Cloudbrink Network Firewall as-a-Service

Cloudbrink's Network Firewall as-a-Service (FWaaS) feature enables customers to implement network level (layer-3/4) firewalling rules for remote workers accessing datacenter apps (private apps) hosted inside a physical on-prem or cloud IaaS VPC network. Similar to a typical enterprise perimeter network firewall that allows only allow listed traffic, Cloudbrink Network Firewall as-a-Service allows only allow listed traffic from the remote users.

Overview

The Cloudbrink Brink App acts like a deny-all firewall by default. Only administrative configured traffic is tunnelled through Cloudbrink into the datacenter. With the enhanced Network Firewall as-a-Service feature, administrators may configure policies that can define the allow listed apps at Domain-name, IP address, Port and Protocol level details.

Advantages of the Cloudbrink Network Firewall as-a-Service

1. **Enforce firewall rules very close to the origin or source of the traffic:** The Brink App is installed and running on the users' endpoint. The Brink App enforces the firewall rules defined by the admininistrator on the endpoint, which is the origin or source of the traffic. Enforcing firewall rules very close to the origin prevents the data to traverse out of the endpoint and prevents other types of MITM or DDoS type of attacks.
2. **Edge-native service:** The Cloudbrink Network FWaaS is a cloud-based edge service that is configured and managed from a central cloud administration console.
3. **Consistent policy enforcement:** Since the firewall rules are defined centrally, the policies are enforced consistently irrespective of any number of datacenters or apps a user might be accessing.
4. **User and App awareness:** The primary distinction between traditional enterprise perimeter firewalls and Cloudbrink's Network FWaaS is the latter's ability to incorporate user and application awareness into rule definitions, a feature not available in conventional layer-3/4 firewalls.

How does the Cloudbrink Firewall work?

Cloudbrink follows the 'principle of least privilege' model. So, all destinations are denied by default for every device-user-group. Administrators must explicitly allow the set of destinations (IP addresses and domain names) that are permited for specific device-user-groups.

The administrator, upon assigning an enterprise service configuration to a specific IP address or domain name, links this service to a designated device-user-group through a resource template. Consequently, only users within this group are granted access to the specified IP address and domain name, with all other destinations being automatically blocked by default.

Configuration for an IP address may range from a single address with a /32 subnet mask to larger subnets (/24, /16, etc.). Similarly, the domain name configuration can target a precise Fully Qualified Domain Name (FQDN) or encompass a broader top-level domain.

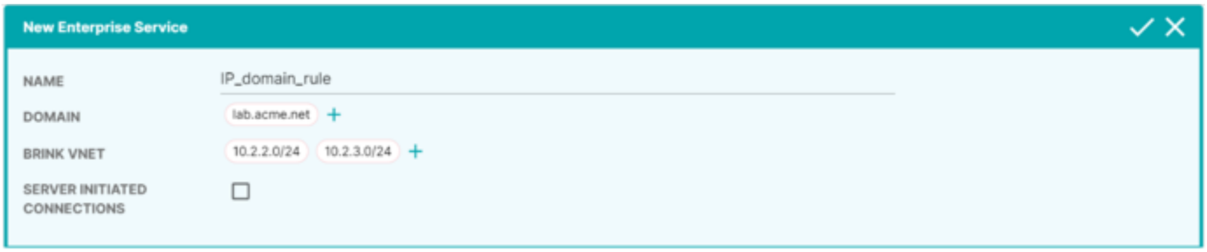
Port & Protocol Based Policies

The 13.1 release allows administrators to create more detailed allowlist policies that can include specific ports or port ranges, as well as protocol details. Traffic that exactly fits these defined criteria is permitted by Cloudbrink, and all other traffic is blocked. If ports or protocols are not specified, with only IP addresses and domain names configured, it defaults to 'any port' and 'any protocol', serving as wildcards.

Configuration

Below are some examples of configuring firewall rules.

i) IP-address and domain-named based rules

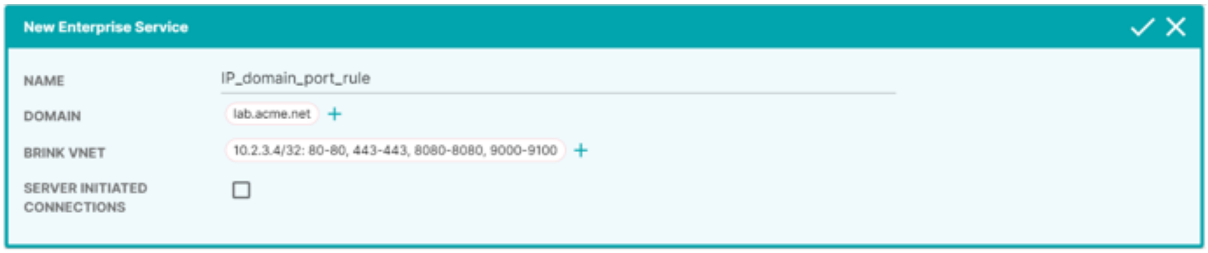


New Enterprise Service

NAME	IP_domain_rule
DOMAIN	lab.acme.net
BRINK VNET	10.2.2.0/24 10.2.3.0/24
SERVER INITIATED CONNECTIONS	□

With above configuration, users can access all destination IP addresses and to any port and any protocol in the two subnets 10.2.2.0/24 and 10.2.3.0/24.

ii) IP, domain and port based rules



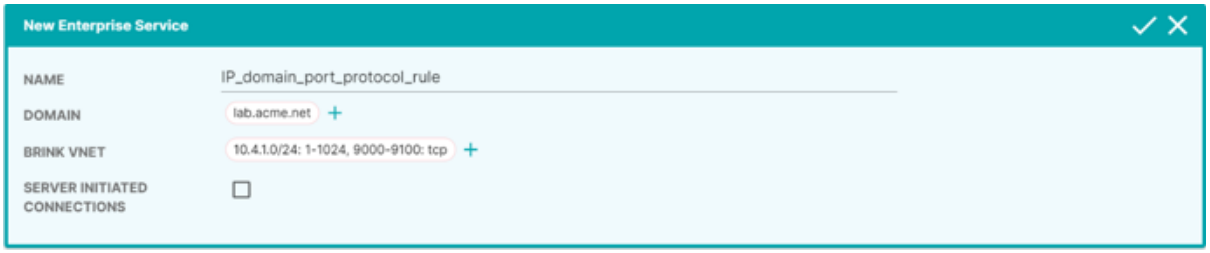
New Enterprise Service

NAME	IP_domain_port_rule
DOMAIN	lab.acme.net
BRINK VNET	10.2.3.4/32: 80-80, 443-443, 8080-8080, 9000-9100
SERVER INITIATED CONNECTIONS	□

With above configuration, users can access only one IP address (10.2.3.4/32) and only specific ports 80,443,8080 and 9000-9100. Protocol can be any (TCP, UDP, etc.)

Note: Traffic to 10.2.3.4 IP but any other port (say port = 5000) will be blocked.

iii) IP, domain, port and protocol based rule



New Enterprise Service ✓ ✕

NAME IP_domain_port_protocol_rule

DOMAIN lab.acme.net +

BRINK VNET 10.4.1.0/24: 1-1024, 9000-9100: tcp +

SERVER INITIATED CONNECTIONS □

With above configuration, users can access any IP address in the subnet 10.4.1.0/24 but only on port ranges 1-1024 or 9000-9100 and only on TCP protocol.

Note: Any other port or other protocol (say UDP) will be blocked.

Note: Traffic to 10.4.1.100 IP, on port 5000 and protocol TCP will be blocked

Note: Traffic to 10.4.1.100 IP on port 9000 and protocol UDP will be blocked

Configuration

Administrators should understand the following behaviors when implementing port and protocol-based policies:

1. The server-initiated connections feature will not consider the port or protocol parameters. The source-IP address of server that is initiating the connection must be within the IP range specified in the enterprise-service.
   a. If the Brink App initiated ping to the server, and if the server immediately initiates ping to Brink App, it will fail due to the port based rule.
2. When conflicting policies are configured, below methods are used to resolve the conflict.
   a. If two policies have the same IP subnet, but the port parameter in one policy and protocol parameter in another policy, then port-based policy is evaluated first and then the protocol based policy.
   b. If a port is falling under two ranges in two different policies, the policy with lesser range will be chosen.
   c. If two policies have same port but one policy specifies protocol also, then more granular matched policy (port as well as protocol) will be chosen.
4. To edit an existing port configuration, admin has to delete and re-add the vnet configuration. Editing only port parameter is not allowed.
5. For default route case (0.0.0.0/0), port and protocol parameters are not allowed.
6. DNS port 53 is not allowed to be configured in the port parameter.

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

CLOUDBRINK
Hybrid Access as a Service