

Bypassing Netskope for improved performance

Method-1 (Sample Configuration): Bypassing using Custom Firewall Application

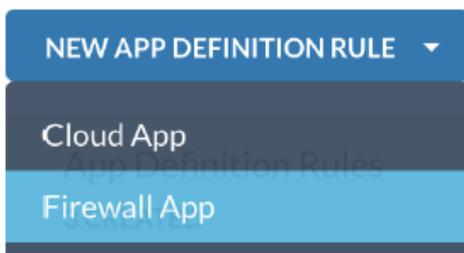
If the exception traffic destination IP address/subnet/CIDR (or) Domains, protocol (TCP, UDP) and ports are available then this method is preferable.

Important notes:

- In the firewall application definition, it is recommended to configure fine grained custom application rules including IP address/Domains, protocol and ports specific to voice/video traffic.
- For IPSec/GRE GW steering methods, we recommend customers to configure equivalent bypass rules in access gateways in their client network.
- If FQDN/PQDN is used in custom firewall applications, then we need to make sure to send DNS traffic also through the cloud firewall so that the firewall can be aware of IP to domain mapping. This is needed only for IPSec/GRE GW steering methods and customers can't configure bypass rules in their access gateways.

Configuration Steps:

1. Create the Custom Firewall Application in Settings > Security Cloud Platform > TRAFFIC STEERING > App Definition with IP addresses/FQDN, Protocols (TCP, UDP) and ports



New App Definition Rule: Firewall App ×

APPLICATION

DESTINATION IP

PROTOCOL

2. Add the custom application to New Application exception in Settings > Security Cloud Platform > TRAFFIC STEERING > Steering Configuration page

New Exception
✕

Exceptions allow for certain types of traffic to bypass Netskope and go straight to its destination. To add a new exception, specify the type of traffic.

EXCEPTION TYPE*

Application ▾

Applications = [Application_Voice_Traffic]

Bypass
Traffic will go straight to destination.

Bypass, except for DNS traffic
Only non-DNS Traffic will go straight to its destination if selected application also covers DNS traffic.

NOTES

Add a note for this exception (optional)

CANCEL

ADD

Address	Protocol	Ports	Is Bypass Required
---------	----------	-------	--------------------

<p>3.238.83.128/25, 3.251.93.0/26, 3.133.18.38/32, 3.135.139.181/32, 13.51.179.176/32, 13.228.200.40/32, 52.76.233.79/32, 52.221.167.63/32, 54.253.118.63/32, 54.253.248.99/32, 54.253.250.85/32, 54.253.254.161/32, 54.254.43.153/32, 165.75.5.0/24</p>	<p>TCP</p>	<p>443,1720,1935,506 0-5061,30000- 50000</p>	<p>Yes</p>
<p>"204.141.11.0/24", "204.141.12.0/24", "204.141.217.0/24"</p>	<p>TCP</p>	<p>443, 80, 8080</p>	<p>No</p>
<p>3.238.83.128/25, 3.251.93.0/26, 3.133.18.38/32, 3.135.139.181/32, 13.51.179.176/32, 13.228.200.40/32, 52.76.233.79/32, 52.221.167.63/32, 54.253.118.63/32, 54.253.248.99/32, 54.253.250.85/32, 54.253.254.161/32, 54.254.43.153/32, 165.75.5.0/24</p>	<p>UDP</p>	<p>443,1719,5060,400 00-50000</p>	<p>Yes</p>

"204.141.11.0/24", "204.141.12.0/24", "204.141.217.0/24"	UDP	443, 80, 8080	No
204.141.12.0/24 3.251.93.0/26 13.228.200.40/32 54.254.43.153/32 52.206.127.180/32 34.192.154.13/32	TCP	443, 40000-50000	Yes
204.141.12.0/24 3.251.93.0/26 13.228.200.40/32 54.254.43.153/32 52.206.127.180/32 34.192.154.13/32	UDP	443, 40000-50000	Yes

Configuration Steps

We will configure GlobalMeet voice traffic bypass using Custom Firewall Application (Method-1).

1. Create the 2 Custom Firewall Applications in Settings > Security Cloud Platform > TRAFFIC STEERING > App Definition with IP addresses/FQDN, Protocols (TCP, UDP) and ports

Example: UDP

Edit Definition Rule: Firewall App
✕

APPLICATION

[GlobalMeet UDP]
▼

DESTINATION IP

3.238.83.128/25,
3.251.93.0/26,
3.133.18.38/32,
3.135.139.181/32,
10.54.170.176/28

Example: TCP

Edit Definition Rule: Firewall App

APPLICATION

[GlobalMeet TCP]

DESTINATION IP

3.238.83.128/25,
3.251.93.0/26,
3.133.18.38/32,
3.135.139.181/32,
40.54.170.177/23

PROTOCOL

TCP

443, 1720, 1935, 5060-5061, 30000-50000

CANCEL SAVE

2. Add the custom application to New Application exception in Settings > Security Cloud Platform > TRAFFIC STEERING > Steering Configuration page

New Exception



Exceptions allow for certain types of traffic to bypass Netskope and go straight to its destination. To add a new exception, specify the type of traffic.

EXCEPTION TYPE*

Application

Applications = [GlobalMeet TCP] [GlobalMeet UDP]

Bypass

Traffic will go straight to destination.

Bypass, except for DNS traffic

Only non-DNS Traffic will go straight to its destination if selected application also covers DNS traffic.

 This steering configuration is currently not steering DNS traffic. [Edit Steering Config](#)

NOTES

GlobalMeet Audio/Video Bypass

CANCEL

ADD

3. Validate bypass location is at the client in Security Cloud Platform > Traffic Steering > Steering Configuration > Edit > Cloud, Web and Firewall > Bypass exception traffic at "Client"

NAME

Default tenant config

TRAFFIC STEERING

NON-STANDARD PORTS

TRAFFIC STEERING

Specify what kind of traffic you'd like to steer to Netskope.

 Enable Dynamic Steering ⓘ**Cloud, Web and Firewall** ⓘ

All Traffic ▾

Bypass exception traffic at [Client](#) ▾**DNS Traffic**

None ▾

Private Apps ⓘ

All Private Apps ▾

Netskope will **not steer** ▾ private apps
in presence of other steering methods.

CANCEL

SAVE

Revision #2

Created 8 May 2025 11:53:51 by Matt Engel

Updated 8 May 2025 12:17:27 by Matt Engel