# Troubleshoot Secure Access Resource Connector Deployment and Connectivity on Google Cloud Docker

## Contents

## Issue

Attempts to deploy the Secure Access Resource Connector on Docker were unsuccessful.

Although the connector installed correctly, connectivity to Cisco Secure Access could not be established.

Diagnostic checks reported tunnel disconnection and server communication errors.

The environment uses Red Hat 9 virtual machines hosted in Google Cloud, connected through a Fortinet firewall wit

Troubleshooting revealed potential MTU mismatches between network interfaces as a contributing factor.

## Environment

- Technology: Solution Support (SSPT - contract required)
- Subtechnology: Secure Access -
  Resource Connector (Install, Upgrade, Registration, Connectivity, Private Resource)
- Platform: Red Hat 9 Virtual Machines on Google Cloud
- Network: Fortinet firewall between Secure Access and VM ("any any" rule in place)
- Connector Region: iuvz83r.mxc1.acgw.sse.cisco.com
- Google Cloud VPC default MTU: 1460 bytes
- Docker bridge (docker0) default MTU: 1500 bytes (before change)
- Single network interface (eth0) per VM

## Resolution

Follow these steps to diagnose and resolve Secure Access Resource Connector connectivity issues in a Docker/Goog

### Check DNS Resolution for the Connector Region

Use `nslookup` to confirm the Secure Access region can be resolved from the VM.

```
nslookup iuvz83r.mxc1.acgw.sse.cisco.com
```

Example output:

```
Server:         64.102.6.247
Address:        64.102.6.247#53
Non-authoritative answer:
Name:   iuvz83r.mxc1.acgw.sse.cisco.com
Address: 163.129.128.72
Name:   iuvz83r.mxc1.acgw.sse.cisco.com
Address: 163.129.128.70
Name:   iuvz83r.mxc1.acgw.sse.cisco.com
Address: 163.129.128.66
Name:   iuvz83r.mxc1.acgw.sse.cisco.com
Address: 163.129.128.68
```

## Check Network Connectivity to Secure Access

Use `ping` and `telnet` to validate connectivity to Secure Access from the VM.

```
ping iuvz83r.mxc1.acgw.sse.cisco.com
```

Example output:

```
PING iuvz83r.mxc1.acgw.sse.cisco.com (163.129.128.66) 56(84) bytes of data.
64 bytes from 163.129.128.66: icmp_seq=1 ttl=57 time=44.7 ms
64 bytes from 163.129.128.66: icmp_seq=2 ttl=57 time=43.8 ms
...
telnet iuvz83r.mxc1.acgw.sse.cisco.com 443
```

Example output:

```
Trying 163.129.128.66...
Connected to iuvz83r.mxc1.acgw.sse.cisco.com.
Escape character is '^]'.
```

## Check for Tunnel Connectivity and Run Diagnostics

Run the connector diagnostic utility to check tunnel status.

```
/opt/connector/data/bin/diagnostic
```

Example output:

```
###check tunnel connection:
```

```
error: tunnel is not connected
```

## Verify Network Interface and MTU Settings

Check IP addresses and MTU of all interfaces using `ifconfig` and `ip a`.

```
ifconfig
ip a
```

Example output for eth0 and docker0:

```
[root@degcpprcra02 ~]# ifconfig
docker0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet x.x.x.x netmask x.x.x.x broadcast x.x.x.x
inet6 fe80::1c66:46ff:fe1d:8bed prefixlen 64 scopeid 0x20<link>
ether 1e:66:46:1d:8b:ed txqueuelen 0 (Ethernet)
RX packets 974 bytes 119775 (116.9 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 848 bytes 161554 (157.7 KiB)
TX errors 0 dropped 2 overruns 0 carrier 0 collisions 0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1460
inet x.x.x.x netmask x.x.x.x broadcast 0.0.0.0
ether 42:01:c0:a8:80:b0 txqueuelen 1000 (Ethernet)
RX packets 20175 bytes 7755728 (7.3 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 21550 bytes 31402300 (29.9 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

## Check if TCP Traffic Is Captured

Use `tcpdump` to capture traffic between the VM and Secure Access region.

```
tcpdump -i eth0 host iuvz83r.mxc1.acgw.sse.cisco.com
```

Example output (showing no packets captured):

```
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C
0 packets captured
6 packets received by filter
0 packets dropped by kernel
```

### Destroy and Reinstall the Connector if Necessary

Stop and destroy the connector if diagnostics and techsupport are not functioning:

```
/opt/connector/install/connector.sh stop --destroy
cd /opt
rm -rf connector
```

### Reinstall the Connector and Generate Tech Support Output

After reinstalling, generate tech support to capture error logs:

```
/opt/connector/data/bin/techsupport > techsupport.txt
Sample output showing connection errors:
2026-02-13 23:48:20.398772500  >> warning: Connection attempt has failed.
2026-02-13 23:48:20.398775500  >> warning: Unable to contact iuvz83r.mxc1.acgw.sse.cisco.com.
2026-02-13 23:48:20.398775500  >> error: Connection attempt has failed due to server communication erro
2026-02-13 23:48:20.398887500  >> state: Disconnected
```

## Adjust Docker MTU to Match Google Cloud VPC and VM Interface

Change the MTU on the Docker bridge interface to match the Google Cloud VPC default (1460 bytes):

```
ip link set dev docker0 mtu 1460
```

Verify MTU change:

```
ip a
```

Example output:

```
docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1460 qdisc noqueue state UP group default
link/ether 1e:66:46:1d:8b:ed brd ff:ff:ff:ff:ff:ff
inet x.x.x.x brd x.x.x.x scope global docker0
    valid_lft forever preferred_lft forever
inet6 fe80::1c66:46ff:fe1d:8bed/64 scope link
    valid_lft forever preferred_lft forever
```

### Persist Docker MTU Change in `/etc/docker/daemon.json`

Edit `/etc/docker/daemon.json` and add or update the `mtu` value:

```
{
  ...
  "mtu": 1460
}
```

### Restart the VM to Apply the MTU Configuration

Restart the complete VM to ensure the MTU settings are fully applied. This is necessary, because it is possible that r

After following these steps, connectivity to Secure Access was successfully established, and configuration could be c

## Cause

The root cause was an MTU mismatch between the Docker bridge interface (docker0) and the Google Cloud VPC/V

This mismatch caused fragmentation or dropped packets, preventing the Secure Access Resource Connector from es

## Related Content

- https://securitydocs.cisco.com/docs/csa/olh/120695.dita
- https://securitydocs.cisco.com/docs/csa/olh/120776.dita
- https://securitydocs.cisco.com/docs/csa/olh/120727.dita
- https://securitydocs.cisco.com/docs/csa/olh/120772.dita
- https://securitydocs.cisco.com/docs/csa/olh/120762.dita
- https://securitydocs.cisco.com/docs/csa/olh/120685.dita
- Cisco Technical Support & Downloads