

Elevating the WAN Edge with the Meraki MX

CISCO Live !

Bruce Newton
Solutions Engineer – Networking

Session ID: BRKENT-2567

Cisco Webex App

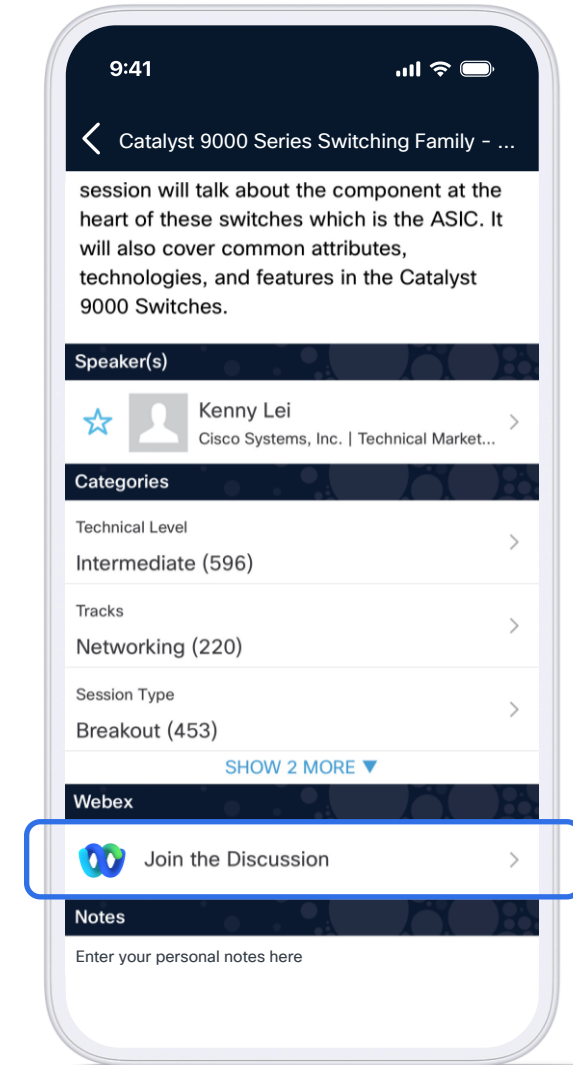
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until 14 November 2025.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENT-2567>

Who am I?



Radio Broadcast Engineer



Systems Administrator

Network Administrator

Solution Architect



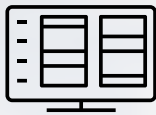
Solutions Engineer



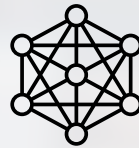
Trail Runner



The MX can't do that, right?



Simplicity

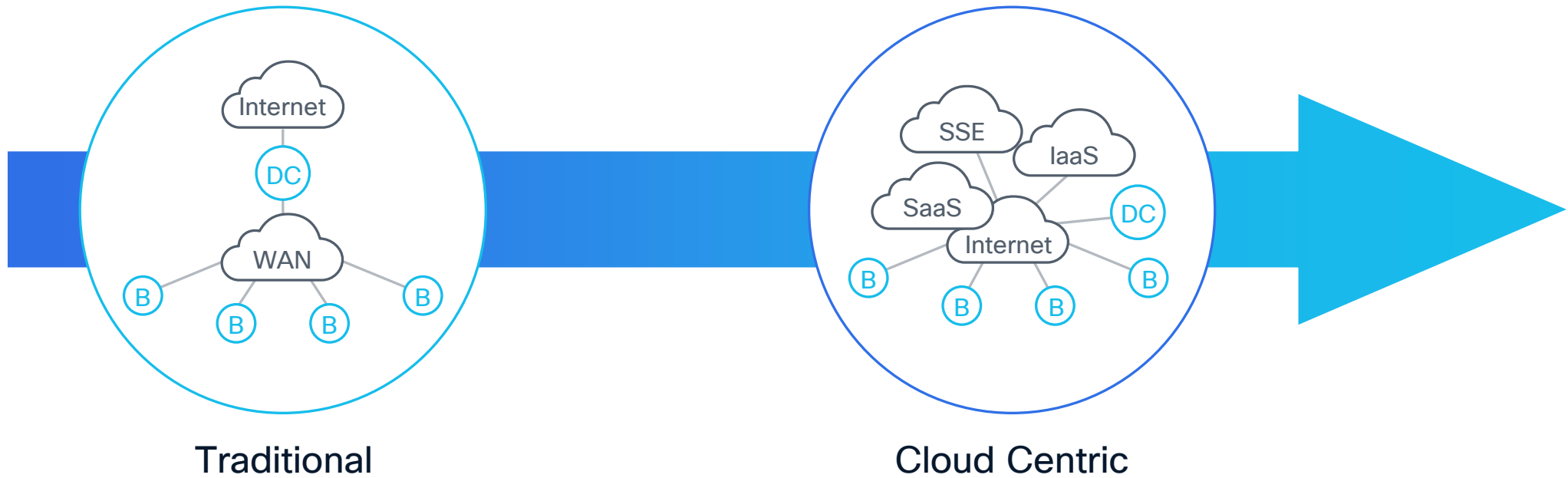


Connectivity



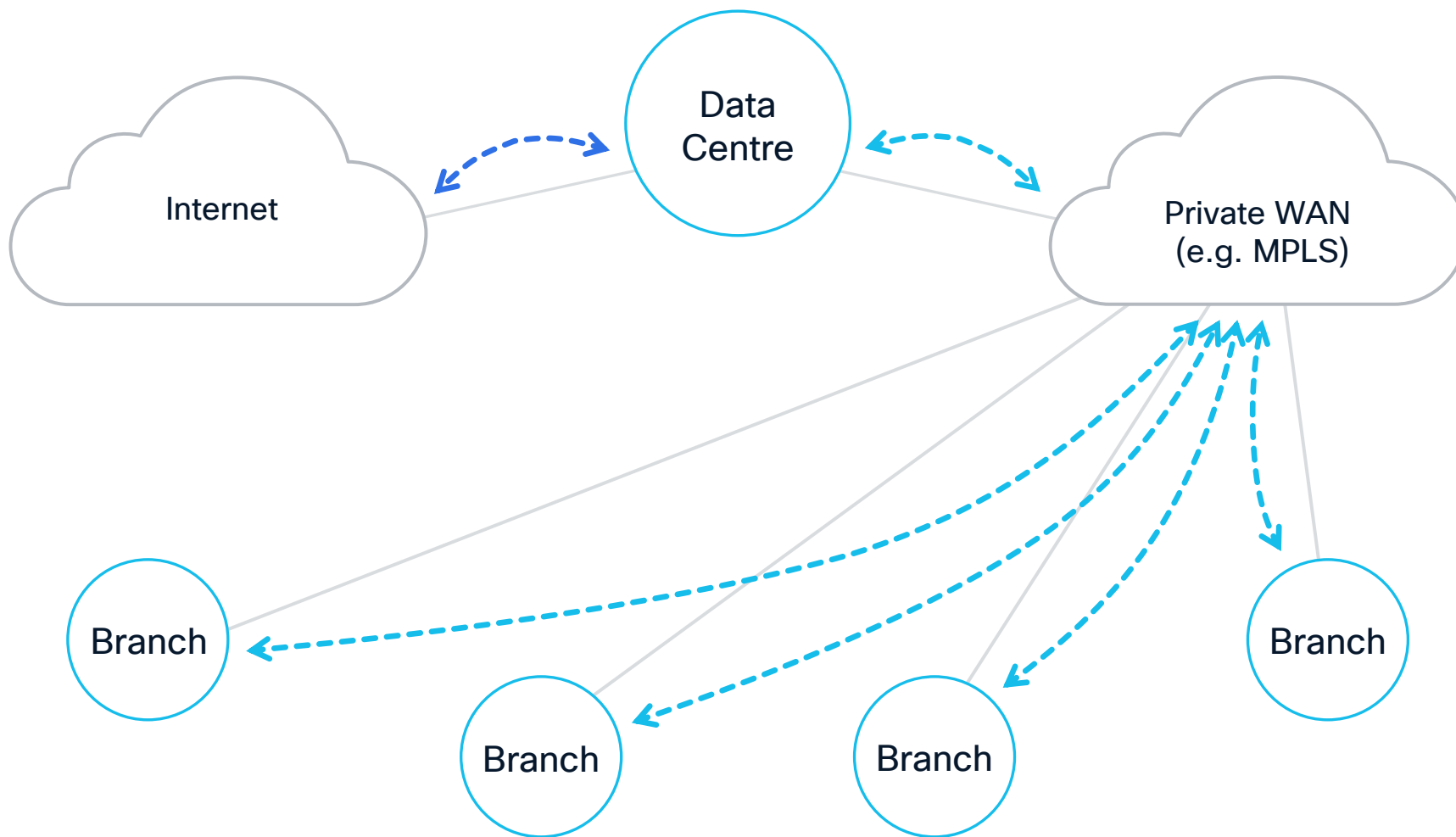
Security

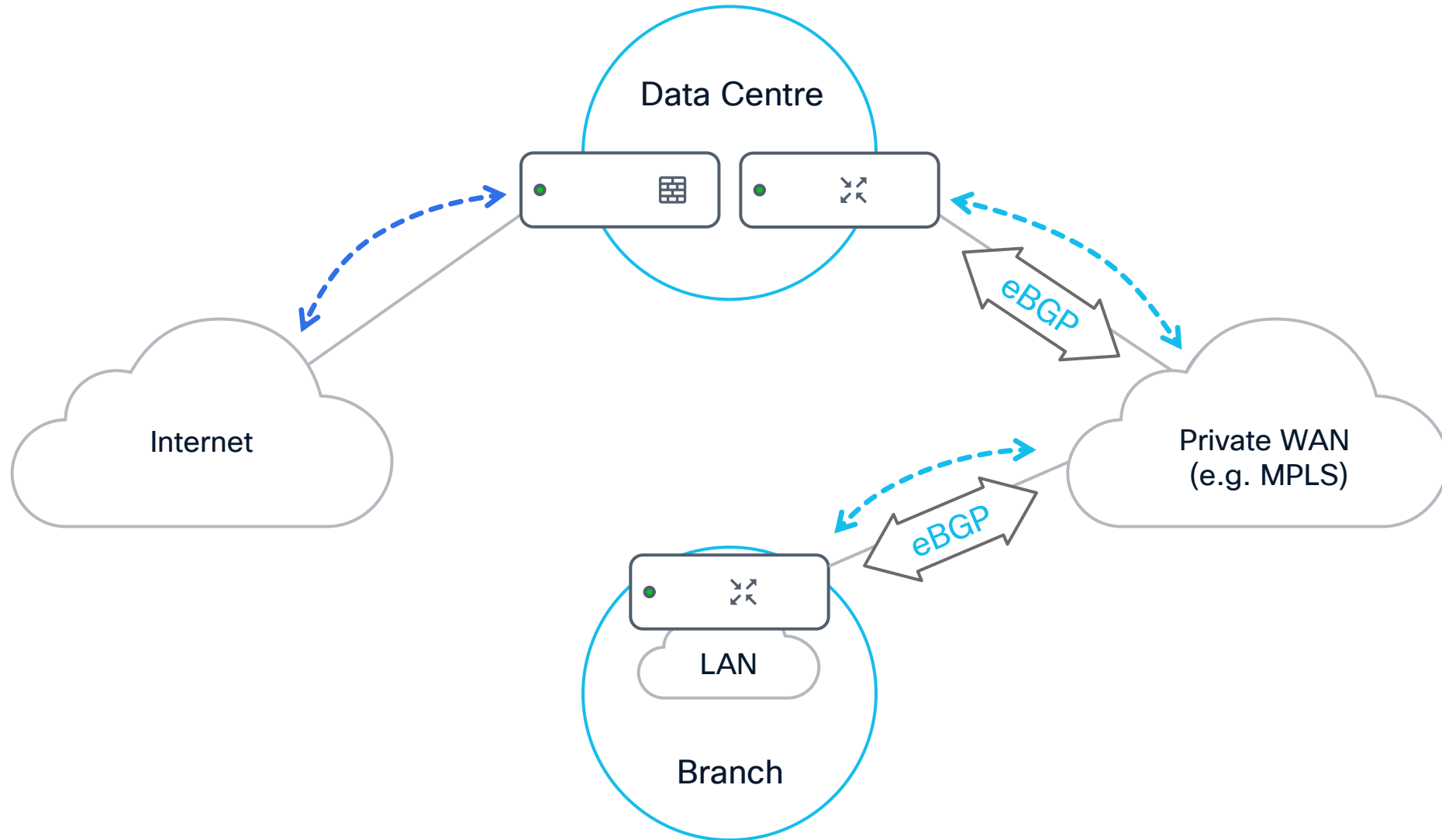
Our journey today



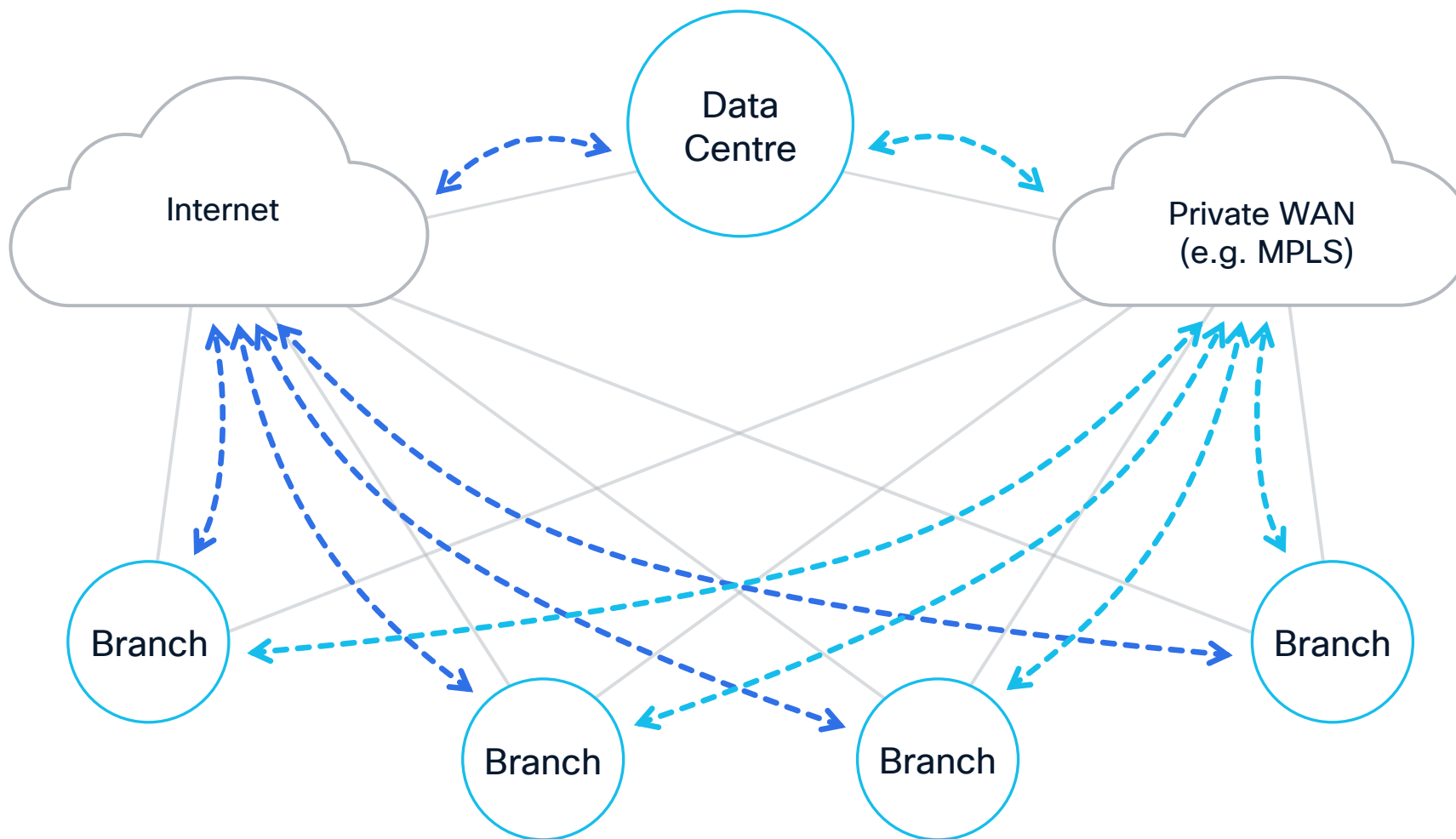
The background of the slide is an abstract design featuring flowing, wavy lines in various shades of blue and white. A large, white rectangular box is positioned on the left side of the slide, serving as a container for the main text.

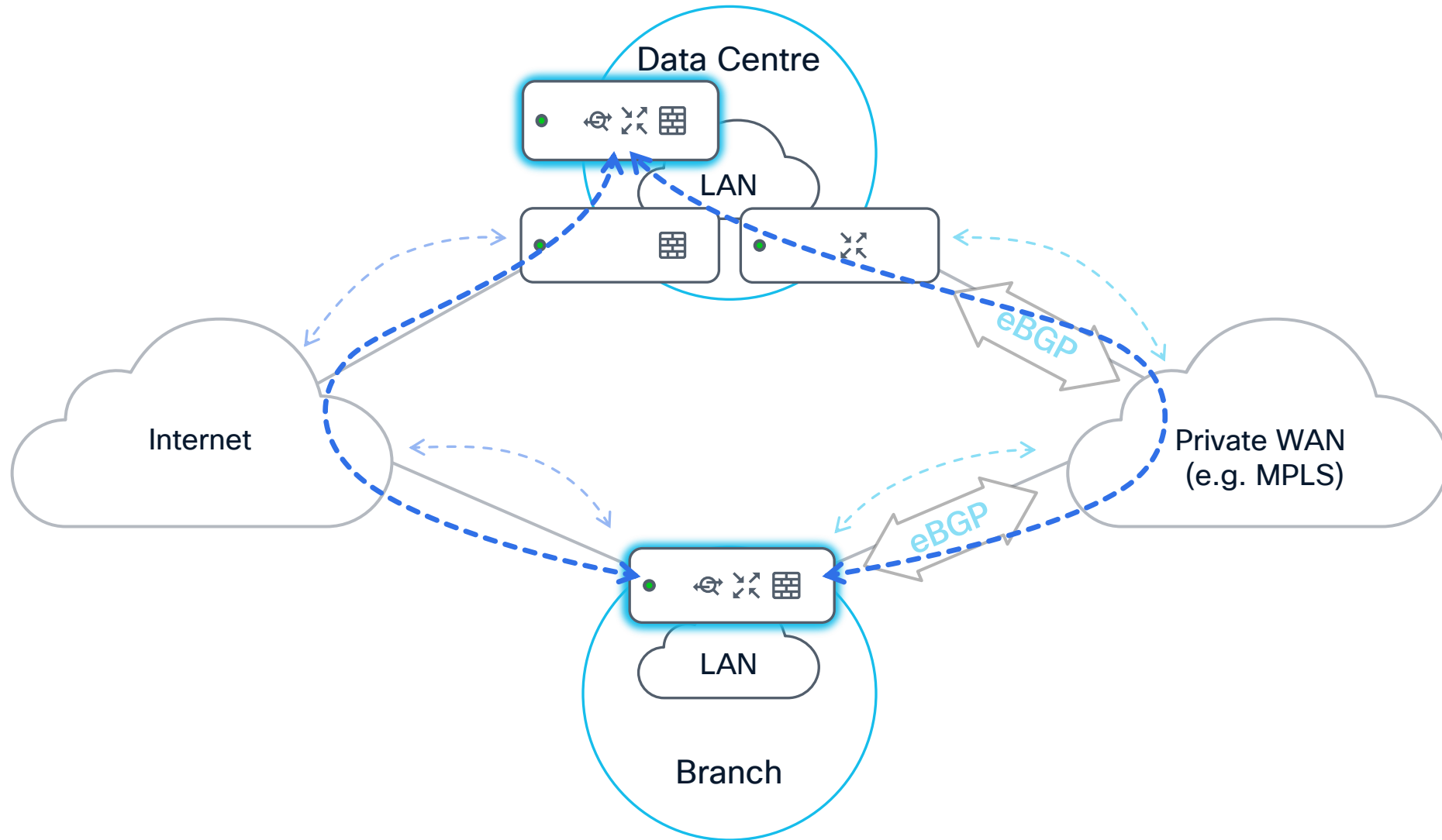
In the beginning





Securing the WAN



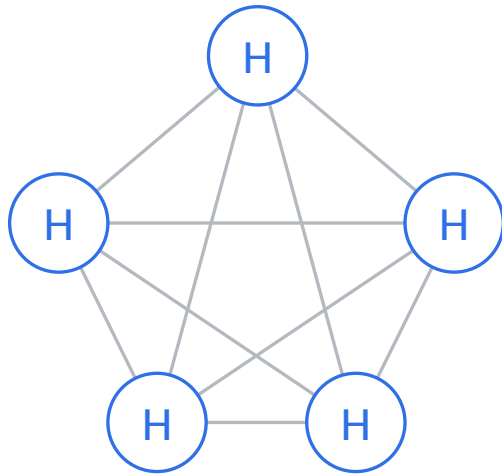


Design Considerations

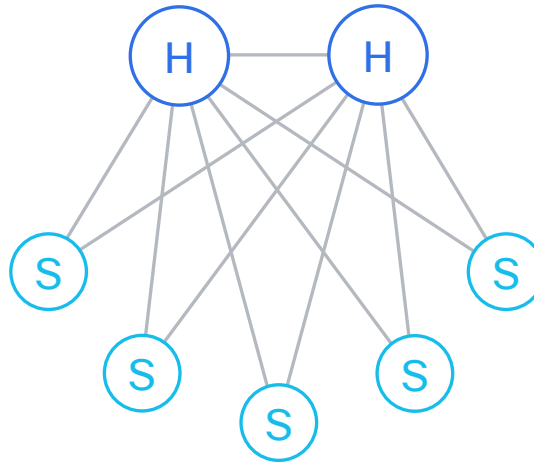
Design Considerations

SD-WAN Topology

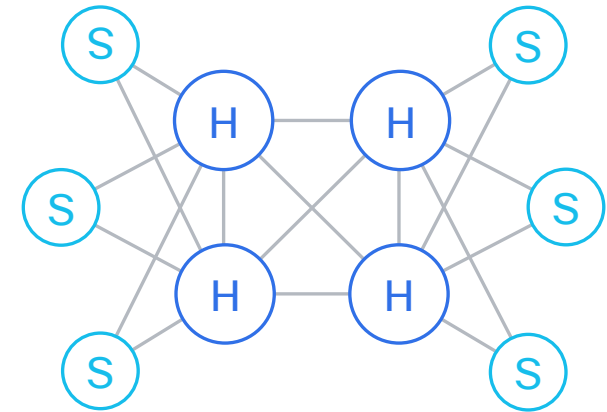
Full Mesh



Hub and Spoke



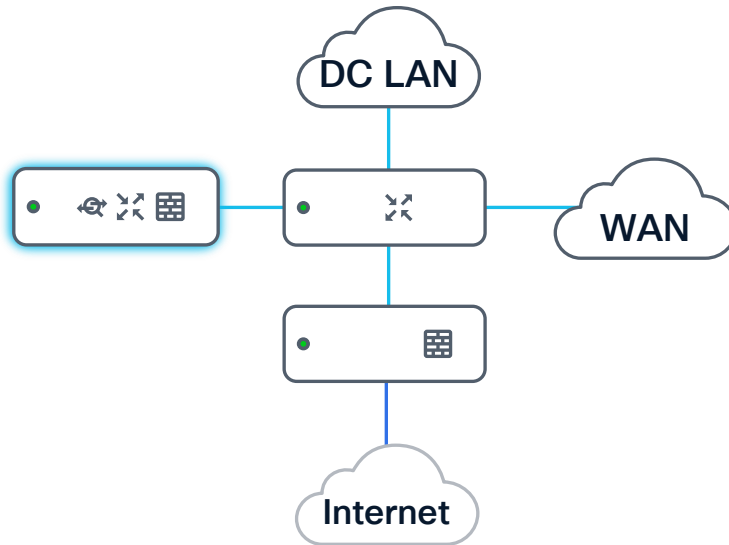
Hybrid



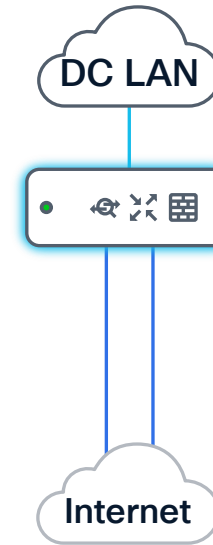
Design Considerations

Head-end Design

One-Arm Concentrator



NAT/Routed Mode



Design Considerations

MX Appliance Sizing

	MX67	MX68	MX75	MX85	MX95	MX105	MX250	MX450
Firewall Throughput	700 Mbps	700 Mbps	1 Gbps	1 Gbps	3 Gbps	5 Gbps	7.5 Gbps	10 Gbps
RFC2544 - 1518 Byte								
Firewall Throughput	700 Mbps	700 Mbps	1 Gbps	1 Gbps	3 Gbps	5 Gbps	7 Gbps	10 Gbps
EMIX								

	MX67	MX68	MX75	MX85	MX95	MX105	MX250	MX450
Maximum Site to Site VPN Tunnel Count	50	50	75	200	500	1,000	3,000	5,000
Recommended Maximum Site to Site VPN Tunnel	50	50	75	100	250	500	1,000	1,500

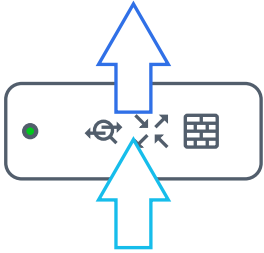
	MX67	MX68	MX75	MX85	MX95	MX105	MX250	MX450
Maximum Concurrent Sessions	25,000	25,000	50,000	125,000	200,000	250,000	500,000	1,000,000

Traffic Forwarding

Traffic Forwarding

Network Address Translation

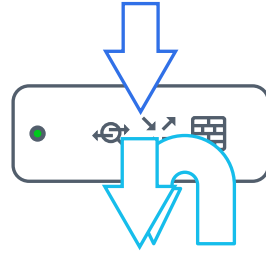
Default



Outbound traffic NAT to
WAN IP address

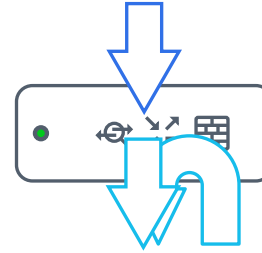
NAT can be disabled

Port Forward



Inbound WAN port
forwarded to inside IP
address and port

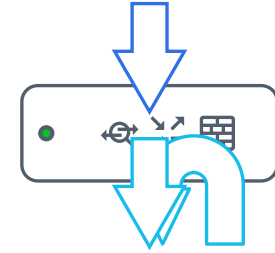
1:1 NAT



Inbound IP address
NATed to inside IP
address

Ensure outbound traffic is
routed out same WAN
interface

1:Many NAT



Inbound IP address and
port NATed to inside IP
address and port

Outbound traffic
sourced from MX WAN
IP address

Hairpin routing on all 'inbound' port forwards/NAT with source re-write

Traffic Forwarding

Traffic Shaping/Policing

Link Shaping

SD-WAN & traffic shaping

Uplink configuration

WAN 1	100 Mbps	details
WAN 2	100 Mbps	details
Cellular	50 Mbps	details

Controls inbound and
outbound traffic on WAN
Ratio used for load-balancing
of traffic across interfaces

Per Client Shaping

Global bandwidth limits

Per-client limit [details](#) ☐ Enable SpeedBurst

Applied to all clients, for all
routed traffic

Class Shaping

Traffic shaping rules

Default Rules

Rule #1

Definition
This rule will be enforced on
traffic matching any of these
expressions.

[Add +](#)

Bandwidth limit
5 Mbps [details](#)

Priority

DSCP tagging

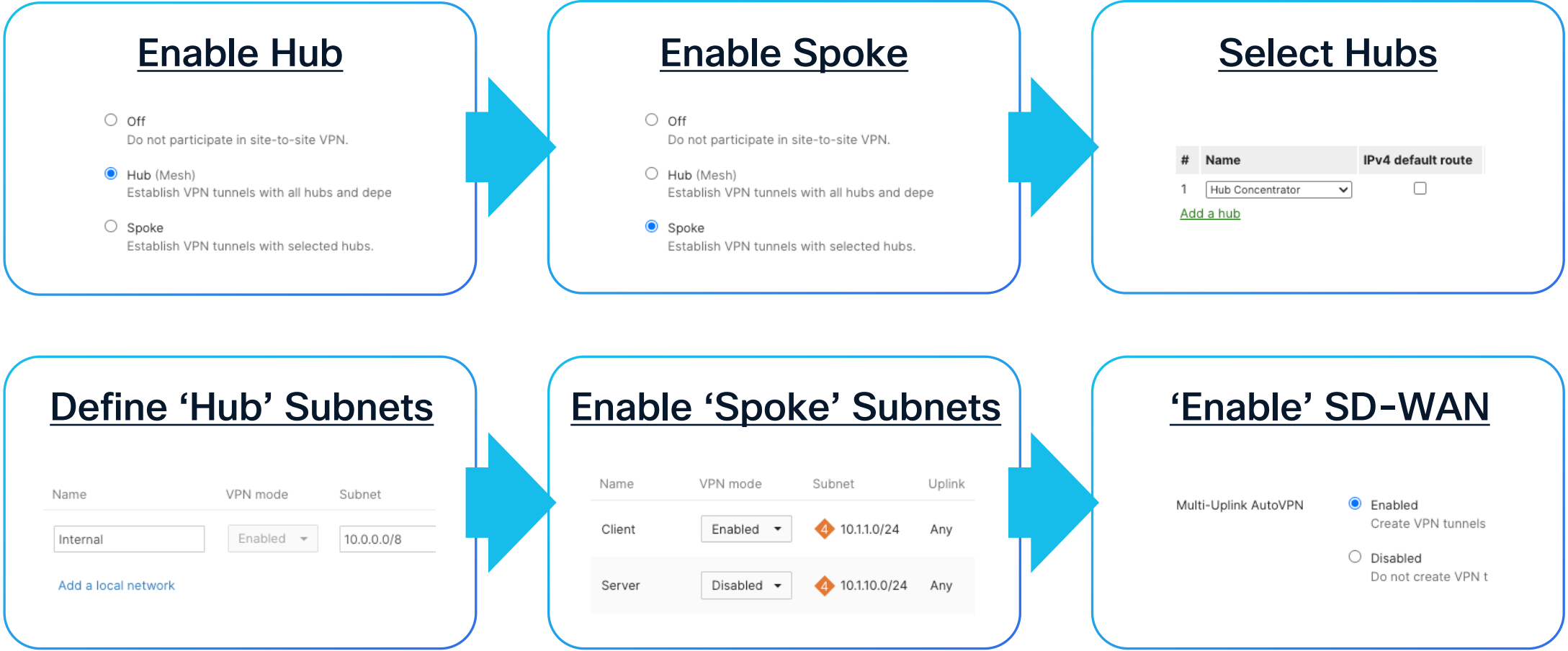
[Add a new shaping rule](#)

Eight user definable classes
Four CBWFQ queues
Applied to all routed traffic

Can be overridden by Group Policy on client or VLAN

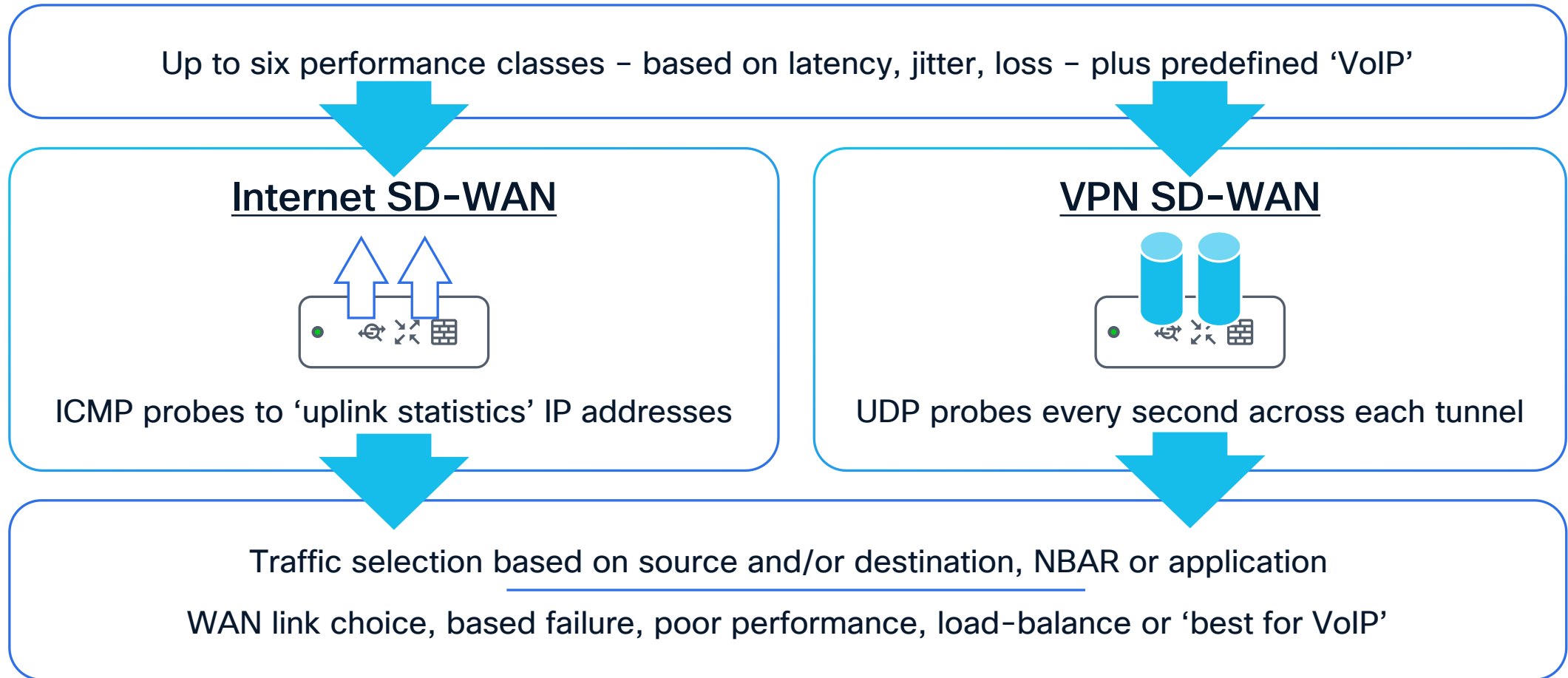
Traffic Forwarding

‘Three-click’ SD-WAN



Traffic Forwarding

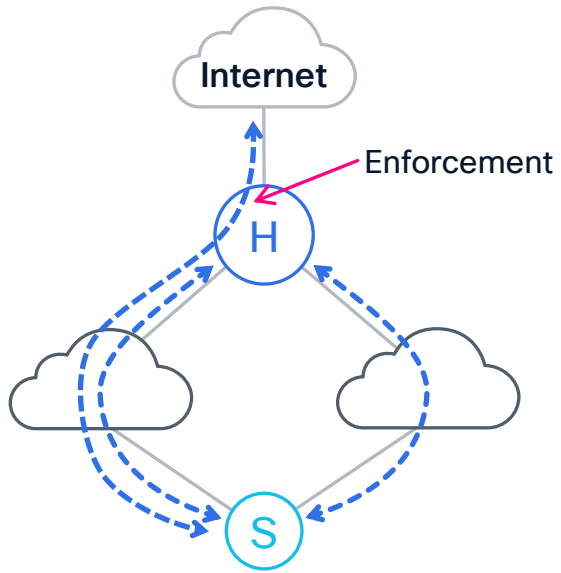
SD-WAN Path Selection



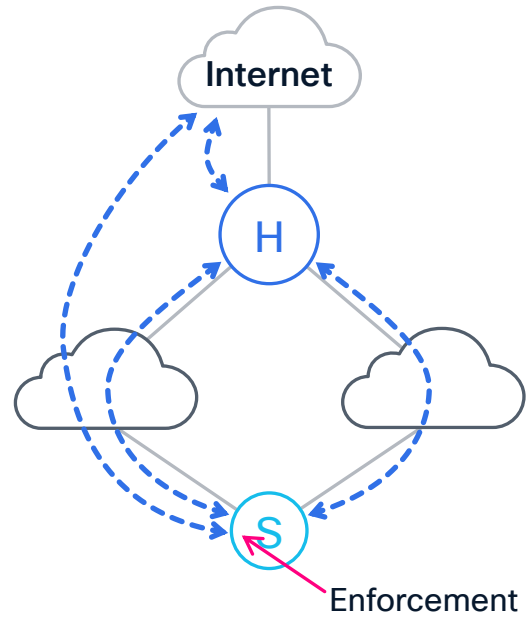
Securing the Edge

Securing the Edge

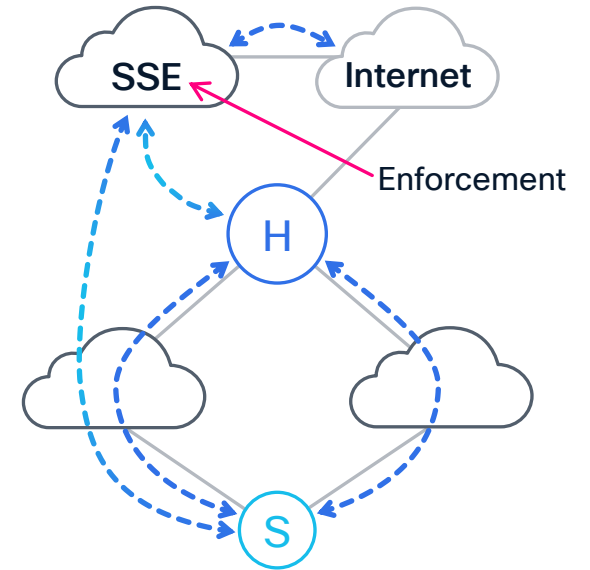
Data Centre



Local Breakout

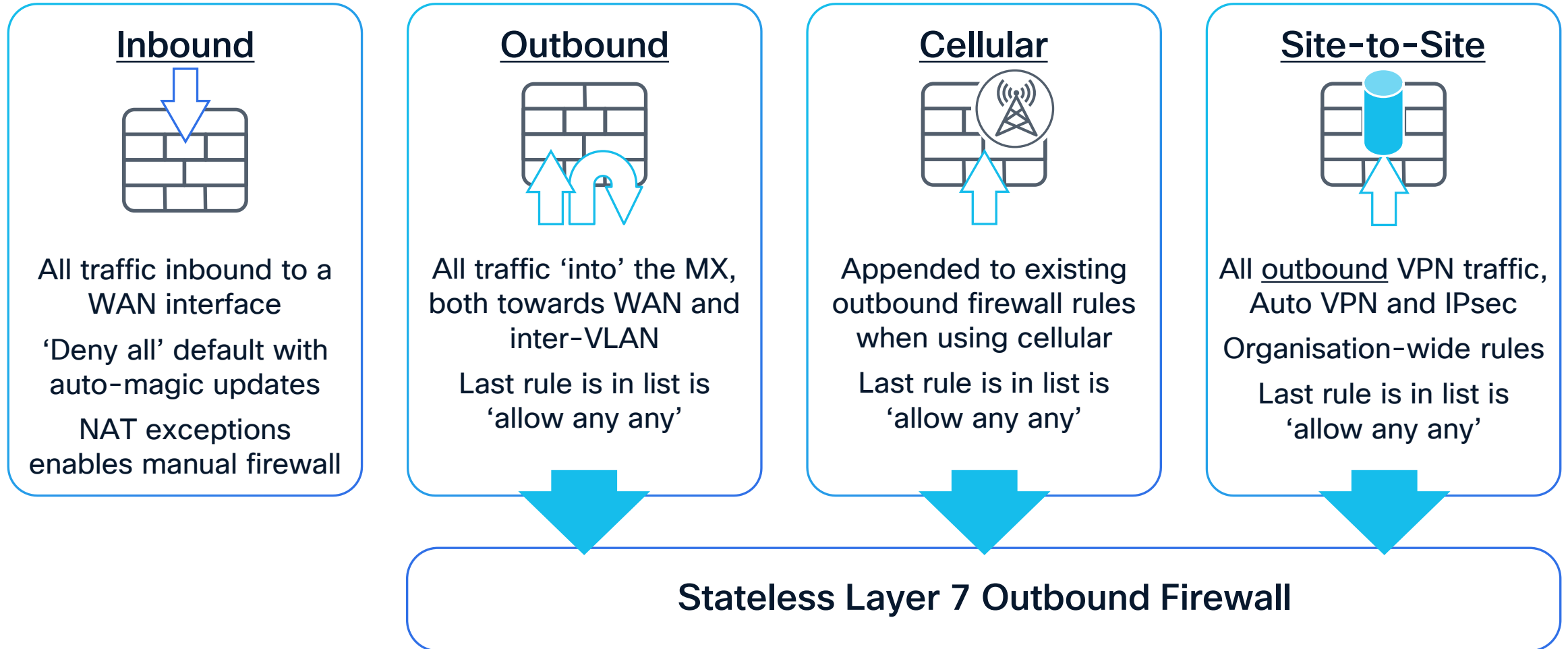


Security Service Edge



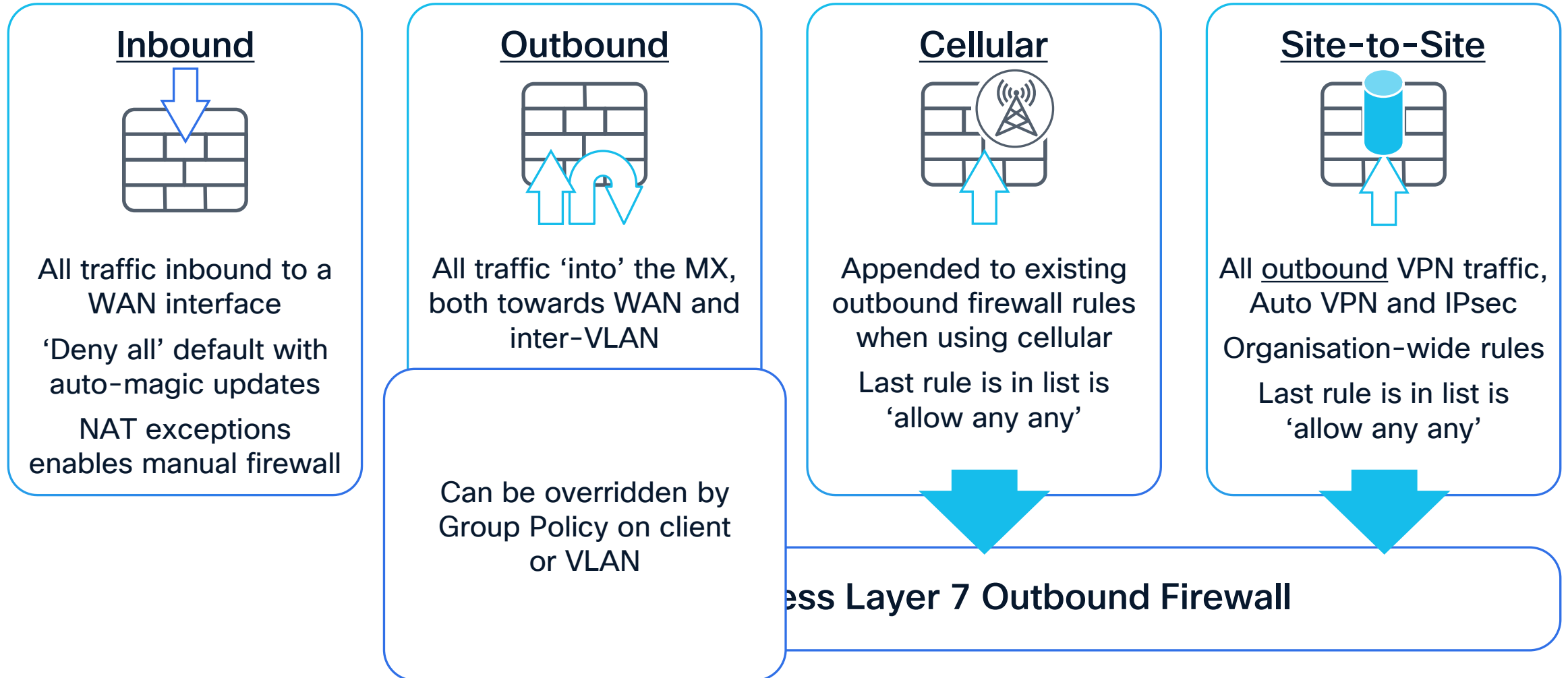
Securing the Edge

Firewall



Securing the Edge

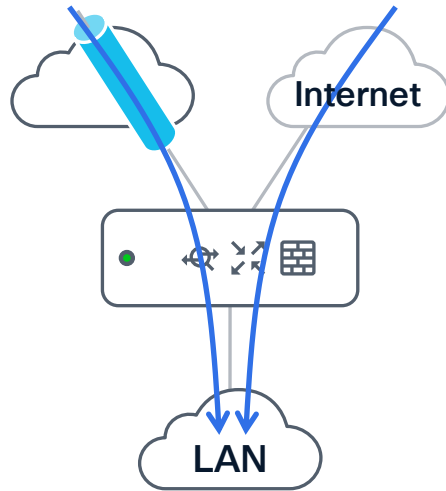
Firewall



Securing the Edge

Threat Protection

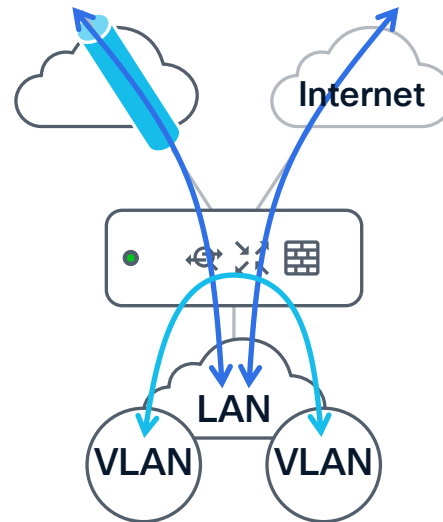
Cisco AMP



Enabled or Disabled
Configurable exclusions
either URL or File

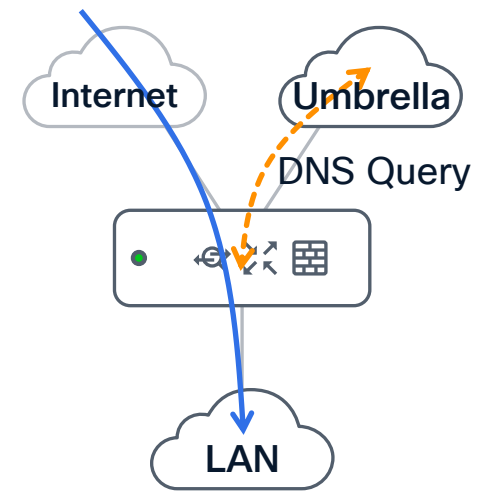
Note: ensure traffic analysis in enabled

IDS/IPS



Disabled, IDS or IPS
Rules can be disabled
Configurable exclusions
either type or IP address

DNS Security



Requires DNS Security
Subscription
Configurable domain
exclusions

Securing the Edge

Content Filtering

Category blocking

Block URLs by website and threat category. See the [full category list](#).

🚫 Block

Content categories

- Adult X
- Pornography X
- Child Abuse Content X
- Terrorism and Violent Extremism X
- Illegal Activities X
- Lotteries X
- Gambling X

Threat categories

- Spam X
- Botnets X
- Spyware and Adware X
- Phishing X
- Malware Sites X
- Open HTTP Proxy X
- Domain Generated Algorithm X
- Cryptojacking X
- Malicious Sites X

URL filtering

Enter specific URLs to block or allow. You can use **Category blocking** to block a large number

🚫 Block

Blocked URL list

Targets specific URLs to block

www.example.com

✅ Allow

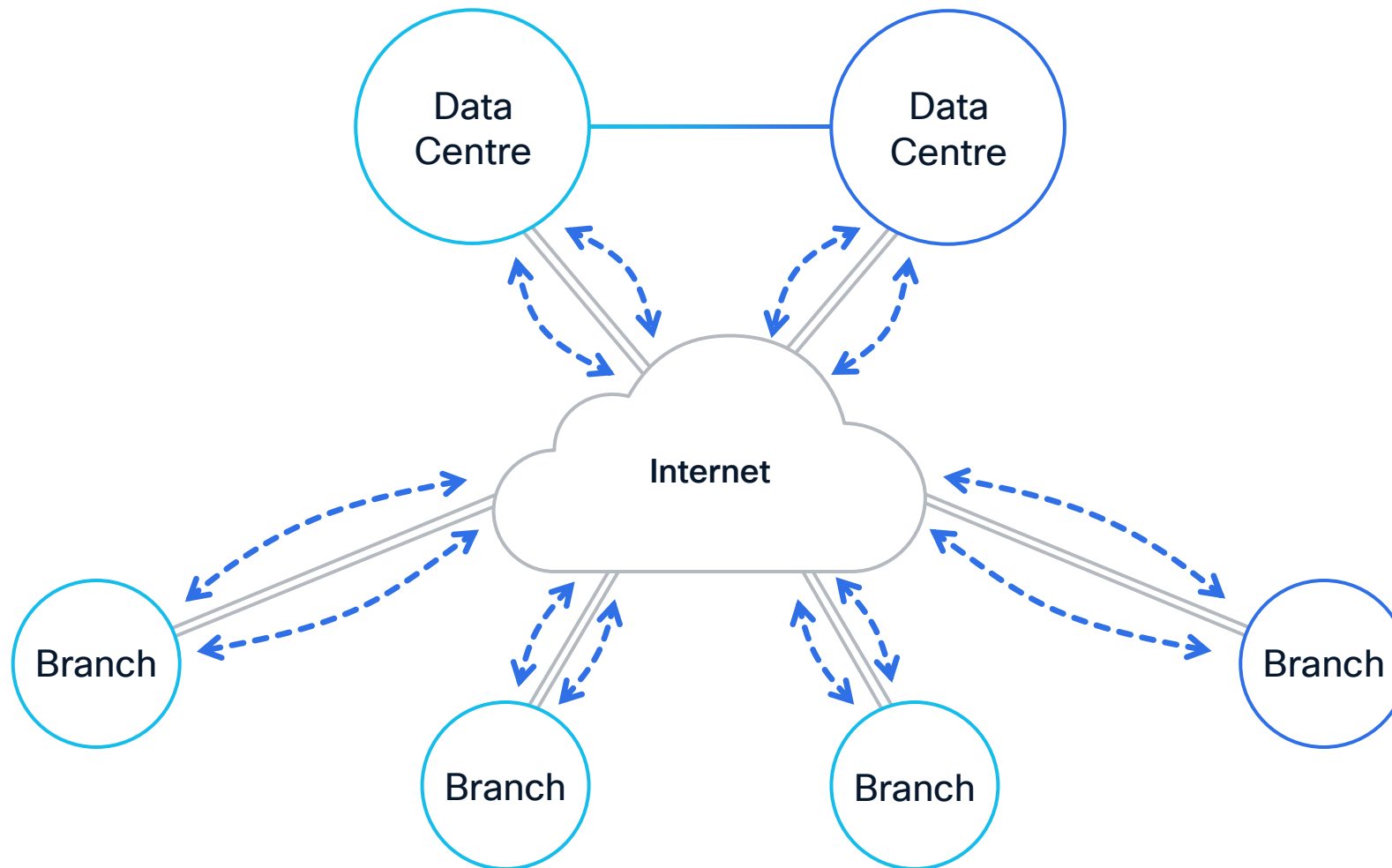
Allowed URL list

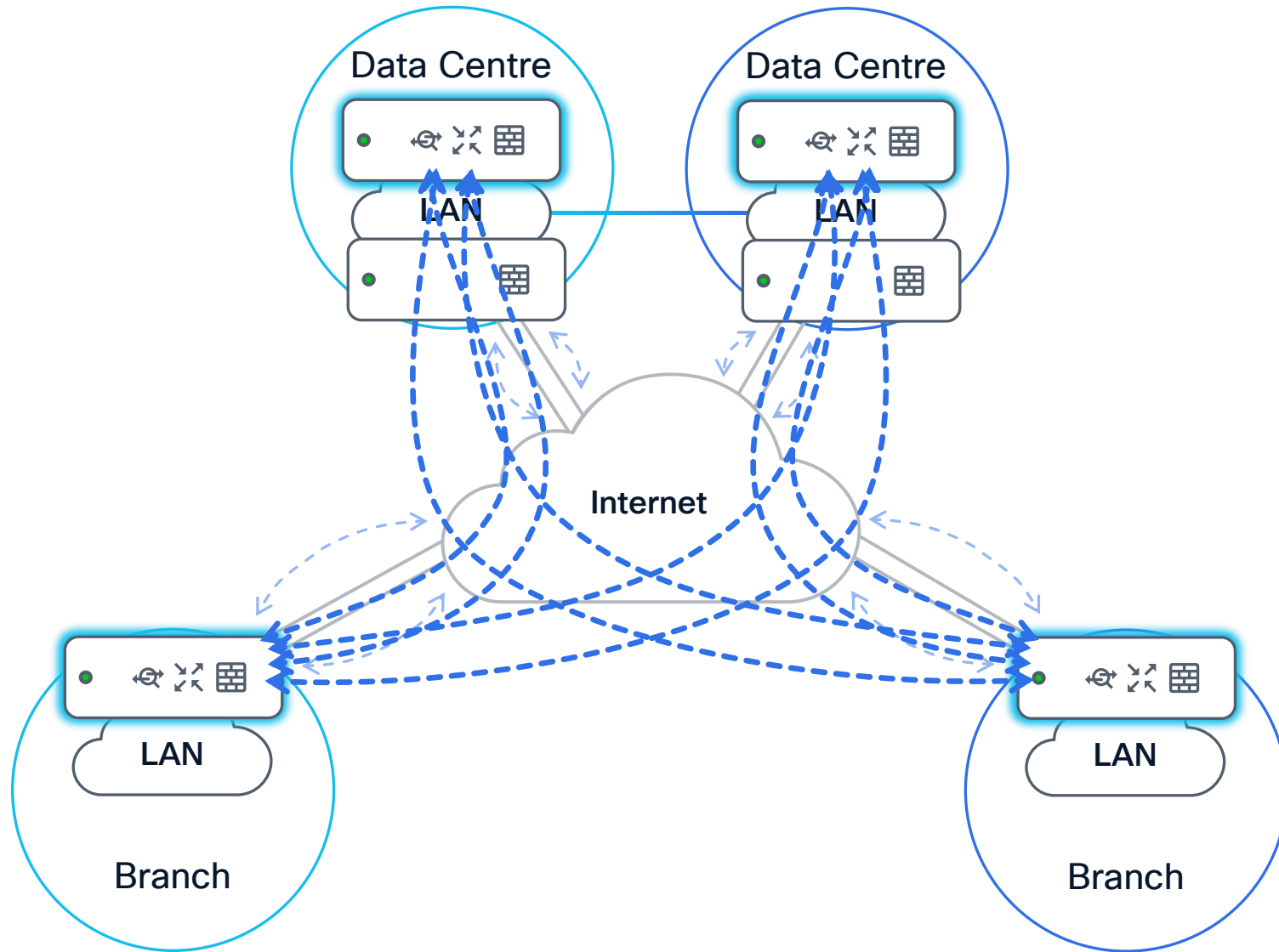
Targets specific URLs to allow

webex.com
wbx2.com
zoom.us
slack-core.com
slack.com

Asterisk (*) only relevant by itself
Allow list takes precedence

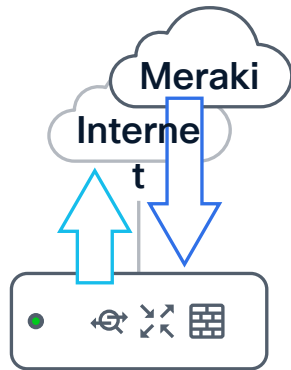
Expanding the business





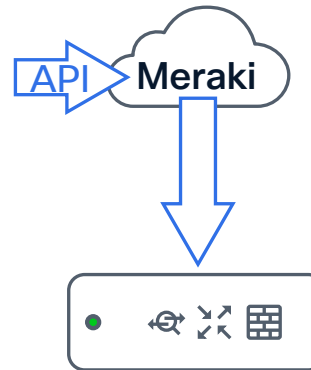
MX SD-WAN Benefits

ZTP



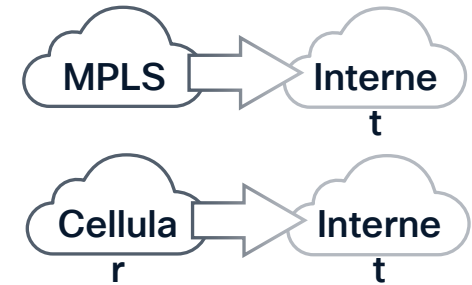
IP Address, DNS and
internet access
Pre-provision configuration
in Meraki Dashboard

Programmable



Python SDK
Ansible Module
Terraform Provider

Transport Independent

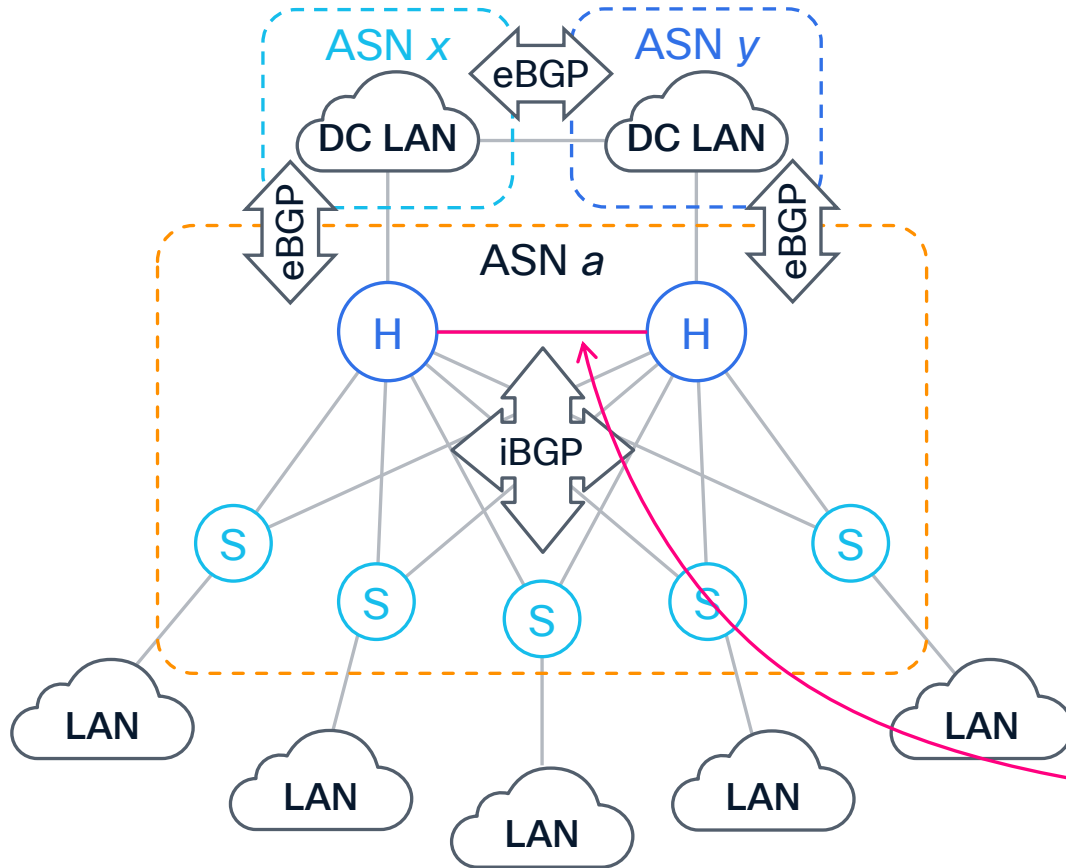


Ease of migration at end
of contract
Temporary cellular
deployments for new sites

Advanced Configurations

Advanced Configurations

Border Gateway Protocol

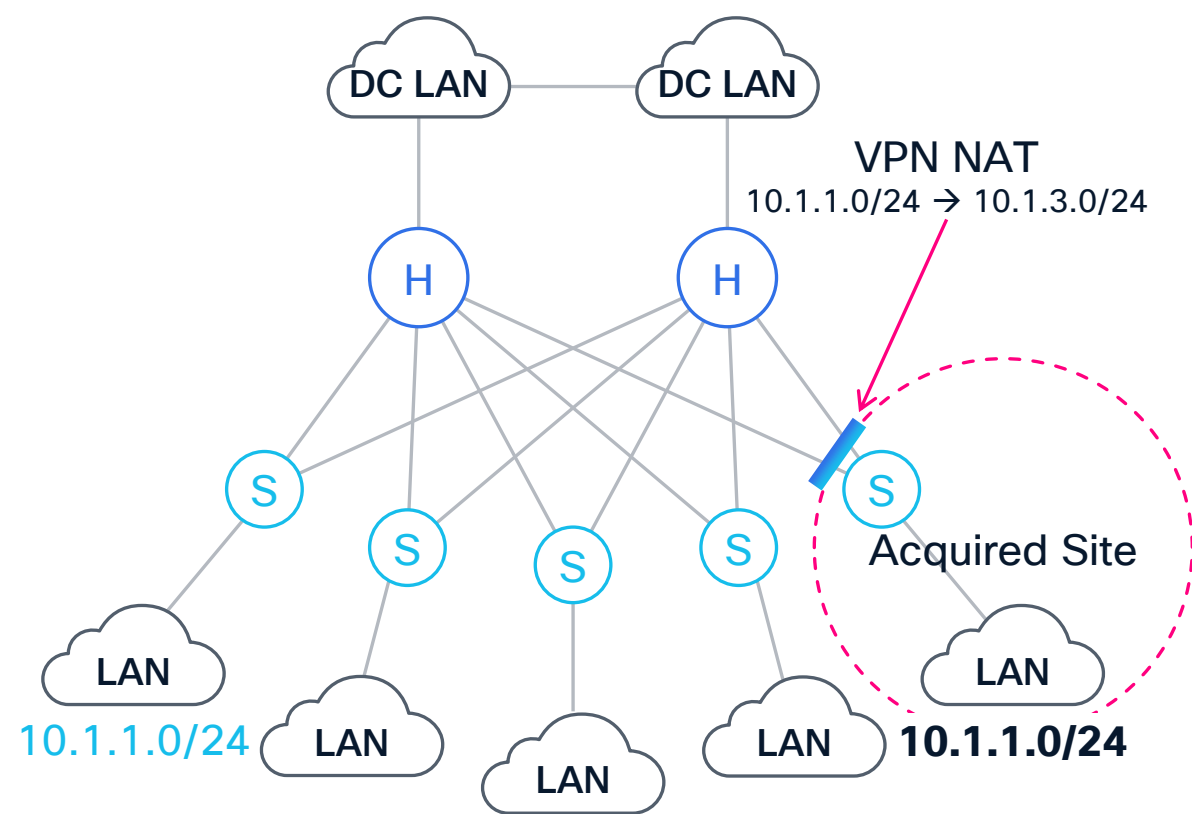


Single AS for SD-WAN fabric
'Receive limit' and 'allow transit'
options to maintain route table integrity
Configurable BGP neighbour attributes:
'AS Path Prepend', 'MED' and 'Weight'
BGP configurable on multiple
interfaces in NAT/routed mode
Note the route priorities for MX (i.e.
BGP is least priority)

This link can be disabled by support

Advanced Configurations

Site-to-Site VPN NAT



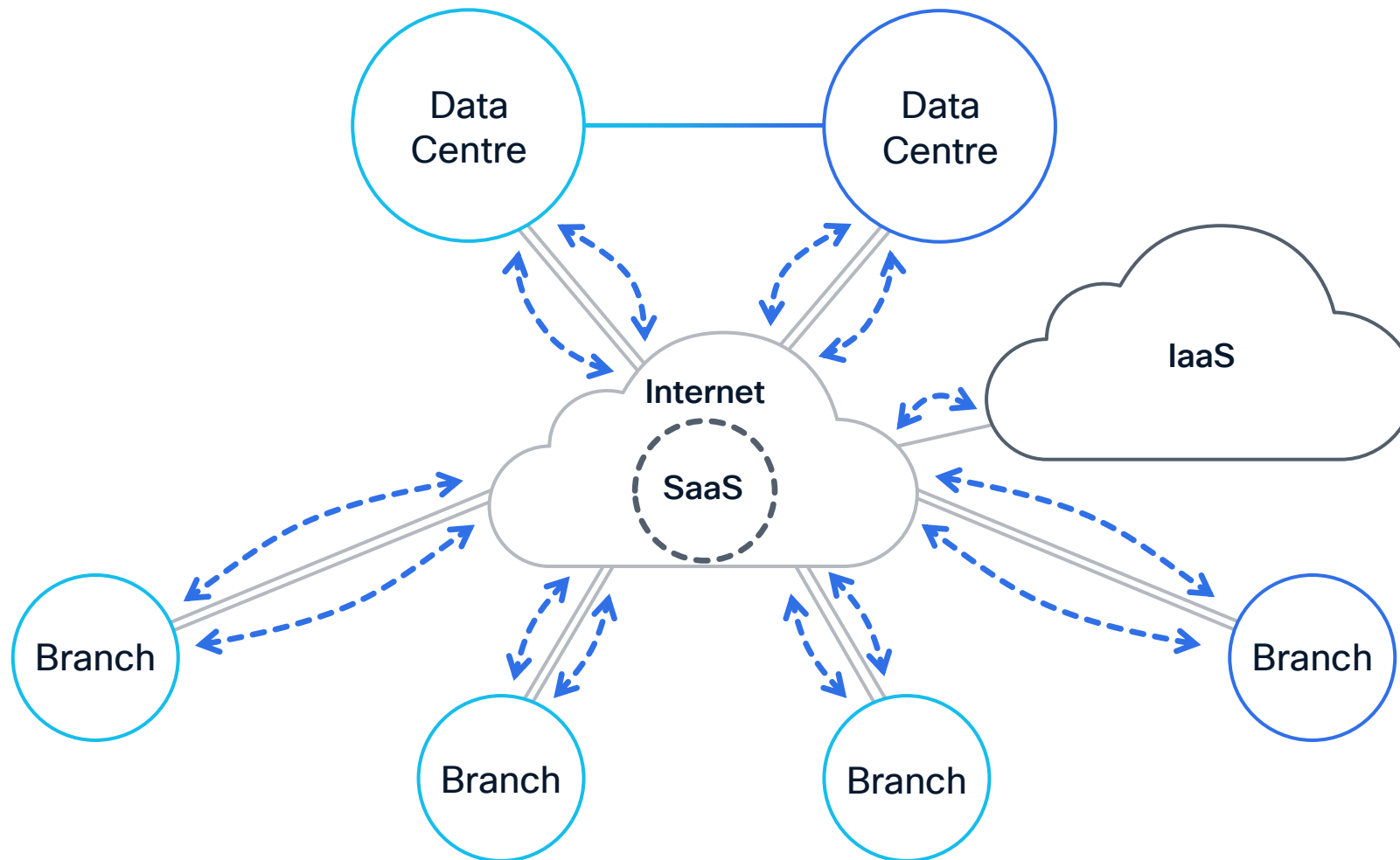
Site-to-Site VPN NAT

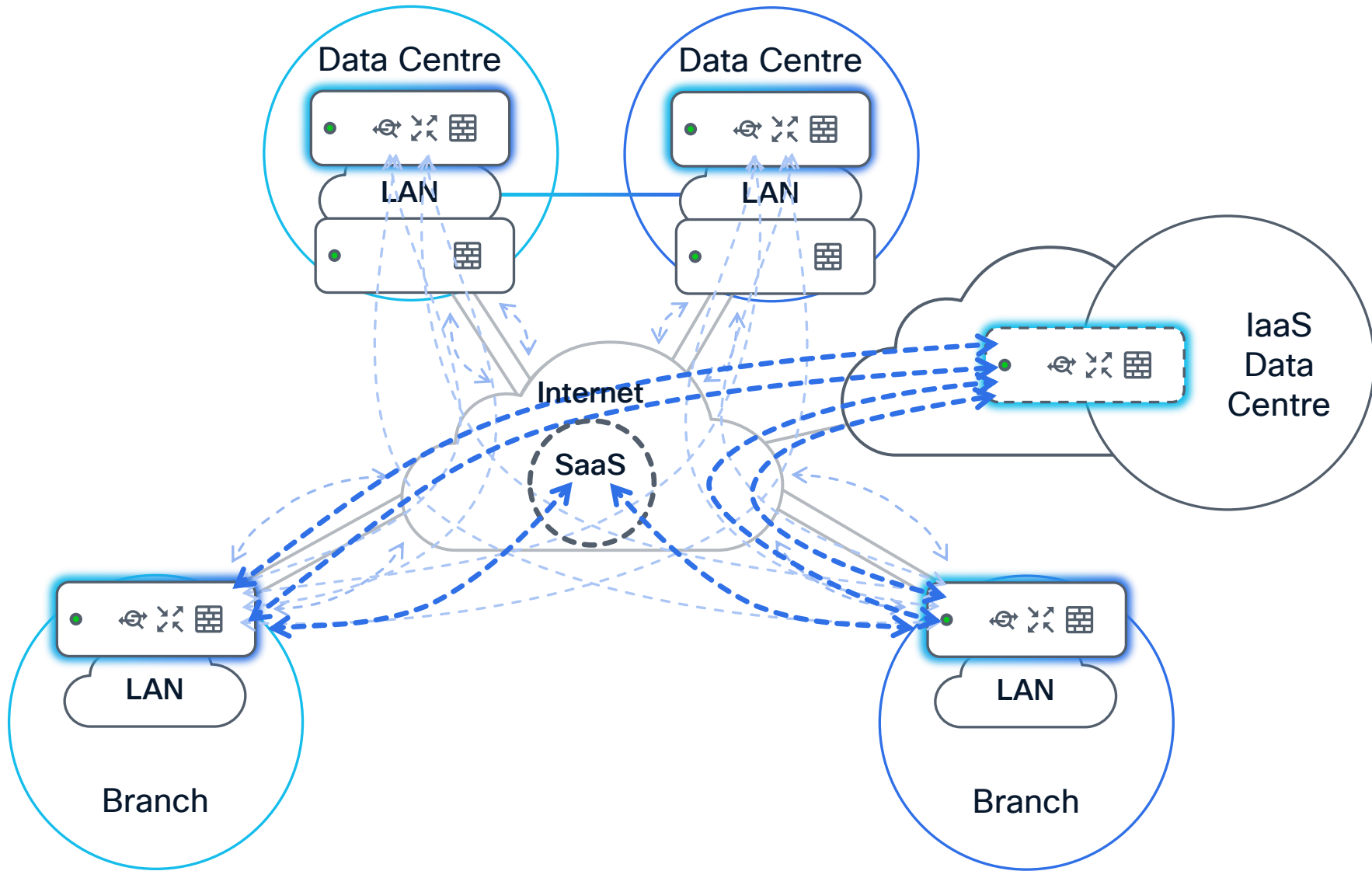


- 1:1 VPN, 'changes' IP addressing for site
- 1:Many NAT, 'shrinks' subnet to single IP address
- Host map available for traffic towards site

Needs to be enabled by support

Moving to the cloud





Connecting to IaaS

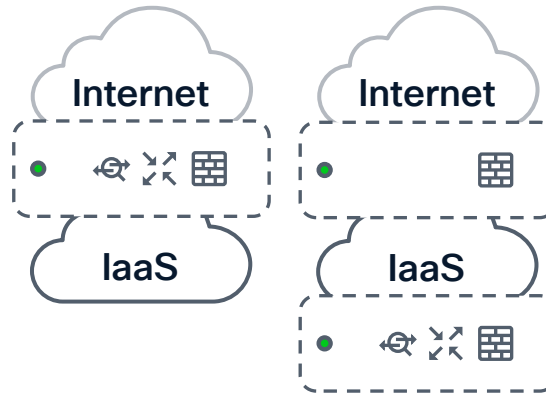
vMX



Virtual MX deployed in public IaaS

Either Enterprise or Advanced Security license

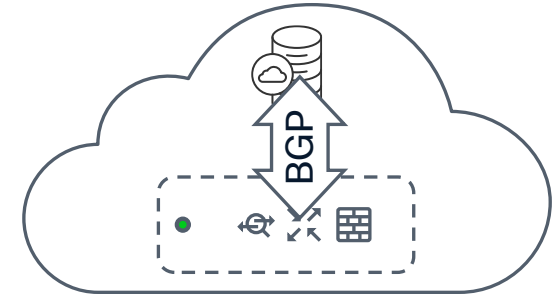
Flexible



NAT/routed mode or VPN concentrator

One WAN interface, and one LAN interface

Dynamic Routing



Use BGP to provide dynamic routing and HA

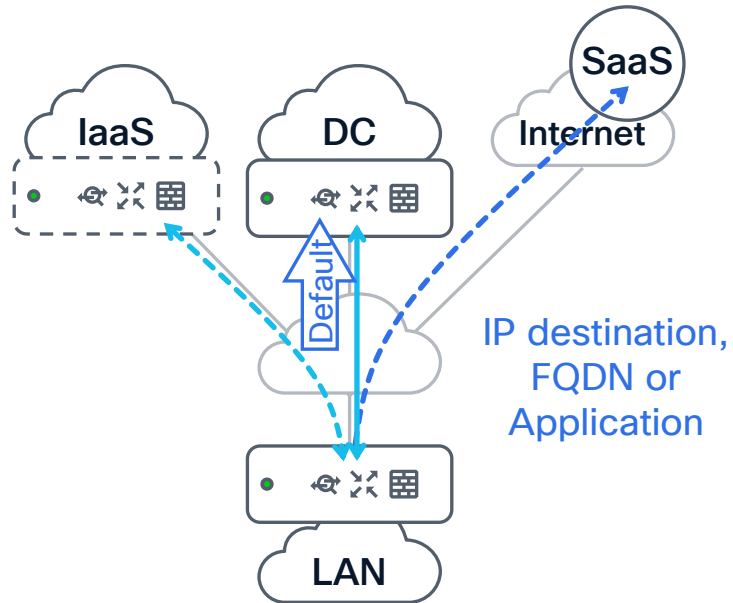
Note limits on BGP prefixes for IaaS providers

One virtual appliance for edge security and SD-WAN

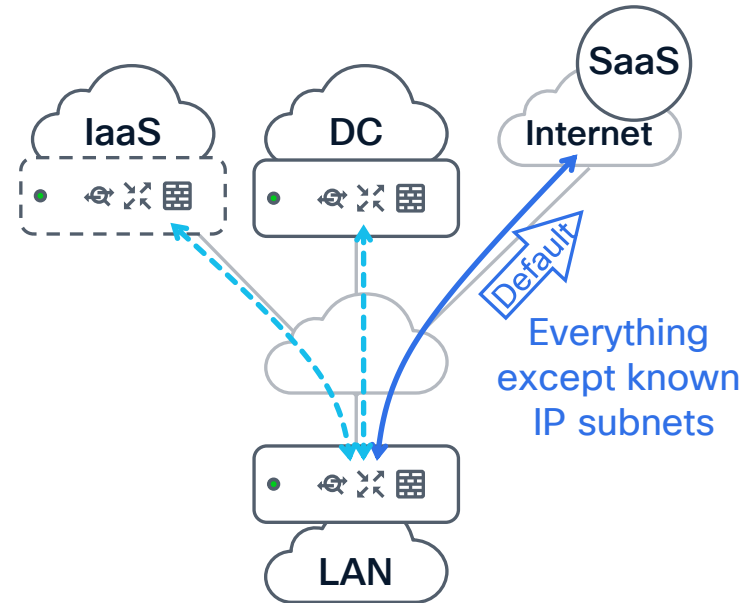
Use Catalyst 8000v for BGP route summarisation

Connecting to SaaS

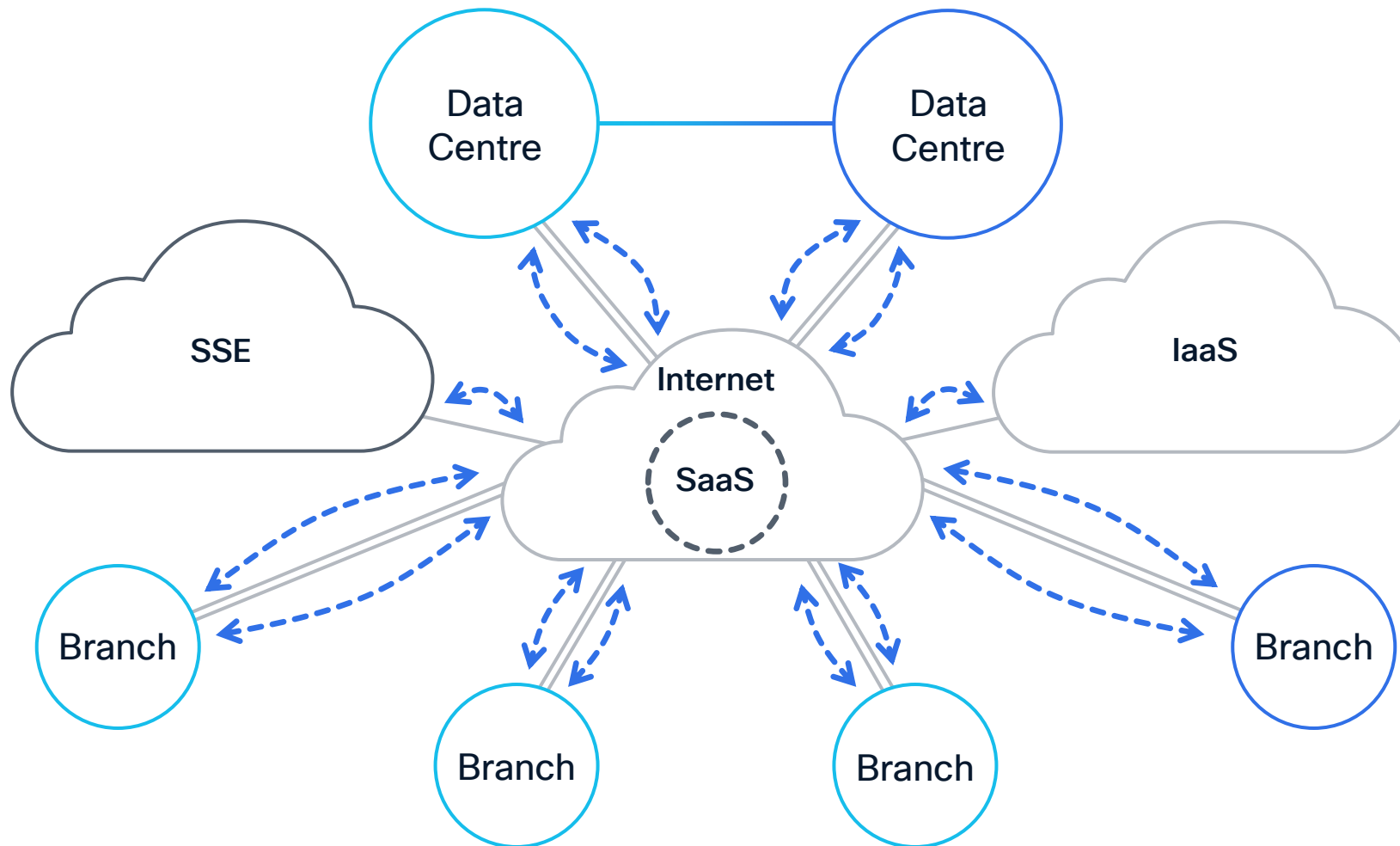
VPN Exclusion (DIA)

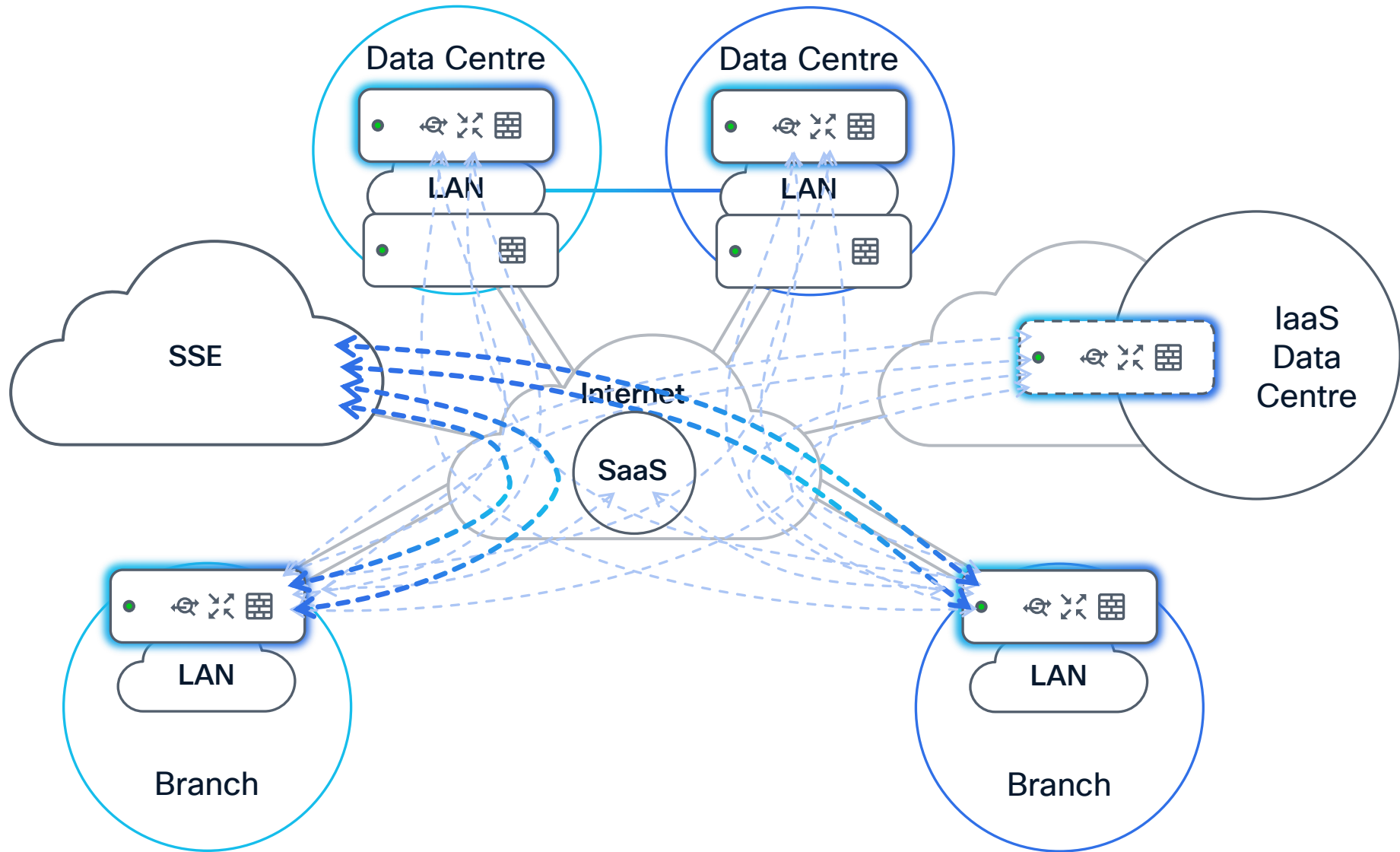


VPN Split Tunnel

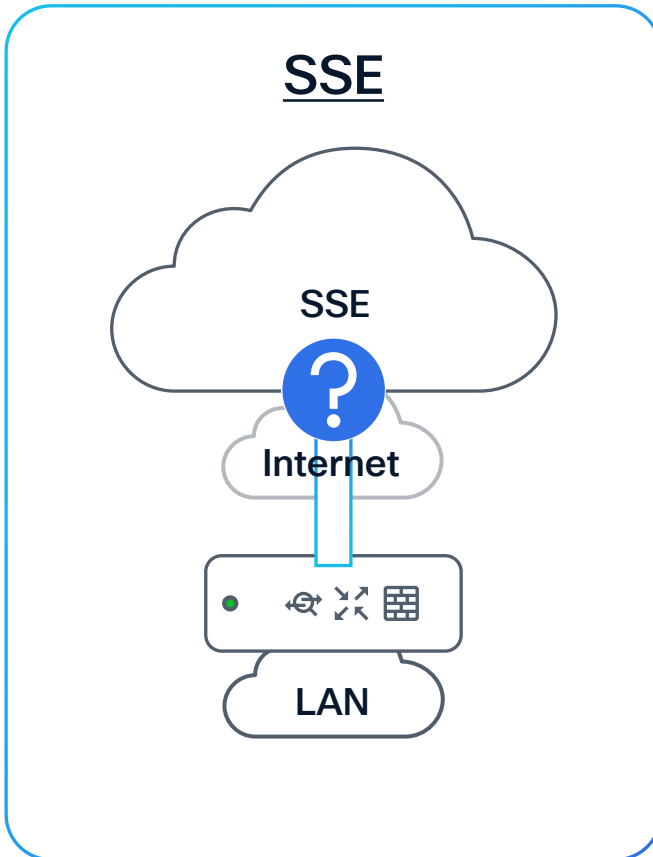
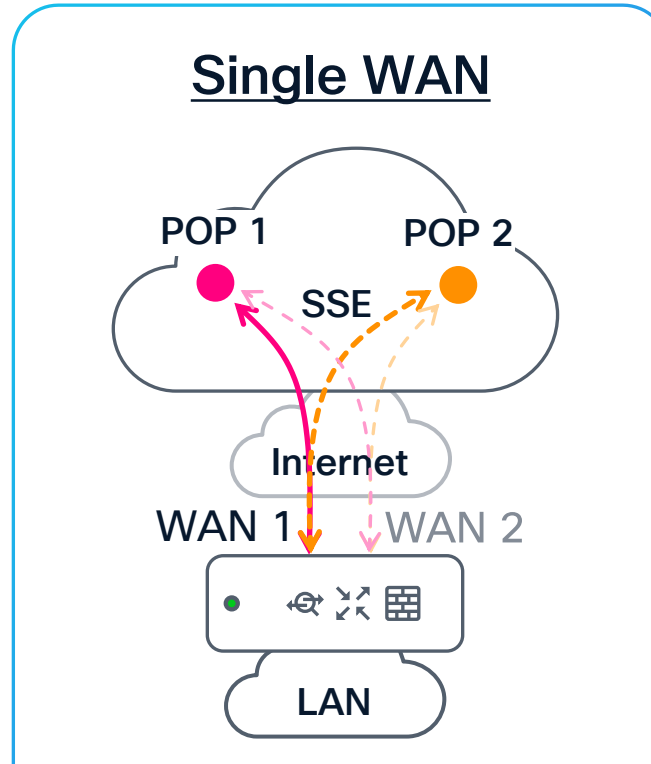
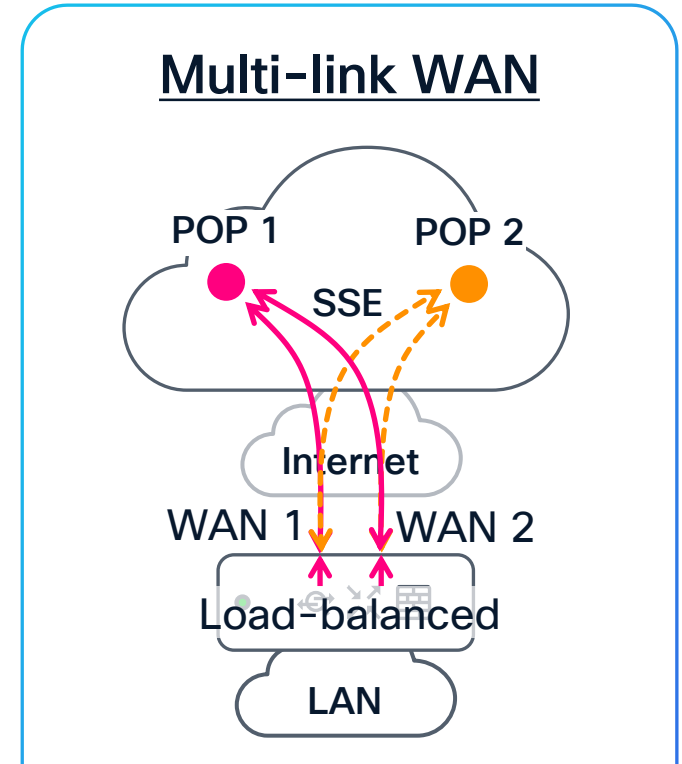


Implementing SSE



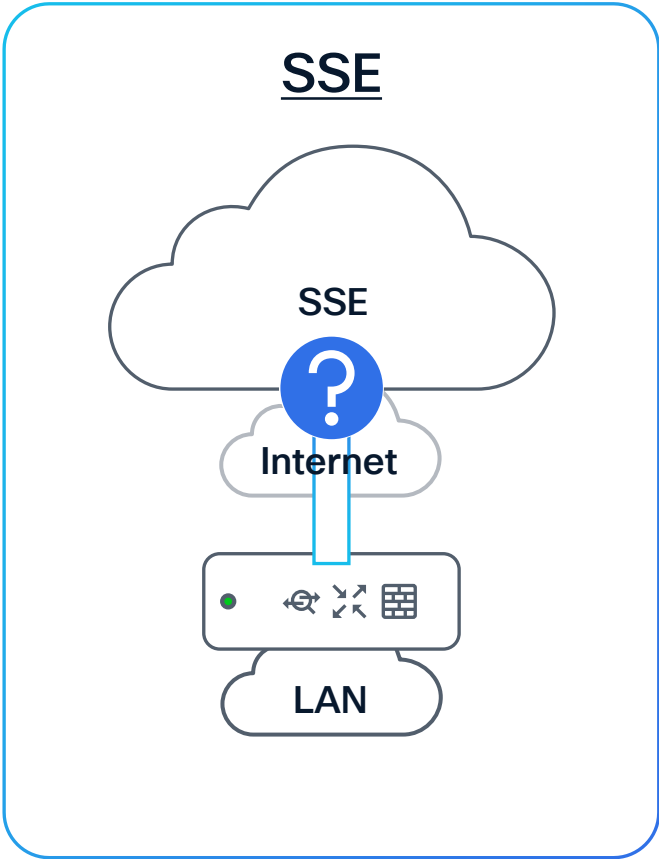
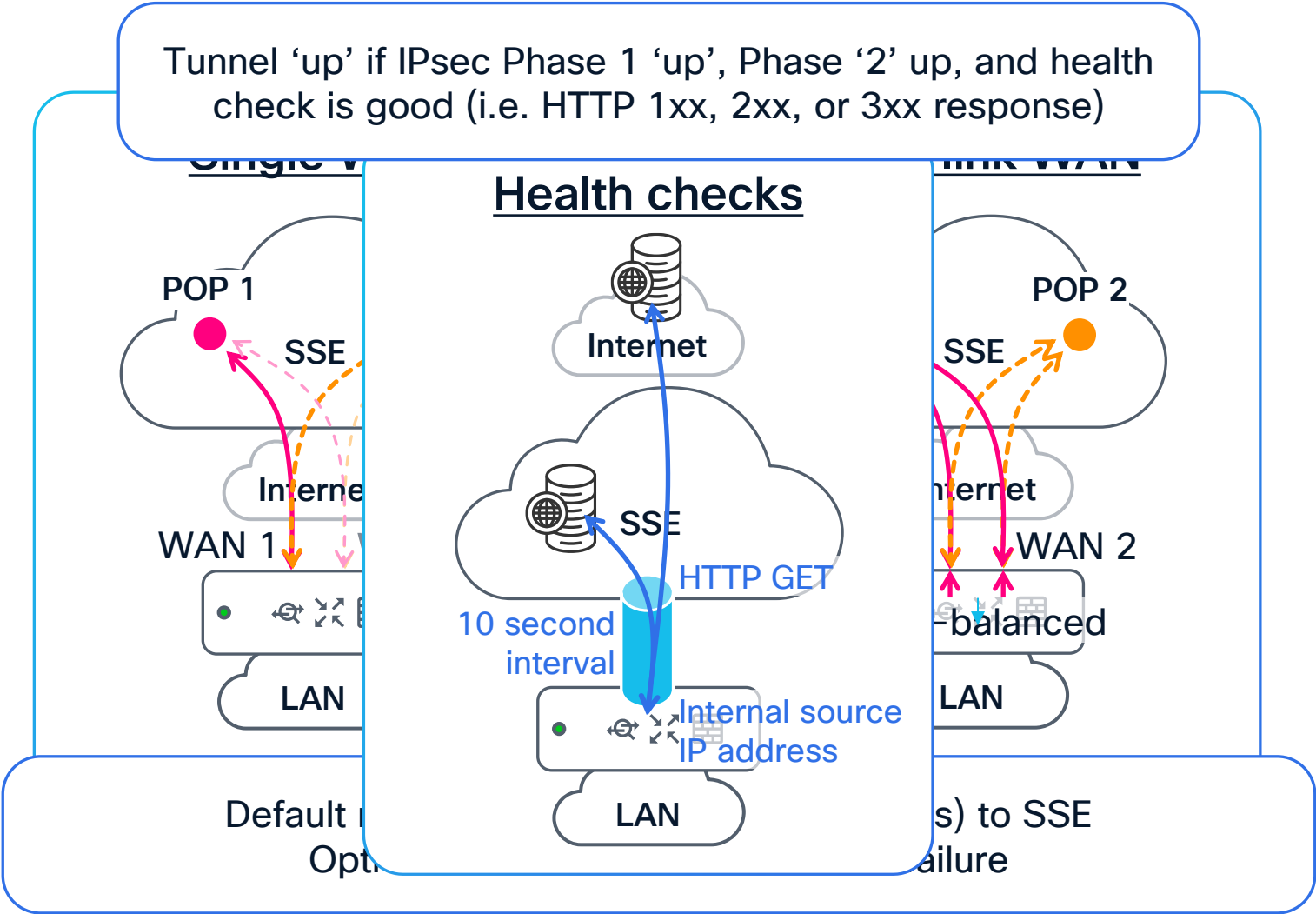


Connecting to SSE



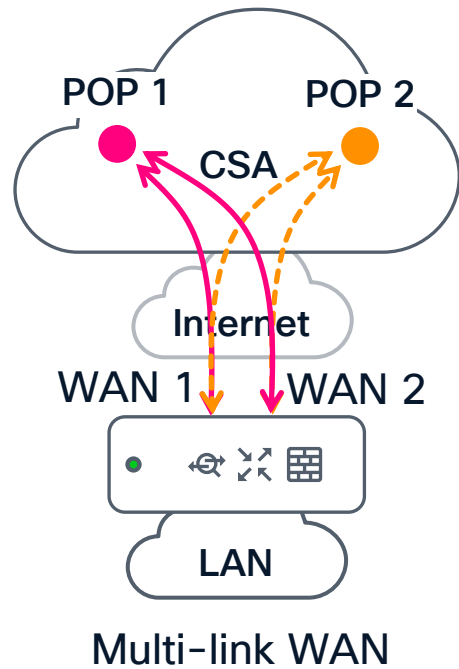
Default route (0.0.0.0/0) via IPsec tunnel(s) to SSE
Option to failover to DIA on tunnel failure

Connecting to SSE

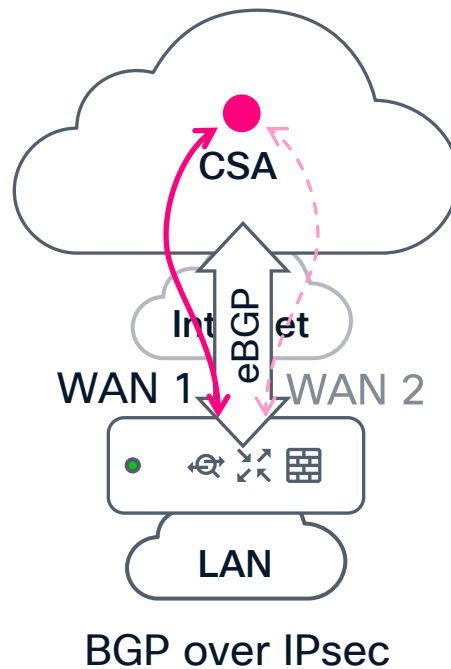


Connecting to Cisco Secure Access

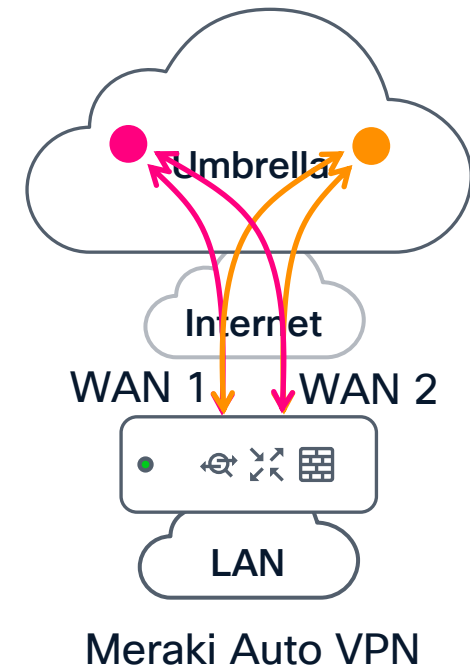
Secure Internet Access



Secure Private Access



Cisco Secure Connect



The background of the slide features a dynamic, abstract pattern of flowing, wavy lines in various shades of blue, from light sky blue to deep navy blue. A prominent white rectangular box is positioned on the left side of the slide, serving as a container for the main text.

Where next?

Thousand Eyes Integration

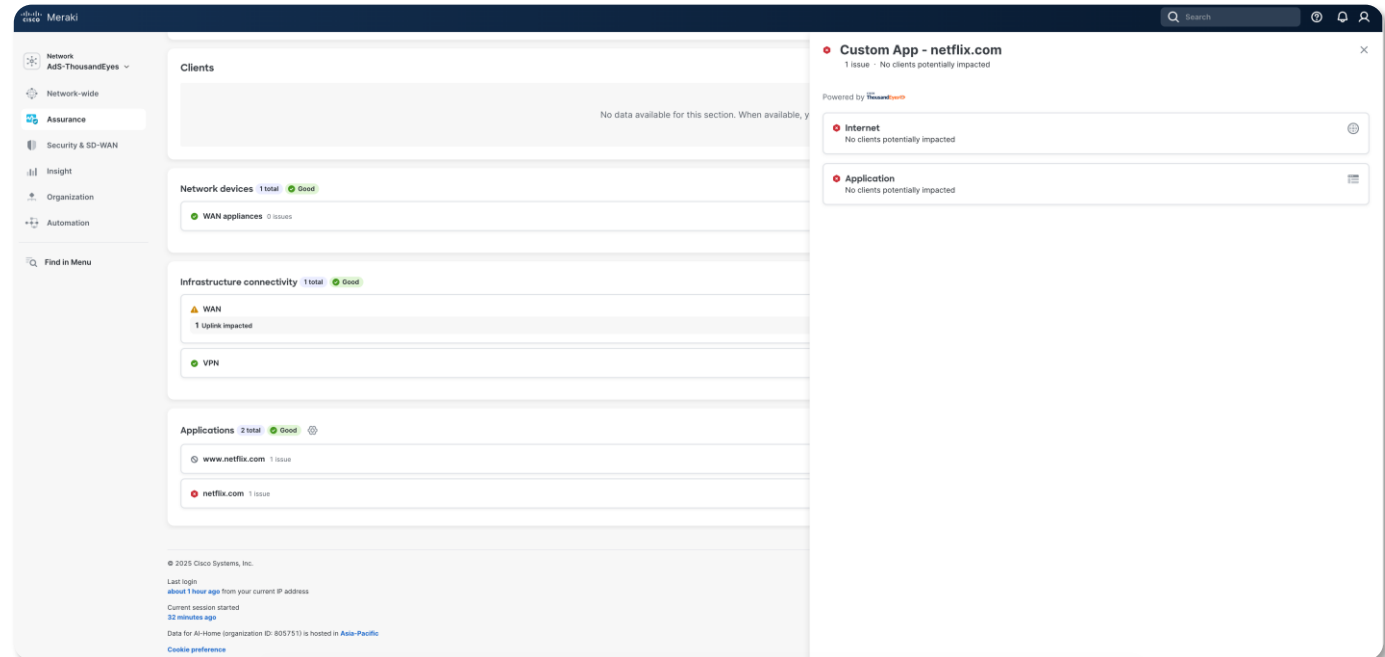
Assurance

Integration of Thousand Eyes
with Meraki Dashboard

Enterprise Agent installed on
MX appliance

Proactive, synthetic testing of
applications

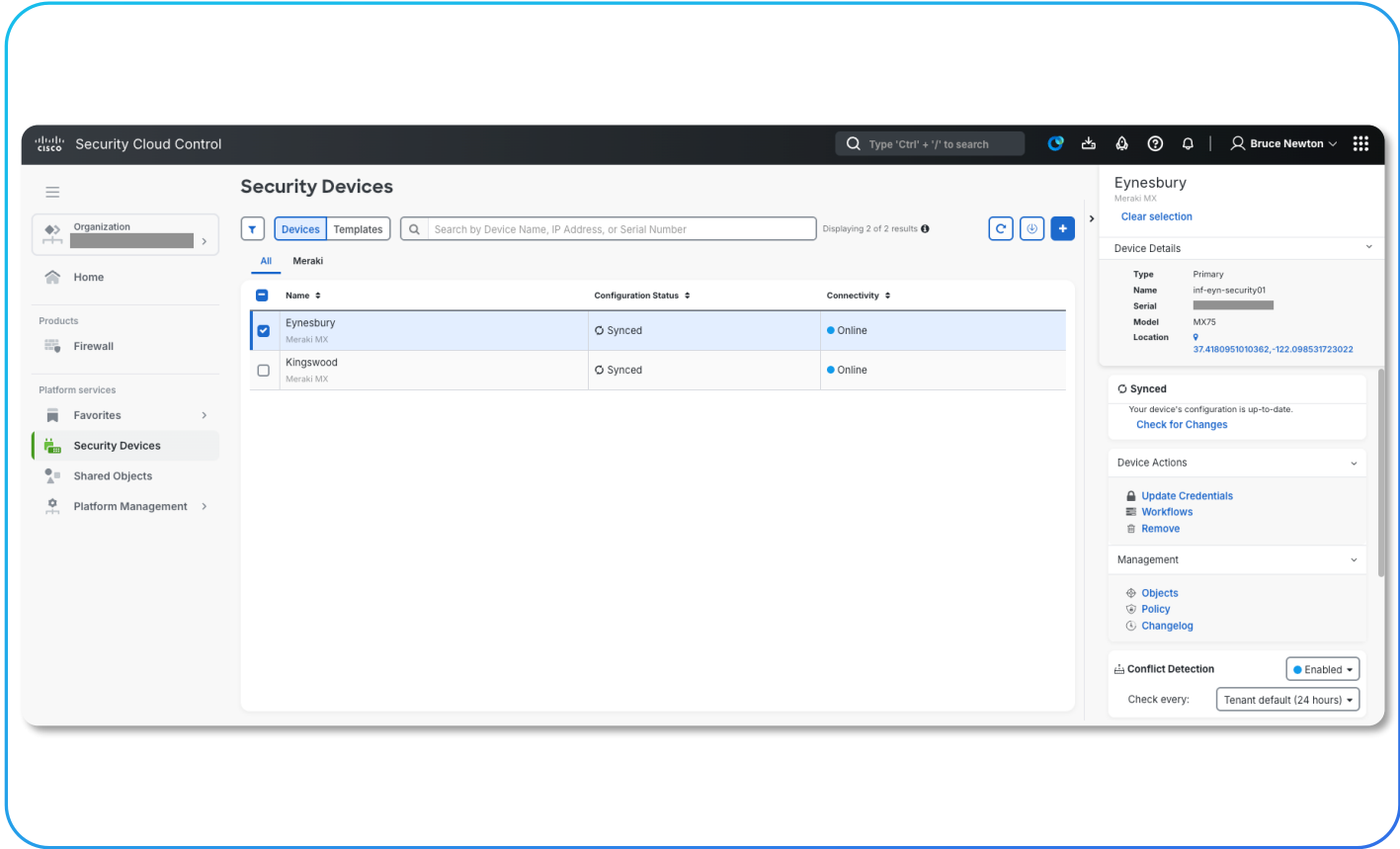
Client impact of application
issues reflected in Dashboard



Security Cloud Control

Centralised Policy

Integration of Security Cloud Control (SCC)
Push centrally defined policy to security appliances



Cisco XDR Integration

Securing the Network

Integration of Cisco Extended
Detection and Response
Visibility of XDR incidents
directly in Dashboard
NetFlow from MX appliance
feeding SCA

Security Center

MX Summary

MX Events

XDR Incidents

13 Incidents

0 New incidents

4 Open incidents

Last 30 days

Assignment

Status

13 Incidents

Priority	Name	Source	Created	Assign
1000	SMB Connection Spike: Internal on 172.31.106.144	Cisco XDR Analytics (org-563ad68f-9f3...	13 days	UD
1000	Malware Executed on MY-DEVICE-42 - Incident by Cisco XDR Aut...	Cisco XDR Automation	16 days	UD
1000	Persistent Remote Control Connections - New External Server	Cisco XDR Analytics	17 days	UD
1000	Malware Executed on MY-DEVICE-42 - Incident by Cisco XDR Aut...	Cisco XDR Automation	1 month	UD
880	Malicious email reported on dcloud[at]dcloud[.]local	Cisco XDR Analytics	16 days	MM
870	DNS Abuse on 64[.]102[.]16[.]247	Cisco XDR Analytics	1 day	UD
720	Malware and phishing on sparrow-meraki-client	Cisco XDR Analytics	15 days	Unas
690	Anomalous Domain Controller Activity on 52[.]216[.]25[.]128	Cisco XDR Analytics	14 days	UD
660	Anomalous domain activity on rod[.]traceableactions[.]com	Cisco XDR Analytics	13 days	D
660	New external server detected on rod[.]traceableactions[.]com	Cisco XDR Analytics	20 days	D

SMB Connection Spike:
Internal on 172.31.106.144

Priority 1000

Status Open: Reported

Reported by Cisco XDR Analytics (org-563ad68f-9f39-4db3-b49f-88edb3a45451)

14 days ago

Assigned to UD

Priority score breakdown

1000

100 Detection Risk

10 Asset Value at Risk

Short description

Device attempted to contact an unusually large number of SMB servers. This can be an indication of malware or abuse.

Long description

Assets 1

Observables 0

Help

View incident in XDR



The MX can do that.

Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Showcase for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you

CISCO Live !

