CHECK POINT™

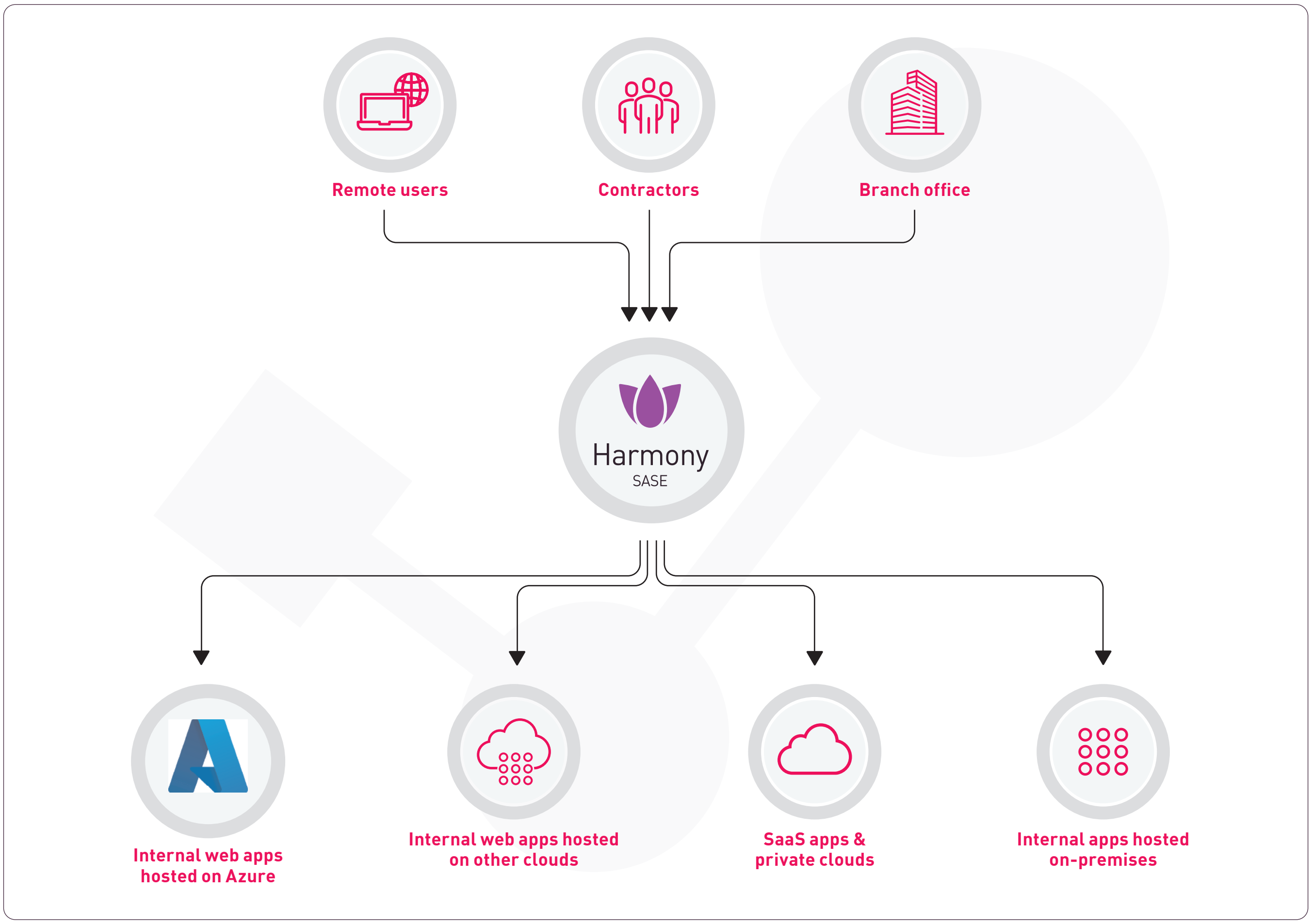
Harmony SASE

Securing Azure Access with Check Point Harmony SASE

Provide Secure Access for All Users, Anywhere to Your Public Cloud Resources

Check Point Harmony Secure Access Service Edge (SASE) enables secure access to company resources in the public cloud whether employees are working from the office or remotely. Administrators, meanwhile, can easily audit team activity and enjoy full network visibility with our single-pane-of-glass management console.

Configuring Azure Access


Remote users
Contractors
Branch office
Harmony
SASE
Internal web apps hosted on Azure
Internal web apps hosted on other clouds
SaaS apps & private clouds
Internal apps hosted on-premises

Connecting a Microsoft Azure environment to your Harmony SASE network is easy.

Virtual Network Gateway

Step 1: Creating the Gateways

The first step is to create a subnet inside the settings of the Azure VNet you want to connect to, and then fill out the subnet details such as the subnet name, and the address range.

Now we can move on creating the actual gateway. During this step you'll supply the gateway name, select the gateway type (VPN), specify a route-based connection, and specify the Vnet you're connecting to.

Next, we need a local network gateway that will instruct the virtual network gateway about the source of the tunnel connection (Harmony SASE in this case). That means you have to provide the local network gateway with your Harmony SASE subnet, Quantum SASE gateway IP, as well as other information such as the location where the local network gateway will be and the gateway SKU.

Step 2: Create the IPSec Tunnel

Finally, it's time to create the tunnel inside the settings of the virtual network gateway we specified earlier. The tunnel details include the connection name, connection type, the virtual network and local gateways we created earlier, and the IPSec shared key. Once that's done you can download your IPSec configuration file.

To ensure maximum availability of your cloud resources, we recommend creating redundant tunnels to your Azure resources for high availability. By default, additional tunnels run in active-active mode where both tunnels are in use to optimize the VPN connection. In addition, should one of the tunnels falter, employee connections will automatically fail over to the working tunnel(s). We do not limit the number of tunnels you can create, nor do we charge extra for additional tunnels–so define as many as necessary.

Step 3: Harmony SASE Settings

To add a tunnel to your Harmony SASE network, choose "Add Tunnel" under the three-dotted menu of the gateway that will connect to Azure. Then fill out the information in the wizard such as the name, shared secret, and ensure that your configuration file settings match those in your Harmony SASE settings for the encryption algorithm, and so on.

Once the settings are confirmed, you have to add the route on the Harmony SASE side that includes the subnets from the Azure side.

Step 4: Set Harmony SASE ZTNA Rules

You should also set access rules within the Harmony SASE management console to enable Zero Trust access to your Azure resources. This way only the individuals and/or groups who actually need access to these resources will have it, while all other employees won't.

Harmony SASE also supports the advanced WireGuard protocol to connect to Azure based on our easy-to-use proprietary connector.

Virtual WAN

Harmony SASE supports creating redundant IPSec VPN connections between an Azure Virtual WAN and a Harmony SASE network in active-passive mode.

To use this approach you must have at least two Harmony SASE gateways running in the same network.

Step 1: Create a Virtual WAN and Virtual Hub on Azure

Creating a Virtual WAN on Azure is extremely straightforward and only requires specifying its name, region and type. If you already have a Virtual WAN running you can skip this step.

Creating a virtual hub requires a little more detail such as specifying an IP address space for the hub, and specifying the hub's capacity–this must reflect the maximum number of VMs that will be connected through this hub.

Step 2: Create a Site in Azure

You must also create a VPN site inside your Virtual WAN. This includes giving the site a meaningful name, specifying the region, name of the device vendor, and then be sure to leave the address space empty.

Once the site is created, you will also need to connect it to your virtual hub.

Step 3: Create the High Availability Tunnel

On the Harmony SASE side click the three-dotted menu on one of the gateways that will connect to your Azure environment. Choose Add Tunnel, select the IPSec option, then choose Redundant Tunnels, and fill out the details.

Next, add the route to your Azure subnet on the Harmony SASE side, and you're ready to test your set-up.

Step 4: Set Harmony SASE ZTNA Rules

You should also set access rules within the Harmony SASE management console to enable Zero Trust access to your Azure resources. This way only the individuals and/or groups who actually need access to these resources will have it, while all other employees won't.

Harmony SASE also supports the advanced WireGuard protocol to connect to Azure based on our easy-to-use proprietary connector.

For more information about connecting to Azure resources see our help center for detailed step-by-step guides.

> "Any remote access is going to come over [the network]. Our attack footprint doesn't exist anymore." - *Brett A. Sudeck, NP Inc.*

Access Your Azure Resources Securely

With a secure, encrypted tunnel between your Harmony SASE gateway and Azure resources employees can connect securely. We also increase your organization's security by hiding the public IP address of your Azure resources. Your Harmony SASE network assigns your Azure VNet an internal IP address, thereby obscuring its public IP from the outside world. Internal IP addresses cannot be used outside the network rendering your Azure resources invisible and inaccessible, which greatly reduces the attack surface.

Should you prefer direct connectivity we also provide users with a static IP address to enable allowlisting. This isn't as secure as implementing a secure tunnel using supported VPN protocols. But allowlisting means that only employees coming through your Harmony SASE private IP address will be able to access your Azure resources. To use IP allowlisting, all you have to do is add a firewall rule on the Azure side that only allows access via your Harmony SASE gateway's IP address.

Harmony SASE also implements granular access on a per-user application basis, which ensures users only have access to the specific applications they need, and not the entire Virtual Network.

Harmony SASE Key Advantages

Faster Connections

We remove the need to route traffic to an on-prem VPN allowing direct access to cloud resources. This means reduced latency, more responsive applications, and increased productivity for your employees

Cover It All With FWaaS

No need to pay extra for a virtual firewall. Reduce costs and complexity with a Firewall as a Service that works across all cloud instances.

Better Network Visibility

With all traffic to your cloud resources routing through Harmony SASE, you will have better visibility into network activity, and detailed logs for SIEM ingestion and investigating security events.

High Availability Tunnels, No Additional Cost

We do not limit the number of tunnels you can create, nor do we charge extra for additional tunnels–so define as many as necessary.

Effortless Deployment

In minutes, you can deploy a company network, and set up secure connections to cloud and on-premises resources.

Easy Zero Trust Network Access (ZTNA)

IT professionals can easily enforce Zero Trust Network Access policies for individuals or groups quickly and easily. Enforce granular permissions that restrict access to sensitive on-prem and cloud applications.

Broad IdP Support

Harmony SASE supports custom identity management lists and integrates with many trusted and well-known IdP services such as G Suite, JumpCloud, Microsoft Azure AD, and Okta.

Secure Connections for Remote Workers

Administrators can enhance network security with IPSec or WireGuard tunnels between the Harmony SASE gateway and company resources.

About Harmony SASE

Check Point's Harmony SASE is a robust, yet easy-to-use, converged networking and network security platform that connects all users, in the office or remote, to all resources, located on-prem or in the cloud. It is a cloud-delivered service that includes advanced capabilities such as zero trust remote access, Internet access control, malware protection, firewall as a service, and SD-WAN. It enables any business to 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.

Request a Demo

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com