排除Google Cloud Docker上的安全访问资源连接器部署和连接故障

目录

问题

尝试在Docker上部署安全访问资源连接器失败。

虽然连接器安装正确，但无法建立与Cisco Secure Access的连接。

诊断检查报告隧道断开和服务器通信错误。

该环境使用托管在Google云中的Red Hat 9虚拟机，通过Fortinet防火墙通过“any any”规则连接。

故障排除发现网络接口之间可能存在MTU不匹配是促成因素之一。

环境

- 技术：解决方案支持（SSPT — 需要合同）
- 子技术：安全访问 — 资源连接器（安装、升级、注册、连接、专用资源）
- 平台：Google Cloud上的Red Hat 9虚拟机
- 网络：安全访问和虚拟机之间的Fortinet防火墙（采用“任意”规则）
- 连接器区域： iuvz83r.mxc1.acgw.sse.cisco.com
- Google Cloud VPC默认MTU:1460字节
- Docker bridge(docker0)默认MTU:1500字节（更改前）
- 每个VM的单个网络接口(eth0)

分辨率

按照以下步骤诊断并解决Docker/Google云环境中的安全访问资源连接器连接问题：

检查连接器区域的DNS解析

使用`nslookup`确认可以从VM解析安全访问区域。

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

示例输出：

```
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
```

检查网络连接和安全访问

使用ping和telnet验证从VM到Secure Access的连接。

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

示例输出：

```
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
```

示例输出：

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

检查隧道连接并运行诊断

运行连接器诊断实用程序以检查隧道状态。

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

示例输出：

```
###check tunnel connection:
error: tunnel is not connected
```

检验网络接口和MTU设置

使用ifconfig和ip a检查所有接口的IP地址和MTU。

```
ifconfig
ip a
```

eth0和docker0的输出示例：

```
[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
```

检查是否捕获了TCP流量

使用tcpdump捕获VM和安全访问区域之间的流量。

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

示例输出（显示未捕获数据包）：

```
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
```

销毁并重新安装连接器（如有必要）

如果诊断和技术支持无法正常工作，请停止并销毁连接器：

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

重新安装连接器并生成技术支持输出

重新安装后，请生成技术支持以捕获错误日志：

```
/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
```

调整Docker MTU以匹配Google Cloud VPC和VM接口

更改Docker网桥接口上的MTU以匹配Google Cloud VPC默认值（1460字节）：

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

验证MTU更改：

```
ip a
```

示例输出：

```
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
```

在/etc/docker/daemon.json中保持Docker MTU更改

编辑/etc/docker/daemon.json并添加或更新mtu值：

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

重新启动虚拟机以应用MTU配置

重新启动完整的VM以确保MTU设置已完全应用。这是必要的，因为可能只有重新启动Docker服务不会对所有网络组件实施MTU更改。

完成这些步骤后，成功建立到安全访问的连接，并且可以完成配置。

原因

根本原因是Docker网桥接口(docker0)和Google Cloud VPC/VM网络接口(eth0)之间的MTU不匹配。Google Cloud VPC和VM接口默认的MTU为1460字节，而Docker默认MTU为1500字节。

此不匹配导致分段或丢弃数据包，阻止安全访问资源连接器建立隧道。调整MTU值解决了连接问题。

相关内容

- 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
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。