AppGate SDP Basic Troubleshooting Labs

Lefteris Chairetakis

Zahir Alli

October-2019

Singapore

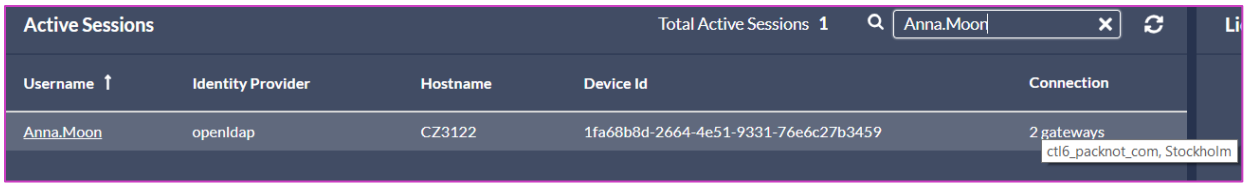
Table of Contents

Troubleshooting Lab 1 – Troubleshooting connection to resource behind the Gateway

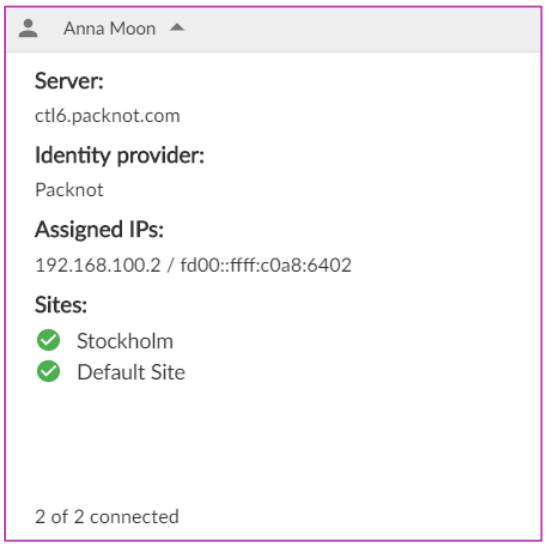
Distribution users log back in their AppGate Clients in the morning at work but nobody from their group seems to have access to the Production Site resources in Stockholm. As an AppGate admin you are called to fix that. What would be the troubleshooting steps to remedy this situation?

1) Do the users have connectivity to the Site in the first place? Where can you check for that?

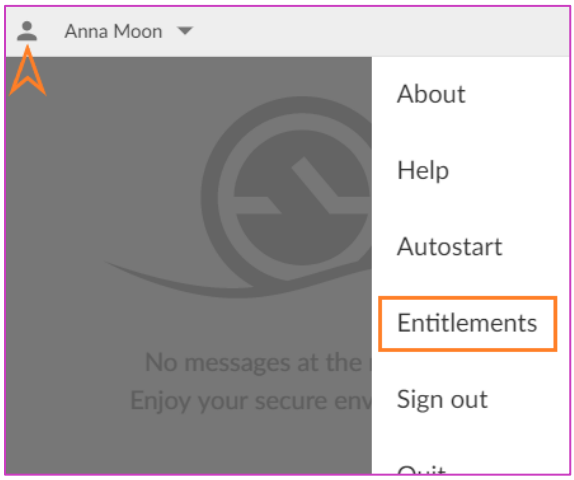
From the admin UI:

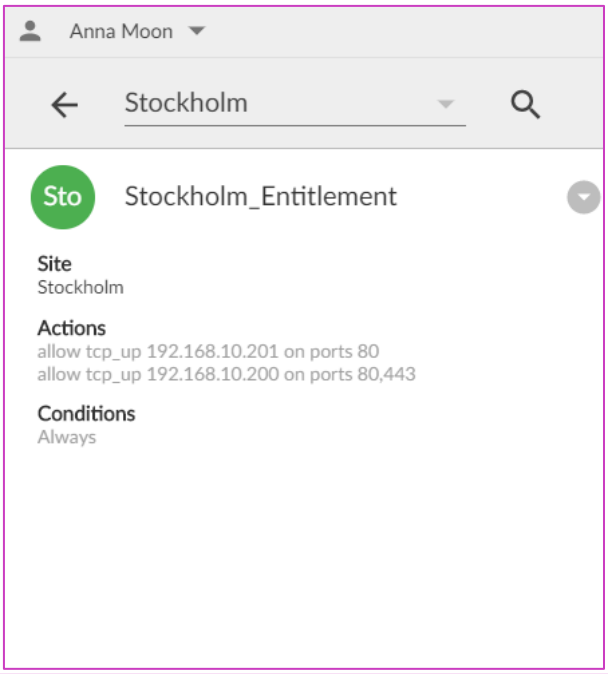


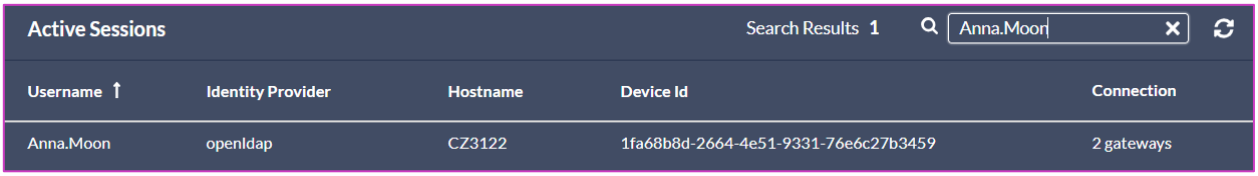
From the Client:

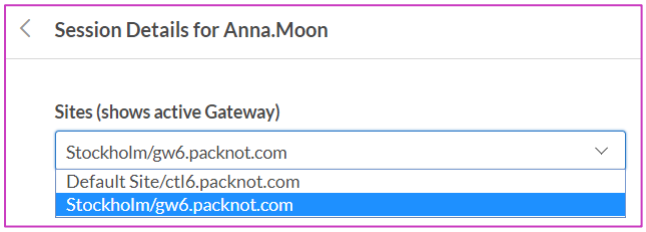


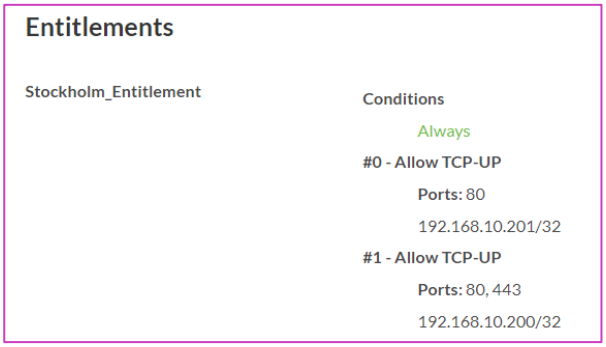
2) Once it has been checked that connectivity to the Site exists and the tunnel between the User and the Gateway is up, pick a user and make sure that they have the proper Entitlements for this Site assigned. How can you check that from the Client side? From the admin UI side?











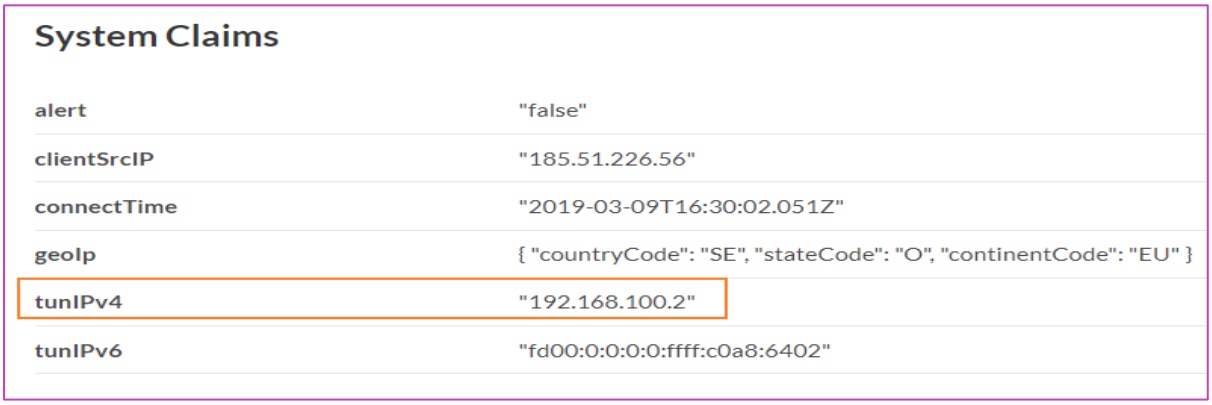
3) Once confirmed that the users have the proper Entitlements assigned, check the routing table on the user's machine to verify the routes to the resources behind the GW have been injected there.

```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      172.16.42.1     172.16.42.3     40
         10.10.0.2  255.255.255.255         On-link  192.168.100.2      1
     10.10.10.202  255.255.255.255         On-link  192.168.100.2      1
     10.10.10.203  255.255.255.255         On-link  192.168.100.2      1
     10.10.20.201  255.255.255.255         On-link  192.168.100.2      1
      13.53.35.74  255.255.255.255      172.16.42.1     172.16.42.3     40
    52.47.188.231  255.255.255.255      172.16.42.1     172.16.42.3     40
        127.0.0.0        255.0.0.0         On-link       127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link       127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link       127.0.0.1    331
     172.16.42.0    255.255.255.0         On-link     172.16.42.3    296
     172.16.42.1  255.255.255.255         On-link     172.16.42.3     40
     172.16.42.3  255.255.255.255         On-link     172.16.42.3    296
   172.16.42.255  255.255.255.255         On-link     172.16.42.3    296
   192.168.10.200  255.255.255.255         On-link  192.168.100.2      1
   192.168.10.201  255.255.255.255         On-link  192.168.100.2      1
     192.168.56.0    255.255.255.0         On-link    192.168.56.1    281
     192.168.56.1  255.255.255.255         On-link    192.168.56.1    281
   192.168.56.255  255.255.255.255         On-link    192.168.56.1    281
   192.168.100.2  255.255.255.255         On-link  192.168.100.2      257
        224.0.0.0        240.0.0.0         On-link       127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link    192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link     172.16.42.3    296
  255.255.255.255  255.255.255.255         On-link       127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link    192.168.56.1    281
  255.255.255.255  255.255.255.255         On-link     172.16.42.3    296
  255.255.255.255  255.255.255.255         On-link  192.168.100.2      257
===========================================================================
```

So far, we have confirmed that distribution users have connectivity to the Site, they are assigned the proper Entitlements needed for accessing the resources residing in the Stockholm Site and they have the correct routes to the resources via the tunnel interface.

However, distribution users are still not able to connect to the resources behind the Gateway. What could it be wrong? Since we have confirmed the Client side, let's move our investigation to the Gateway side and make sure that the traffic from the Clients is arriving and leaving the Gateway as well.

4) Pick a distribution user and look up for them in the AppGate admin Dashboard/UI under the Active sessions. Under System Claims, check for their tunIPv4 address. This is the IP that has been assigned to their tunneling driver on their machine.



5) SSH to the Gateway they are trying to connect – gwX.packnot.com according to the digit you are assigned – and check which is the tun device on the GW for that IP as shown in the example below:

```
cz@gw6:~$ ip add | grep 192.168.100.2
    inet 127.0.1.1 peer 192.168.100.2/32 scope host tun0
```

6) Next, have the user try to access the resource by accessing **192.168.10.200** or http://production.packnot.intra/ in their browser and do a **tcpdump** on the GW as below. Can you confirm that the traffic from the Client arrives at the Gateway?

```
cz@gw6:~$ sudo tcpdump -i tun0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on tun0, link-type RAW (Raw IP), capture size 262144 bytes
```

7) If the traffic arrives at the Gateway, then what remains to be checked is if it also leaves the Gateway or for some reason it is blocked. To confirm that, do a **tcpdump** on interface etho to see if traffic is going out of the GW to the protected resource – in your case http://production.packnot.intra/ (192.168.10.200):

```
cz@gw6:~$ sudo tcpdump -i eth0 dst host 192.168.10.200
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Is there any traffic destined for the remote host captured on the Gateway interface when the user tries to access the webpage?

If not, then this means that the client traffic cannot leave the Gateway. Time to check the configuration on the Gateway Appliance itself to figure out why the Client traffic is blocked!

Troubleshooting Lab 2 – Troubleshooting client connection to the Controller

You are an AppGate admin and your company cybersecurity team was doing an audit and pen test for AppGate while you were on vacation, you are back, and all users report they can't access the Controller, you try that yourself and still no luck! How to troubleshoot that?

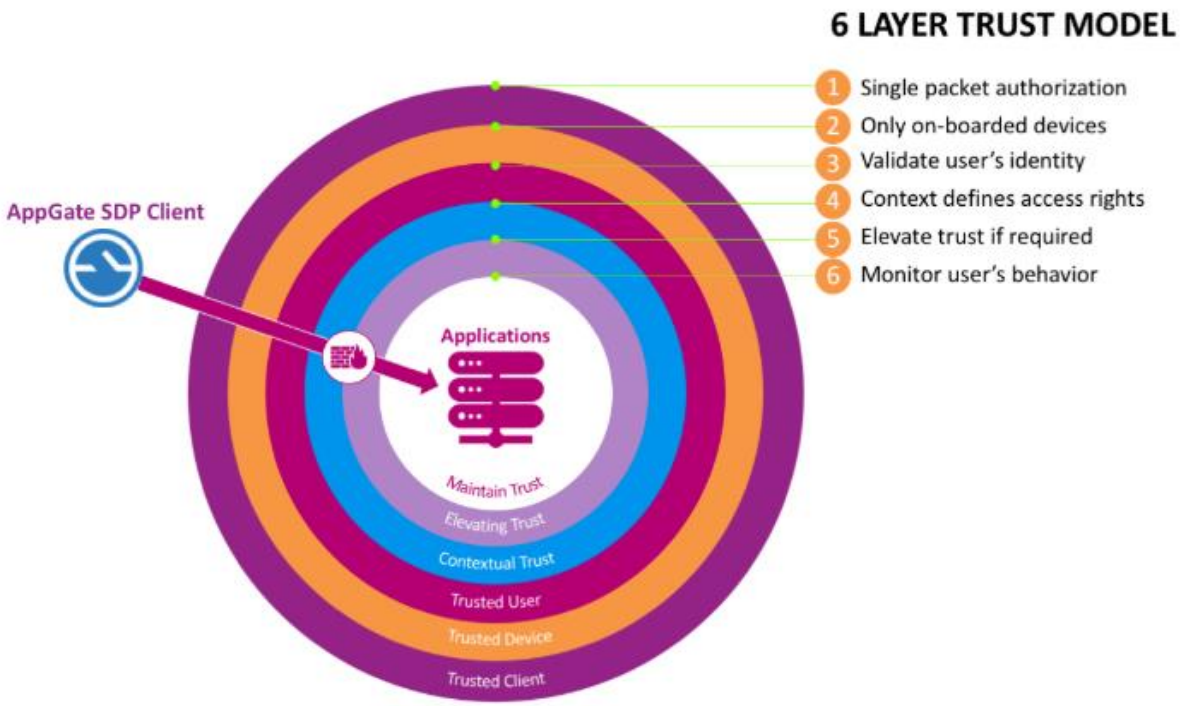
a) What is the error message you get when trying to connect? Which is the kind of logs you should be looking at first? Based on your machine's OS, check the following link from our admin guide to find the right path to those:

https://sdphelp.cyxtera.com/adminguide/v4.3/client-deploymanage.html

What is the error you are getting in the logs?

b) Once you have figured out what the issue has been above, you are attempting to connect again but still no luck. Access is denied. What is the error you get this time on your client? Do the logs shed any light on what the issue is this time?

Remember the multi-layer authorization model we talked about earlier:



At which stage of connection attempt are you currently found? Could it be an issue with SPA – SPA key used is wrong? Is there any indication it could be an on-boarding issue? What about the user's identity validation? Is the user authenticated successfully against our trusted account source? How can you check that from the admin UI as an administrator?

All the above could be potential reasons that would prevent a user from connecting with their client in the first place

Troubleshooting Lab 3 – Client cannot reach resources

You have successfully resolved the client connection issue to the Controller and users can login successfully now. However, they are not able to browse to http://distribution.packnot.intra anymore. What may have gone wrong this time?

Hint:- in the IT world, documentation is always very useful :-)

Troubleshooting Lab 4 – Client cannot reach resources at the Stockholm Site

Finally, after having fixed users connectivity issues to the Controller and your protected resources, you have become an AppGate Geek in your company :)

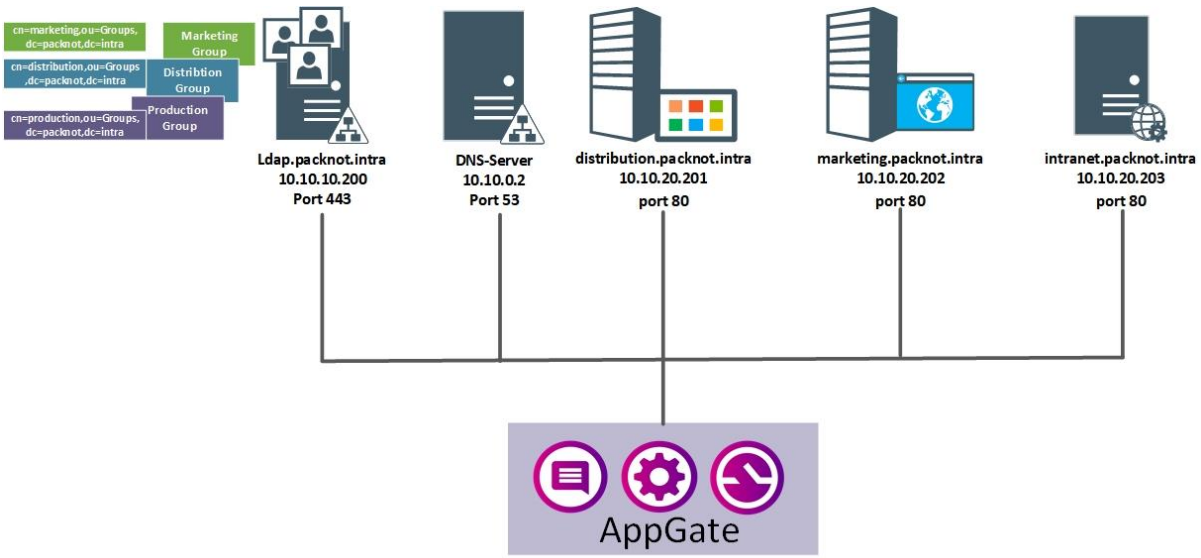
Later on, some users report they can't access the Stockholm site at http://production.packnot.intra/ anymore, you try that yourself and indeed it is not working. How to solve that?

Just like we did in Troubleshooting Lab 1, trace the packet-flow from your client all the way to the end server behind the Stockholm GW and make sure traffic is leaving the GW.

Hint: Can you tell what is the originating IP of your traffic when you are trying to access the production website? Provided that you have no access to the infrastructure behind the Gateway, what could you do as an AppGate admin to fix this issue?

Appendix: AppGate Training Environment

Pcknont HQ Infrastructure



Packnot Production-Site Infrastructure