

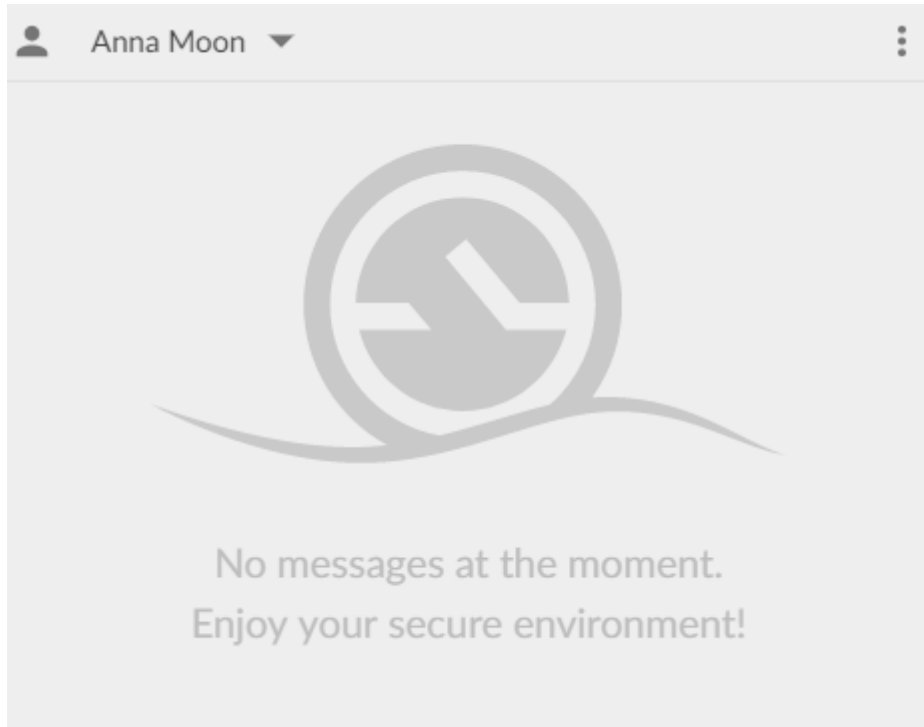
# Real world Scenario

**AppGate**SDP  
*Access, evolved.*

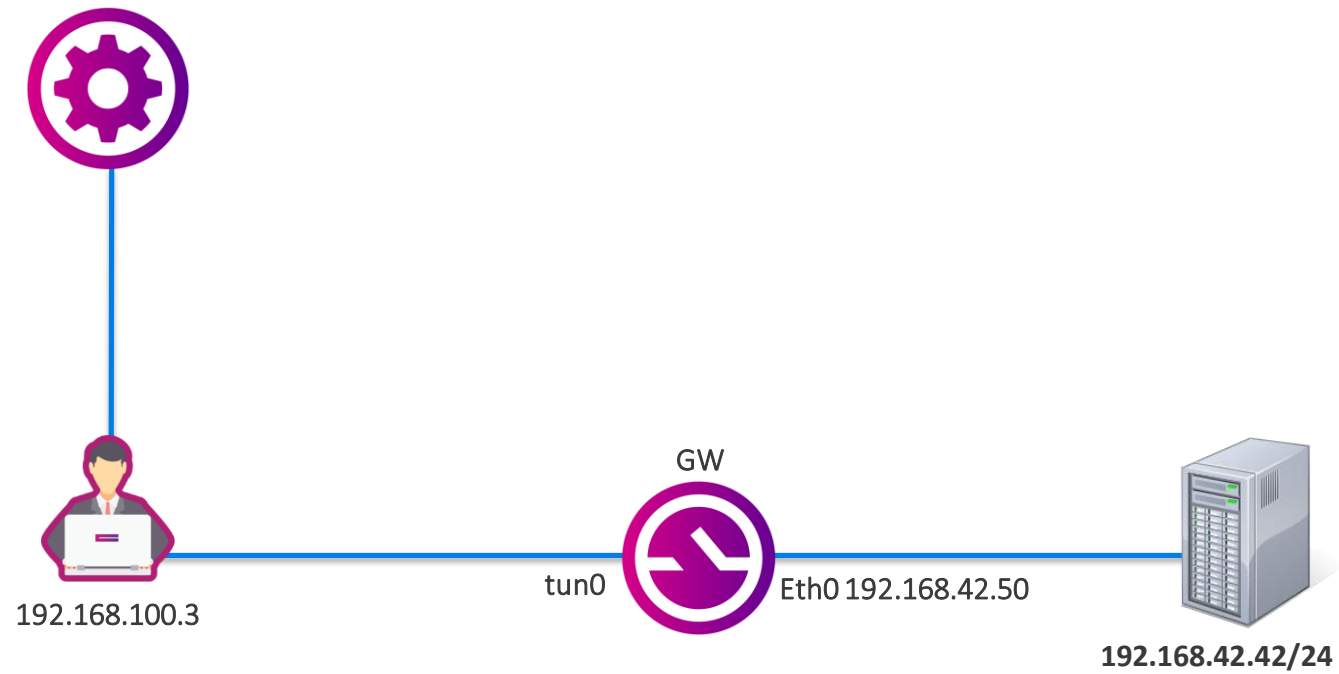
Cyxtera proprietary

# Scenario #1 - Appliance Side troubleshooting

- Anna is connecting but can't reach the server behind the GW



# Network design



# Controller & Client

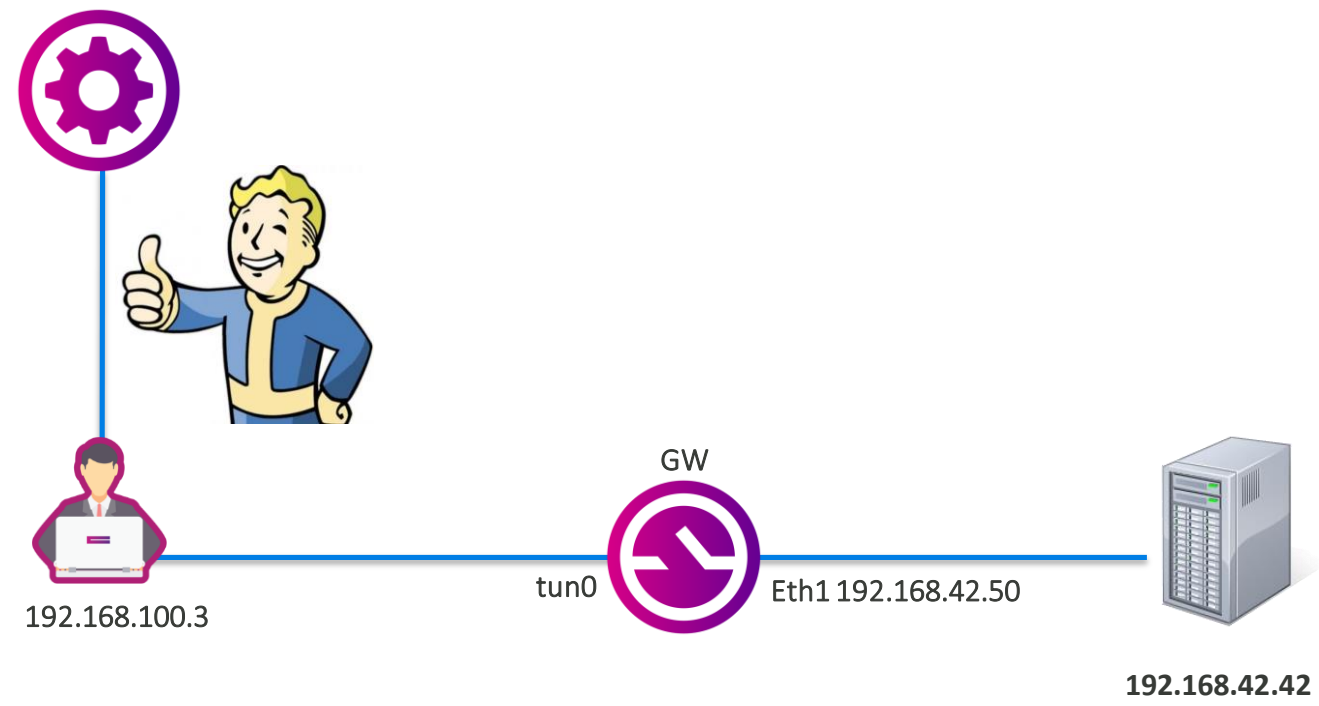
- 1. Client getting proper entitlement
- 2. Route correct on Client

IPv4 Route Table

=====

Active Routes:

Network Destination		Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	172.17.60.254	172.17.60.18		281
127.255.255.255	255.255.255.255	On-link	127.0.0.1		331
172.17.40.8	255.255.255.255	172.17.60.254	172.17.60.18		25
192.168.42.42	255.255.255.255	On-link	192.168.100.3		1
192.168.42.43	255.255.255.255	On-link	192.168.100.3		1
192.168.42.44	255.255.255.255	On-link	192.168.100.3		1
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	172.23.6.254		281
224.0.0.0	240.0.0.0	On-link	172.17.60.18		281
255.255.255.255	255.255.255.255	On-link	127.0.0.1		331



# Troubleshoot Connection to GW

1- Check the tun IP of client from Active session –System Claims

Active Sessions				Total Active Sessions 1	Q	↺
Username	Identity Provider	Hostname	Device Id	Connection		
Anna Moon	local	CYXSELP0001	820aac816b614b4c80a4bdbb19c48278	1 gateway		

▼ System Claims	
geolp	{"countryCode":"SE","continentCode":"EU"}
alert	false
connectTime	2018-01-26T07:19:49.255Z
tunIPv4	192.168.100.3
clientSrcIP	109.225.111.18

# Troubleshoot Connection to GW

2- Check which tun 192.168.100.3 on GW

```
cz@asdemo5:~$ ip add | grep 192.168.100.3  
    inet 127.0.1.1 peer 192.168.100.3/32 scope host tun0
```

3- TCPdump in tun0 to see if the traffic arrive

```
cz@asdemo5:~$ sudo tcpdump -i tun0  
[sudo] password for cz:  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on tun0, link-type RAW (Raw IP), capture size 262144 bytes  
07:29:40.494888 IP 192.168.100.3 > 192.168.42.42: ICMP echo request, id 1, seq 29, length 40  
07:29:45.273080 IP 192.168.100.3 > 192.168.42.42: ICMP echo request, id 1, seq 30, length 40  
^C
```

# Troubleshoot Connection to GW

4- Check packet on the outgoing interface of GW that facing the server

```
cz@asdemo5:~$ ip add | grep 192.168.42.50  
    inet 192.168.42.50/24 scope global eth1
```

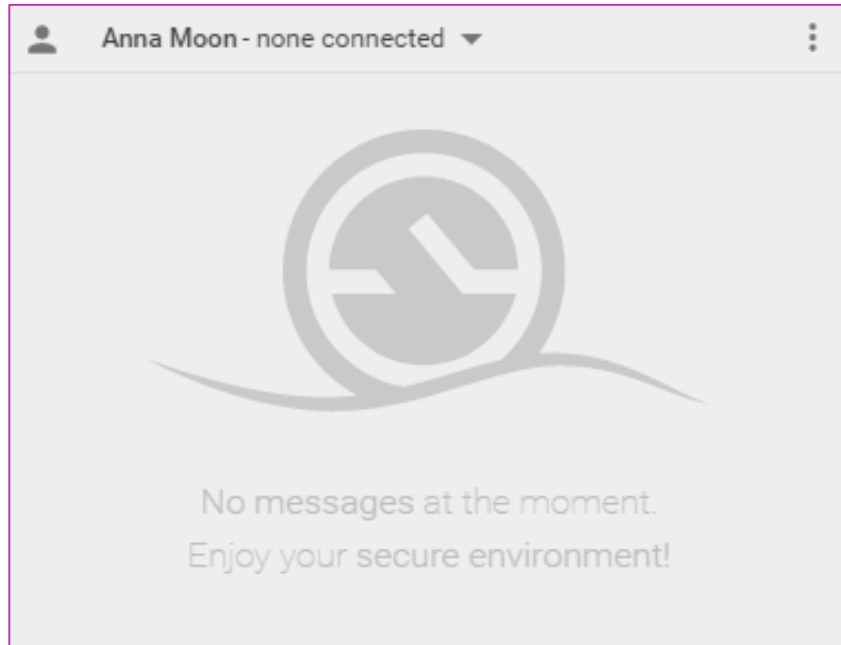
5- Tcpdump on eth1 to see if traffic going out of GW to Server

```
cz@asdemo5:~$ sudo tcpdump -i eth1  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes  
07:35:59.559021 IP 192.168.100.3.55456 > 192.168.42.43.domain: 11647+ A? d.docs.live.net. (33)  
07:36:00.279035 IP 192.168.100.3 > 192.168.42.42: ICMP echo request, id 1, seq 105, length 40  
07:36:05.275511 IP 192.168.100.3 > 192.168.42.42: ICMP echo request, id 1, seq 106, length 40
```

Traffic is leaving the GW so check the route between GW and Server

# Scenario #2 - Client Side troubleshooting

- Anna is not connecting





# Client Side troubleshooting

- Checking client log seem connection to controller is OK

```
[2018-02-20T16:24:25.021Z] Info : Setting controller URL to 'https://sdp6.appgate.com/'.
[2018-02-20T16:24:25.028Z] Info : CA certificate found in the storage for 'sdp6.appgate.com'.
[2018-02-20T16:24:25.031Z] Info : Resolving hostname 'sdp6.appgate.com'
[2018-02-20T16:24:25.139Z] Info : Trying to connect 'sdp6.appgate.com/18.195.206.116' with SPA UdpTcp and key name 'Built-in-be85360895242'.
[2018-02-20T16:24:25.558Z] Info : Using Controller API V4
[2018-02-20T16:24:25.574Z] Info : Certificate is already trusted. Moving on..
[2018-02-20T16:24:25.576Z] Info : Retrieving provider names from controller.
[2018-02-20T16:24:25.616Z] Info : Provider names: [local, openldap]
[2018-02-20T16:24:25.629Z] Info : Provider 'Packnot' selected.
[2018-02-20T16:24:25.633Z] Info : User input required for 'ConnectCredentialsLoginHandler'.
[2018-02-20T16:24:53.654Z] Info : Logging in using 'openldap'.
[2018-02-20T16:24:53.658Z] Info : Authenticating for the first time. RememberMe: False, Credentials: [Username 'anna.moon']
[2018-02-20T16:24:53.662Z] Info : Retrieving claims token.
[2018-02-20T16:24:53.666Z] Info : Fetching on-boarding cookie for 'OnBoardingCookie-29:4a:aa:69:1b:62:0a:b0:3a:93:0e:4e:76:ec:8b:41:c0:e7:b8:20:55:72:bb:43:4f:c9:fd:de:0a:be:fa:a3-openldap-anna.moon' from secure storage.
[2018-02-20T16:24:53.670Z] Info : On-boarding cookie available for 'OnBoardingCookie-29:4a:aa:69:1b:62:0a:b0:3a:93:0e:4e:76:ec:8b:41:c0:e7:b8:20:55:72:bb:43:4f:c9:fd:de:0a:be:fa:a3-openldap-anna.moon'.
[2018-02-20T16:24:53.751Z] Info : Authentication succeeded. Claims Token: [TokenId: cc45f3dc-d8a2-4e1e-b87d-63ed9a37c327, DistinguishedName: CN=26fedfae3cd74fe9b9a153bf8ce3707c,CN=Anna.Moon,OU=openldap, FirstName: Anna, LastName: Moon, ExpirationTime: 2018-02-21 17:24:55], On-demand Claims: [], Device Scripts: []
[2018-02-20T16:24:54.091Z] Info : Processing on-demand Claims: []
[2018-02-20T16:24:54.092Z] Info : Getting entitlement tokens for the first time.
[2018-02-20T16:24:54.094Z] Info : Retrieving entitlement tokens.
[2018-02-20T16:24:54.198Z] Info : New 2 entitlement tokens retrieved.
[2018-02-20T16:24:54.208Z] Info : Updating vpn certificate.
[2018-02-20T16:24:54.213Z] Info : Retrieving VPN certificate.
[2018-02-20T16:24:54.225Z] Info : No VPN certificate found in secure storage for 'CN=26fedfae3cd74fe9b9a153bf8ce3707c,CN=Anna.Moon,OU=openldap'. Generating a key-pair for a new one.
[2018-02-20T16:24:58.021Z] Info : A new key-pair for VPN certificate is generated. Requesting for controller to create a certificate out of it.
[2018-02-20T16:24:58.108Z] Info : New VPN certificate for 'CN=26fedfae3cd74fe9b9a153bf8ce3707c,CN=Anna.Moon,OU=openldap' is retrieved from controller. Storing it in secure storage.
[2018-02-20T16:24:58.109Z] Info : VPN certificate retrieved for CN=26fedfae3cd74fe9b9a153bf8ce3707c,CN=Anna.Moon,OU=openldap.
[2018-02-20T16:29:54.293Z] Info : Processing on-demand Claims: []
```

# However checking tun log showing the issue

```
[2018-02-20T16:35:10.782Z] Info : [Tokyo] Connecting to TLS://175.41.226.236:443 ...
[2018-02-20T16:35:10.788Z] Info : [Tokyo] Verification enabled for sdp6-tokyo.appgatex.com
[2018-02-20T16:35:10.789Z] Info : [Main site] Connecting to TLS://18.195.206.116:443 ...
[2018-02-20T16:35:10.789Z] Info : [Main site] Verification enabled for sdp6.appgatex.com
[2018-02-20T16:35:10.966Z] Info : [Main site] Connected (187ms)
[2018-02-20T16:35:10.974Z] Warn : Failed to find TAP device
[2018-02-20T16:35:10.974Z] Warn : Failed to initiate tun device
[2018-02-20T16:35:10.974Z] Info : [Main site] Closing (Failed to assign IP to tun device)
[2018-02-20T16:35:10.974Z] Info : Sending <{"jsonrpc": "2.0", "method": "status", "params": {"id": "staticid", "sites": {"Tokyo": {"gw-id": "Tokyo", "status": "down", "error": "Failed to assign IP to tun device", "code": 11},
"Main site": {"gw-id": "sdp6_appgatex_com", "status": "down", "error": "Failed to assign IP to tun device", "code": 11}}} }>
[2018-02-20T16:35:11.783Z] Info : [Tokyo] Connected (1000ms)
[2018-02-20T16:35:11.790Z] Warn : Failed to find TAP device
[2018-02-20T16:35:11.791Z] Warn : Failed to initiate tun device
[2018-02-20T16:35:11.791Z] Info : [Tokyo] Closing (Failed to assign IP to tun device)
[2018-02-20T16:35:11.791Z] Info : Sending <{"jsonrpc": "2.0", "method": "status", "params": {"id": "staticid", "sites": {"Tokyo": {"gw-id": "Tokyo", "status": "down", "error": "Failed to assign IP to tun device", "code": 11},
"Main site": {"gw-id": "sdp6_appgatex_com", "status": "down", "error": "Failed to assign IP to tun device", "code": 11}}} }>
```

# The end

**AppGate**SDP  
*Access, evolved.*

Cyxtera proprietary