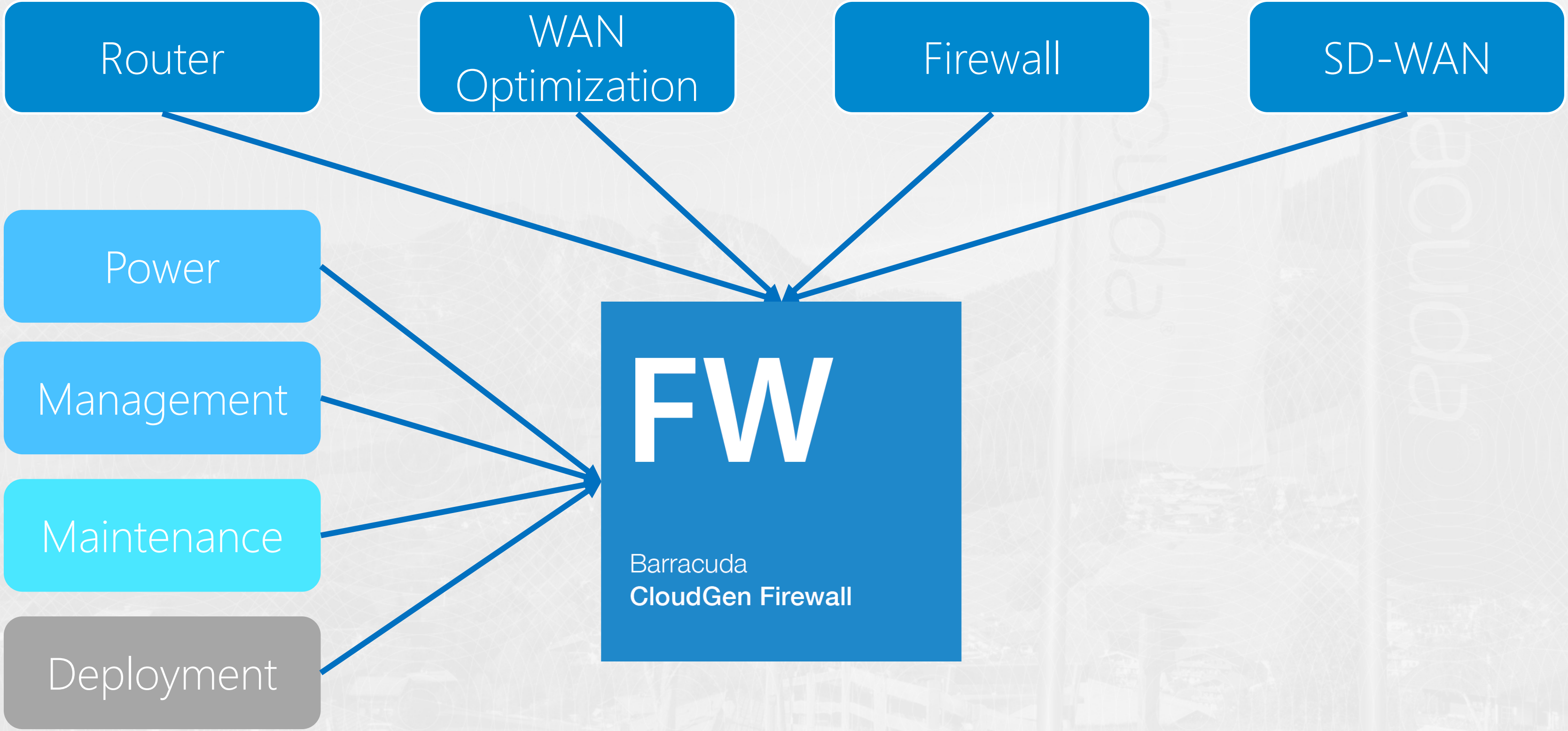
Reduce Complexity

Reduce Complexity

Complexity reduction

Router	WAN Optimization	Firewall	SD-WAN
Power	Power	Power	Power
Management	Management	Management	Management
Maintenance	Maintenance	Maintenance	Maintenance
Deployment	Deployment	Deployment	Deployment

Complexity reduction



Integrated DSL modem

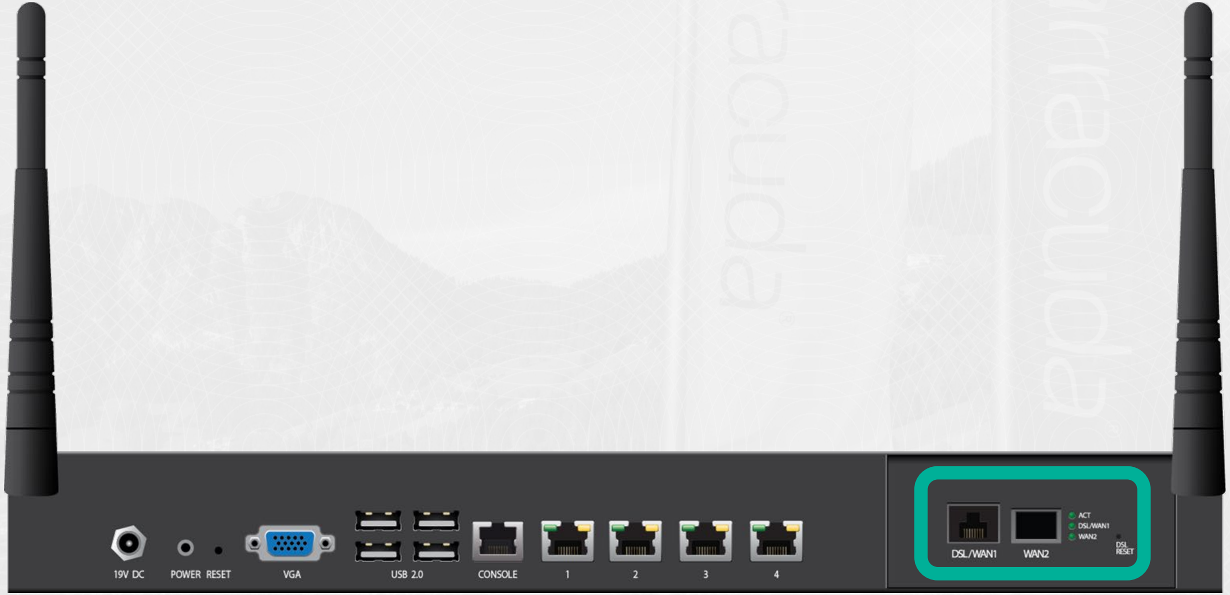
F82 Annex-A

F82 Annex-B

No external

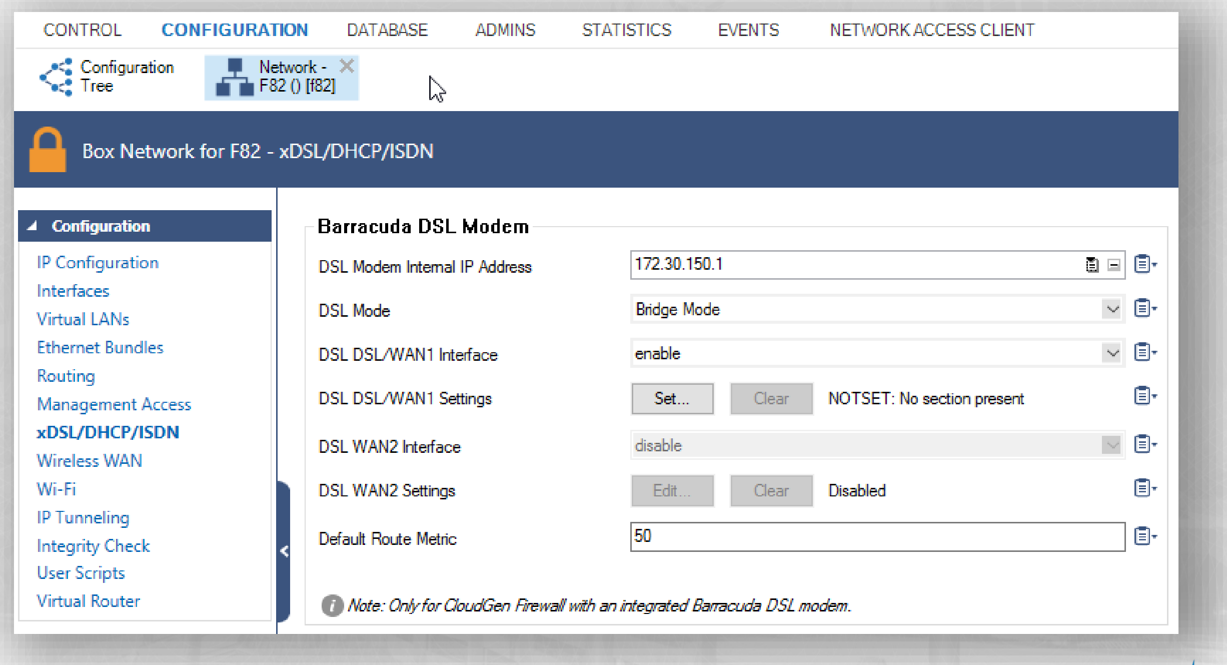
DSL modem

necessary



Integrated DSL Modem

- Configuration via CC
- Monitoring via FW



Box Network for F82 - xDSL/DHCP/ISDN

Barracuda DSL Modem

DSL Modem Internal IP Address	172.30.150.1
DSL Mode	Bridge Mode
DSL DSL/WAN1 Interface	enable
DSL DSL/WAN1 Settings	NOTSET: No section present
DSL WAN2 Interface	disable
DSL WAN2 Settings	Disabled
Default Route Metric	50

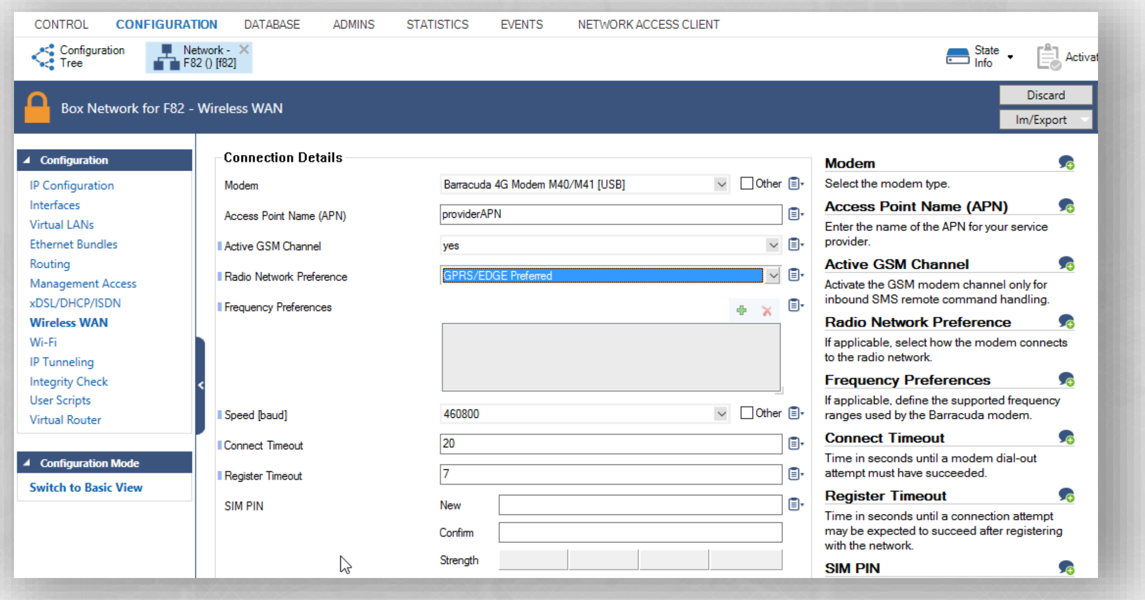
Note: Only for CloudGen Firewall with an integrated Barracuda DSL modem.

Barracuda USB modems

M40/M41 modem

Barracuda USB Modems

- M40/M41 Modem
- Advantage: Configuration via CC
- Disadvantage: For High Availability 2 Modems and 2 SIMs needed, not supported by all providers



Box Network for F82 - Wireless WAN

Connection Details

Modem: Barracuda 4G Modem M40/M41 [USB] □ Other

Access Point Name (APN): providerAPN

Active GSM Channel: yes

Radio Network Preference: GPRS/EDGE Preferred

Frequency Preferences

Speed [baud]: 460800 □ Other

Connect Timeout: 20

Register Timeout: 7

SIM PIN: New / Confirm / Strength

Modem
Select the modem type.

Access Point Name (APN)
Enter the name of the APN for your service provider.

Active GSM Channel
Activate the GSM modem channel only for inbound SMS remote command handling.

Radio Network Preference
If applicable, select how the modem connects to the radio network.

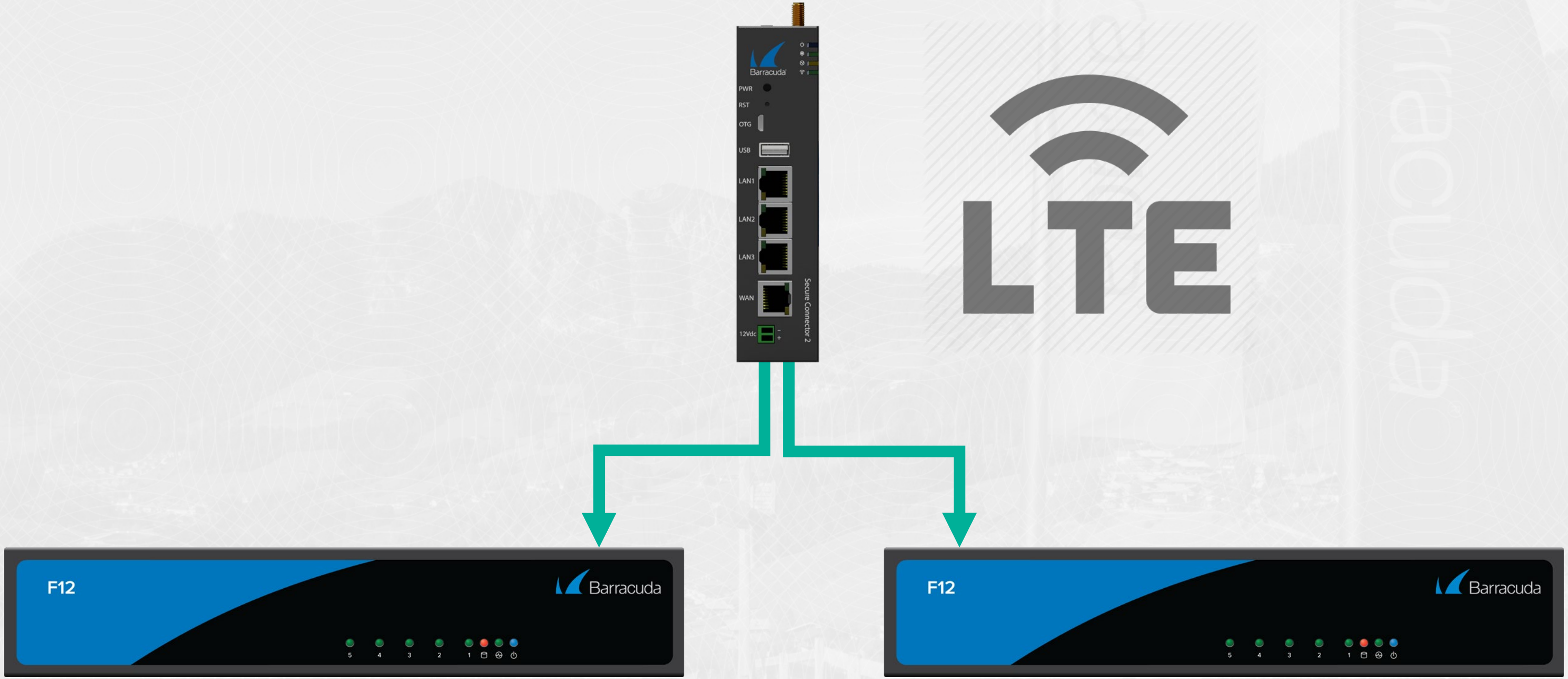
Frequency Preferences
If applicable, define the supported frequency ranges used by the Barracuda modem.

Connect Timeout
Time in seconds until a modem dial-out attempt must have succeeded.

Register Timeout
Time in seconds until a connection attempt may be expected to succeed after registering with the network.

SIM PIN

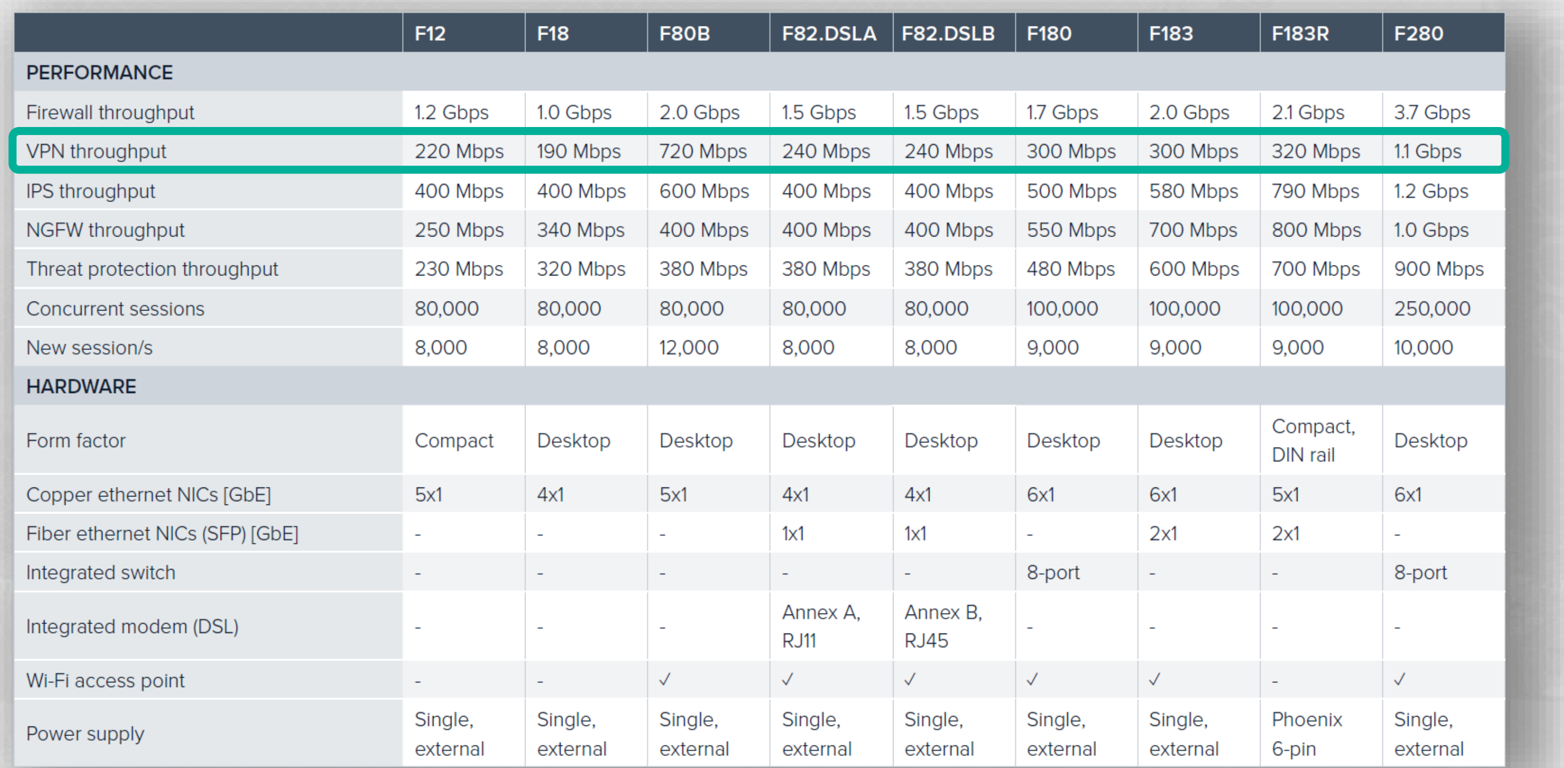
Secure Connector SC 2.4 / SC 2.6



Sizing

SD WAN sizing

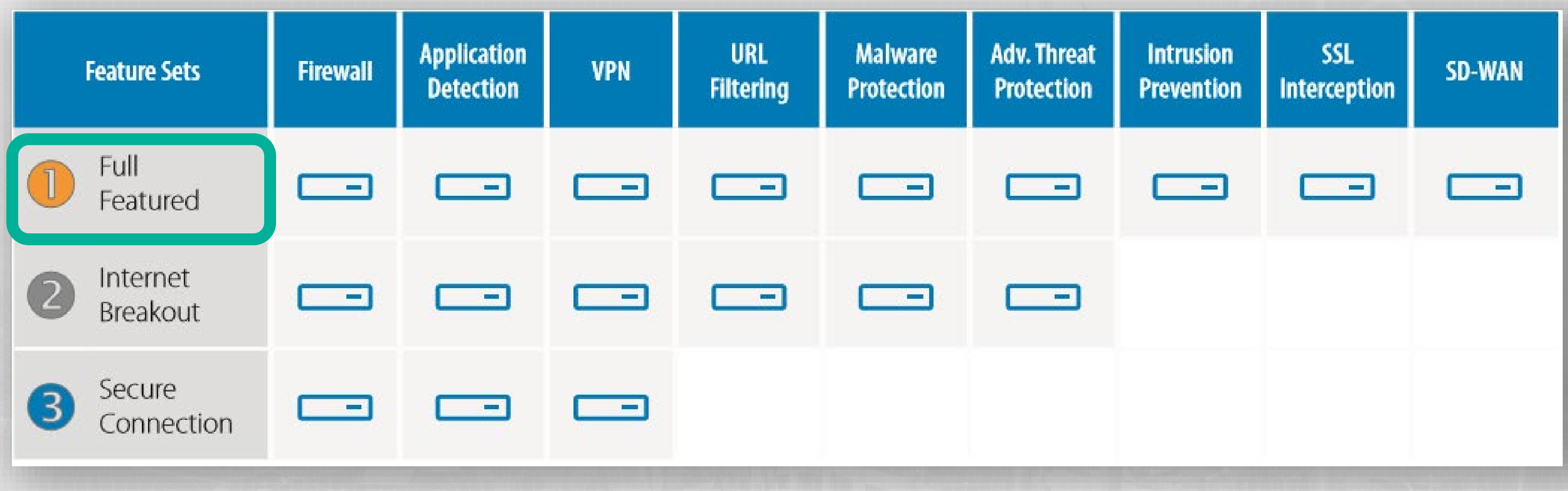
VPN performance is based on 1415 Byte UDP packets, bidirectional using BreakingPoint traffic generator.



	F12	F18	F80B	F82.DSLA	F82.DSLB	F180	F183	F183R	F280
PERFORMANCE									
Firewall throughput	1.2 Gbps	1.0 Gbps	2.0 Gbps	1.5 Gbps	1.5 Gbps	1.7 Gbps	2.0 Gbps	2.1 Gbps	3.7 Gbps
VPN throughput	220 Mbps	190 Mbps	720 Mbps	240 Mbps	240 Mbps	300 Mbps	300 Mbps	320 Mbps	1.1 Gbps
IPS throughput	400 Mbps	400 Mbps	600 Mbps	400 Mbps	400 Mbps	500 Mbps	580 Mbps	790 Mbps	1.2 Gbps
NGFW throughput	250 Mbps	340 Mbps	400 Mbps	400 Mbps	400 Mbps	550 Mbps	700 Mbps	800 Mbps	1.0 Gbps
Threat protection throughput	230 Mbps	320 Mbps	380 Mbps	380 Mbps	380 Mbps	480 Mbps	600 Mbps	700 Mbps	900 Mbps
Concurrent sessions	80,000	80,000	80,000	80,000	80,000	100,000	100,000	100,000	250,000
New session/s	8,000	8,000	12,000	8,000	8,000	9,000	9,000	9,000	10,000
HARDWARE									
Form factor	Compact	Desktop	Desktop	Desktop	Desktop	Desktop	Desktop	Compact, DIN rail	Desktop
Copper ethernet NICs [GbE]	5x1	4x1	5x1	4x1	4x1	6x1	6x1	5x1	6x1
Fiber ethernet NICs (SFP) [GbE]	-	-	-	1x1	1x1	-	2x1	2x1	-
Integrated switch	-	-	-	-	-	8-port	-	-	8-port
Integrated modem (DSL)	-	-	-	Annex A, RJ11	Annex B, RJ45	-	-	-	-
Wi-Fi access point	-	-	✓	✓	✓	✓	✓	-	✓
Power supply	Single, external	Single, external	Single, external	Single, external	Single, external	Single, external	Single, external	Phoenix 6-pin	Single, external

SD WAN sizing

Choose the „Full Featured“ use case, because of local breakout in branches



Feature Sets	Firewall	Application Detection	VPN	URL Filtering	Malware Protection	Adv. Threat Protection	Intrusion Prevention	SSL Interception	SD-WAN
1 Full Featured	▭	▭	▭	▭	▭	▭	▭	▭	▭
2 Internet Breakout	▭	▭	▭	▭	▭	▭			
3 Secure Connection	▭	▭	▭						

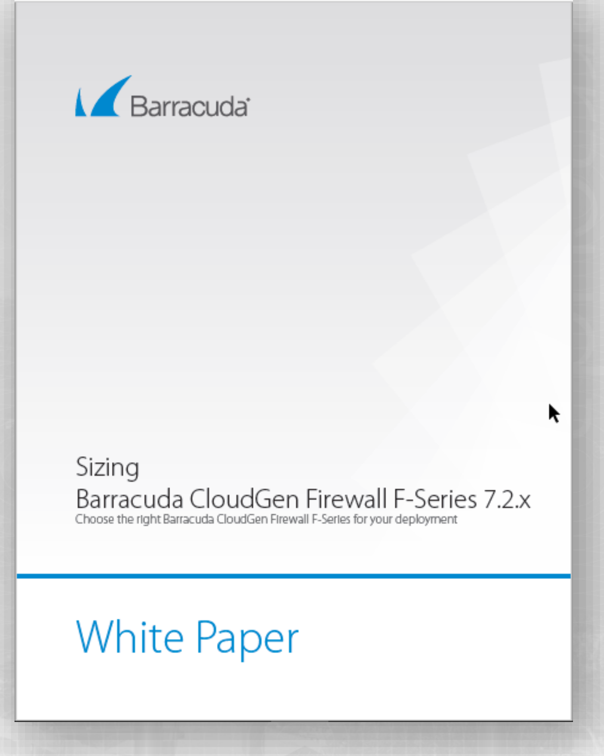
Firewall Sizing - Sources

Cloudgen Sizing Whitepaper

Excel Sizing Calculator

Datasheets

Product Overview



Barracuda

Sizing

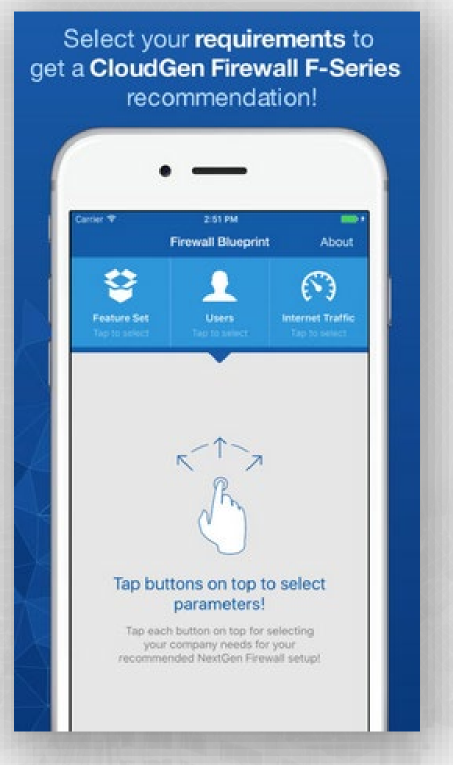
Barracuda CloudGen Firewall F-Series 7.2.x

Choose the right Barracuda CloudGen Firewall F-Series for your deployment

White Paper

Firewall Sizing - Sources

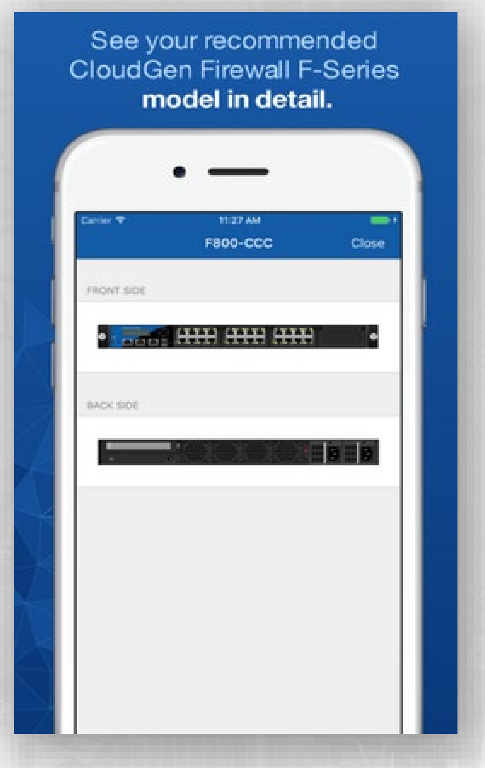
Firewall BluePrint App for iOS



Select your **requirements** to get a **CloudGen Firewall F-Series** recommendation!

Tap buttons on top to select parameters!

Tap each button on top for selecting your company needs for your recommended NextGen Firewall setup!

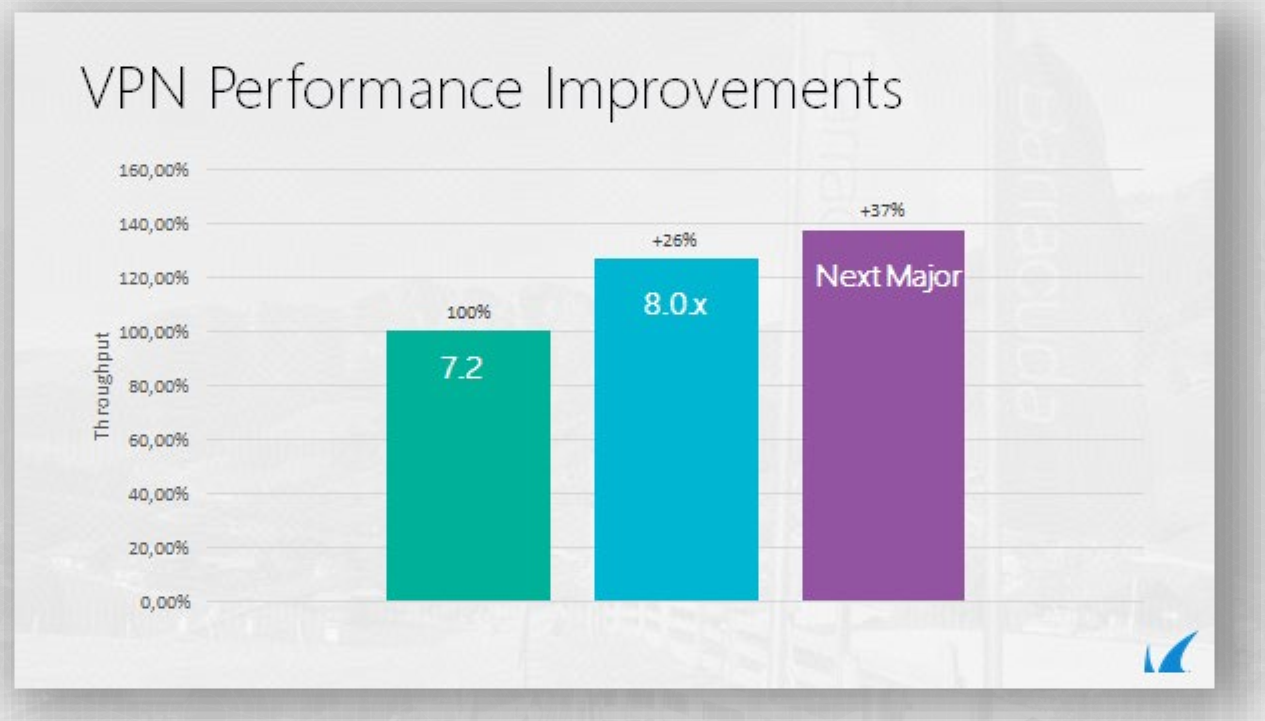


See your recommended CloudGen Firewall F-Series **model in detail.**

Performance tuning - VPN

Realease the Handbrake

VPN Performance Improvements



VPN Performance Improvements

Firewall default limits

Be aware that there are default configurations that limit the box performance!

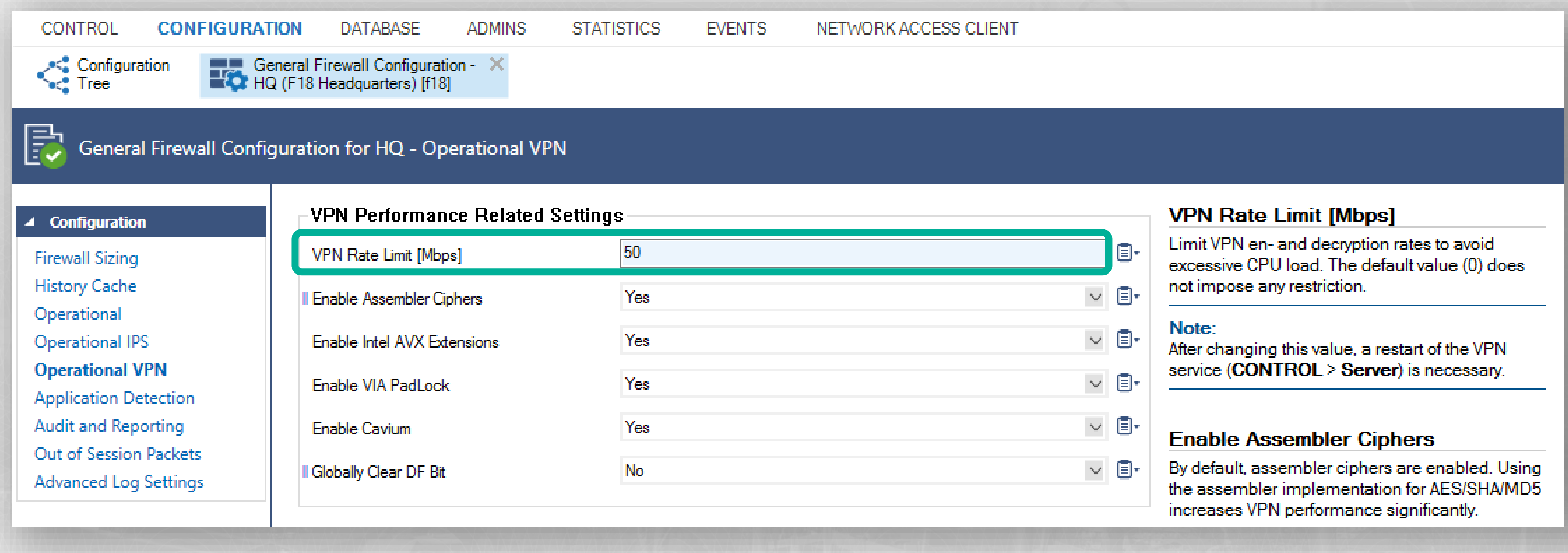
- on smaller boxes

- VPN limits

- Performance limits

Firewall default limits

General firewall configuration F18



General Firewall Configuration for HQ - Operational VPN

VPN Performance Related Settings

VPN Rate Limit [Mbps]	50
Enable Assembler Ciphers	Yes
Enable Intel AVX Extensions	Yes
Enable VIA PadLock	Yes
Enable Cavium	Yes
Globally Clear DF Bit	No

VPN Rate Limit [Mbps]

Limit VPN en- and decryption rates to avoid excessive CPU load. The default value (0) does not impose any restriction.

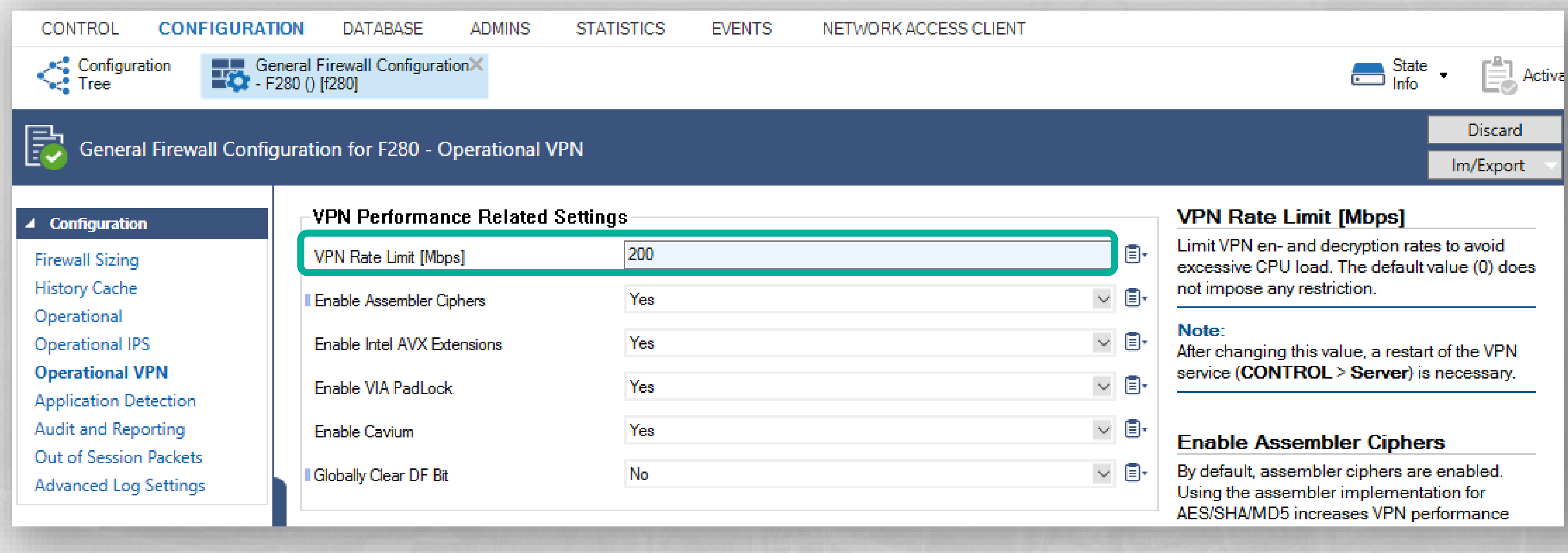
Note:
After changing this value, a restart of the VPN service (**CONTROL** > **Server**) is necessary.

Enable Assembler Ciphers

By default, assembler ciphers are enabled. Using the assembler implementation for AES/SHA/MD5 increases VPN performance significantly.

Firewall default limits

General firewall configuration F280



General Firewall Configuration for F280 - Operational VPN

VPN Performance Related Settings

VPN Rate Limit [Mbps]	200
Enable Assembler Ciphers	Yes
Enable Intel AVX Extensions	Yes
Enable VIA PadLock	Yes
Enable Cavium	Yes
Globally Clear DF Bit	No

VPN Rate Limit [Mbps]

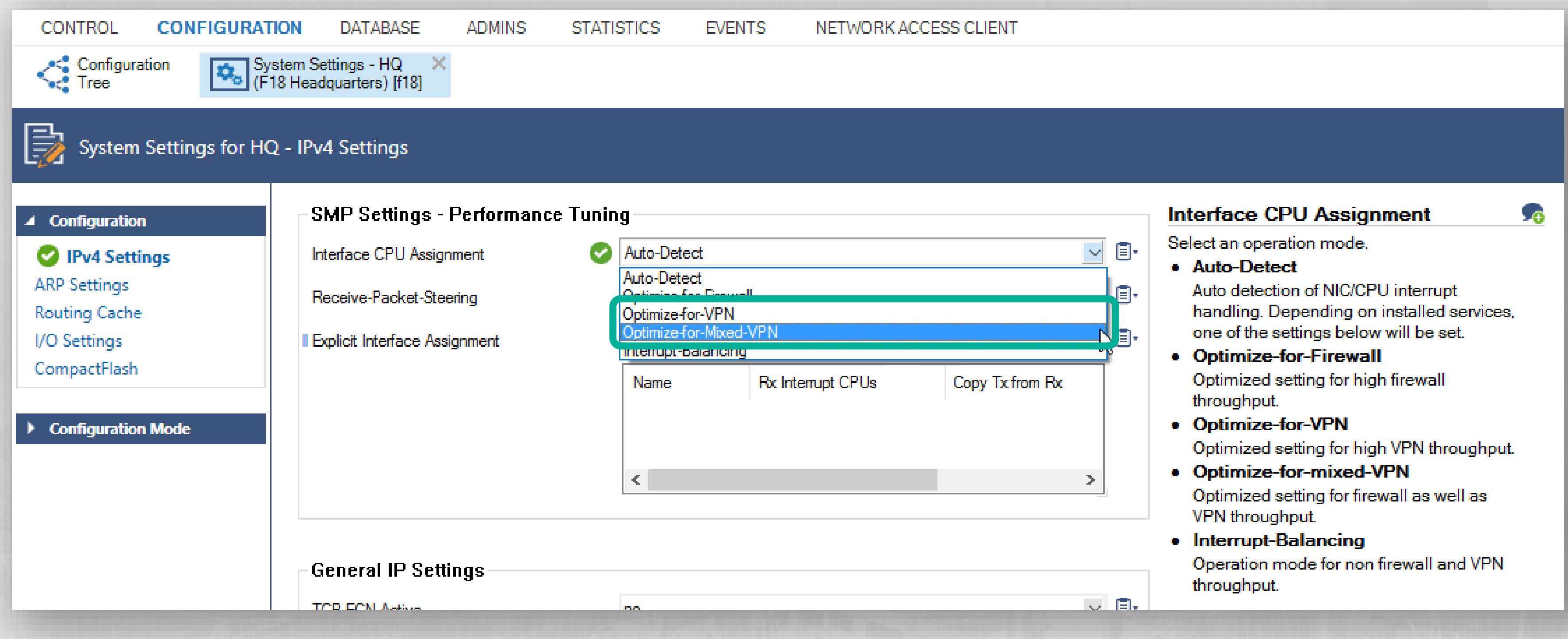
Limit VPN en- and decryption rates to avoid excessive CPU load. The default value (0) does not impose any restriction.

Note:
After changing this value, a restart of the VPN service (**CONTROL** > **Server**) is necessary.

Enable Assembler Ciphers

By default, assembler ciphers are enabled. Using the assembler implementation for AES/SHA/MD5 increases VPN performance

Firewall performance tuning



CONTROL | CONFIGURATION | DATABASE | ADMINS | STATISTICS | EVENTS | NETWORK ACCESS CLIENT

Configuration Tree | System Settings - HQ (F18 Headquarters) [f18]

System Settings for HQ - IPv4 Settings

- Configuration
  - IPv4 Settings
  - ARP Settings
  - Routing Cache
  - I/O Settings
  - CompactFlash
- Configuration Mode

SMP Settings - Performance Tuning

Interface CPU Assignment: Auto-Detect

- Auto-Detect
- Optimize-for-Firewall
- Optimize-for-VPN
- Optimize-for-Mixed-VPN
- Interrupt-Balancing

Receive-Packet-Steering

Explicit Interface Assignment

Name	Rx Interrupt CPUs	Copy Tx from Rx

General IP Settings

TCP ECN Active: no

Interface CPU Assignment

Select an operation mode.

- **Auto-Detect**
  Auto detection of NIC/CPU interrupt handling. Depending on installed services, one of the settings below will be set.
- **Optimize-for-Firewall**
  Optimized setting for high firewall throughput.
- **Optimize-for-VPN**
  Optimized setting for high VPN throughput.
- **Optimize-for-mixed-VPN**
  Optimized setting for firewall as well as VPN throughput.
- **Interrupt-Balancing**
  Operation mode for non firewall and VPN throughput.

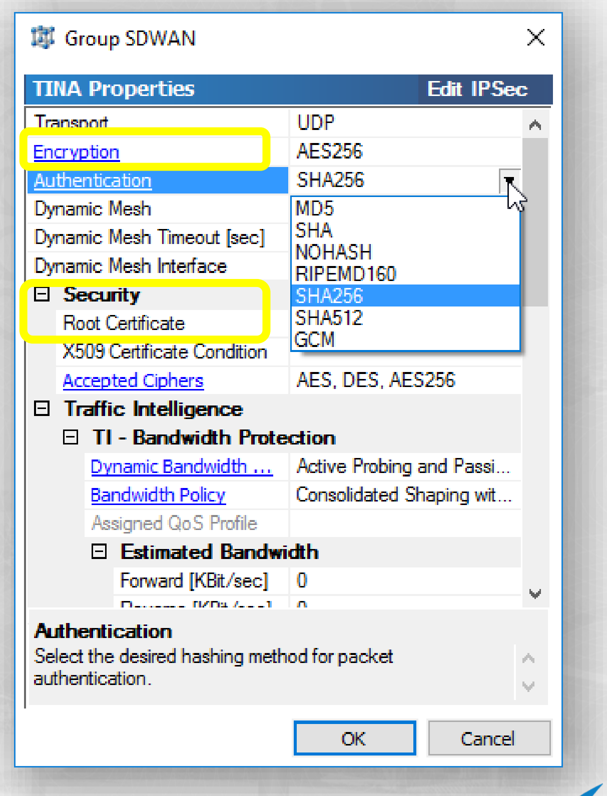
VPN performance tuning

- Use AES 128 / AES 256

Hardware acceleration by Intel AES/NI

- Use SHA256 instead of SHA512

SHA512 has a big performance impact, (20-30%) but increases security only slightly



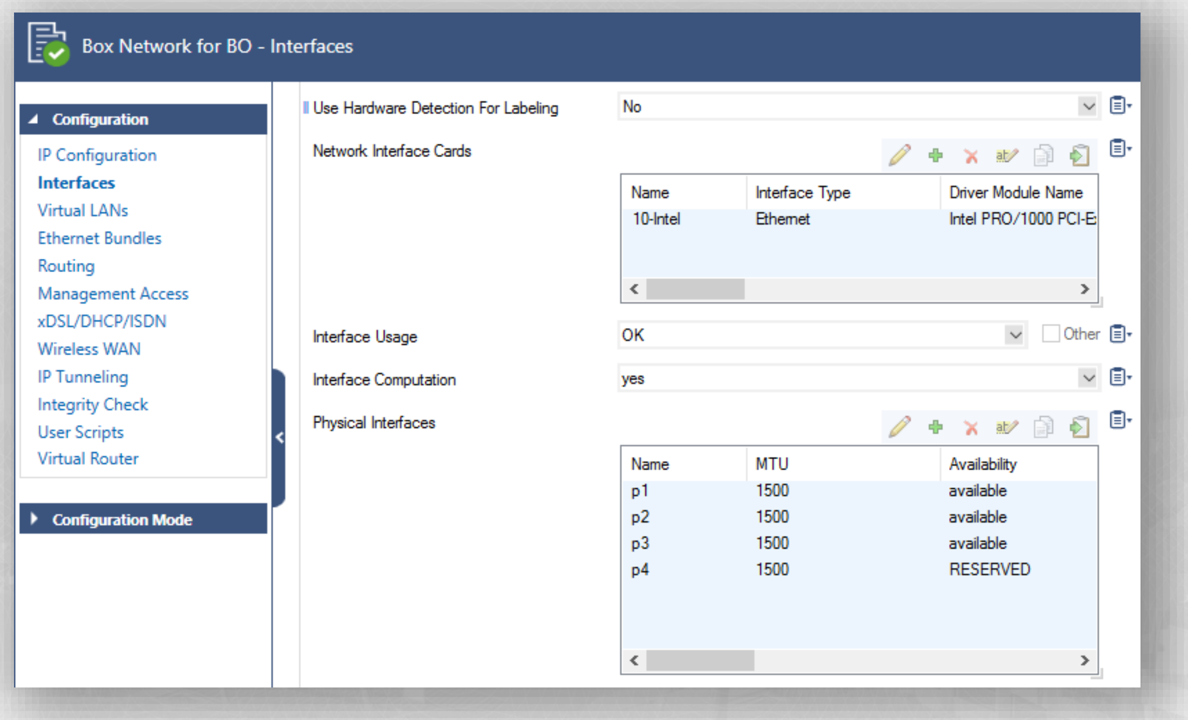
Transport	UDP
Encryption	AES256
Authentication	SHA256
Dynamic Mesh	
Dynamic Mesh Timeout [sec]	
Dynamic Mesh Interface	
⊟ **Security**	
Root Certificate	
X509 Certificate Condition	
Accepted Ciphers	AES, DES, AES256
⊟ **Traffic Intelligence**	
⊟ **TI - Bandwidth Protection**	
Dynamic Bandwidth ...	Active Probing and Passi...
Bandwidth Policy	Consolidated Shaping wit...
Assigned QoS Profile	
⊟ **Estimated Bandwidth**	
Forward [KBit/sec]	0
Reverse [KBit/sec]	0

Authentication
Select the desired hashing method for packet authentication.

Performance tuning – MTU size

MTU size - Interfaces

Network – Interfaces



Box Network for BO - Interfaces

Use Hardware Detection For Labeling: No

Network Interface Cards

Name	Interface Type	Driver Module Name
10-Intel	Ethernet	Intel PRO/1000 PCI-E

Interface Usage: OK □ Other

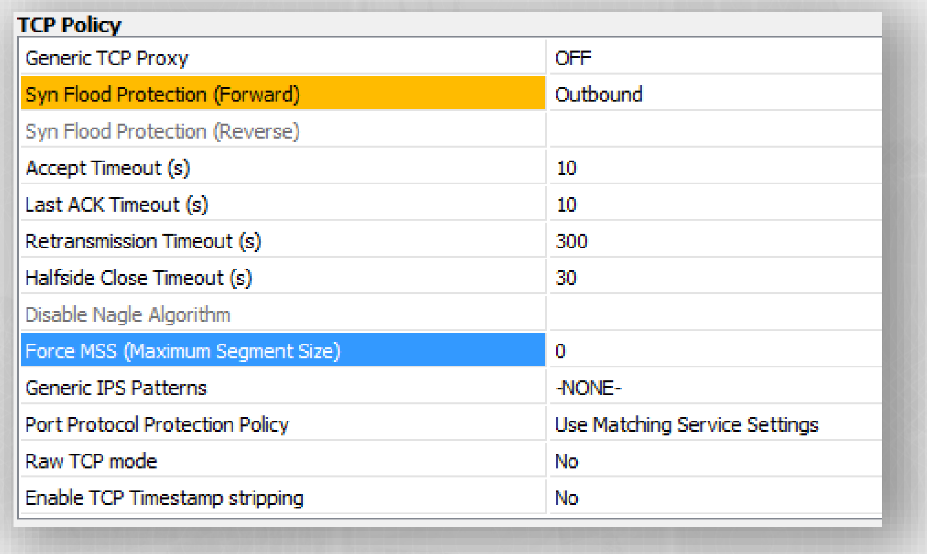
Interface Computation: yes

Physical Interfaces

Name	MTU	Availability
p1	1500	available
p2	1500	available
p3	1500	available
p4	1500	RESERVED

MSS size

- Firewall rule – advanced settings
- Force MSS (Maximum Segment Size)



TCP Policy

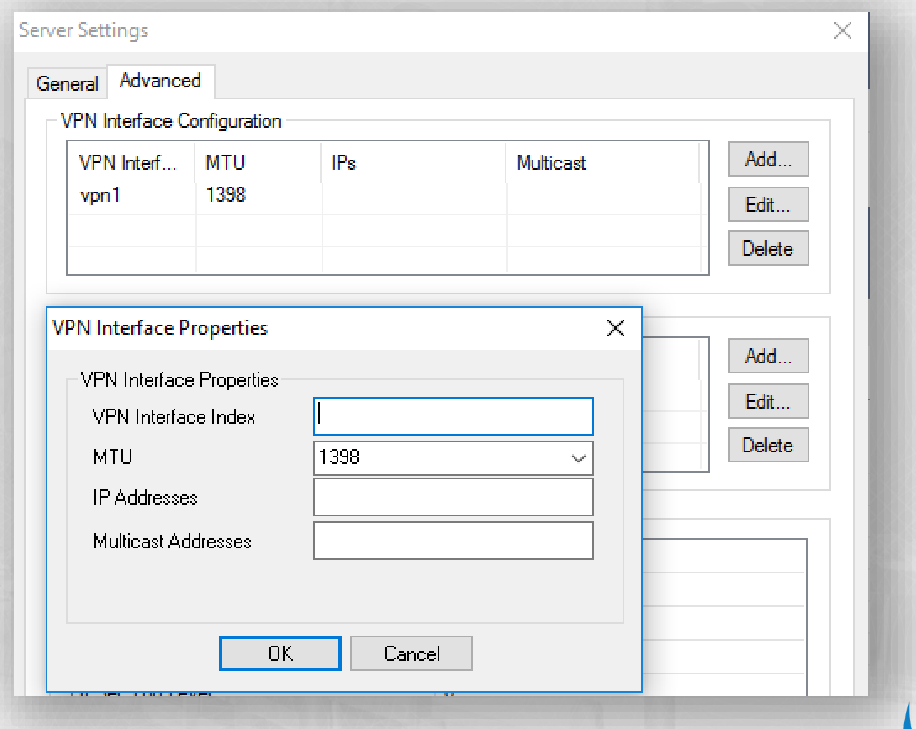
Generic TCP Proxy	OFF
Syn Flood Protection (Forward)	Outbound
Syn Flood Protection (Reverse)	
Accept Timeout (s)	10
Last ACK Timeout (s)	10
Retransmission Timeout (s)	300
Halfside Close Timeout (s)	30
Disable Nagle Algorithm	
Force MSS (Maximum Segment Size)	0
Generic IPS Patterns	-NONE-
Port Protocol Protection Policy	Use Matching Service Settings
Raw TCP mode	No
Enable TCP Timestamp stripping	No

Checks the SYN and SYN–ACK TCP packets for an MSS that is larger than the configured MSS. If the MSS TCP attribute is smaller, the packet is rewritten with the configured MSS. Use this feature for VPNs to force a TCP MSS that fits the MTU of the VPN tunnel device. For IPv4, the maximum transmission size must be at least 40 bytes smaller than the MTU.

MTU size – VPN interface

VPN settings - Server settings – Advanced

- VPN interface configuration
- Default value is 1398
- Should be set to 1398 minus the difference between 1500 and MTU of output device



Server Settings

VPN Interface Configuration

VPN Interf...	MTU	IPs	Multicast
vpn1	1398		

VPN Interface Properties

VPN Interface Properties

VPN Interface Index

MTU 1398

IP Addresses

Multicast Addresses

VPN Performance Testing

Testing with SMB / CIFS Traffic

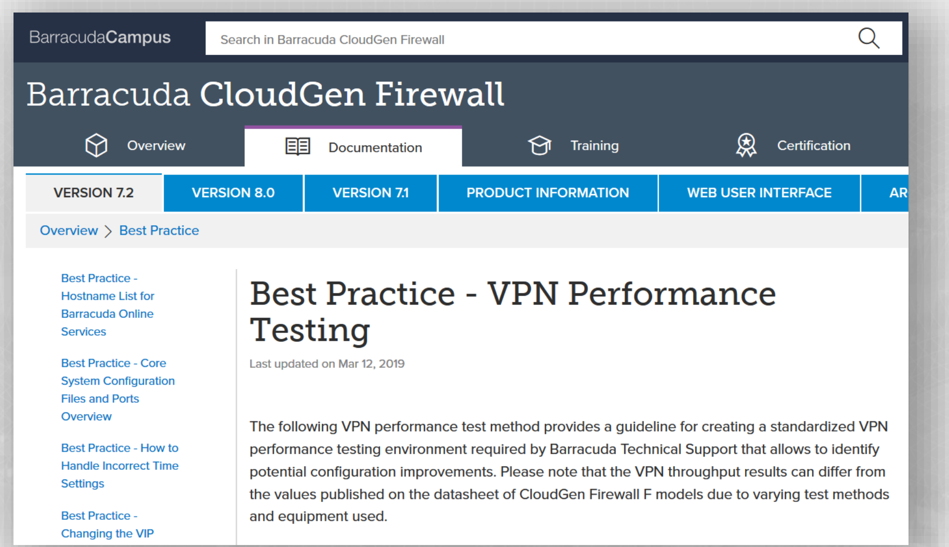
- When testing performance with SMB/CIFS traffic an be difficult to receive reproducible results.
- When testing the same VPN tunnel with iperf and CIFS traffic, expect the transfer rate for the file transfer to be slower than the iperf value.

- Calculate the theoretical TCP throughput to know the theoretical bandwidth of the connection: https://www.switch.ch/network/tools/tcp_throughput

- If file transfer performance is very low, verify that you are not affected by issues with TCP receive windows scaling on Microsoft Windows. A quick search will offer troubleshooting steps and solutions for this problem.

Best Practice - VPN Performance Testing

https://campus.barracuda.com/product/cloudgenfirewall/doc/73718988/best-practice-vpn-performance-testing/



BarracudaCampus
Search in Barracuda CloudGen Firewall
Barracuda CloudGen Firewall
Overview
Documentation
Training
Certification
VERSION 7.2
VERSION 8.0
VERSION 7.1
PRODUCT INFORMATION
WEB USER INTERFACE
AR
Overview > Best Practice
Best Practice - Hostname List for Barracuda Online Services
Best Practice - Core System Configuration Files and Ports Overview
Best Practice - How to Handle Incorrect Time Settings
Best Practice - Changing the VIP

Best Practice - VPN Performance Testing

Last updated on Mar 12, 2019

The following VPN performance test method provides a guideline for creating a standardized VPN performance testing environment required by Barracuda Technical Support that allows to identify potential configuration improvements. Please note that the VPN throughput results can differ from the values published on the datasheet of CloudGen Firewall F models due to varying test methods and equipment used.

SD-WAN & VRF

VRF - Virtual Routing and Forwarding

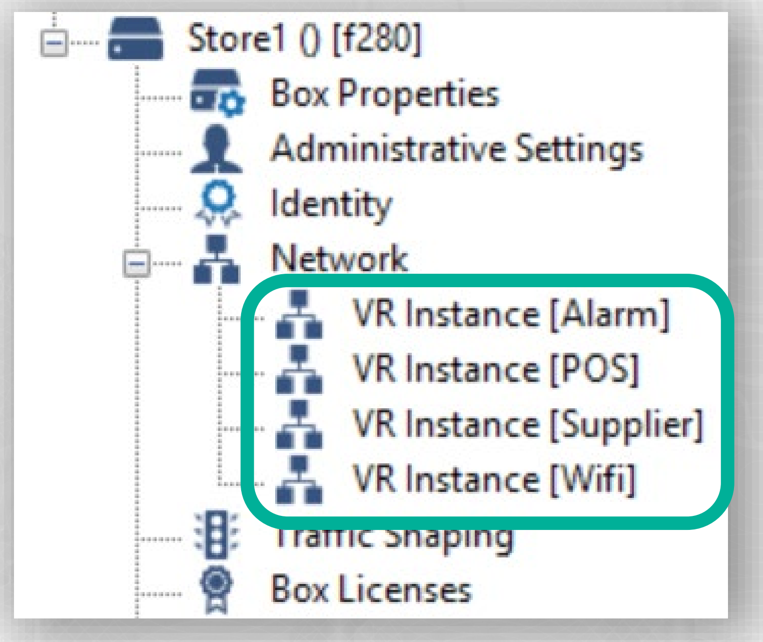
Very common in retail, where traditionally MPLS

- Digital transformation of the store
- Store in store concepts
- External suppliers
- Network overlaps

SD-WAN & VRF

Example Configuration

- Retailer with multiple VR Instances



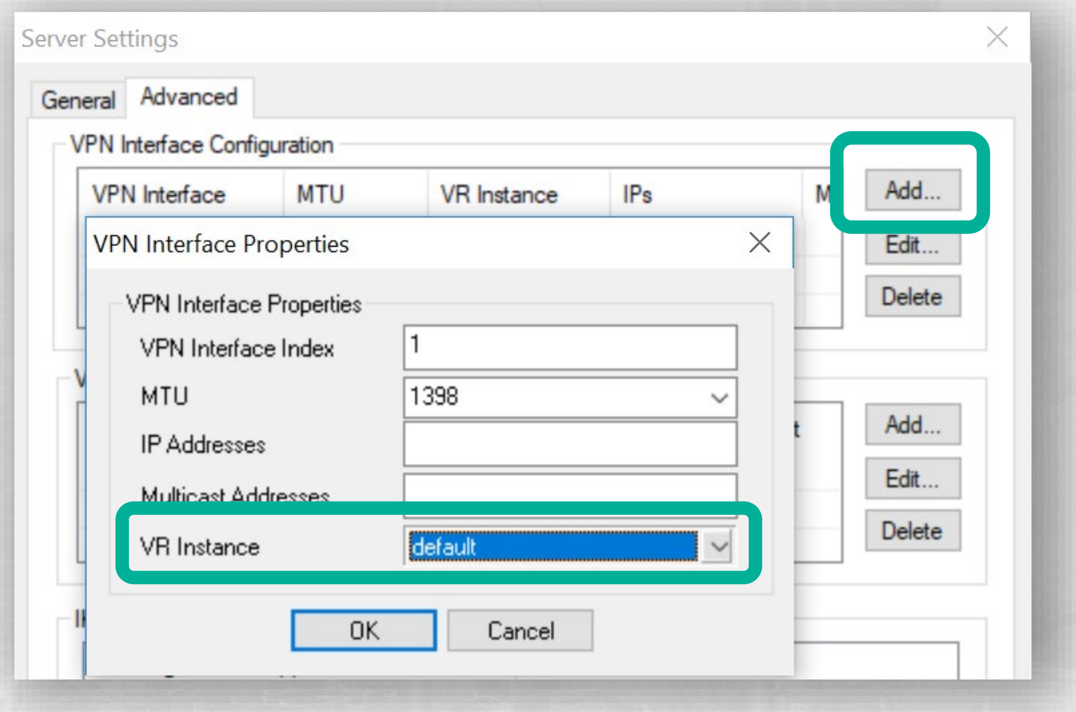
Store1 () [f280]

- Box Properties
- Administrative Settings
- Identity
- Network
  - VR Instance [Alarm]
  - VR Instance [POS]
  - VR Instance [Supplier]
  - VR Instance [Wifi]
- Traffic Shaping
- Box Licenses

SD-WAN & VRF

VPN Settings – Server Settings

- Advanced
  - VR Instance



VPN Interface Properties

VPN Interface Properties

VPN Interface Index: 1

MTU: 1398

IP Addresses:

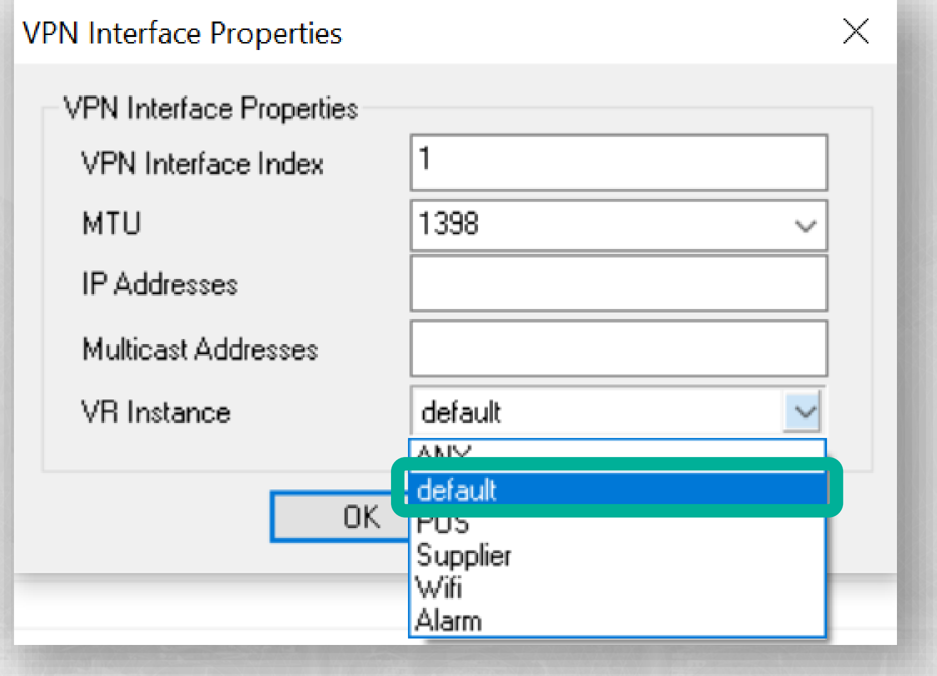
Multicast Addresses:

VR Instance: default

SD-WAN & VRF

VPN Interface Properties

- default
- single additional VRF
- ANY



VPN Interface Properties

VPN Interface Properties

VPN Interface Index: 1

MTU: 1398

IP Addresses:

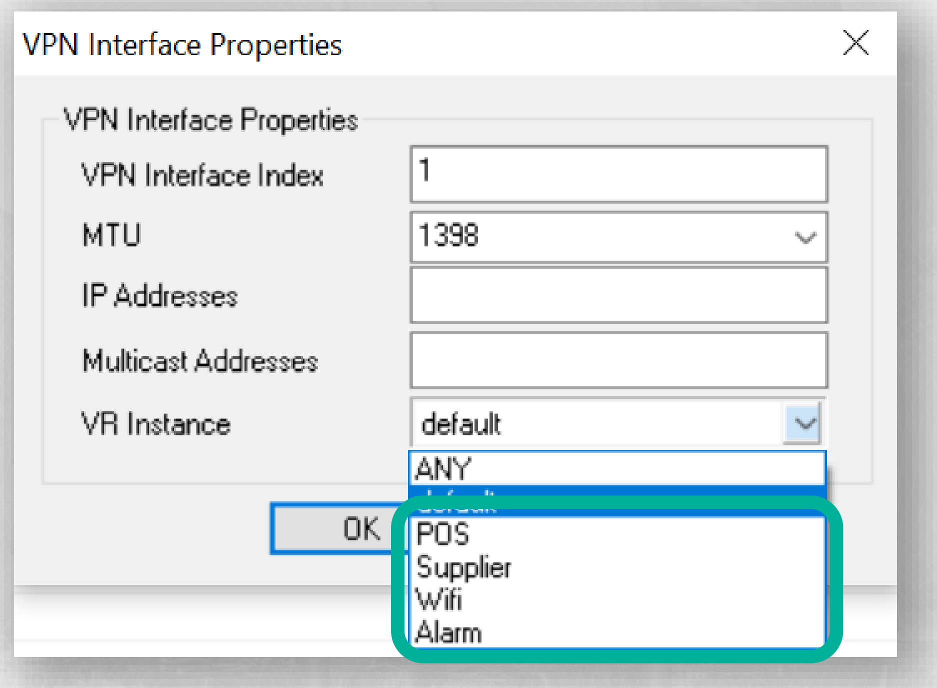
Multicast Addresses:

VR Instance: default

SD-WAN & VRF

VPN Interface Properties

- default
- single additional VRF
- ANY



VPN Interface Properties

VPN Interface Properties

VPN Interface Index: 1

MTU: 1398

IP Addresses:

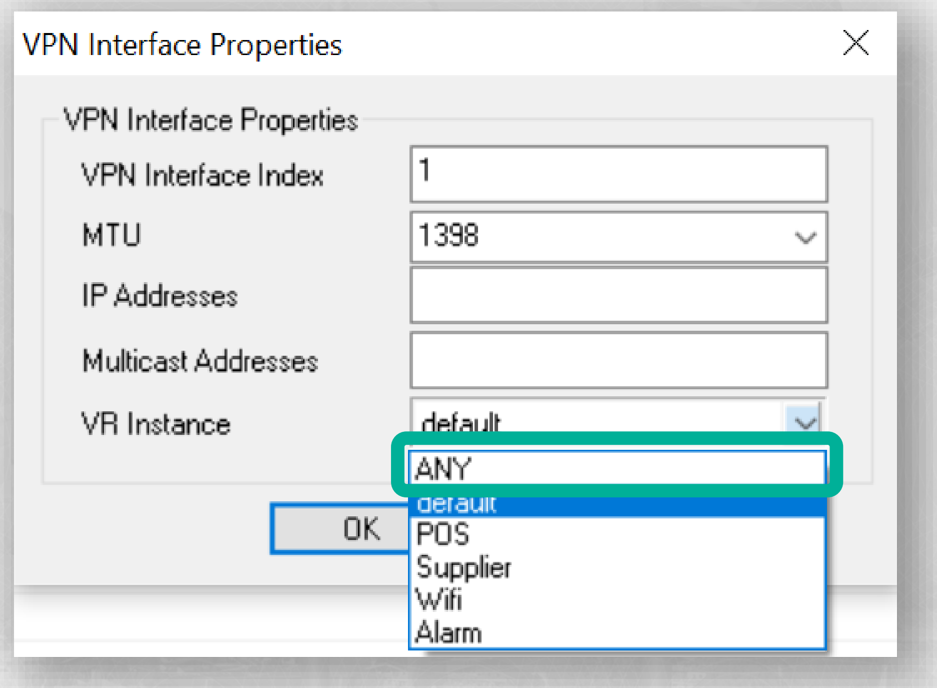
Multicast Addresses:

VR Instance: default

SD-WAN & VRF

VPN Interface Properties

- default
- single additional VRF
- ANY



VPN Interface Properties

VPN Interface Properties

VPN Interface Index: 1

MTU: 1398

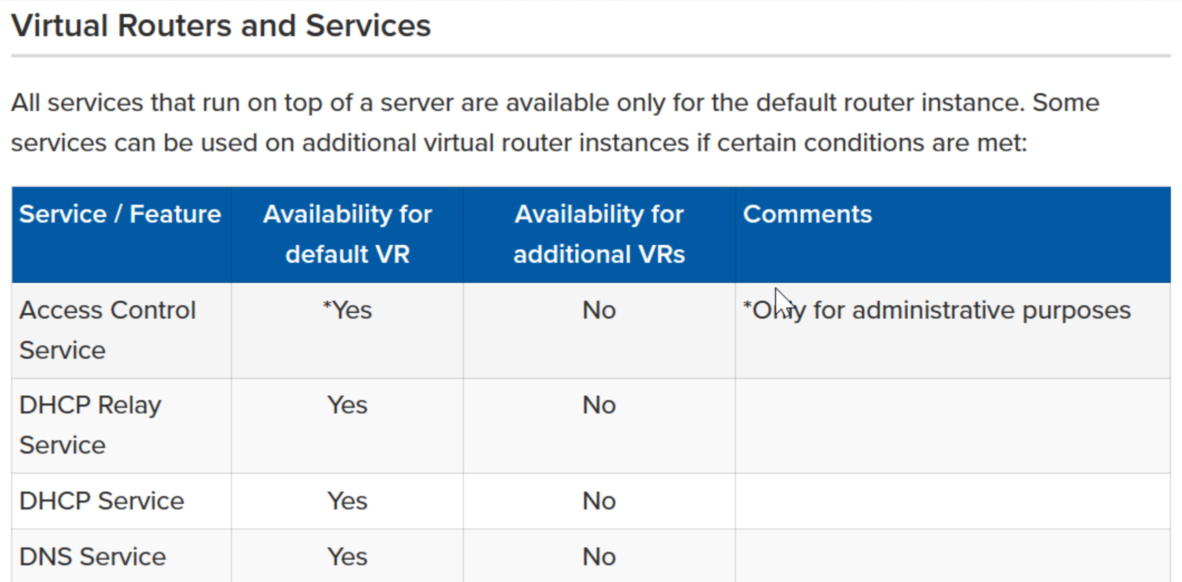
IP Addresses:

Multicast Addresses:

VR Instance: default

VRF limitations

Be aware of the service limitations



Virtual Routers and Services

All services that run on top of a server are available only for the default router instance. Some services can be used on additional virtual router instances if certain conditions are met:

Service / Feature	Availability for default VR	Availability for additional VRs	Comments
Access Control Service	*Yes	No	*Only for administrative purposes
DHCP Relay Service	Yes	No	
DHCP Service	Yes	No	
DNS Service	Yes	No	

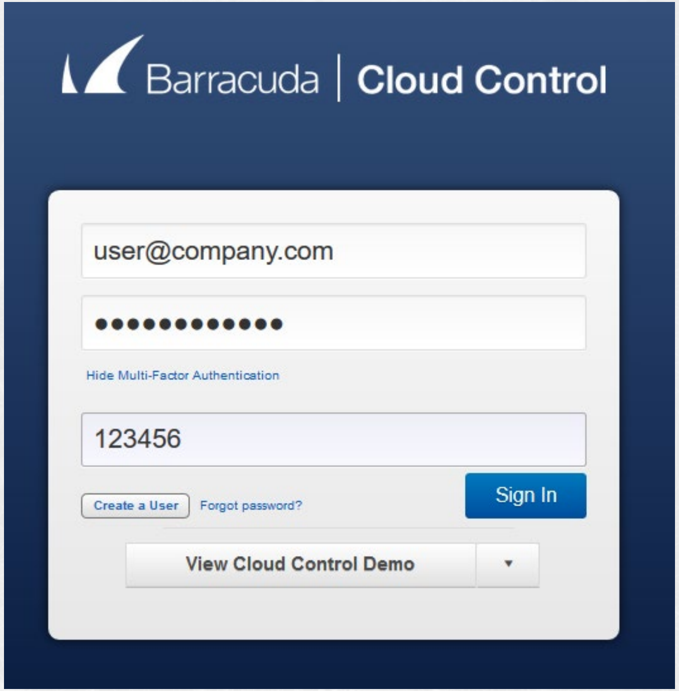
https://campus.barracuda.com/product/cloudgenfirewall/doc/74549106/virtual-routing-and-forwarding-vrf/

Zero-touch deployment

ZTD account - Do not use personal account!

Do not use personal accounts because:

- user might change password
- user might change role or leave company
- user might enable multi-factor authentication



Barracuda | Cloud Control

user@company.com

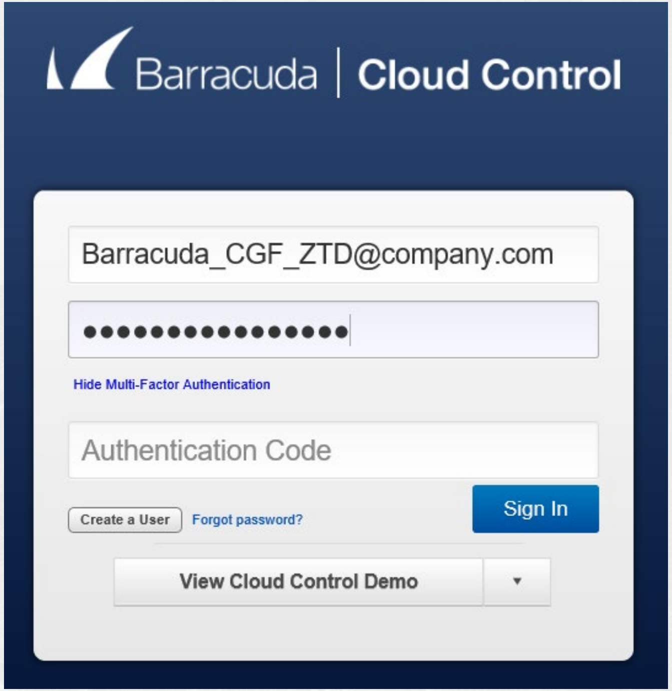
●●●●●●●●●●●●●

Hide Multi-Factor Authentication

123456

ZTD account – Use generic account

- Setup a generic account in your directory / email system
- Do not enable two-factor authentication



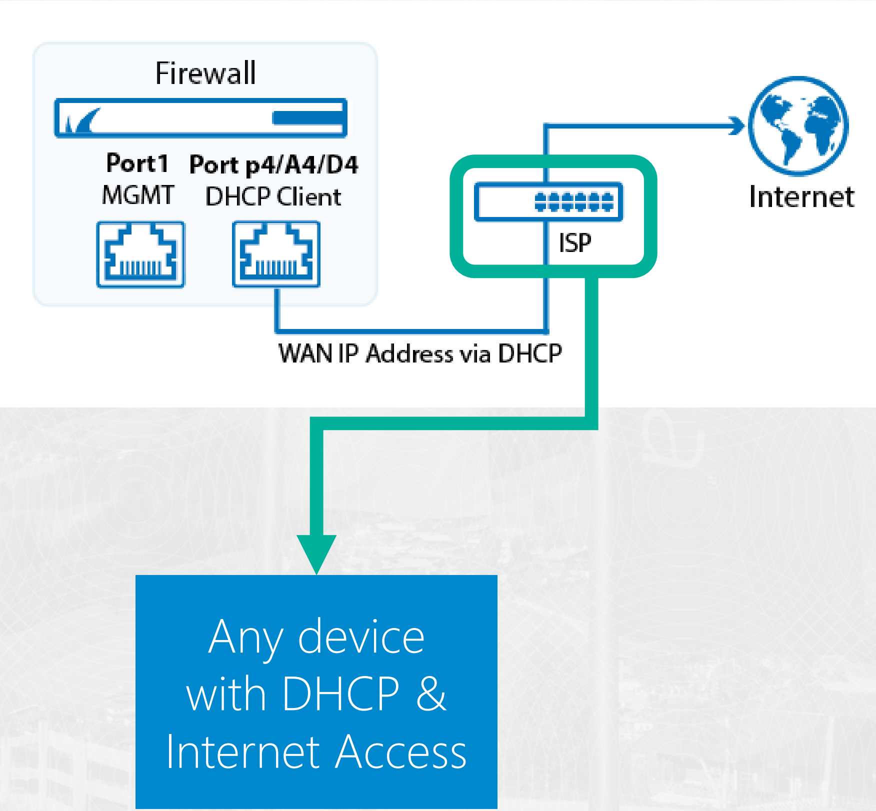
Barracuda_CGF_ZTD@company.com

●●●●●●●●●●●●●●●●

Barracuda | Cloud Control
Hide Multi-Factor Authentication
Authentication Code
Sign In
Create a User
Forgot password?
View Cloud Control Demo ▾

ZTD requirements

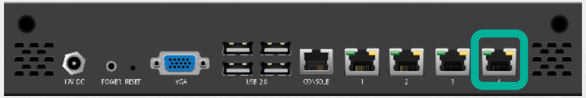
- DHCP lease
- DNS server reachable to resolve ztd.barracudanetworks.com
- Firewall port 443 outgoing open , NTP
- You can temporarily use any device like:
  - LAN port of existing firewall
  - LTE router
  - other router with DHCP enabled

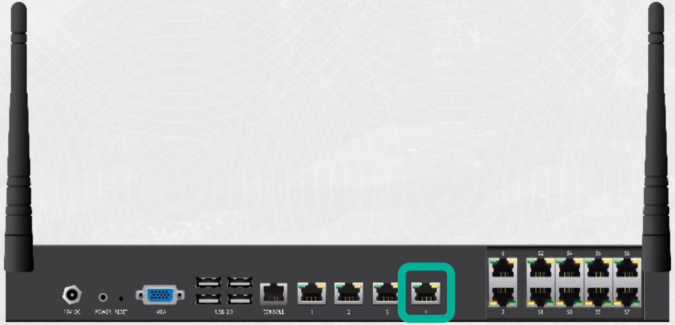


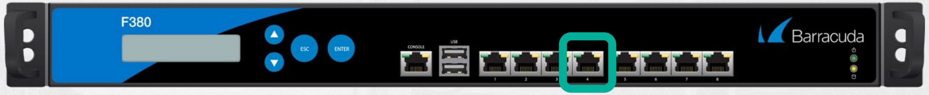
Any device with DHCP & Internet Access

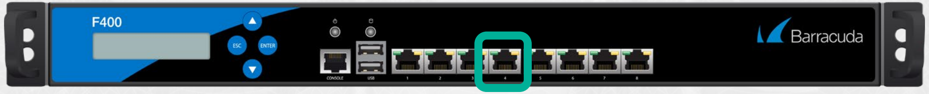
DHCP interface

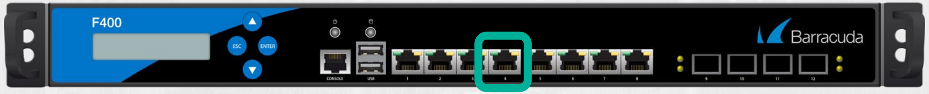
F12 - F800 – DHCP client listens on port p4 – leave it there











What else can be zero-touch?

Boxes get delivered with customer specific configuration

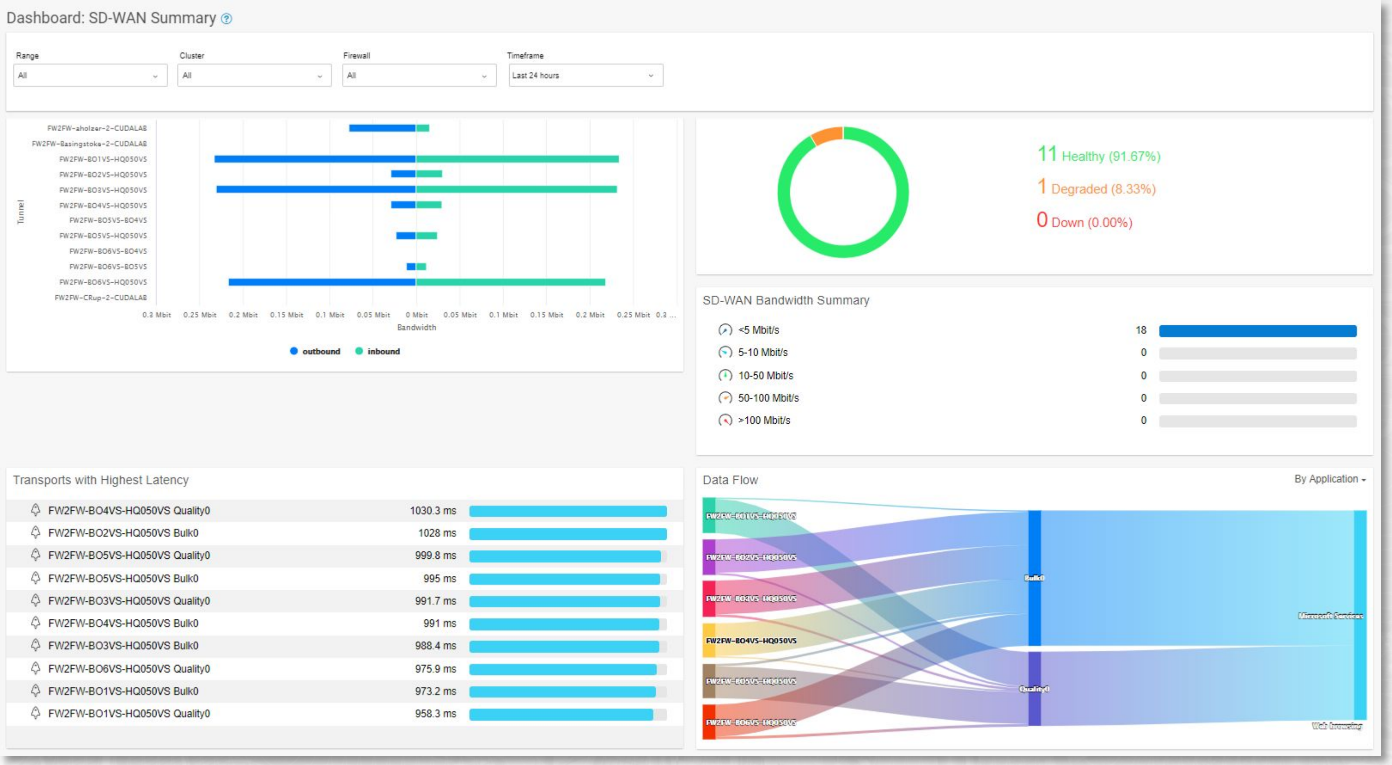
- Only available for large scale projects – talk to Barracuda Sales

USB stick

- From customer perspective the USB stick with image & config is also zero-touch if provider field services fulfils it

Firewall Insights

Firewall Insights



Dashboard: SD-WAN Summary

Range: All

Cluster: All

Firewall: All

Timeframe: Last 24 hours

11 Healthy (91.67%)

1 Degraded (8.33%)

0 Down (0.00%)

SD-WAN Bandwidth Summary

<5 Mbit/s	18
5-10 Mbit/s	0
10-50 Mbit/s	0
50-100 Mbit/s	0
>100 Mbit/s	0

Transports with Highest Latency

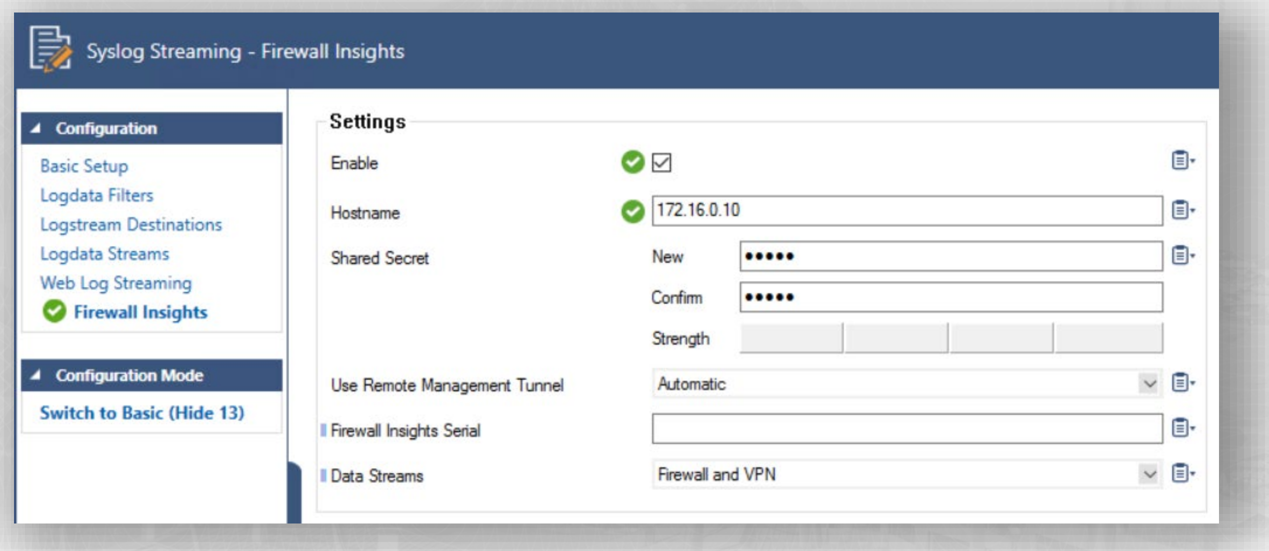
FW2FW-BO4VS-HQ050VS Quality0	1030.3 ms
FW2FW-BO2VS-HQ050VS Bulk0	1028 ms
FW2FW-BO5VS-HQ050VS Quality0	999.8 ms
FW2FW-BO5VS-HQ050VS Bulk0	995 ms
FW2FW-BO3VS-HQ050VS Quality0	991.7 ms
FW2FW-BO4VS-HQ050VS Bulk0	991 ms
FW2FW-BO3VS-HQ050VS Bulk0	988.4 ms
FW2FW-BO6VS-HQ050VS Quality0	975.9 ms
FW2FW-BO1VS-HQ050VS Bulk0	973.2 ms
FW2FW-BO1VS-HQ050VS Quality0	958.3 ms

Data Flow

Firewall Insights

Configure Barracuda Firewall Insights in syslog streaming

Barracuda Firewall Control Center -> use repository links



Syslog Streaming - Firewall Insights

Settings

Enable ✓ ☑

Hostname ✓ 172.16.0.10

Shared Secret New ●●●●● Confirm ●●●●● Strength

Use Remote Management Tunnel: Automatic

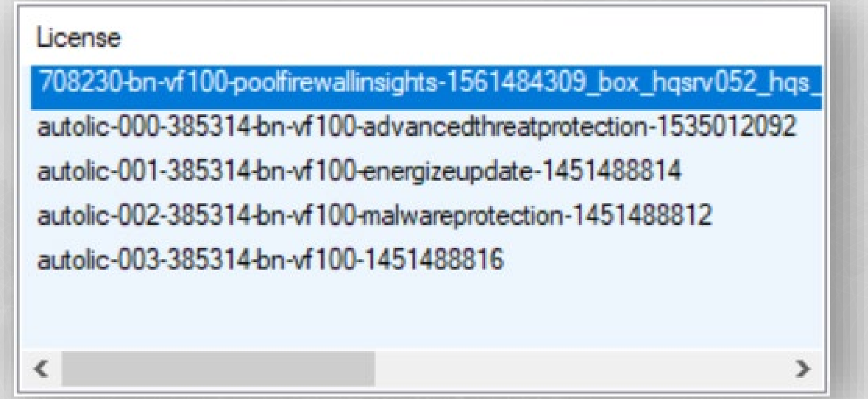
Firewall Insights Serial:

Data Streams: Firewall and VPN

Firewall Insights

For Barracuda Firewall Insights you need:

- A license for Barracuda Firewall Insights Server
- A subscription for Barracuda Firewall Insights on every CloudGen Firewall you want to connect to your Firewall Insights



License

```
708230-bn-vf100-poolfirewallinsights-1561484309_box_hqsrv052_hqs_
autolic-000-385314-bn-vf100-advancedthreatprotection-1535012092
autolic-001-385314-bn-vf100-energizeupdate-1451488814
autolic-002-385314-bn-vf100-malwareprotection-1451488812
autolic-003-385314-bn-vf100-1451488816
```

All license need to be ordered!

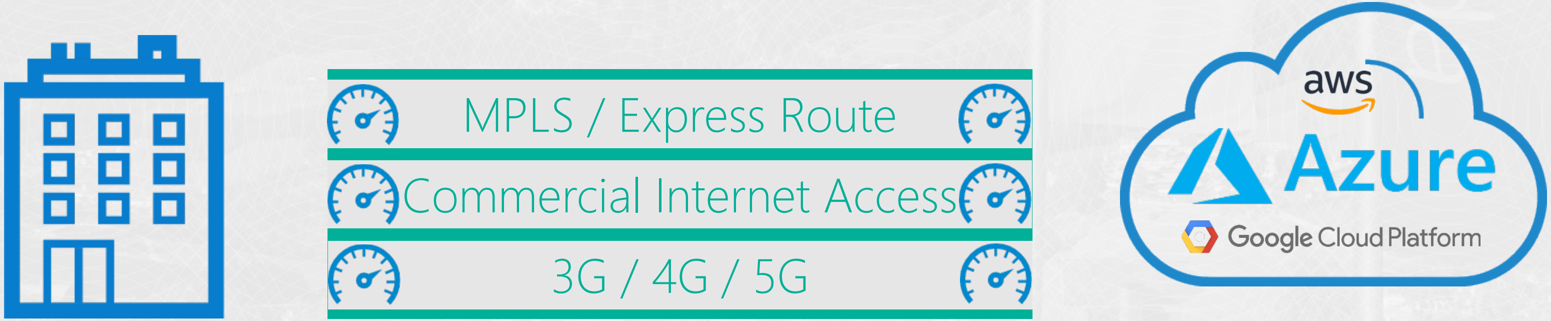
SD-WAN & The Public Cloud

Cloud-generation SD-WAN

Enable multi-cloud-connectivity

SaaS / PaaS / IaaS

BARRACUDA NETWORKS
Barracuda CloudGen Firewall F82 v7.2.3
SOFTWARE-DEFINED WIDE AREA NETWORK
NSS LABS
RECOMMENDED
JUNE
2019

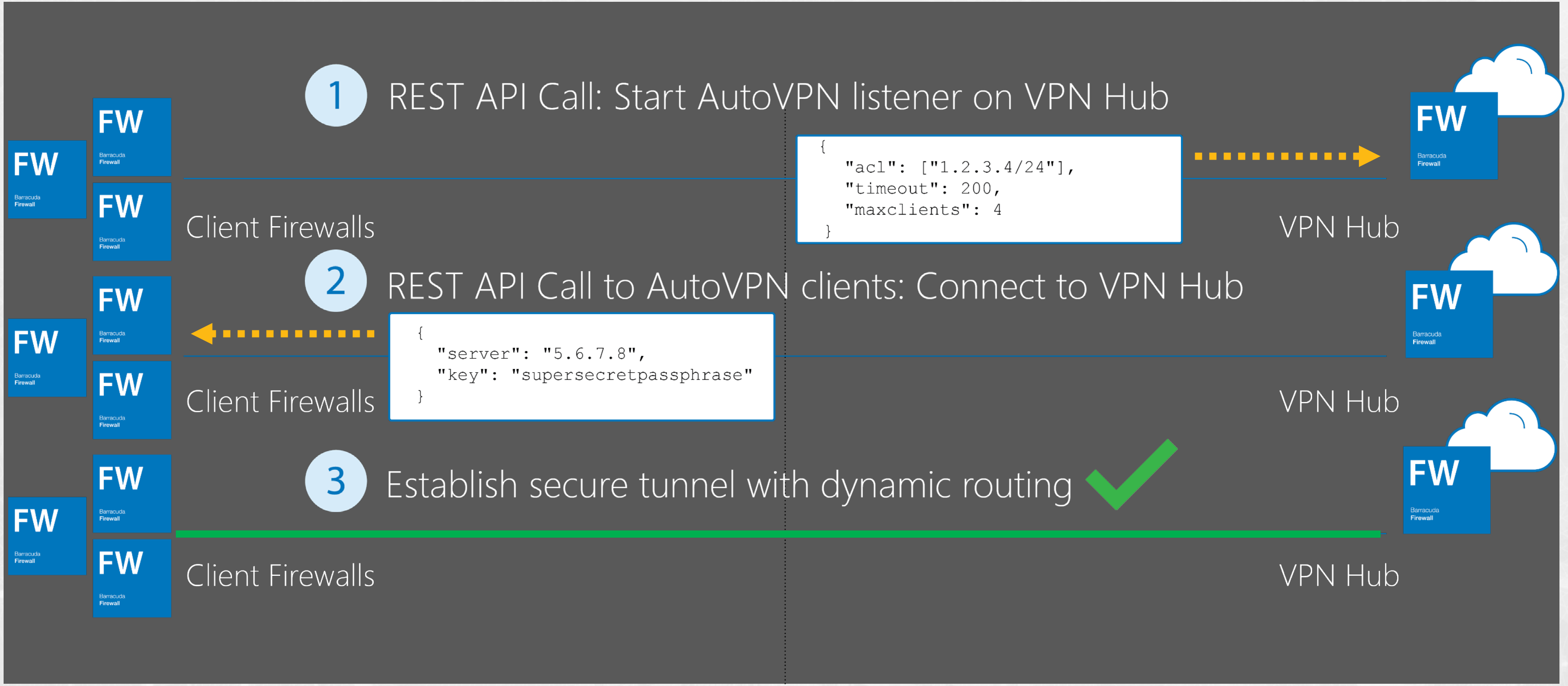


MPLS / Express Route

Commercial Internet Access

3G / 4G / 5G

Creating VPN Tunnels with AutoVPN



1 REST API Call: Start AutoVPN listener on VPN Hub

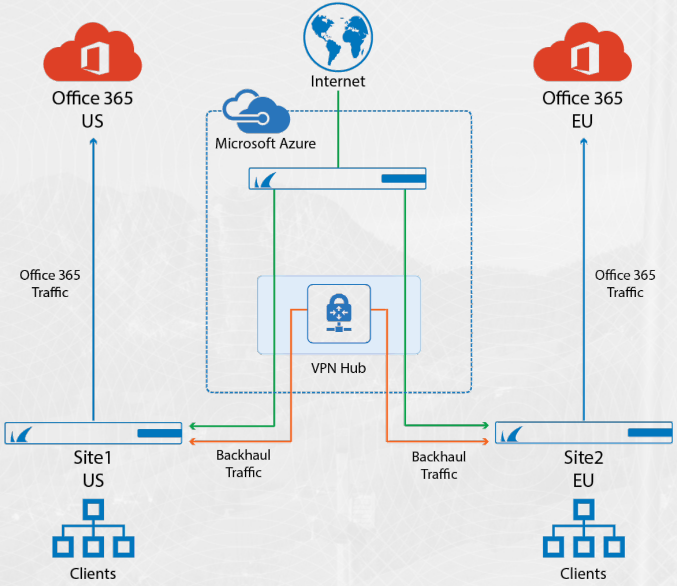
```
{
   "acl": ["1.2.3.4/24"],
   "timeout": 200,
   "maxclients": 4
 }
```

2 REST API Call to AutoVPN clients: Connect to VPN Hub

```
{
  "server": "5.6.7.8",
  "key": "supersecretpassphrase"
}
```

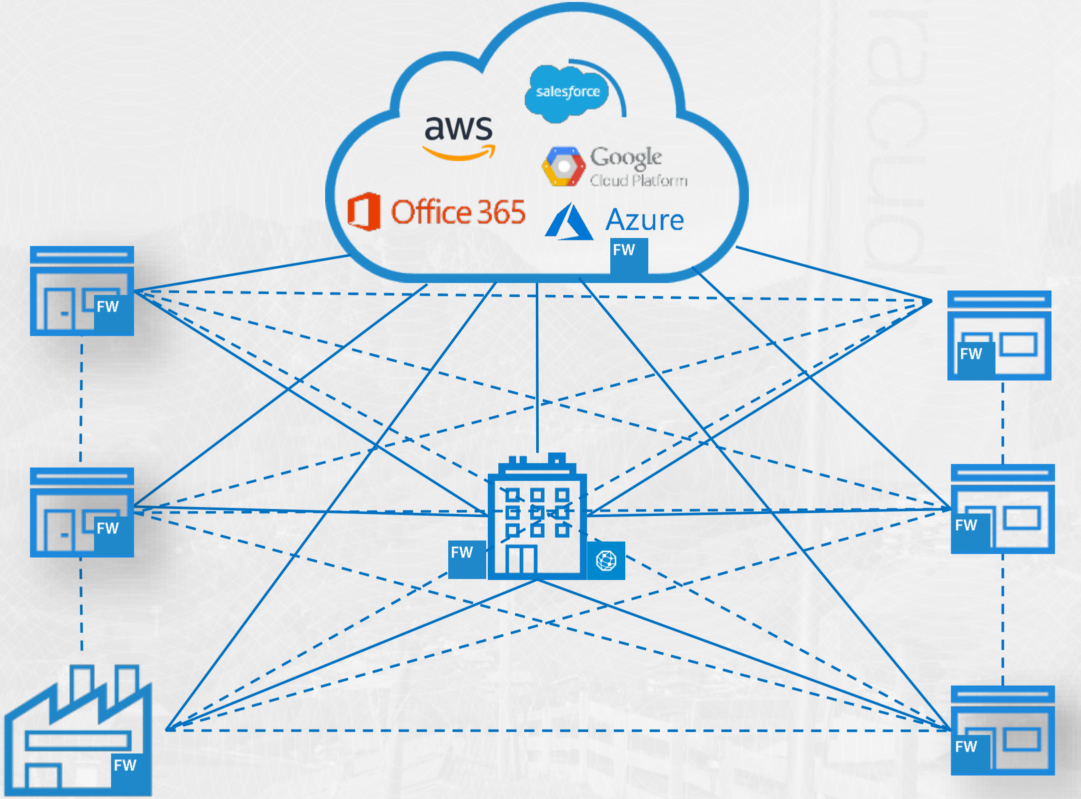
3 Establish secure tunnel with dynamic routing ✓

SD WAN – Microsoft vWAN Integration

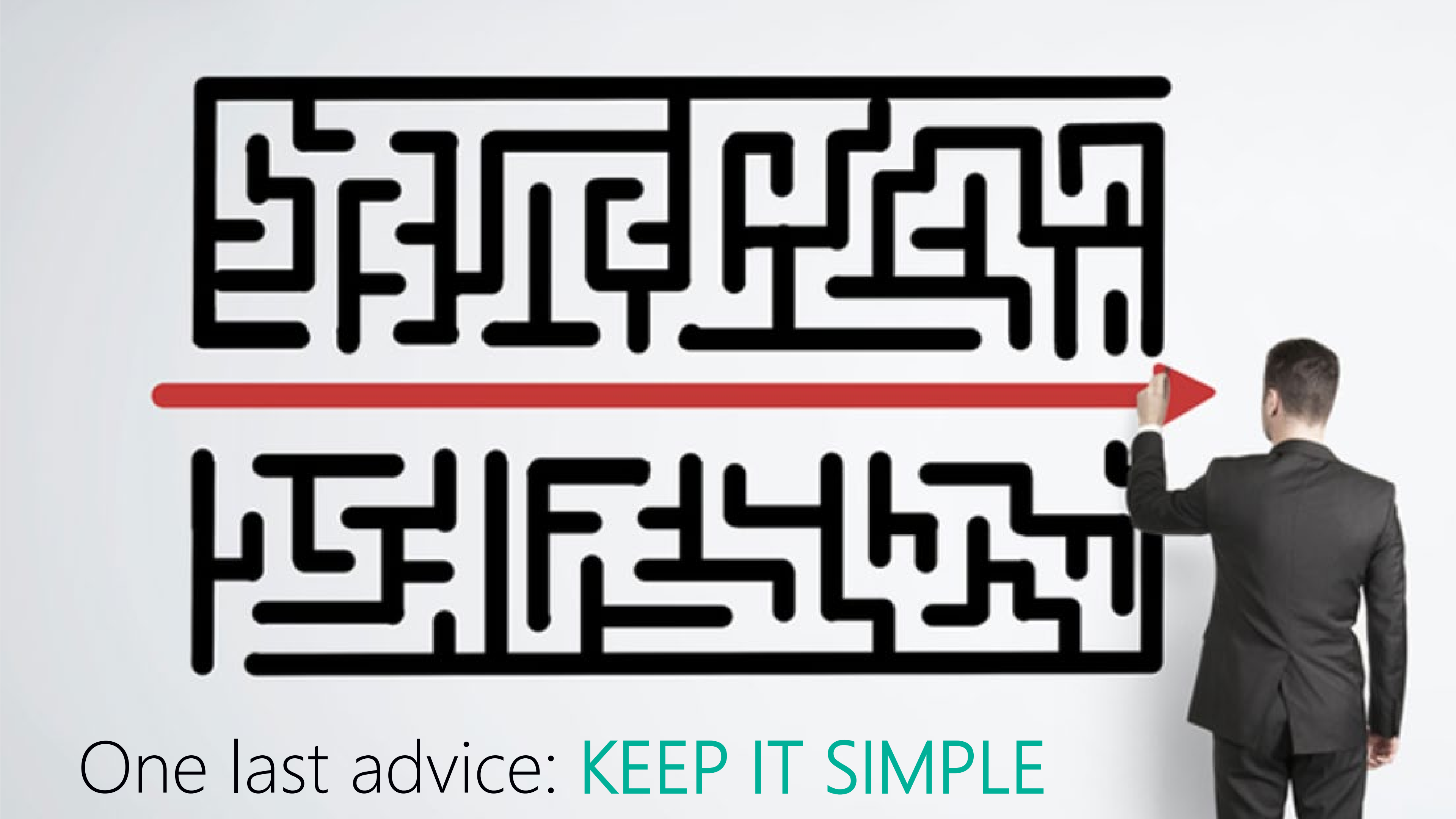


https://campus.barracuda.com/product/cloudgenfirewall/doc/78808340/how-to-configure-automatic-connectivity-to-azure-virtual-wan

SD WAN integrates in your existing network



SD-WAN Wrap Up



One last advice: KEEP IT SIMPLE

Thank you

Barracuda

TECHSUMMIT19

BARRACUDA TECHNICAL SUMMIT