

# HOW TO IMPLEMENT SD-WAN FOR YOUR ORGANIZATION

A SIMPLE TECHNICAL INTRO



# EXECUTIVE SUMMARY

Software-defined WAN (SD-WAN) simplifies the management and operation of a WAN (Wide Area Network) by decoupling or separating the networking hardware from the mechanisms that control the network. In other words, SD-WAN essentially creates a logical overlay on top of physical networks that enables central management or orchestration of the WAN.

## Benefits of SD-WAN

### Agility

With the ability to manage the network via a software overlay, new networking services can be delivered in a fraction of the time that it would take for an on-site technician to do the same work.

### Better User Experience

SD-WAN application performance is monitored for changes in latency, jitter and packet loss. When performance falls below an optimal level, traffic is dynamically routed to another link, ensuring users and applications are always connected.

### OPEX Savings

with multiple links to choose from: MPLS, broadband, and wireless, organizations can build higher-performance WANs using lower-cost and commercially available Internet access.



# BUILDING BLOCKS OF SD-WAN

## Overlay

An overlay network provides site-to-site connectivity (e.g. VPN). Options include edge routers, software based white boxes, and a vast array of software-defined WAN (SD-WAN) appliances.

## Underlay

An underlay or breakout network provides a direct site-to-internet connection, and includes transport and circuit types such as Multiprotocol Label Switching (MPLS), broadband internet (e.g. DSL, copper cable and optic fiber), wireless (e.g. 5G) and local Internet service providers (ISPs) and mobile network operators (MNOs).

## Network Policy

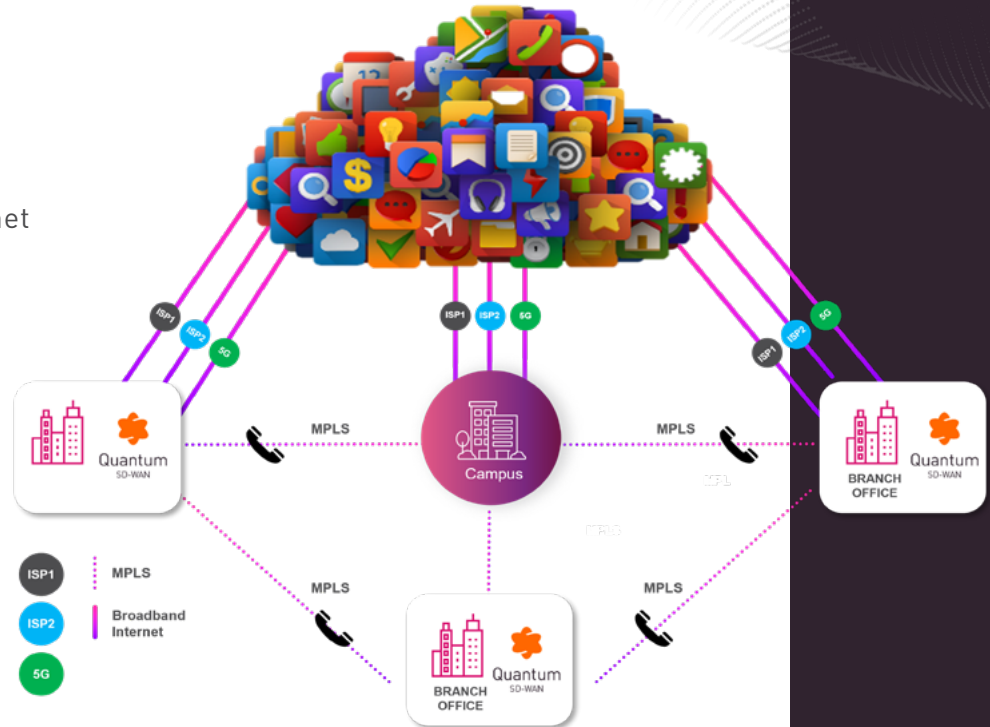
Organizations define a policy in software for routing apps, mitigating performance problems associated with latency, jitter, or packet loss to give users an optimal experience at the lowest possible operating costs.

## Cloud Orchestration

Automates the provisioning, management, operation and monitoring of the Wide-Area Network (WAN).

## Security

Ideally, a complete security stack is integrated with networking and delivered either on-prem or as a cloud service.





# THREE TYPES OF SD-WAN STEERING BEHAVIORS

You can use SD-WAN for:

## Local Breakout

To control and select the best path for outbound traffic to cloud applications and the Internet.

## VPN Overlay

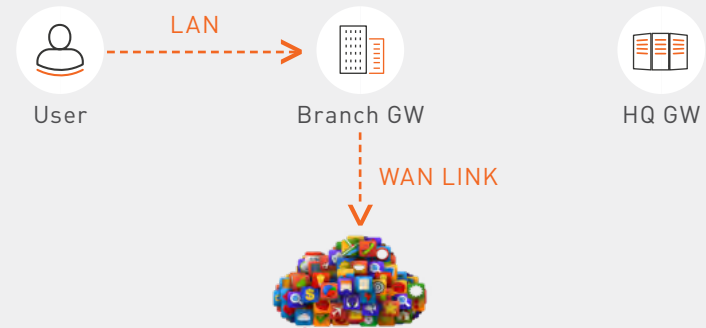
To control the best VPN path between VPN peers, for routing internal traffic between the organization's sites, either from VPN spokes to a central hub (e.g. Branch gateways to Headquarters gateways, or Satellites to Center), or between VPN sites in a mesh topology.

## Backhaul

To route Internet traffic on VPN spoke sites through the Headquarters over a VPN tunnel. This connection uses the overlay-based connection from the Branch to the Center, and a Breakout-based connection from the Center to the Internet.

## Steering Behaviors

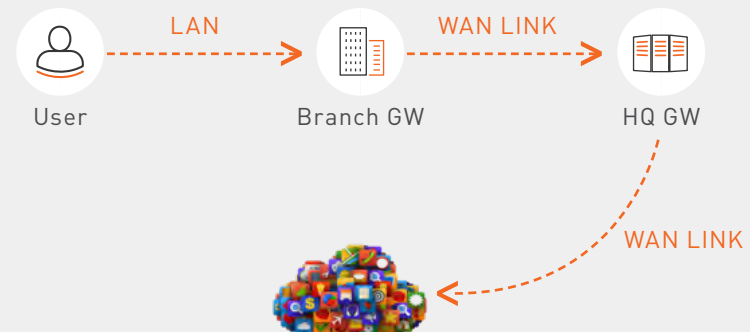
### Local Breakout



### VPN Overlay



### Backhaul







# LOCAL BREAKOUT (UNDERLAY)

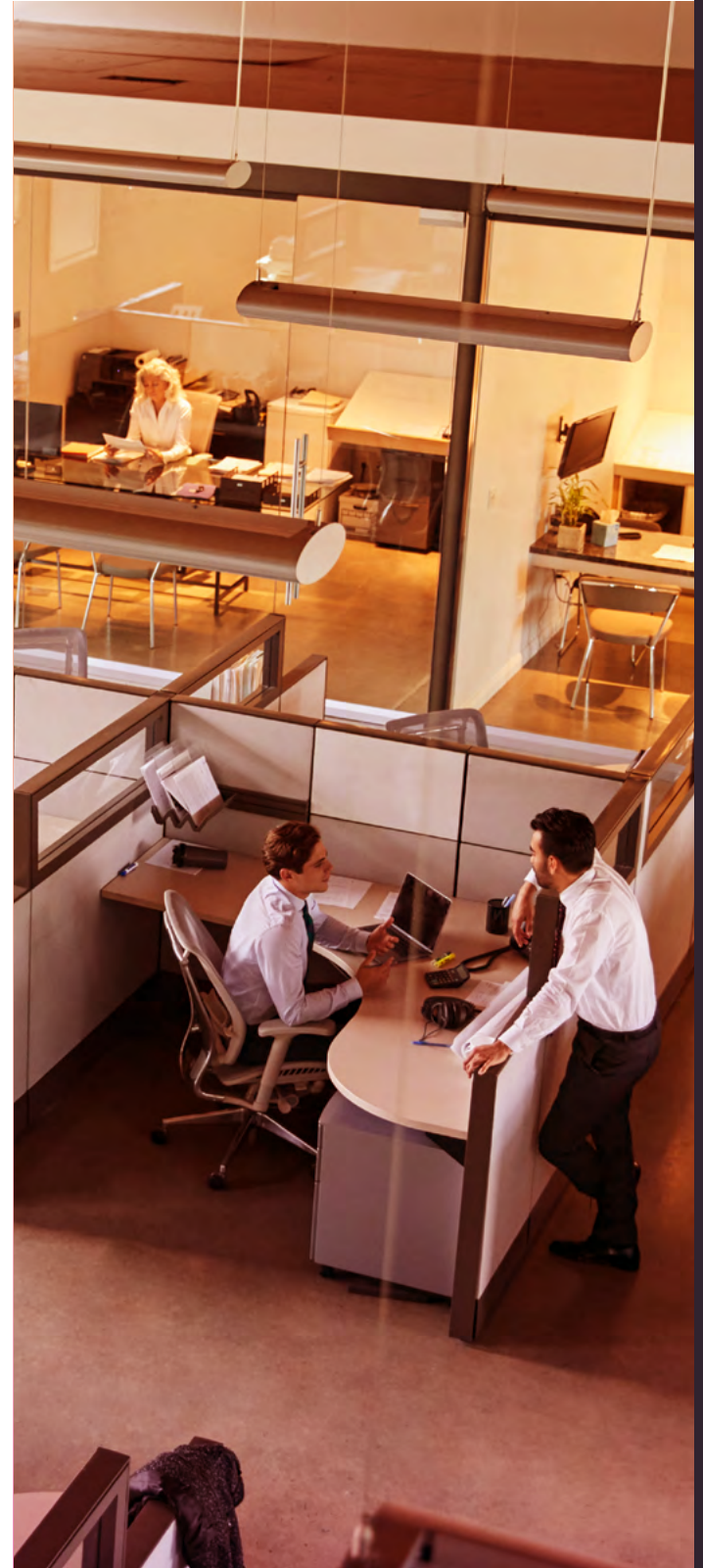
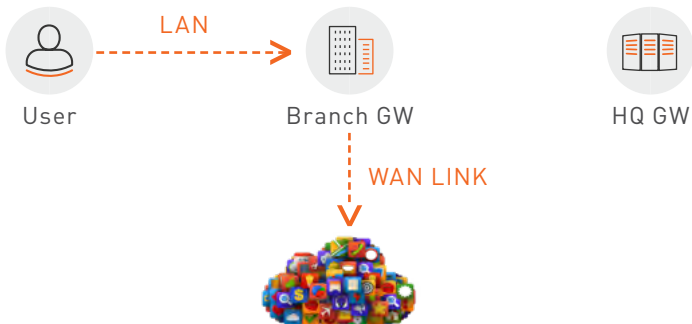
## TRAFFIC STEERING DIRECT-TO-INTERNET

This connection type represents direct links to the Internet with more than one ISP or MNO.

You can use a Local Breakout for:

-  A firewall with two ISP links, or one ISP link and one wireless link
-  A remote site with one primary and one backup MNO link.
-  Connect Zoom application traffic over an ISP link with low latency.
-  Connect backup transfer traffic over a low-cost ISP link with higher latency.

### Directly to Internet Local Breakout



# VPN OVERLAY

## TRAFFIC STEERING FROM SITE-TO-SITE

This connection type represents a direct WAN link with encrypted traffic to Headquarters.

**You can use a VPN Overlay for:**

- Connecting to a Remote Desktop server installed on an internal network behind the Headquarters firewall.
- Connecting from an internal network behind a branch firewall to a Remote Desktop server, when a direct low latency WAN link.

When the latency of the direct WAN link becomes greater than the latency of the direct MPLS Link, the Remote Desktop connection must go over a direct MPLS link.

### From site to site VPN Overlay





# BACKHAUL

## TRAFFIC STEERING VIA CENTRAL SITE TO INTERNET

This connection sends traffic from VPN spoke sites to the Internet through a Central VPN hub site.

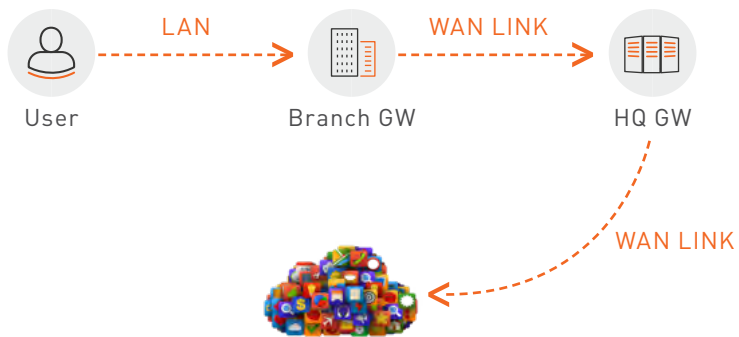
### You can use a Backhaul for:

Sending some traffic directly over the local Internet link, and other traffic through the Headquarters for better security inspection.

This provides redundancy for the local Internet connection of the VPN spoke site.

If the local Internet connection goes down, the VPN spoke site uses the Backhaul over an MPLS line to reach the Internet through Headquarters.

### Via central site to Internet Backhaul



# GETTING STARTED WITH SD-WAN

The next pages provide a basic high-level overview of how to deploy SD-WAN in your organization, including:



Connecting your environment



Setting up your steering policy



Monitoring your network connections





# SD-WAN DEPLOYMENT

## 1 | Connect the Overlay to the Cloud Orchestration

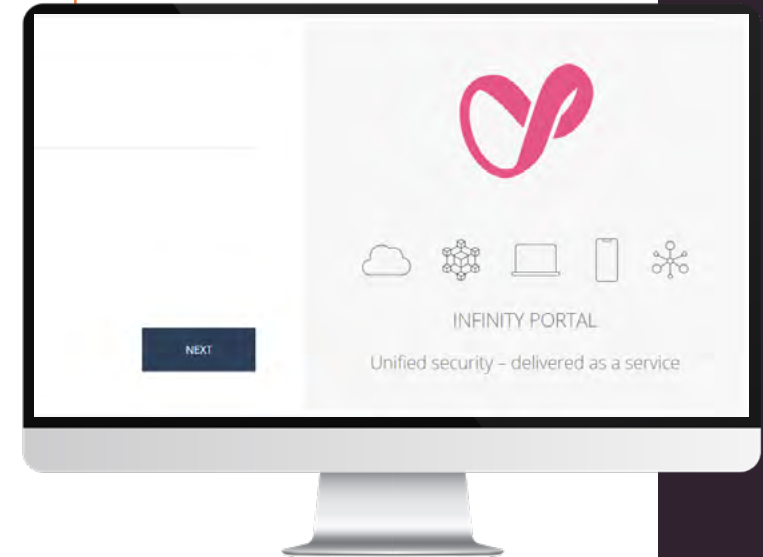
### Step 1

SD-WAN deployment begins with connecting your overlay components to your cloud-delivered management services.

Simply connect your security management to SD-WAN cloud services (Quantum Smart-1). This connects and establishes trust with your existing security overlay. Use existing objects and services to set the SD-WAN policy and manage your Software-defined networking from the cloud.

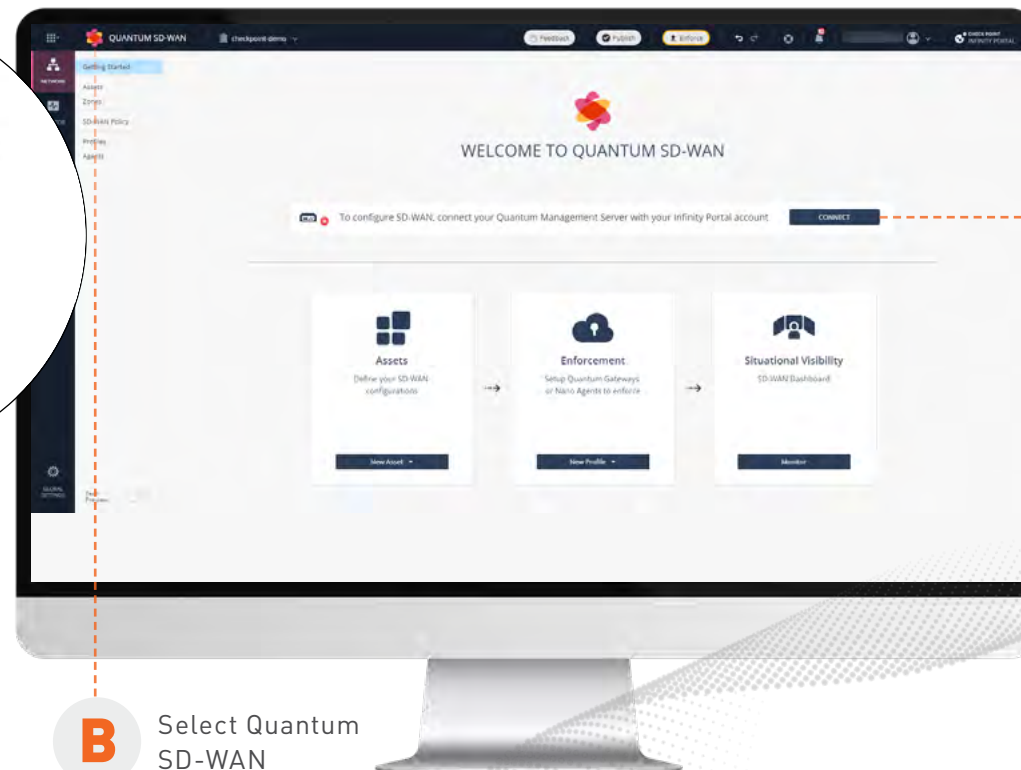
A

Create an Infinity Portal Account  
[portal.checkpoint.com](https://portal.checkpoint.com)



C

Connect to Quantum Smart-1



B

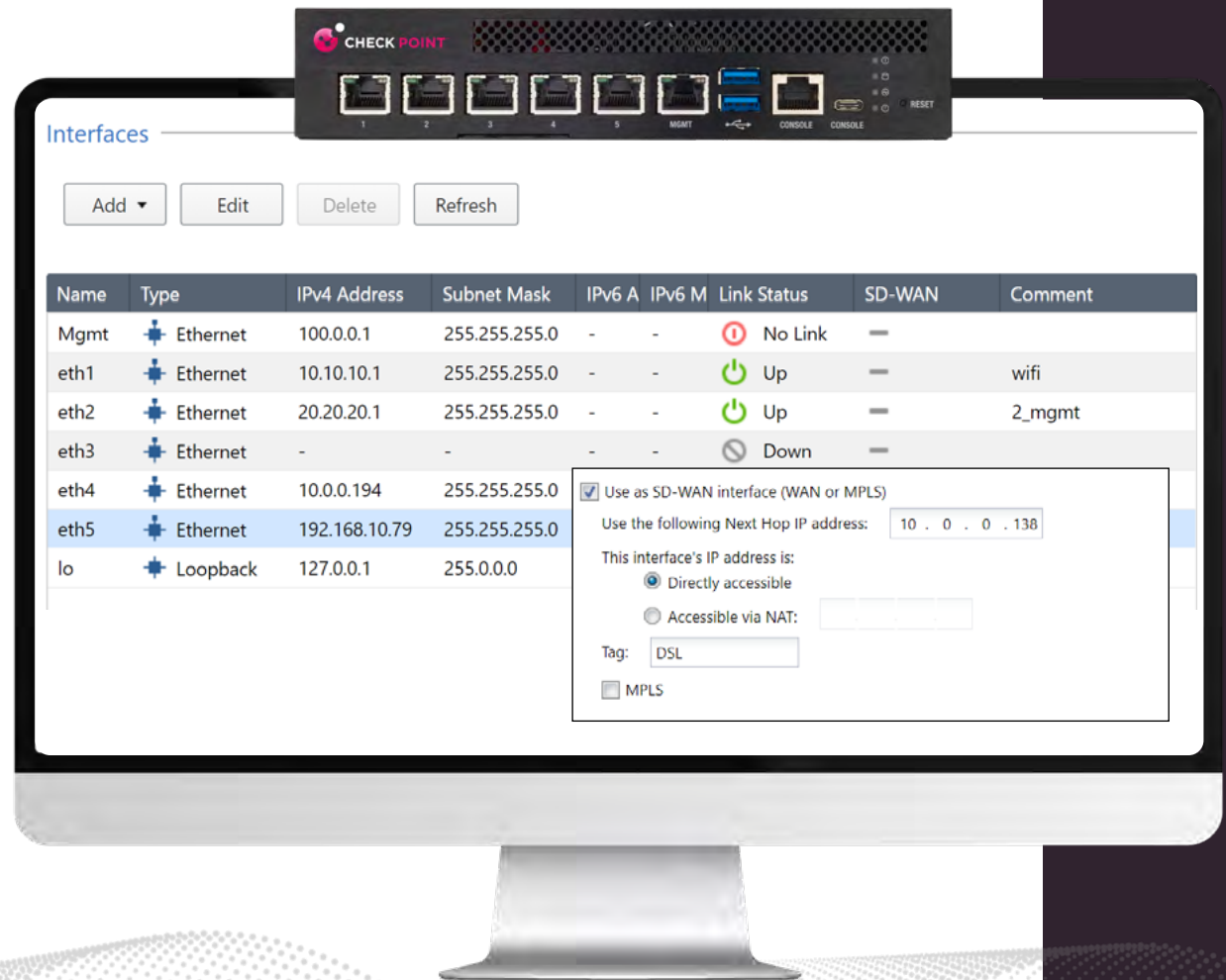
Select Quantum SD-WAN

# SD-WAN DEPLOYMENT

## 2 | Configure the Underlay SD-WAN circuits

### Step 2

The next step is mapping your physical network interfaces to a common, logical SD-WAN network topology so that multiple network appliances can be managed as one.

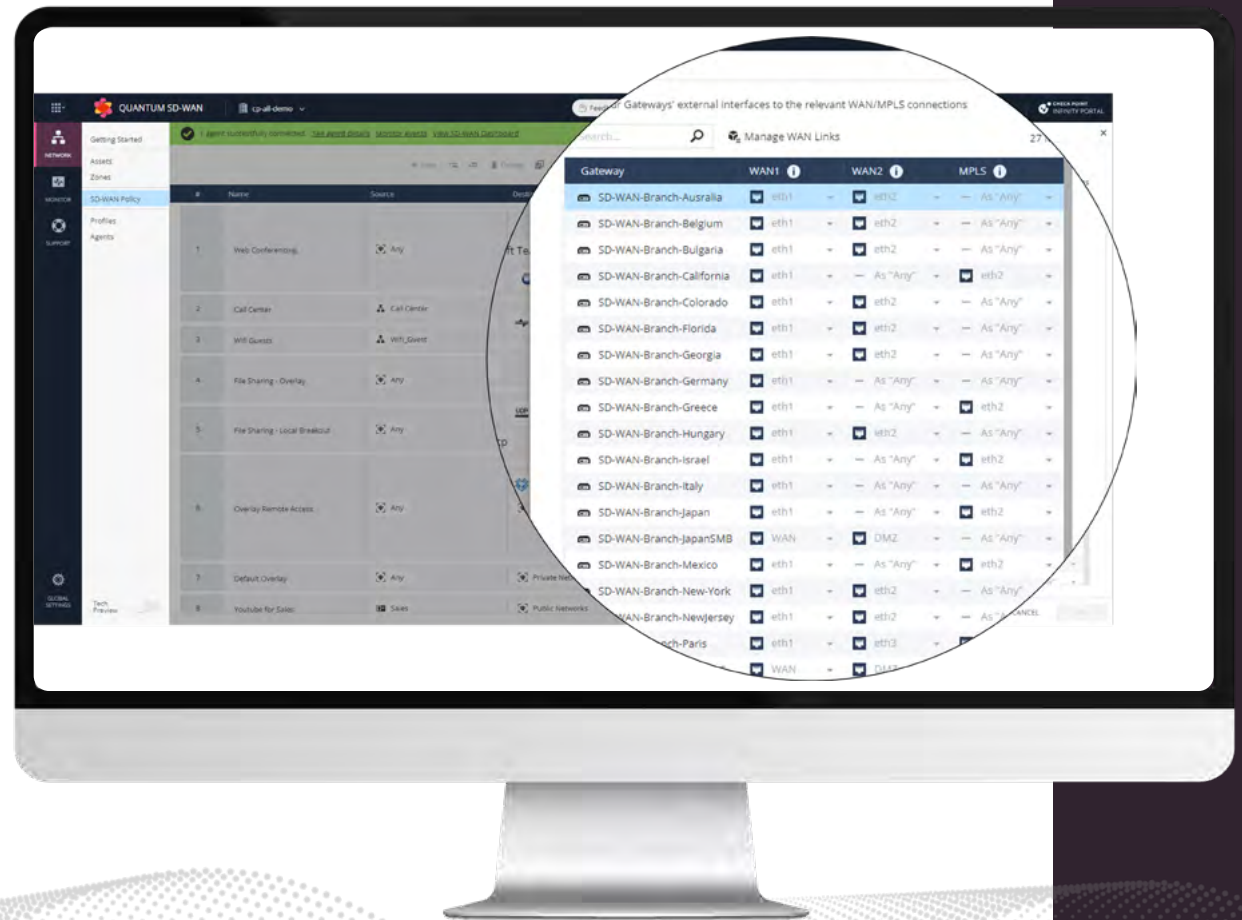


# SD-WAN DEPLOYMENT

## 2-A | The SD-WAN circuits form a Common Topology

### Step 2-A

With object sharing between existing security management and your SD-WAN cloud services, the common SD-WAN network topology is already set in your SD-WAN policy.





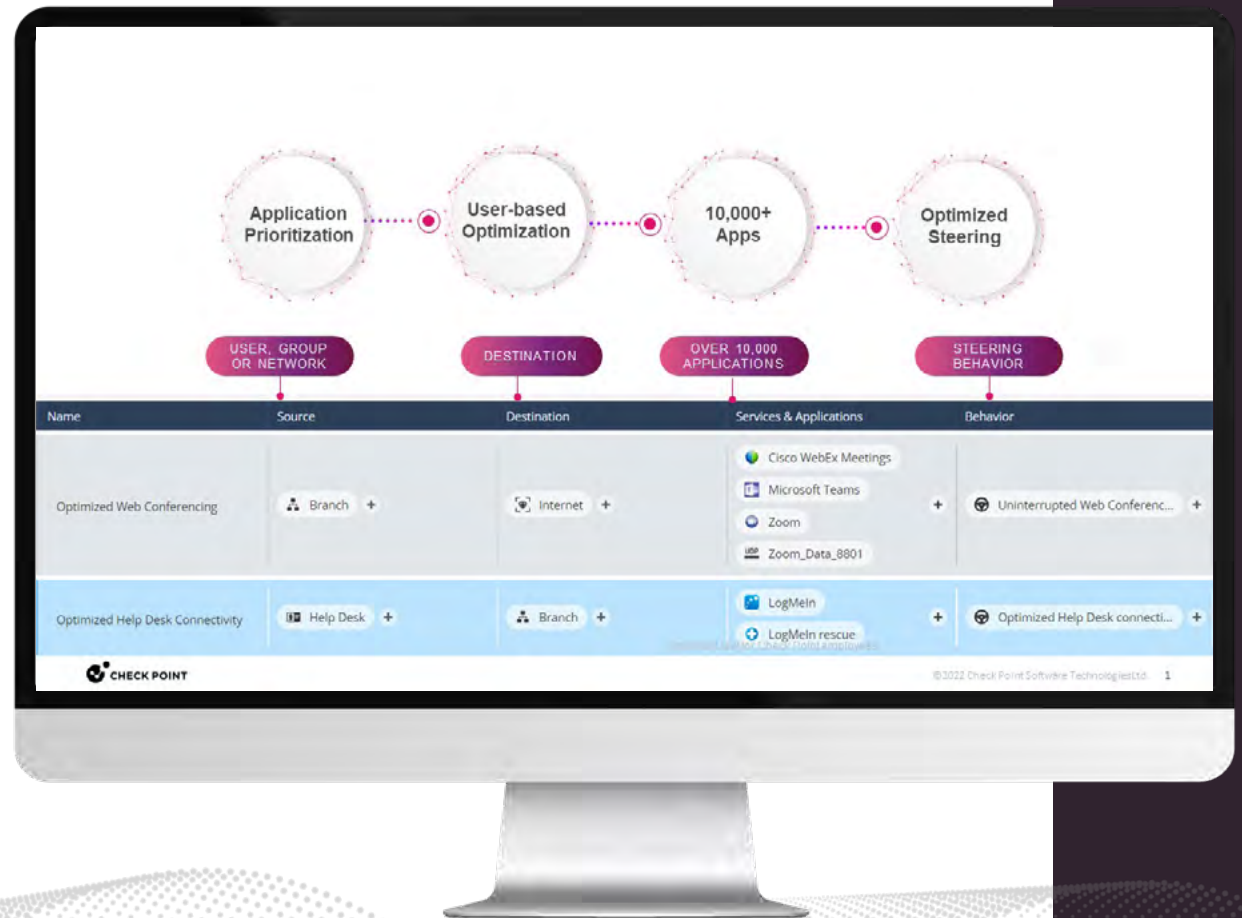
# SD-WAN DEPLOYMENT

## 3 | Define the Network Policy

### Step 3

Next, define how you want to steer network traffic. Source, destination and service objects shared with security management match on the first packet. Traffic sources can be a user, user group or branch/site.

For granular control select from 10,000+ apps in the security management library.



# SD-WAN DEPLOYMENT

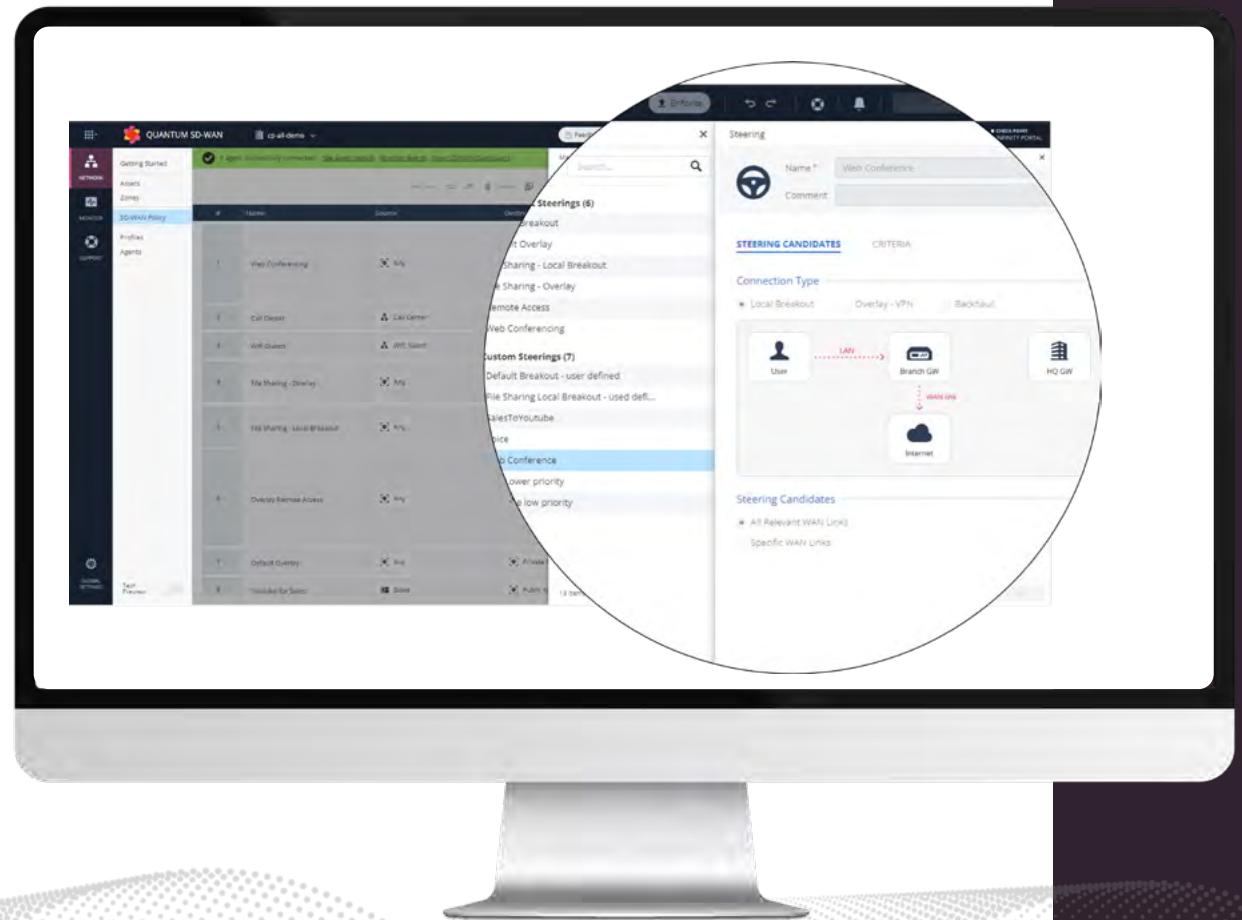
## 3-A | Customize Default Steering Behaviors

### Step 3-A

Customize the default steering behaviors to ensure traffic dynamically fails over to another link when network performance falls below an optimum service level.

Steering candidates include the 3 steering behaviors: local breakout, VPN overlay and backhaul.

Criteria include the links and their performance SLAs.



# SD-WAN DEPLOYMENT

## 3-B | Customize Your Steering SLAs

### Step 3-B

#### Define SLAs for Dynamic Auto-Steering

SD-WAN, with its real-time monitoring of SLA parameters, such as latency, jitter, and packet loss, empowers businesses to intelligently route traffic based on connection quality.

By analyzing these metrics across network links, SD-WAN selects paths with lower latency, minimal jitter, and minimal packet loss, thereby improving data transmission speed, ensuring reliable performance for time-sensitive applications, and delivering a seamless user experience.

With its dynamic routing capabilities, SD-WAN optimizes network resources by leveraging multiple connection options, allowing organizations to prioritize critical applications and achieve enhanced application performance.

#### Aggregate Bandwidth

Ensure the ability to aggregate link capacity utilizing links from multiple service providers. Bandwidth aggregation eliminates the need to designate redundant tunnels that sit idle in active/standby mode until needed.

The screenshot displays the 'Steering' configuration window. At the top, there's a 'Name' field set to 'Optimized Web Conferencing' and an empty 'Comment' field. Below this, the 'CRITERIA' tab is selected, showing 'STEERING CANDIDATES' and 'CRITERIA' sub-tabs. Under 'Thresholds', a note states: 'Connection will be steered to WAN links that meet the following thresholds:'. Three input fields are shown: 'Latency up to:' with a value of 150 ms, 'Jitter up to:' with a value of 30 ms, and 'Packet Loss up to:' with a value of 1 %. Below this, the 'WAN Link Utilization' section has two radio buttons: 'Link Aggregation - Use all WAN Links that meet the threshold' (unselected) and 'Prioritize - Select WAN Link based on tiebreakers' (selected). Under 'Prioritize', there are two sub-options: 'Link attributes' (selected) and 'Manual order of WAN Links'. A table is shown with columns: 'Priority', 'Attribute', and 'Margin'. The table contains three rows: 1. Priority 1, Attribute 'Latency (ms)', Margin 10. 2. Priority 2, Attribute 'Packet Loss (%)', Margin 1. 3. Priority 3, Attribute 'Jitter (ms)', Margin 3. At the bottom right are 'CANCEL' and 'OK' buttons.

Priority	Attribute	Margin
1	Latency (ms)	10
2	Packet Loss (%)	1
3	Jitter (ms)	3

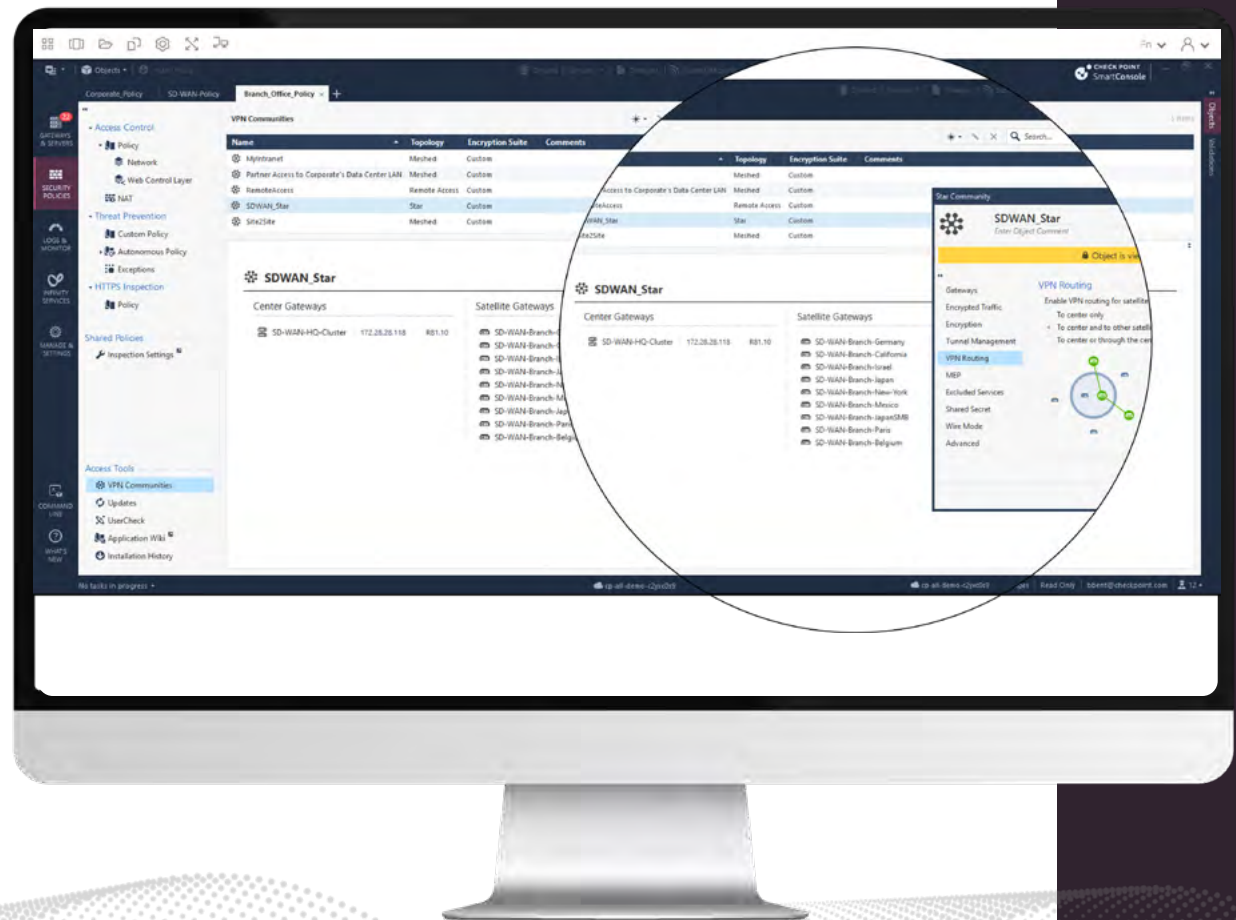


# SD-WAN DEPLOYMENT

## 3-C | Configure the VPN Overlay and Backhaul

### Step 3-C

Configuring the VPN overlay is done in security management where the VPN community is set. In this case a star topology connects all remote sites with headquarters, encrypting traffic within a VPN. Traffic is routed between remote sites via a central hub. This is also used to backhaul traffic from remote sites through headquarters to the Internet if a local Internet breakout link fails.



# MONITOR YOUR WIDE AREA NETWORK TRAFFIC

## Advanced Analytics

Advanced real-time monitoring and analytics should be easily available on a dedicated dashboard. Look for live monitoring of link SLAs (also called thresholds), analytics on link swaps and overall network health.

This provides both an at-a-glance overview with the ability to drill down for more detail, if needed, to maintain branch connectivity.



Branch-level visibility with central management

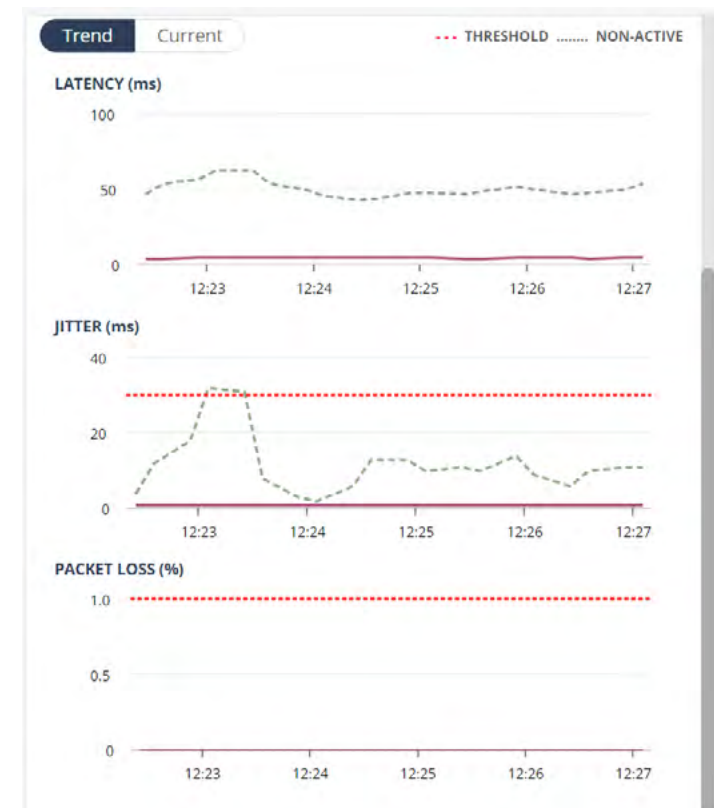
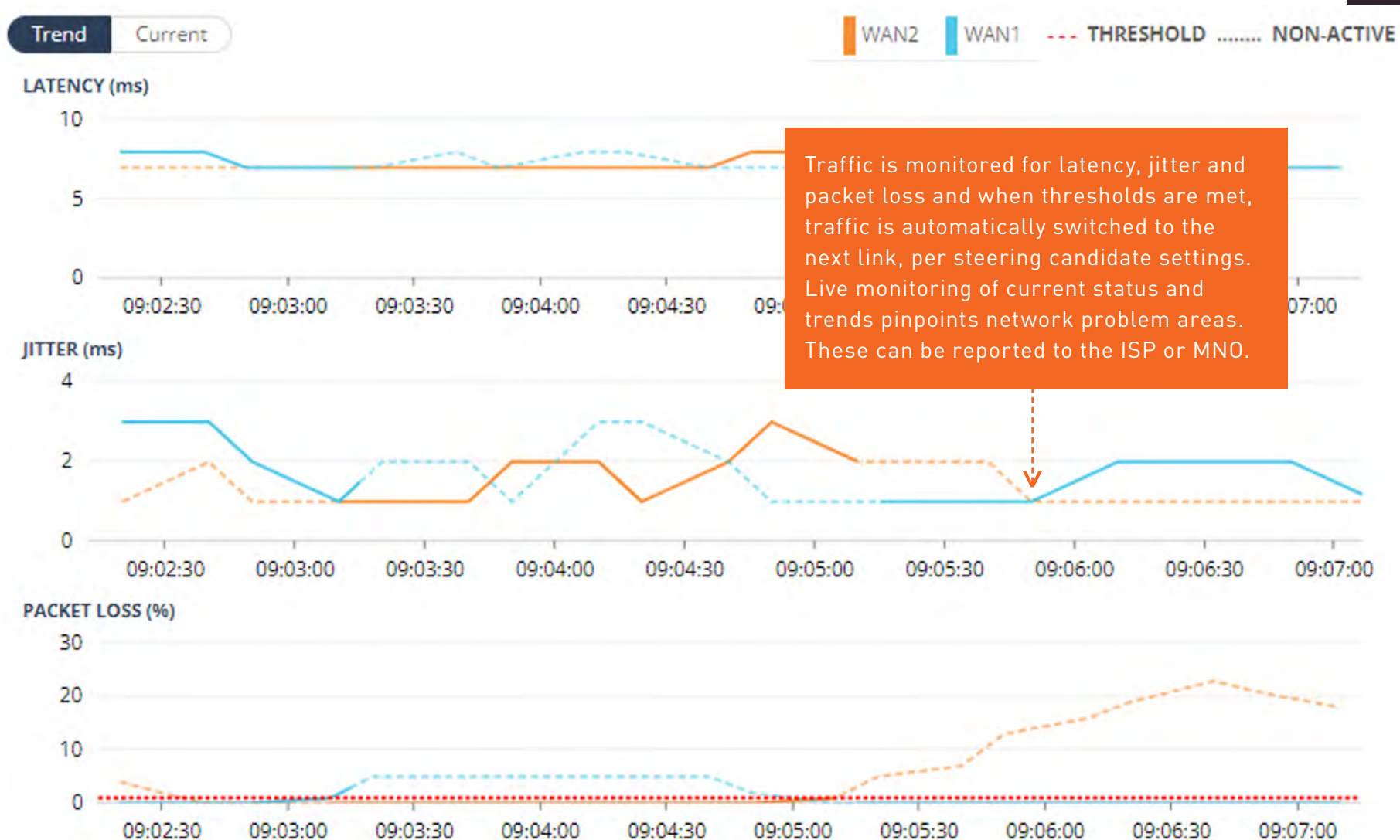


Figure 2: Monitor link health against target thresholds

## Monitor Link Health

Traffic should be monitored for latency, jitter or packet loss to enable automated link swapping, switching from one link to another when defined traffic thresholds are exceeded.

# LIVE MONITORING OF DYNAMIC LINK SWAPS



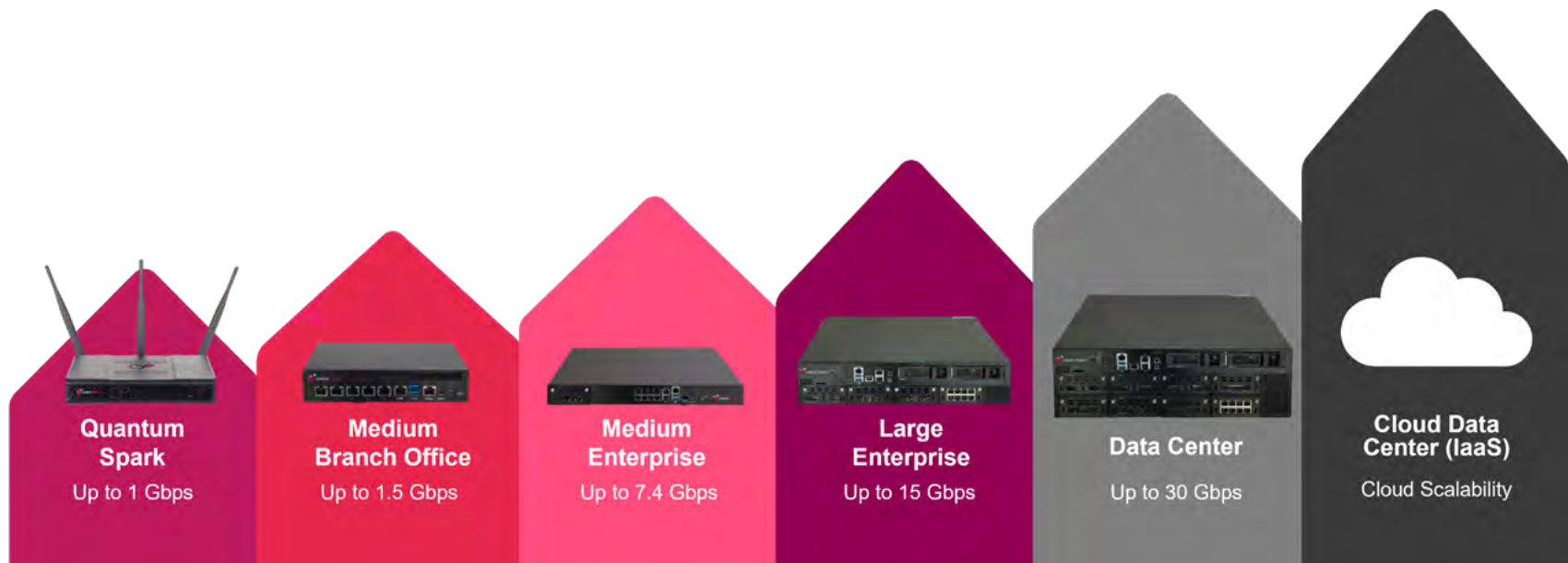


# GET STARTED WITH QUANTUM SD-WAN

## IMPROVE PERFORMANCE AND LOWER COSTS IN 3 EASY STEPS

If Check Point Quantum Firewalls are already deployed, SD-WAN can be activated on the current appliance. No additional hardware is required.

- 1 | Create a Cloud Services Account  
[portal.checkpoint.com](https://portal.checkpoint.com)
- 2 | Select Quantum SD-WAN
- 3 | Connect to Smart-1





## INTEGRATING SD-WAN SECURITY

### WHY IT MATTERS

Securing a variety of locations, connections and applications that make up internal networks and the network edge can quickly become complicated. Most SD-WAN vendors include a level of basic security, leaving organizations to fill in gaps by deploying multiple solutions across their infrastructure. However, this "patchy integration" approach presents challenges.

## MEET QUANTUM SD-WAN

Quantum SD-WAN is a software blade in Quantum Gateways that unifies the best security with optimized internet and network connectivity.

Deployed at the branch level, it provides comprehensive prevention against zero-day, phishing, and ransomware attacks, while optimizing routing for users and over 10,000 applications.

To ensure uninterrupted web conferencing, the solution monitors internet connectivity for latency, jitter, and packet loss, performing sub-second failover for unstable connections.

For consistent protection and connectivity across users and branch offices, Quantum SD-WAN and Harmony Connect (SSE) combine to deliver a complete security and internet access solution (SASE) managed from the Check Point Infinity cloud platform.

**To learn more about Quantum SD-WAN, visit:**

<https://www.checkpoint.com/quantum/sd-wan/>

**Or sign up for a demo here:**

<https://pages.checkpoint.com/quantum-sd-wan-demo-request.html>

**To explore all our SD-WAN security solutions, visit:**

<https://www.checkpoint.com/solutions/sd-wan-security/>

