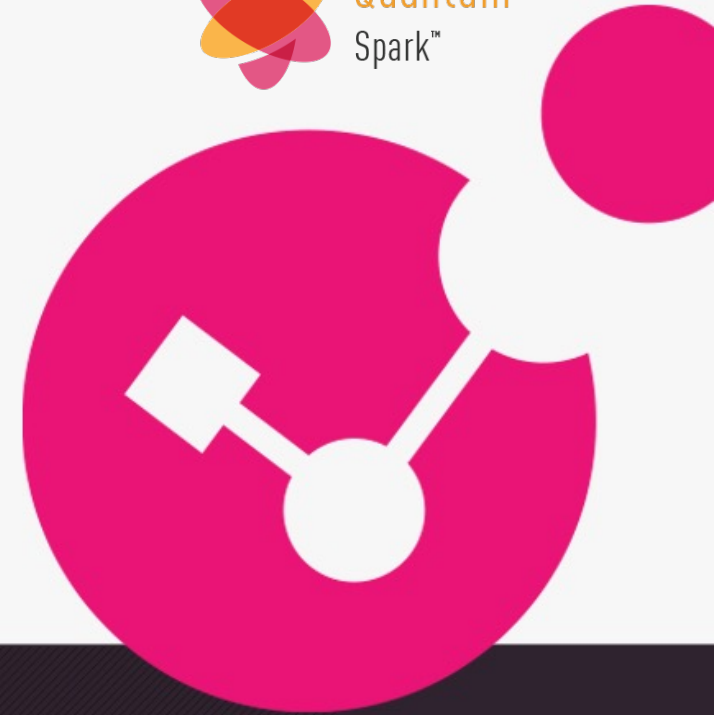




# SMB MASTERS #2

Sparkling Innovations for 2023



YOU DESERVE THE BEST SECURITY

# Agenda

- Welcome
- Quantum Spark 1500 Pro Series
- Latest Features of R81.10.05
- Quantum SD-WAN and IoT Protect
- Infinity Spark
- 2023 Spark Roadmap

# Introducing Quantum Spark 1500 Pro line

Industry's first gateway with integrated AI security, 5G, and Wi-Fi 6

**WiFi 6**

4x better in  
dense environments

**5G**

Cellular  
1Gbps throughput



AI powered  
security



Optimal App  
Performance

**2.8Gbps**  
Firewall

**900Mbps**  
Threat Prevention

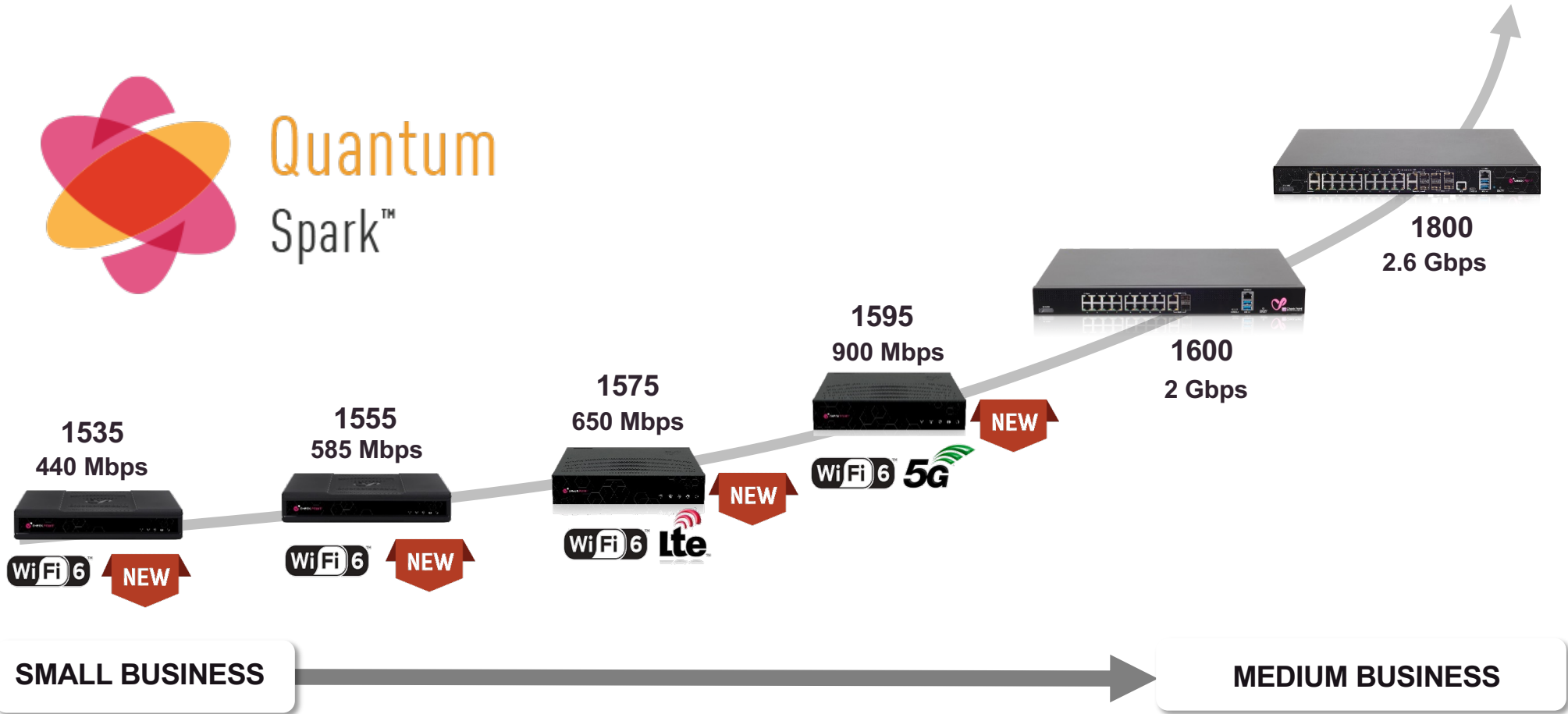
**2x**  
Capacity  
& User Support



# Quantum Spark 1500 Pro



Quantum  
Spark™



# New Features in Quantum Spark R81.10.05

## For SMB Market / Locally managed gateways:

- Two Factor authentication via SMS and email for VPN remote users (worldwide support)
- Easy deployment and use of SSL inspection,
- Enhanced Cluster configuration via WebUI
- Performance boost using Smart Accel engine
- Dr. Spark and Dr.Load

# New Features in Quantum Spark R81.10.05

## For Enterprise Branches (Centrally Managed)

- SD-Wan
- IoT Protect

# Smart Accel

The screenshot displays the configuration interface for Smart Accel on the Quantum Spark Security Gateway. The left sidebar contains navigation options: HOME, DEVICE, ACCESS POLICY (highlighted with a red box), THREAT PREVENTION, VPN, USERS & OBJECTS, and LOGS & MONITORING. The main content area is titled "Smart Accel: Improves connectivity and optimizes the load on the Quantum Spark Security Gateway". It features a sub-section "Smart Accel Services" (highlighted with a red box) with a toggle switch set to "OFF" and a "Services" icon. Below this, it indicates "12/15 services selected". A "Policy Bypass" section is also visible.

Smart Accel: Improves connectivity and optimizes the load on the Quantum Spark Security Gateway

Smart Accel Services

OFF Services

12/15 services selected


Policy Bypass


# Smart Accel

The screenshot shows the configuration page for Smart Accel in a security gateway. The left sidebar contains navigation options: HOME, DEVICE, ACCESS POLICY (highlighted), THREAT PREVENTION, VPN, USERS & OBJECTS, and LOGS & MONITORING. The main content area is titled "Smart Accel: Improves connectivity and optimizes the load on the Quantum Spark Security Gateway". It features a "Smart Accel Services" section with a toggle switch set to "ON" and a "Services" icon, indicating that 12/15 services are selected. Below this is a "Policy Bypass" section.

Smart Accel: Improves connectivity and optimizes the load on the Quantum Spark Security Gateway

Smart Accel Services

ON  Services


 12/15 services selected


Policy Bypass



# Smart Accel


Smart Accel Services











ON  Services

 12/15 services selected

Policy Bypass

SMART ACCEL SERVICES

Type to filter 

<input type="checkbox"/>	Name
<input type="checkbox"/>	 Corporate Services
<input type="checkbox"/>	 Apple
<input checked="" type="checkbox"/>	 Check Point services
<input checked="" type="checkbox"/>	 Google services
<input checked="" type="checkbox"/>	 Microsoft Updates
<input checked="" type="checkbox"/>	 Media Streaming Services
<input checked="" type="checkbox"/>	 Amazon Prime
<input checked="" type="checkbox"/>	 Disney Plus
<input checked="" type="checkbox"/>	 Netflix
<input checked="" type="checkbox"/>	 Spotify

Apply  Cancel

# SSL Inspection by Device Type

SSL Inspection Policy: Inspect outgoing traffic that is encrypted by the Secure Sockets Layer (SSL) protocol

SSL traffic inspection  
 HTTPS Categorization  
 Off

SSL Inspection  
To deploy SSL inspection, download CA certificate and install it on the hosts behind this gateway | [More info...](#)  
[Download CA Certificate](#)

Protocols to inspect  
 HTTPS  IMAPS  POP3S

Assets to inspect  
 Desktop  Computer  Laptop  Inspect other assets...  All assets

SSL traffic inspection bypass policy

Wireless networks to bypass:  
 Trusted networks  
 Untrusted networks

Categories to bypass:  
 Health  Media Streams  
 Government/Military  Well known update services | [More info](#)  
 Financial Services  Bypass other categories and sites...

Assets to bypass:  
 MacOS  
[Bypass by MAC](#) | [Bypass by IP](#)

Tracking  
 Enable inspect logs  
 Enable bypass logs  
 Enable wireless bypass logs

# SSL Inspection by Device Type

The screenshot displays the 'SSL Inspection Policy' configuration page in the Check Point management console. The left-hand navigation pane shows the following menu items: HOME, DEVICE, ACCESS POLICY (highlighted with a red box), THREAT PREVENTION, VPN, USERS & OBJECTS, and LOGS & MONITORING. Under 'ACCESS POLICY', the sub-menu includes Firewall (Blade Control, Policy, Servers, NAT, VoIP, Smart Accel), User Awareness (Blade Control), QoS (Blade Control, Policy), and SSL Inspection (Policy, Exceptions, Advanced). The 'Policy' item under 'SSL Inspection' is highlighted with a red box.

The main content area is titled 'SSL Inspection Policy: Inspect outgoing traffic that is encrypted by the Secure Sockets Layer (SSL) protocol'. It features the following sections:

- SSL Inspection:** Includes radio buttons for 'SSL traffic inspection' (selected and highlighted with a red box), 'HTTPS Categorization', and 'Off'. A 'Download CA Certificate' button is also present.
- Protocols to inspect:** Includes checkboxes for 'HTTPS' (checked), 'IMAPS', and 'POP3S'.
- Assets to inspect:** Includes checkboxes for 'Desktop', 'Computer', and 'Laptop' (all checked). It also features 'Inspect other assets...' (highlighted with a blue box) and 'All assets' (highlighted with a purple box).
- SSL traffic inspection bypass policy:**
  - Wireless networks to bypass:** Includes checkboxes for 'Trusted networks' and 'Untrusted networks'.
  - Categories to bypass:** Includes checkboxes for 'Health' (checked), 'Government/Military' (checked), 'Financial Services' (checked), 'Media Streams', 'Well known update services | More info', and 'Bypass other categories and sites...'.
  - Assets to bypass:** Includes a checkbox for 'MacOS' and links for 'Bypass by MAC' and 'Bypass by IP'.
- Tracking:** Includes checkboxes for 'Enable inspect logs', 'Enable bypass logs', and 'Enable wireless bypass logs' (all checked).

# SSL Inspection by Device Type

The screenshot displays the 'SSL Inspection by Device Type' configuration page. The background shows various settings for protocols, assets, bypass policies, and tracking. A modal dialog box titled 'OTHER ASSETS' is open, showing a search bar and a list of asset types. The 'Asset Type' header is selected, and the list includes Alarm, Arduino, Audio player, AV Receiver, Baby monitor, Barcode scanner, and Cable box. Below the list, three items are selected: Computer, Desktop, and Laptop. The 'Apply' button is highlighted.

**Protocols to inspect**

- HTTPS
- IMAPS
- POP3S

**Assets to inspect**

- Desktop
- Computer
- Laptop
- Inspect other assets...

**SSL traffic inspection bypass policy**

**Wireless networks to bypass:**

- Trusted networks
- Untrusted networks

**Categories to bypass:**

- Health
- Government/Military
- Financial Services
- Media Streams
- Well known update services
- Bypass other categories and

**Assets to bypass:**

- MacOS

[Bypass by MAC](#) | [Bypass by IP](#)

**Tracking**

- Enable inspect logs
- Enable bypass logs
- Enable wireless bypass logs

# Two Factor Authentication by Email and SMS

The screenshot displays the configuration interface for VPN Remote Access Control on a Quantum Spark 1590 Appliance. The interface is accessed via a web browser at the URL `https://172.28.32.55:4434/?token=ab003b4757fc1ef8575be865305bb78#app.VPNRemoteAccess`. The left sidebar shows navigation options: HOME, DEVICE, ACCESS POLICY, THREAT PREVENTION, VPN, USERS & OBJECTS, and LOGS & MONITORING. The main content area is titled 'VPN Remote Access Control' and includes a 'Remote Access' toggle set to 'On'. Below this, there are informational messages: 'No local users and groups are defined with VPN Remote Access permissions' and 'Static IP for Remote Access: 172.28.32.55'. There are three checked checkboxes: 'Allow traffic from Remote Access users', 'Log traffic from Remote Access users', and 'Require users to confirm their identity using two-factor authentication | Configure...'. The 'VPN Remote Access users can connect via:' section lists four options: 'Check Point VPN clients' (checked), 'Mobile client' (checked), 'SSL VPN' (unchecked), and 'Windows VPN Client' (unchecked). At the bottom of the configuration area, there are 'Apply' and 'Cancel' buttons. The status bar at the bottom indicates 'Internet connected' and 'Up to date' at 09:27 AM.

# Two Factor Authentication by Email and SMS

The screenshot displays the Check Point Quantum Spark VPN Remote Access Control interface. A modal window titled "TWO-FACTOR AUTHENTICATION SETTINGS" is open, showing the "Configuration" tab. The "SMS" checkbox is checked, and the "Use Check Point SMS provider service" radio button is selected. The "Message" field for SMS is populated with "Check Point remote access verification code:". The "Email - Using Check Point email provider service" checkbox is unchecked. The "Message" field for email is empty. The "Apply" and "Cancel" buttons are visible at the bottom of the modal and the main interface.

VPN Remote Access Control

Remote Access

On

Off

VPN Remote Access users can connect via:

- Check Point VPN clients
- Mobile client
- SSL VPN
- Windows VPN Client

**TWO-FACTOR AUTHENTICATION SETTINGS**

Configuration Advanced

SMS

Use Check Point SMS provider service

Use external SMS provider

DynamicID URL:

Provider user name:

Provider password:

API ID:

Message: Check Point remote access verification code:

Email - Using Check Point email provider service

Message:

Apply Cancel

Apply Cancel

Internet connected

Up to date 09:27 AM

# Two Factor Authentication by Email and SMS

The screenshot displays the Check Point Quantum Spark 1590 Appliance interface for VPN Remote Access Control. A modal window titled "TWO-FACTOR AUTHENTICATION SETTINGS" is open, showing configuration options for SMS and Email. The "Email - Using Check Point email provider service" option is checked and highlighted with a red box. The "SMS" option is also checked, but the "Use External SMS provider" radio button is selected. The "Message" field for the email provider is empty.

VPN Remote Access Control

Remote Access: On

VPN Remote Access users can connect via:

- Check Point VPN clients
- Mobile client
- SSL VPN
- Windows VPN Client

**TWO-FACTOR AUTHENTICATION SETTINGS**

Configuration | Advanced

SMS

Use Check Point SMS provider service

Use External SMS provider

DynamicID URL:

E.g. https://api.example.com/http/sendmsg?api\_id=\$APIID&user=\$USERNAME&password=\$PASSWORD&to=\$PHONE&text=\$MESSAGE

Provider user name:

Provider password:

API ID:

Message:

Email - Using Check Point email provider service

Message:

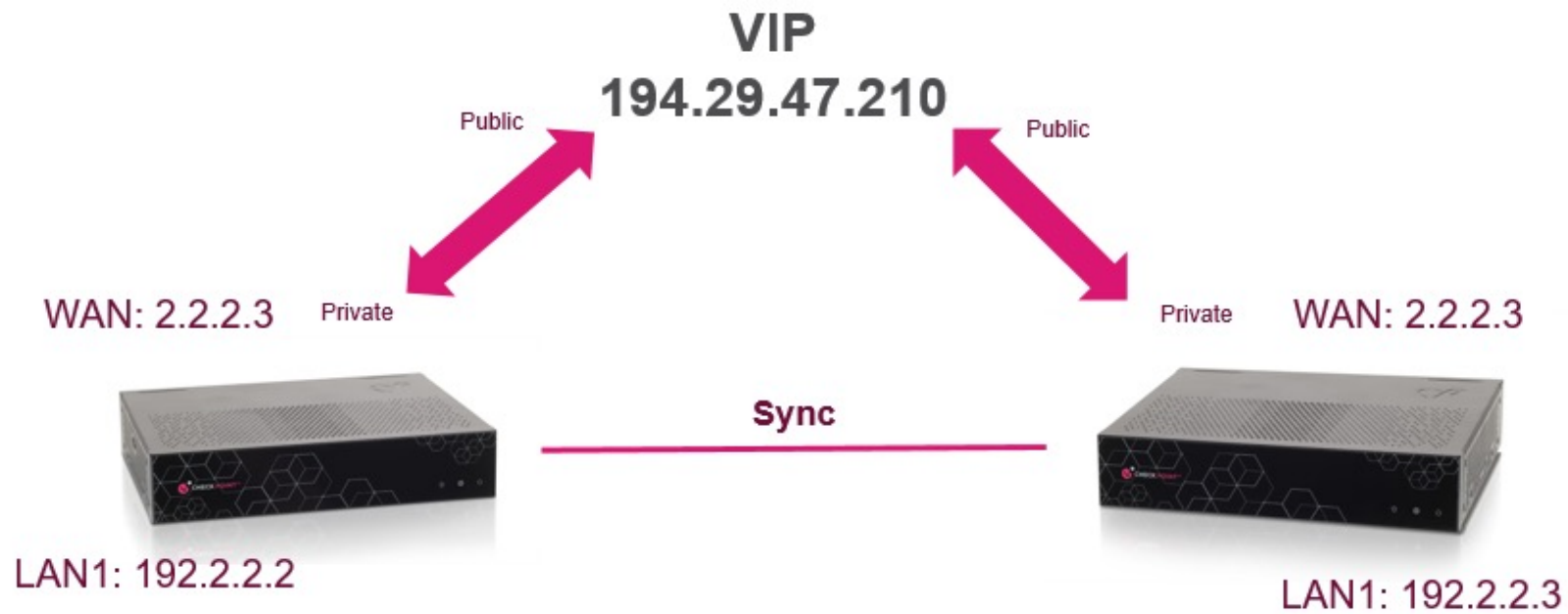
Apply Cancel

Apply Cancel

Internet connected | Up to date | 09:28 AM

# CLUSTER ENHANCEMENTS

## Scope Local





# Configuration sync between cluster members

New local connection on the Active member (still private):

Name	Local IP Address	Subnet Mask	MAC Address	Status
LAN1 (High Availability)	192.168.1.101	255.255.255.0	08:1c:75:95:ed:7c	Disabled
LAN2 (Sync)	10.231.148.1	255.255.255.0	08:1c:75:95:ed:7c	2.3 Giga/Full Duplex
LAN3 (High Availability)	3.3.3.101	255.255.255.0	08:1c:75:95:ed:7c	1 Giga/Full Duplex
LAN3.385 (High Availability)	85.85.85.101	255.255.255.0	08:1c:75:95:ed:7c	Up
LAN3.386	86.86.86.101	255.255.255.0	08:1c:75:95:ed:7c	Up
LAN4			08:1c:75:95:ed:7c	Disabled
LAN5			08:1c:75:95:ed:7c	Disabled
LAN6			08:1c:75:95:ed:7c	Disabled
LAN7			08:1c:75:95:ed:7c	Disabled
LAN8			08:1c:75:95:ed:7c	Disabled
LAN9			08:1c:75:95:ed:7c	Disabled
LAN10			08:1c:75:95:ed:7c	Disabled
LAN11			08:1c:75:95:ed:7c	Disabled
LAN12			08:1c:75:95:ed:7c	Disabled
LAN13			08:1c:75:95:ed:7c	Disabled
LAN14			08:1c:75:95:ed:7c	Disabled
LAN15			08:1c:75:95:ed:7c	Disabled
LAN16			08:1c:75:95:ed:7c	Disabled
LAN17			08:1c:75:95:ed:7c	Disabled
LAN18			08:1c:75:95:ed:7c	Disabled

New connection view on High Availability screen:

Name	Status	IP Address	Member IP Address
LAN1	High Availability	192.168.1.101/24	Primary: 192.168.1.101, Secondary: 192.168.1.102
LAN2	Sync		Primary: 10.231.148.1, Secondary: 10.231.148.2
LAN3	High Availability	3.3.3.101/24	Primary: 3.3.3.101, Secondary: 3.3.3.102
LAN3.385	High Availability	85.85.85.101/24	Primary: 85.85.85.101, Secondary: 85.85.85.102
LAN3.386	Non-HA	86.86.86.101/24	
Internet2	High Availability	10.75.32.89/24	Primary: 10.75.32.87, Secondary: 10.75.32.88

# Dr.Spark

The screenshot displays the Quantum Spark 1595 Appliance web interface. The top navigation bar includes the user 'admin', 'Log Out', and 'Help / Support' links. The left sidebar contains a menu with categories: HOME, DEVICE (highlighted), ACCESS POLICY, THREAT PREVENTION, VPN, and USERS & OBJECTS. The main content area is divided into 'Network' and 'System' sections. Under 'Tools', several diagnostic utilities are listed, with 'Generate Dr. Spark Report' and 'Dr. Spark - Load' highlighted with red boxes. Below the tools list, there are sections for 'Ping or Trace an IP Address' and 'Perform a DNS Lookup'.

Quantum Spark  
1595 Appliance

admin | Log Out | Help / Support

- Network
  - Internet
  - Wireless
  - Local Network
  - Hotspot
  - MAC Filtering
  - DNS
  - Proxy
- System
  - System Operations
  - Administrators
    - Administrator Access
    - Device Details
    - Date and Time
    - DDNS & Device Access
  - Tools
- Advanced Routing

Tools: Various Tools used to diagnose problems with the appliance

- Monitor System Resources: Display CPU usage, memory usage and processes
- Show Routing Table: Display the routing table of the gateway
- Show Router Configuration: Show router configuration for specific protocol/settings
- Test Cloud Services Ports: Verify that the appliance could connect to Cloud Services
- Tcpdump Tool: Packet Capture
- DSL Statistics
- Monitor Cellular Modem
- Generate CPIInfo File
- Generate Dr. Spark Report**
- Dr. Spark - Load**

Ping or Trace an IP Address

Host name or IP address:  Ping Traceroute

Perform a DNS Lookup

# Dr.Spark



**Dr. Spark - 2023-01-24 21:58:58**

Generated with Dr. Spark version 992002379 on locally Quantum Spark version: R81.10.05 build number : 200

V1-WiFi6-5G

✕

- ▼ Policy and Configuration i
- Administrator Security Settings i
- Policy Status ✔
- Access Rule ✔
- Certificates ✔
- RAD Daemon Status i
- MultiWstlsd Check i
- Internet Object ✔
- Certificates Expiration i
- ▼ Status !

### Policy Status

— Summary

Test passed.  
There is no policy installation issue.

### Access Rule

— Summary

Test passed.  
Illegal access rules was not found.

# Dr.Load

## Gateway Performance:

Number of hosts: 38

Number of connections: 1346

Connection rate: 2326 per second

Throughput:

Receive: 189765 Kbps

Transmit: 228976 Kbps

Packet Rate:

Receive: 679 packets per second

Transmit: 989 packets per second

SSL is disabled

-----Blade Status-----

VPN-RA is disabled

VPN-S2S is disabled

NGTP is active

----CPU and Memory----

Available CPU: 30.14%

Available memory on the Gateway: 965324 KB

Fw1 memory consumption: 14%

SFWD memory consumption: 140972 KB

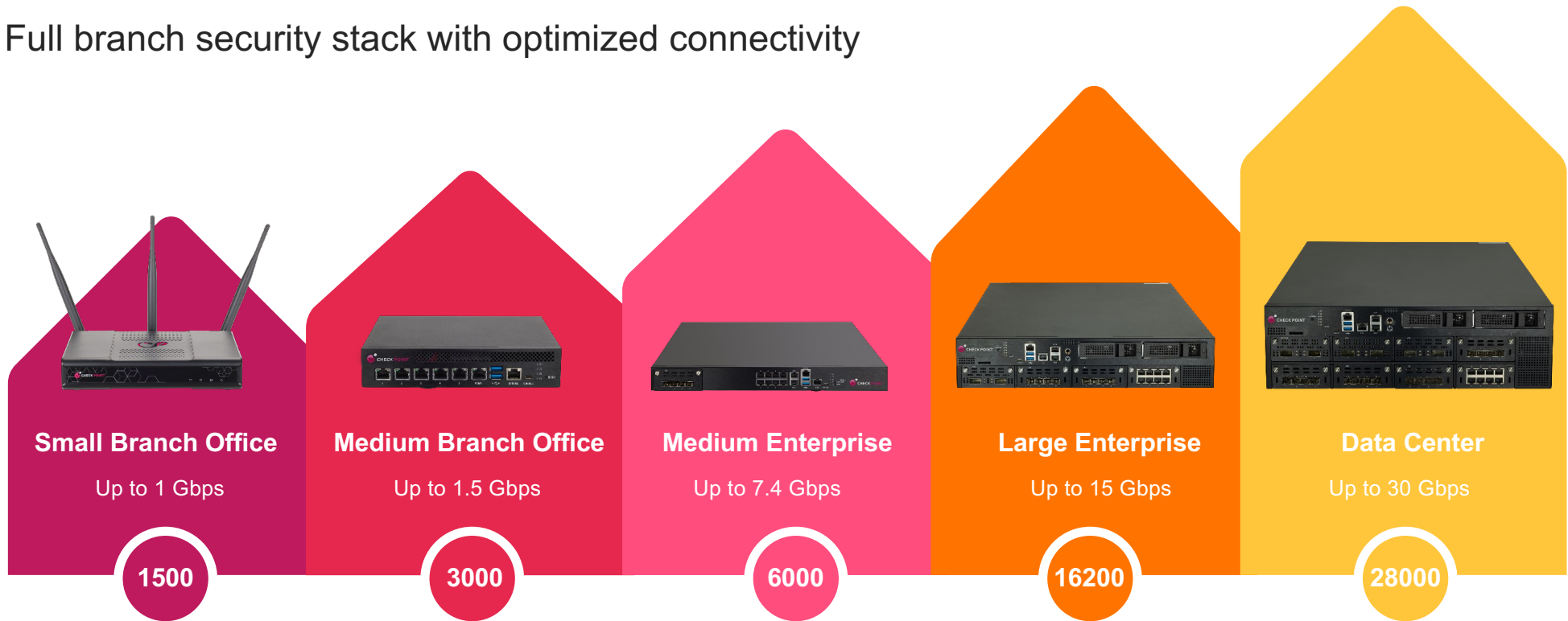
SD-WAN AND IOT SECURITY FOR  
CENTRALLY MANAGED GATEWAYS

**QUANTUM SD-WAN AND  
QUANTUM IOT PROTECT**

# Supported in a broad range of Spark and Quantum Gateways



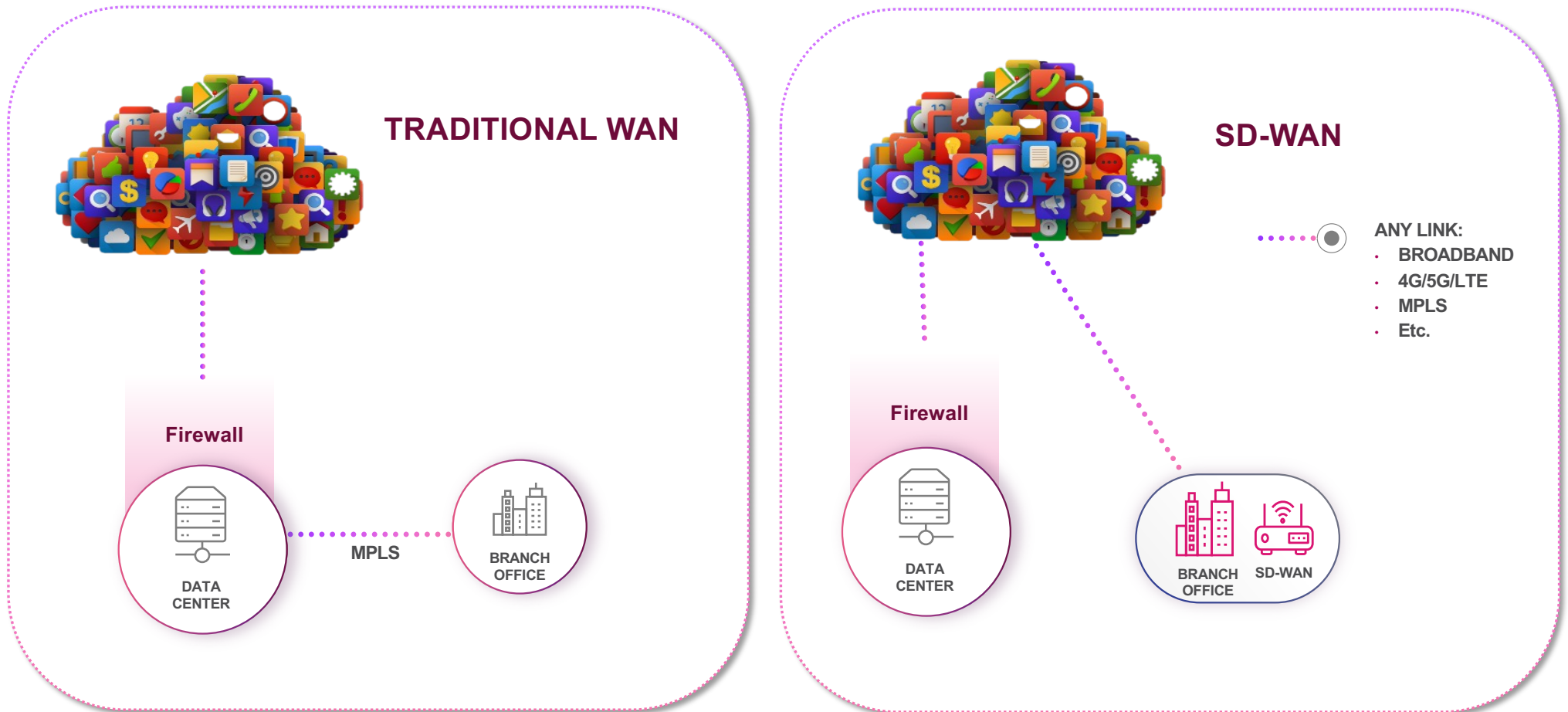
Full branch security stack with optimized connectivity



**THREAT PREVENTION + IoT Security/SD-WAN\* THROUGHPUT**

\*estimated

# CLOUD ADOPTION REQUIRES A NEW NETWORK ARCHITECTURE: SD-WAN



# Unifying best security with optimized internet and network connectivity

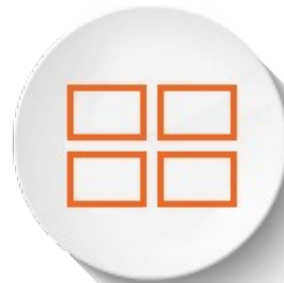


UNCOMPROMISING  
**BRANCH SECURITY**



**Prevent** attacks on the branch -  
zero-days, phishing, ransomware

**NO MORE ZOOM™**  
INTERRUPTIONS



**Rich capabilities:**  
sub-second failover, optimized  
policies for 10,000+ apps

A COMPLETE  
**SASE SOLUTION**



**Complete** Security + Internet  
Access Solution (SASE)



The SD-WAN software blade is  
**AVAILABLE TODAY**  
as a service,  
at a simple monthly price



Starting at  
**\$14.8**  
Per Month

## **SD-WAN**

Blade for Small Branch

**1535**  
Base Appliance



Starting at  
**\$328**  
Per Month

## **SD-WAN**

Blade for Enterprise

**6200**  
Enterprise Appliance



Introducing Quantum IoT Protect

The **Only** Autonomous  
IoT Threat Prevention



Quantum  
IoT Protect



# Autonomous Protection for IoT Devices

1 MAP, ASSESS & PROFILE

Asset Type	Count	Recently discovered
Smart Locks	1,024	24
Printers	282	8
IP Cameras	176	8
Smart TVs	24	...
Projectors	18	18 (NEW)
Coffee Machines	16	...
Smoke Alarm Detector	10	10

2 AUTONOMOUS ZERO-TRUST NETWORK PROFILES



Printers Practices Assets 164

GENERAL ACCESS CONTROL PRACTICES BEHAVIORS EVENTS

IoT Best Practice Mode: Prevent

Access to internet Mode: As top level

Discovered printers will be able to access only approved destinations (traffic to other destinations will be blocked)

Name	Destination	Service	Description
Brother			
Canon			
HP			
Notification	*hpeprint.com	HTTP HTTPS Jabber	HP ePrint Service Registration and getting notifications about pending printing tasks
Registration and pulling tasks	*hp.com	HTTP HTTPS Jabber	Registration, device configuration, pulling printing tasks and analytics
Telemetry and analytics	download.hpdaas.com	HTTP	Registration, device configuration, pulling printing tasks and analytics

Traffic to other destinations will be blocked

Accelerate Discovery & Protection - from Months to Minutes!

# Autonomous IoT Zero-Trust Network Profiles

Profiles are based on AI and behavioral analysis

Zero-Trust: Allow only necessary device communication

Threat prevention automatically enforced on new assets

The screenshot displays the configuration for 'Printers' in the Check Point management console. The profile is 'IoT Best Practice' and is set to 'Prevent' mode. The configuration is applied to 'Access to internet' with a mode of 'As top level'. A warning message states: 'Discovered printers will be able to access only approved destinations (traffic to other destinations will be block)'. Below this, a table lists the allowed services and destinations for HP printers.

Name	Destination	Service	Description
▶ Brother			
▶ Canon			
▼ HP			
Notification	*.hpeprint.com	HTTP HTTPS HP ePrint Service Jabber	Registration and getting notifications about pending printing tasks
Registration and pulling tasks	*.hp.com	HTTP HTTPS Jabber	Registration, device configuration, pulling printing tasks and analytics
Telemetry and analytics	download.hpdaas.com	HTTP	Registration, device configuration, pulling printing tasks and analytics

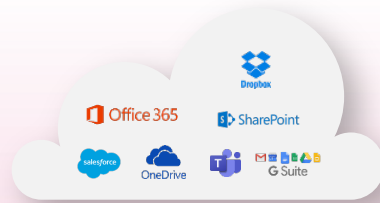
A final warning message at the bottom states: 'Traffic to other destinations will be blocked'.

**CHECK POINT**  
**INFINITY SPARK SECURITY**  
 Endpoint & Mobile | Email & Office | Network



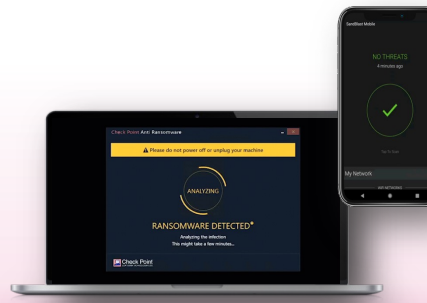
**Secure Your Network**

2.6 Gbps Threat Prevention  
 Performance, Fast Connectivity



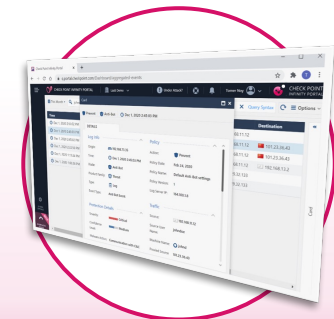
**Secure Your Mailbox & Apps**

99.2% reduction in email  
 phishing attacks



**Secure Your Devices**

Protect user devices against  
 ransomware, phishing and malicious  
 files and apps



**Unified MSP Management**

Decrease MSP operational  
 costs by 50%

# Infinity Spark Complete Security Package

One vendor for best SMB cyberattacks protection

1



**Quantum Spark 1550**  
Bundled for 10 Users  
\$8.90 per user/month

- 10 Endpoint Security Licenses
- 10 Mobile Security Licenses
- 10 Email & Office Licenses

**585 Mb/s Max Bandwidth**

2



**Quantum Spark 1570**  
Bundled for 25 Users  
\$7 per user/month

- 25 Endpoint Security Licenses
- 25 Mobile Security Licenses
- 25 Email & Office Licenses

**650 Mb/s Max Bandwidth**

3



**Quantum Spark 1590**  
Bundled for 50 Users  
\$7 per user/month

- 50 Endpoint Security Licenses
- 50 Mobile Security Licenses
- 50 Email & Office Licenses

**860 Mb/s Max Bandwidth**

4



**Quantum Spark 1600**  
Bundled for 100 Users  
\$6.64 per user/month

- 100 Endpoint Security Licenses
- 100 Mobile Security Licenses
- 100 Email & Office Licenses

**2Gb/s Max Bandwidth**

Protect Your  
Network | Laptops & Mobile Devices | Email & Office Apps

# Pay-As-You-Go for SMB Security

Early Availability

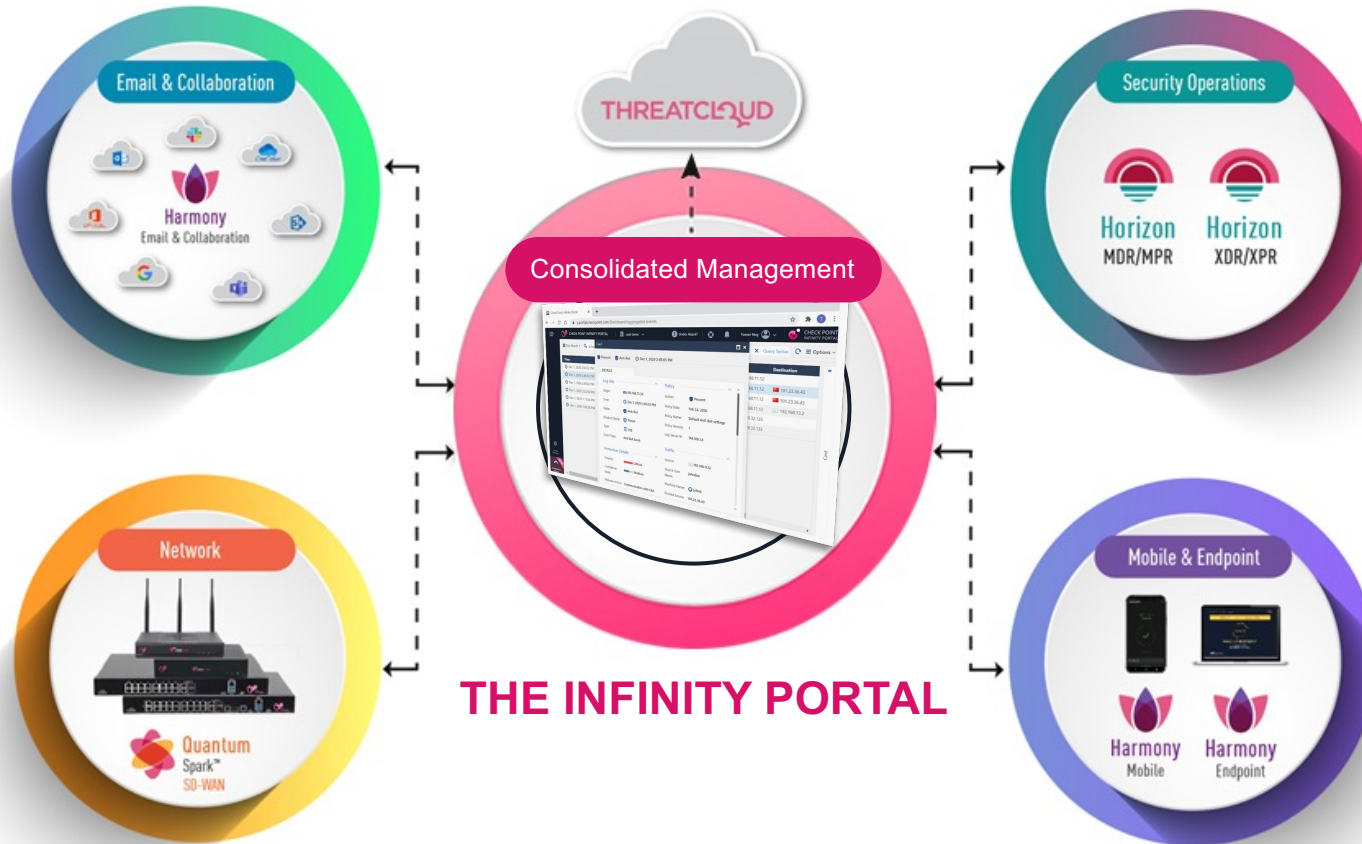
- 1 No minimum order
- 2 Manage from Check Point Infinity Portal
- 3 Grow or shrink at any time

The screenshot displays the 'USAGE' tab for an account named 'Optica'. The interface includes a navigation bar with 'ACCOUNT SETTINGS', 'ADMINISTRATORS', 'SERVICES & CONTRACTS', and 'USAGE'. Below the navigation bar, there is a dropdown menu set to 'This month', a 'License Report' icon, an 'Export' icon, and a search bar. The main content is a table with the following data:

Service name	Package	Avg. monthly usage	Yearly contracts	Monthly PAYG
Harmony Mobile		100 Devices	200	-
CloudGuard Network		50 devices	-	50
Harmony Endpoint	-	355 users	325	30
Harmony Endpoint	BASIC	300 users	300	-
Harmony Endpoint	ADVANCED	55 users	25	30

# Unified Infinity MSP Management for SMBs

SMP available!





# 2023 SPARK ROADMAP

## New Hardware

- **1595 WiFi6 + 5G**
  - WiFi6 4x4 WLE3000HX
  - LTE upgrade to 5G
  - DDR upgrade to 4GB
- **1595R**
  - Rugged Slim Appliance
  - Wired and 5G Flavors
  - FONIC support
- **SG2000**
  - Stronger SoC (24 cores)
  - 4x10GbE+SFP ports



# 2023 SPARK ROADMAP

## Planned Content for R81.10.10

- GRE
- BGP IPv6
- OSPFv3 IPv6
- Jumbo frame support
- Google Authenticator 2FA
- Reset password in WebUI
- Automatically block infected hosts
- Skyline
- Configure 2FA per user
- Bypass Threat Prevention under load
- Support Cluster XL in Bridge Mode
- VPN monitoring in SMP
- SD-WAN for Locally Managed
- IoT locally managed

2023 SPARK ROADMAP

# SD-WAN FOR LOCALLY MANAGED

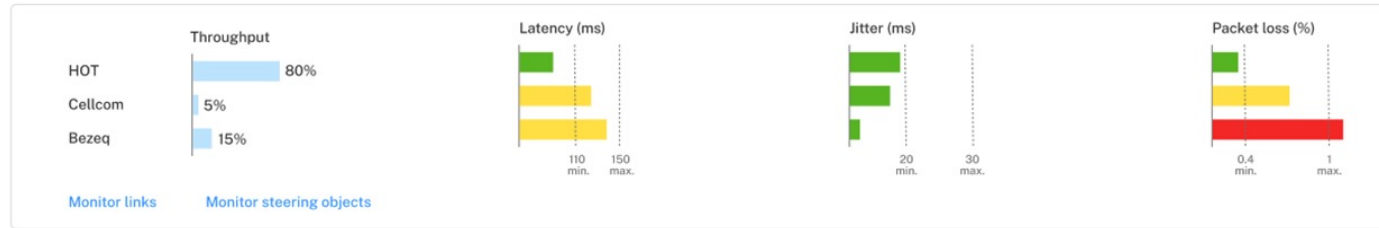
# SD-WAN

- > Home
- > Device
- > Assets & users
- > Access policy
- > Threat prevention
- > **Networking & SD-WAN**
  - > WAN
  - Internet
  - SD-WAN**
  - DNS & Proxy
  - > Local network
  - > Routing
  - > VPN
  - > Logs & monitoring

## SD-WAN Policy

Configure SD-WAN policy for steering traffic by services and applications

Enabled



🔍 Search 4 items

No.	Source	Destination	Application & Services	Steering Object
<b>Manual rules</b>				
1	Any	Internet	Amazon, Facebook, Zoom	appi_steering
<b>Smart SD-WAN rules</b> <input checked="" type="checkbox"/> Enabled				
2	LAN networks	Any	www File Share Pro	File Sharing - Local Breakouts
3	VPN Sites	Any	Zoom	Web Conferencing
4	Any	Any	Access Remote PC, Microsoft Remote Desktop Connection	Remote Access

# SMART SD-WAN

Quantum Spark VNF

HOME  
DEVICE  
ACCESS POLICY  
THREAT PREVENTION  
VPN  
USERS & OBJECTS  
LOGS & MONITORING

- Firewall
  - Blade Control
  - Policy
  - Servers
  - NAT
  - SD-WAN**
  - VoIP
  - Smart Accel
- User Awareness
  - Blade Control
- QoS
  - Blade Control
  - Policy
- SSL Inspection
  - Policy
  - Exceptions
  - Advanced

### SD-WAN

Configure SD-WAN

Smart SD-WAN

[Participating interfaces](#)  
WAN DMZ

[New](#) [Edit](#) [Monitor Links](#)

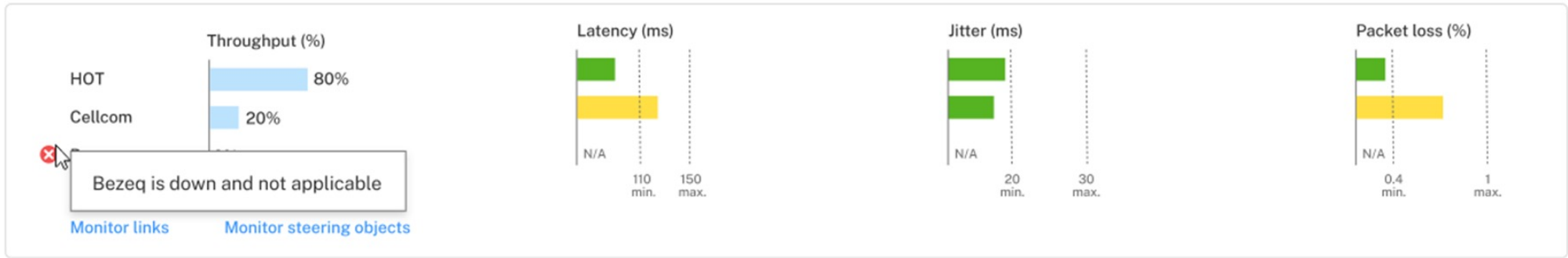
Priority	Source	Destination	Application / Service	Behavior
Custom rules				
Smart rules				
1	* Any	* Any	Skype Zoom Cisco Webex Teams Microsoft Teams	Web_Conferencing
2	* Any	* Any	Box Dropbox FTP Protocol-download UDP based FTP FTP Protocol over HTTP	File_Sharing
3	* Any	* Any	Microsoft Remote Desktop Connection Citrix LogMeIn GoToMyPC (Remote Desktop) TeamViewer	Remote_Access
4	* Any	* Any		Default_Breakout

# MONITORING LINKS

## SD-WAN Policy

Configure SD-WAN policy for steering traffic by services and applications

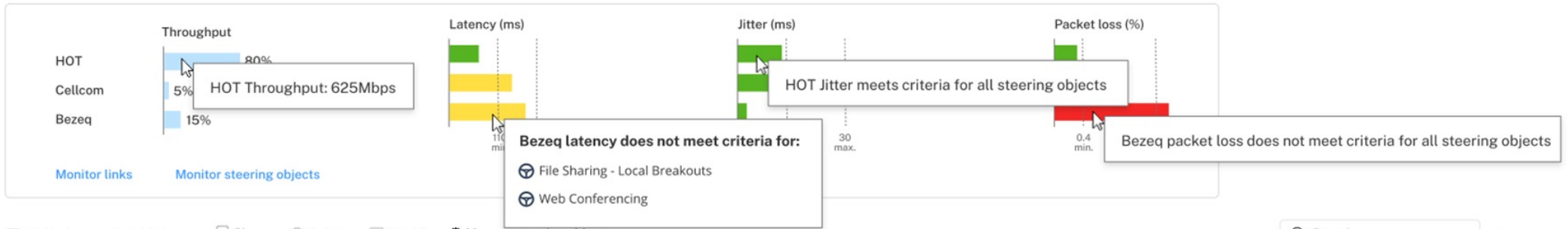
Enabled



## SD-WAN Policy

Configure SD-WAN policy for steering traffic by services and applications

Enabled



# MONITORING STEERING

Monitor steering objects ×

	HOT <sup>ⓘ</sup> Throughput 323Mbps	Cellcom <sup>ⓘ</sup> Throughput 410Mbps	Bezeq <sup>ⓘ</sup> <span style="color: red;">✘</span> Down
<input checked="" type="checkbox"/> File Sharing - Local Breakouts <sup>ⓘ</sup>	<span style="color: green;">✔</span> <b>Selected</b>	Not selected	N/A
<input checked="" type="checkbox"/> appi_steering <sup>ⓘ</sup>	<span style="color: green;">✔</span> <b>Selected</b>	Not selected	N/A
<input checked="" type="checkbox"/> Web Conferencing <sup>ⓘ</sup>	Not selected	<span style="color: green;">✔</span> <b>Selected</b>	N/A
<input checked="" type="checkbox"/> Remote Access <sup>ⓘ</sup>	<span style="color: green;">✔</span> <b>Selected</b>	Not a candidate	N/A

■ Meets criteria    ■ Does not meet criteria    ■ Not a steering candidate

[Close](#)

# CONFIGURE STEERING

The image shows a software interface for configuring steering objects, divided into two main panes: 'Manage steering objects' on the left and 'Edit steering object' on the right.

**Manage steering objects (Left Pane):**

- Search bar: Search...
- Filter: - All
- Steering objects list:
  - appi\_steering (Selected)
  - File Sharing - Local Breakouts
  - Web Conferencing
  - Remote Access

**Edit steering object (Right Pane):**

**Name:** appi\_steering

**Comment:** Optimized with low latency and packet loss recommended for Zoom, ...

**Tags:** Amazon, Facebook, Zoom

**Thresholds:**

- Custom thresholds  Use thresholds from Select...
- Latency up to: 150 ms
- Jitter up to: 20 ms
- Packet loss up to: 0.5 %

**Steering candidates:**

- Links
- HOT
- Cellcom
- Bezeq

**Link utilization:**

- Link aggregation  Prioritize links



# CONFIGURE STEERING

## Steering cadldates ⌵

Links

HOT

Cellcom

Bezeq

## Link utilization ⌵

Link aggregation  Prioritize links

Priority	Link
⋮ 1	HOT
⋮ 2	Cellcom

Cancel

Save

# MONITORING LINKS

MONITOR LINKS <span>×</span>								
Connection	Interface Name	Packet Loss	Latency	Jitter	Transmitted Throughput	Transmitted Packet Rate	Received Throughput	Received Packet Rate
Internet1	WAN	0	5	1	67	18	46	25
Internet2	DMZ	0	6	1	33	16	54	16

[Close](#)

2023 SPARK ROADMAP

# IoT LOCALLY MANAGED

# IoT FLOW

- Device connects to the GW
- The GW collects information on the device
- Query with the device's information is being sent to SMB cloud
- The SMB cloud returns the detected device (i.e Nintendo, Game console)
- The GW sends the result to internal service which return the relevant policy.
- The policy is automatically installed on the GW.



# IoT CONFIGURATION

- New page called “IoT” was added under the access policy
- On this page the IoT policy can managed per device type (i.e cameras, printers and etc)

The screenshot displays the Quantum Spark 1590 Appliance web interface. The top navigation bar includes the user 'admin', 'Log Out', 'Help / Support', and a search bar. The left sidebar shows the navigation menu with 'ACCESS POLICY' selected. The main content area is titled 'IoT' and shows 'IoT Protection enabled' with a link to 'Advanced policy settings'. Below this is a table listing IoT devices and their configurations.

Functions	Assets	Vendors	Access from Internet	Access to the Internet
IP camera	1	D-Link	Drop all	Prevent
Media player	1	Apple	Drop all	Detect

On the right side, there is a detailed view for an 'IP camera' asset. It shows 'Access from the Internet' set to 'Drop all' and 'Access to the Internet' set to 'Prevent'. Below this, there are checkboxes for 'Allow traffic to the internet only to approve destinations' (checked) and 'Drop traffic to other destinations' (unchecked). At the bottom right, there is a table for 'Approved Destinations' for the D-Link vendor.

Vendor	Assets	Approved Destinations
D-Link D-Link	1	ntp1.dlink.com,ntp.dlink.com,tw.signal.mydlink.com

# ACTIVE HOSTS

On this page the IoT policy can managed per specific asset

The screenshot displays a network management interface with a sidebar on the left and a main content area. The sidebar includes sections for Overview, Monitoring, and Troubleshooting. The main content area is titled 'Active Devices: Display devices in the internal networks' and shows a table of active devices. The second row is highlighted in blue, indicating the selected device. To the right of the table, a detailed view of the selected device is shown, including its name, IP address, MAC address, interface, and device type. Below this, a dropdown menu for 'IoT Policy' is open, showing 'Inactive' as the selected option.

Active Devices: Display devices in the internal networks

Active devices  
Display devices in the internal network

Refresh

Name	IP address	Mac address	Interface	Device type
	192.168.1.57	D0:04:0B:FE:C2:39	LAN1	IoT: Point of sale
	192.168.1.56	D0:04:0B:02:0F:38	LAN1	IoT: Media player
	192.168.1.55	D0:04:0B:FB:1D:37	LAN1	IoT: Point of sale
	192.168.1.54	D0:04:0B:88:96:36	LAN1	IoT: Game console
	192.168.1.53	D0:04:0B:5B:50:35	LAN1	Other

Media player  
192.168.1.56 | D0:04:0B:02:0F:38

VendorApple  
ZoneLAN  
InterfaceLAN1  
Activity statusActive  
Object typeNone  
Operating systemtvOS

IoT Policy  
Inactive  
Inactive  
According to function Policy

# ACCESS POLICY

On this Page you can view the auto generated access rules which were installed by the IoT policy

Outgoing Access to the Internet

\* New Edit Delete Enable Clone Customize Messages

No.	Source	Destination	Application / Service	Action	Log	Comment
▼ Auto Generated Rules						
1	IP_camera_D-Link	IP_camera_D-Link_Domains	* Any	Accept	None	Standard default policy is configured in <a href="#">Firewall blade control page</a>
2	Media_player_Apple	Media_player_Apple_Domains	* Any	Accept	None	Standard default policy is configured in <a href="#">Firewall blade control page</a>
3	Media_player	Internet	* Any	Accept	Log	Standard default policy is configured in <a href="#">Firewall blade control page</a>
4	Game_console_Nintendo	Game_console_Nintendo_Domains	* Any	Accept	None	Standard default policy is configured in <a href="#">Firewall blade control page</a>
5	Game_console	Internet	* Any	Accept	Log	Standard default policy is configured in <a href="#">Firewall blade control page</a>
6	All_IoT	Internet	* Any	Block	Log	Standard default policy is configured in <a href="#">Firewall blade control page</a>

Internal and IoT Traffic



# SMB MASTERS #2

Thank you!



YOU DESERVE THE BEST SECURITY