

Cloudbrink Network Firewall as-a-Service

Cloudbrink's **IPSec Peering** feature allows administrators to connect remote users to their existing IPSec infrastructure which can be a datacenter or branch IPSec gateway, an SD-WAN cloud gateway or branch edge appliance. Administrators can deploy Cloudbrink for remote users and take advantage of the application performance and zero-trust security capabilities without any change to their existing networking infrastructure and still provide access to the applications in these networks.

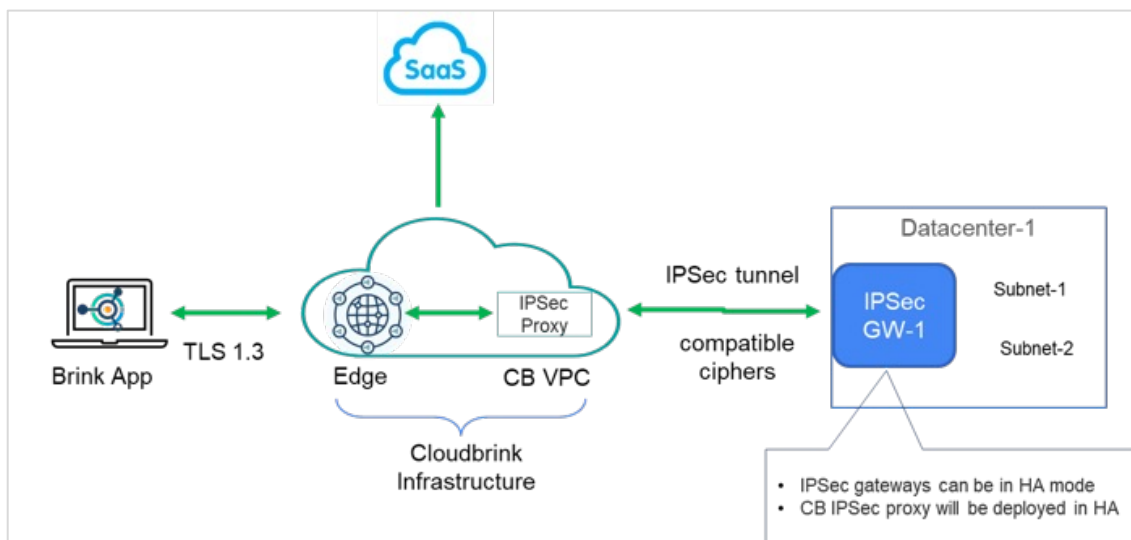
Overview

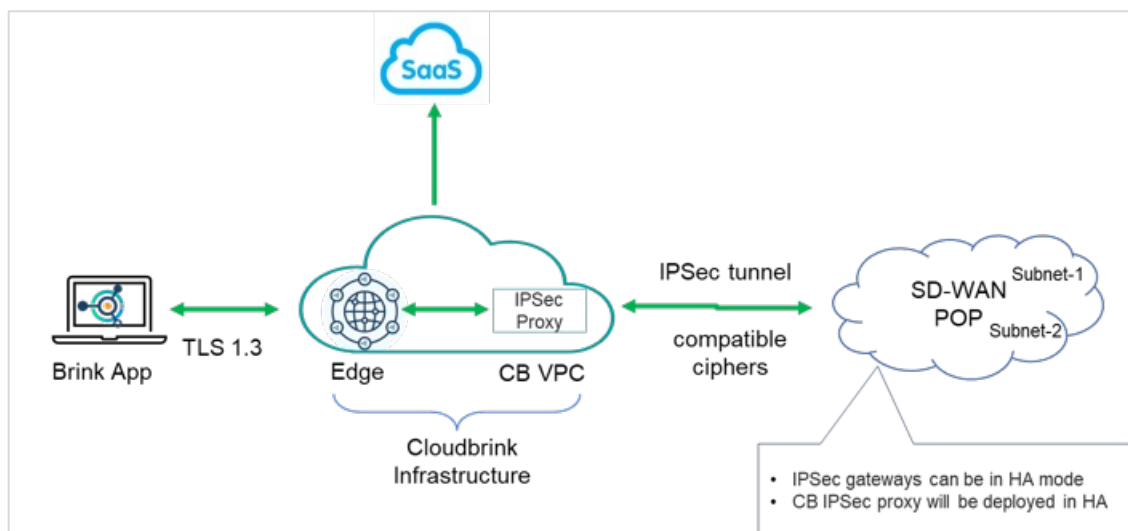
Organizations need to provide a high-performance zero-trust access solution to remote users because user productivity is significantly impacted if the applications are responding slowly. Cloudbrink can improve the application performance by overcoming the last-mile networking challenges (eg: unreliable networks in hotel, airport, shared home WiFi) and providing best user experience.

Administrators want to deploy Cloudbrink for remote users but also want to ensure that this deployment is smooth and doesn't require major changes to their existing networking infrastructure inside their on-prem datacenter or branches. With the Cloudbrink IPSec Peering feature, customers can terminate their remote user connections via Cloudbrink on to their existing IPSec solution that is already deployed inside their datacenters or branches.

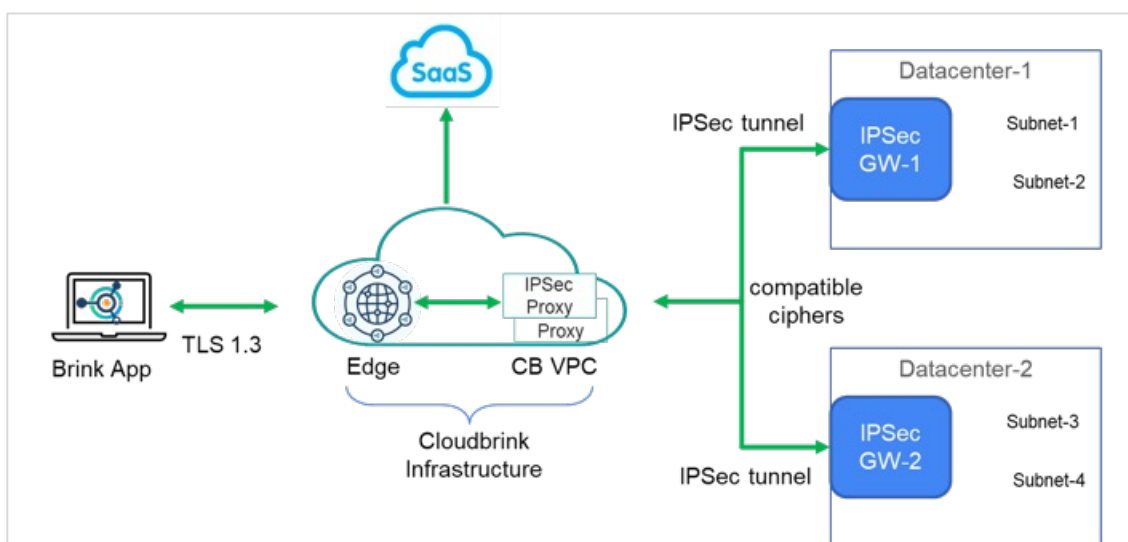
With this feature, customers can benefit from Cloudbrink application performance improvements, zero-trust security for remote users and with no changes to their existing networking infrastructure.

Sample topologies for IPSec Peering Deployments





Sample topology-2



Sample topology-3

Configuration

1. Configure the enterprise-services that represent the networks behind the IPsec Gateway(s) that users need access to.

Configure > Resources > Enterprise-Services

New Enterprise Service

NAME

IPSec_subnets

DOMAIN

internallab.net

BRINK VNET

172.16.20.0/16

192.168.1.100/24

SERVER INITIATED CONNECTIONS

☐

2. Create a new IPSec Gateway by providing the peer IPSec gateway public IP address(es), primary/secondary details, cipher suites to be used for IKE and IPSec, DNS and enterprise-services info (created in step-1).

Configure > Resources > IPSec Gateways

a. Peer Connections

New IPSec Gateway

NAME *

IPSec_endpoint_DC1

Peer Connections

PRIMARY IP ADDRESS *

PRIMARY PRE-SHARED KEY *

SECONDARY IP ADDRESS

SECONDARY PRE-SHARED KE...

DPD TIMEOUT (SEC) 45

b. Tunnel Parameters

Tunnel Parameters

IKE V2 PARAMETERS

IKE SA *

7800

AUTHENTICATION *

Select Hashing

SHA2_256_128 HMAC (128 bit)

IPSEC PARAMETERS

IPSec SA *

3600

AUTHENTICATION *

Select Hashing

SHA2_256_128 HMAC (128 bit)

ENCRYPTION *

Select Encryption

256 bit AES-CBC

DH GROUP *

Select DH Groups

Group 14 (2048-bit keys) with PFS enabled

ENCRYPTION *

Select Encryption

256 bit AES-CBC

Enable PFS

PFS GROUP *

☒

Select PFS Groups

Group 14 (2048-bit keys) with PFS enabled

c. DNS server

DNS Servers

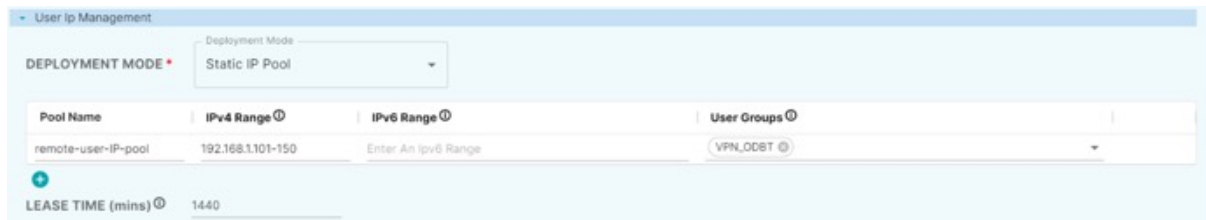
DNS PRIMARY IP

172.16.20.11

DNS SECONDARY IP

172.16.20.12

d. User IP Management



The 'User IP Management' interface shows the 'Deployment Mode' set to 'Static IP Pool'. Below this, there is a table with columns: Pool Name, IPv4 Range, IPv6 Range, and User Groups. The first row contains the values: 'remote-user-ip-pool', '192.168.1.101-150', 'Enter An ipv6 Range', and 'VPN_ODBT'. At the bottom, the 'LEASE TIME (mins)' is set to '1440'.

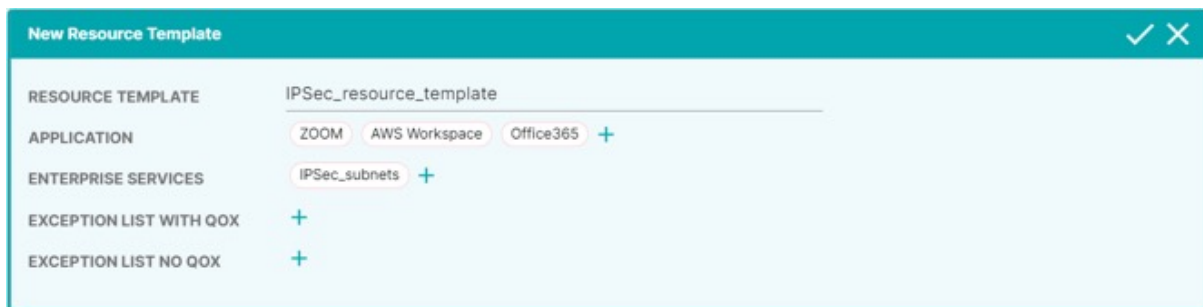
e. Enterprise-services



The 'Enterprise Services' interface shows a dropdown menu for 'ENTERPRISE SERVICES' with 'IPSec_subnets' selected. There are 'CANCEL' and 'SAVE' buttons at the bottom right.

3. Create a new resource-template with the set of applications (application-services and enterprise-services) that will be enabled to remote users.

Configure > Resources > Resource Templates

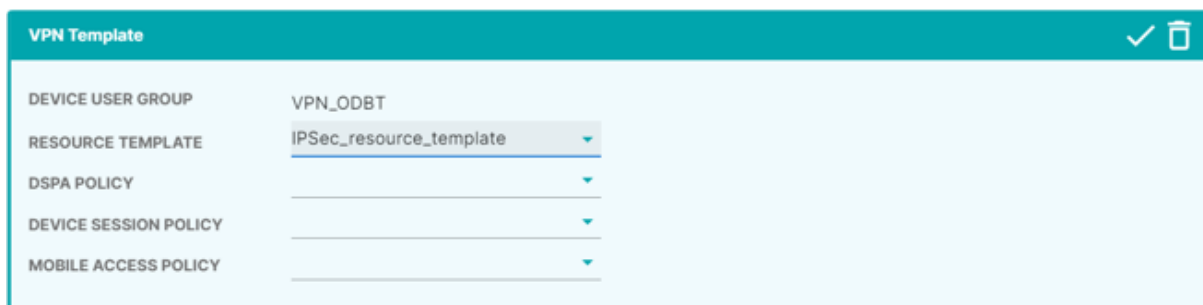


The 'New Resource Template' interface shows the following configuration:

RESOURCE TEMPLATE	IPSec_resource_template
APPLICATION	ZOOM, AWS Workspace, Office365, +
ENTERPRISE SERVICES	IPSec_subnets, +
EXCEPTION LIST WITH QOX	+
EXCEPTION LIST NO QOX	+

4. Assign the resource-template to the appropriate device-user-groups.

Configure > Device User Groups > Device User Group Policies



The 'VPN Template' interface shows the following configuration:

DEVICE USER GROUP	VPN_ODBT
RESOURCE TEMPLATE	IPSec_resource_template
DSPA POLICY	
DEVICE SESSION POLICY	
MOBILE ACCESS POLICY	

5. At this stage, the Cloudbrink endpoints on the IPSec Gateways need to be configured. Administrators need to contact Cloudbrink [support team](#) to get the public IP information of the Cloudbrink IPSec endpoints.

IPSec requires configuration on both sides to create the IPSec tunnels.

With the above configuration, remote users belong to “VPN_ODBT” device-user-group can access all subnets defined under “IPSec_resource_template” via the IPSec gateways defined under “IP-Sec_endpoint_DC1”.

Support

We would love to hear from you! For any questions, concerns, or feedback regarding this feature, please reach out at support@cloudbrink.com

Corporate Headquarters Cloudbrink, Inc.
530 Lakeside Drive, Suite 190, Sunnyvale, CA 94085

