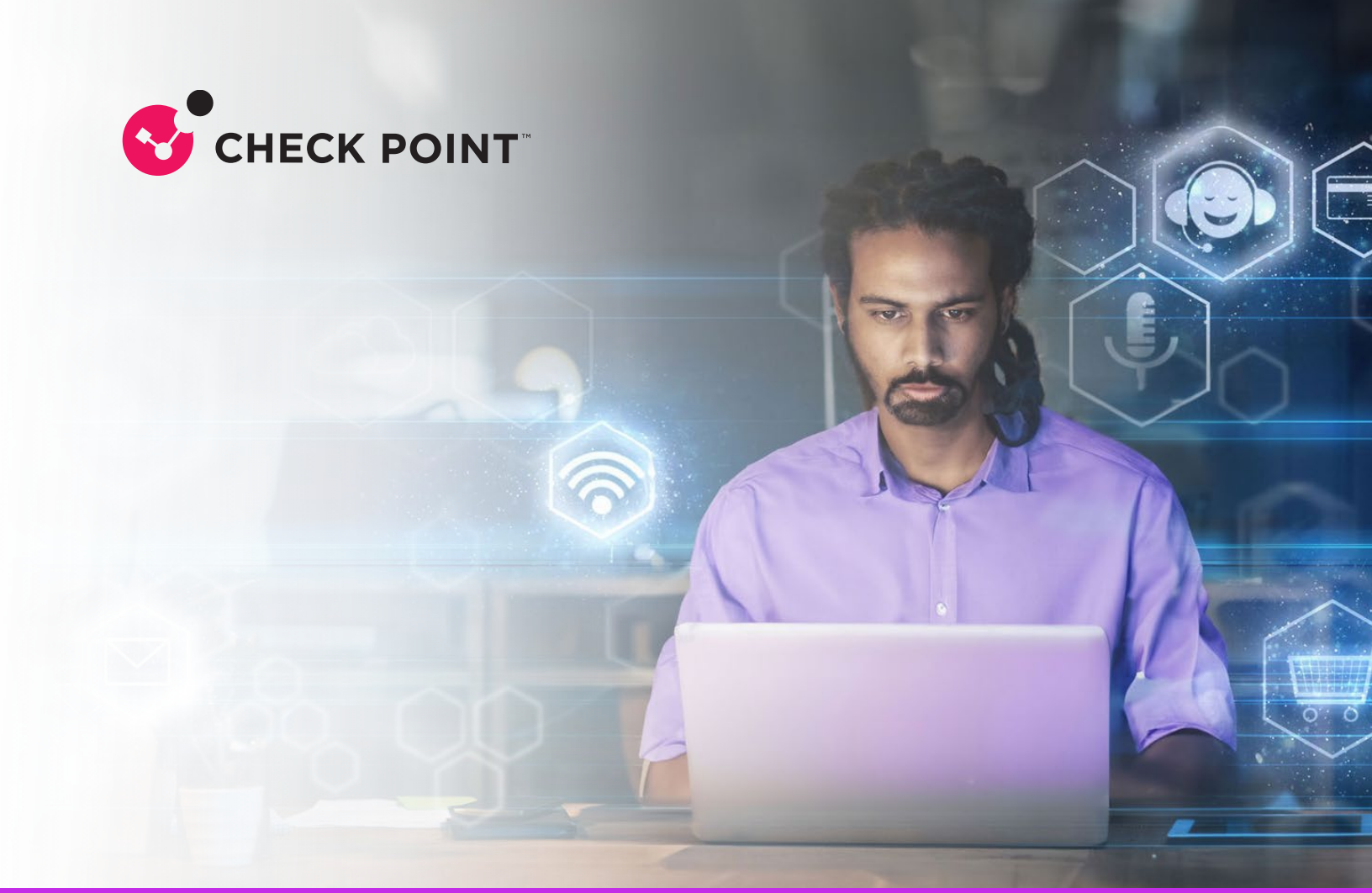
CHECK POINT™



ADVANCED VPN BYPASS RULES: OPTIMIZE YOUR NETWORK PERFORMANCE

Harmony
SASE

Secure remote access is a must-have for modern businesses in order to protect the corporate network from threat actors. There are situations, however, where a VPN connection can impede day-to-day operations. It doesn't always happen, but sometimes a secure tunnel–even one with a high-performance private global backbone–can cause a noticeable lag that hinders performance.

Video conferencing platforms (MS Teams, Webex, Zoom) and IP telephony systems are two of the most common apps that can experience latency issues. The good news is many latency-sensitive applications can be safely left out of the VPN connection via split tunneling since they are already using robust encryption.

Split Tunneling is the practice of routing some web traffic through a VPN tunnel, while allowing other traffic to connect directly.

Split Tunneling by IP

A common way to handle split tunneling is by excluding IP addresses from the VPN tunnel, but this is very difficult to manage.

Split tunneling by IP is often done with address ranges–a shorthand method for specifying groups of consecutively numbered IP addresses such as 3.7.35.0, 3.7.35.1, 3.7.35.2, etc.

Split tunneling for a single service could mean listing dozens or even **hundreds of IP ranges**. In addition, you have to update your exclude list whenever the service adds new IPs or removes old ones. That means a long, tedious practice with no end in sight.

A better alternative is to use what's called a fully qualified domain name (FQDN).

An FQDN is a domain address with a prefix (subdomains in most cases) such as ***outlook.live.com*** or ***mail.google.com***.

FQDNs are the ideal choice for split tunneling since a handful of domains can cover an entire service.

Harmony SASE's FQDN Split Tunneling helps improve performance for latency sensitive apps, reducing issues like lag and stutter, while also making IT teams more efficient.

Split Tunneling the FQDN Way

For each business application there could be a single FQDN to worry about or multiple ones. Google, for example, specifies a number of addresses for Google Meet such as ***meet.google.com***, ***stream.meet.google.com***, and a few others.

Platforms such as Zoom are even simpler since a single rule can cover the entire service. Zoom FQDNs are often based on the customer's company name such as ***companya.zoom.us.*** If Company A were hosting a meeting then it would use their FQDN, but if they were joining a meeting hosted by Company B then it would be hosted on ***companyb.zoom.us.***

Wildcard support lets you easily exclude all possible FQDNs from Zoom with just one rule: ****.zoom.us.***
This ensures that all Zoom meetings will bypass the VPN connection regardless of who's hosting the meeting.

Consult the support forums of your particular business applications to get a list of the necessary FQDNs you need to configure your split tunneling rules.

See our support documentation for a detailed step-by-step guide for creating split tunneling rules.

Exclude Inefficiency with Harmony SASE

Harmony SASE's FQDN Split Tunneling rules are an easy way to ensure that your employees don't have to slow down. Teams using latency sensitive applications won't suffer any lag due to the VPN connection, while IT can quickly set up split tunneling rules.

Regular VPN traffic will also see a boost in performance since many latency-sensitive services require a lot of bandwidth. Excluding those apps from the VPN means a lower load on the connection and better traffic flow for everyone.

With Harmony SASE you can also make sure that bypassed traffic is still protected with our hybrid Internet Access, which runs on the device. Internet Access protects employee web traffic from malware and malicious websites even when users are connecting directly to the internet, and without negatively impacting device performance.

Discover how Harmony SASE can streamline your company's IT operations to keep employees productive and IT teams focused on more pressing tasks.

Book a demo today.

Harmony
SASE

Meet Harmony SASE

2x Faster Internet Security | Full Mesh Private Access | Secure SD-WAN

The internet is the new corporate network, leading organizations to transition to SASE. However current solutions break the user experience with slow connections and complex management.

Harmony SASE is a game-changing alternative that delivers 2x faster internet security combined with full mesh Zero Trust Access and optimized SD-WAN performance—all with an emphasis on ease-of-use and streamlined management.

Combining innovative on-device and cloud-delivered network protections, Harmony SASE offers a local browsing experience with tighter security and privacy, and an identity-centric zero trust access policy that accommodates everyone: employees, BYOD and third parties. Its SD-WAN solution unifies industry-leading threat prevention with optimized connectivity, automated steering for over 10,000 applications and seamless link failover for uninterrupted web conferencing.

Using Harmony SASE, business can build a secure corporate network over a private global backbone in less than an hour. The service is managed from a unified console and is backed by an award-winning global support team that has you covered 24/7.

Harmony SASE is part of the Harmony for Workspace Suite. Harmony helps organizations of all sizes secure their workspaces with a suite of products covering network security across browsers, devices, and cloud.

To learn more, visit https://www.checkpoint.com/harmony/sase/

Book a Demo

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
100 Oracle Parkway, Suite 800, Redwood City, CA 94065 | Tel: 1-800-429-4391

www.checkpoint.com