

# Audit Logs and Simple Troubleshooting

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

Cyxtera proprietary

# Overview

- Audit Logs
  - Log events in the AppGate System
  - Audit logs and User Interface to Audit logs
  - Configure Appliance as Log Server
- Troubleshooting
  - Appliance-level
  - Operational-level
  - Client

# Audit Logs

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

# Debug vs Auditing Logs

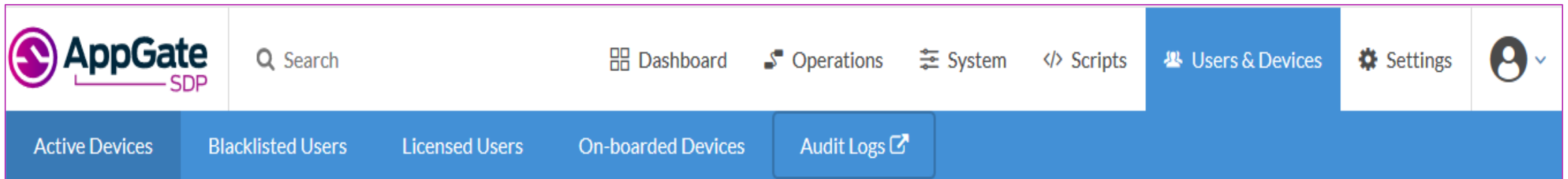
- Debug and Audit logs are **very different**
  - Audit logs are in JSON.
  - Debugs logs output depends on the daemon
- Both Debug & Audit logs are written to **local syslog**
- **Only** Audit Logs are in Kibana

# Log events in the AppGate System

- All appliances create “audit event” logs , Logs are automatically saved on the appliance. If a LogServer has been added to the collective, logs will be routed to the LogServer automatically
- Audit events can be received by a **Log Server** appliances
  - Centrally receives all audit logs
  - Stand alone or co-habit with the controller
  - Traffic is *secured* by a mutually-certificated TLS channel
  - Clients ***do not*** send their logs
- **All** log entries can be sent to rsyslog



- Logstash
  - Input: Parses logs create **json** formatted records
- Elastic search
  - Data: NoSQL, search and analytics engine
- Kibana
  - User Interface: to work with the data



# Auditing with Kibana

- Kibana is part of "**ELK Stack**" open source
  - Elastic Search, Log Stash, Kibana
  - **Not our product**
- Out of box shipped with AppGate
- Customers **should** use their own SIEM like Splunk etc.
- Kibana is only for demos and Small customers

# Audit-log user interface: Kibana

## ■ Discover

- Lets you discover and search the data
- Save/load search expressions
  - example: "authorization failed"

## ■ Visualization

- Lets you create tables and charts of datasets,
  - Example: Firewall IP addresses, top entitlements on gateway X, etc.

## ■ Dashboard

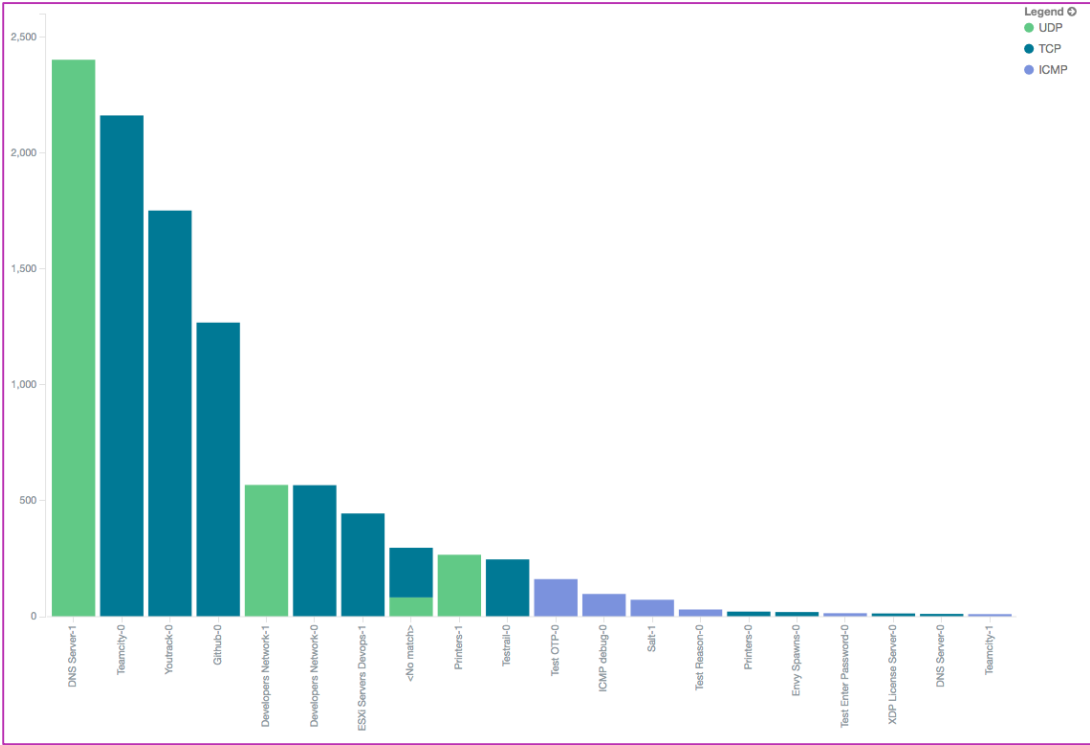
- Lets you create a dashboard with visualizations
- Dashboards can be for example created by use case:
  - User Audits
  - Network audits



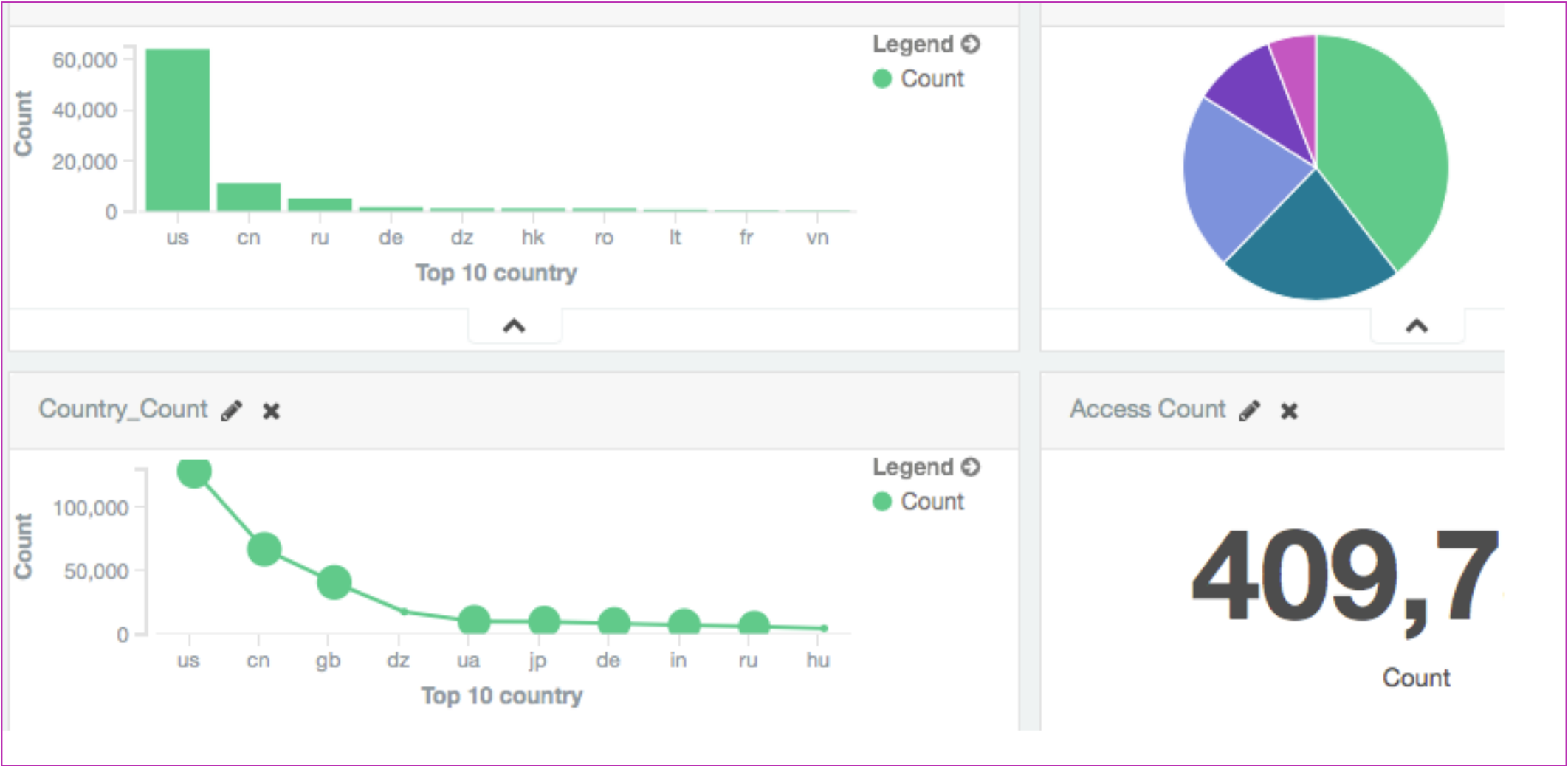
# Examples of audit logs in Kibana

`_exists_:event_type AND daemon:"cz-authord" AND entity_type:condition`

Rule name access per user		
Top 20 rule_name.raw	Top 20 distinguished_name.user.raw	Count
DNS Server-1	kurt.glazemakers	4,472
Teamcity-0	kurt.glazemakers	1,036
Printers-1	kurt.glazemakers	251
Youtrack-0	kurt.glazemakers	161
<No match>	kurt.glazemakers	40
Test Reason-0	kurt.glazemakers	13
ESXi Servers Devops-1	kurt.glazemakers	11
Testrail-0	kurt.glazemakers	10



# More examples (dashboard)



# Configure Appliance as Log Server

- Add a new appliance
- Add function to existing appliance
- Audit Log retention period can be set (defaults to the last 30 days)



**Roles**  
☒ Controller  
☒ LogServer  
**Audit Log Retention (days)**  
  
☒ Gateway

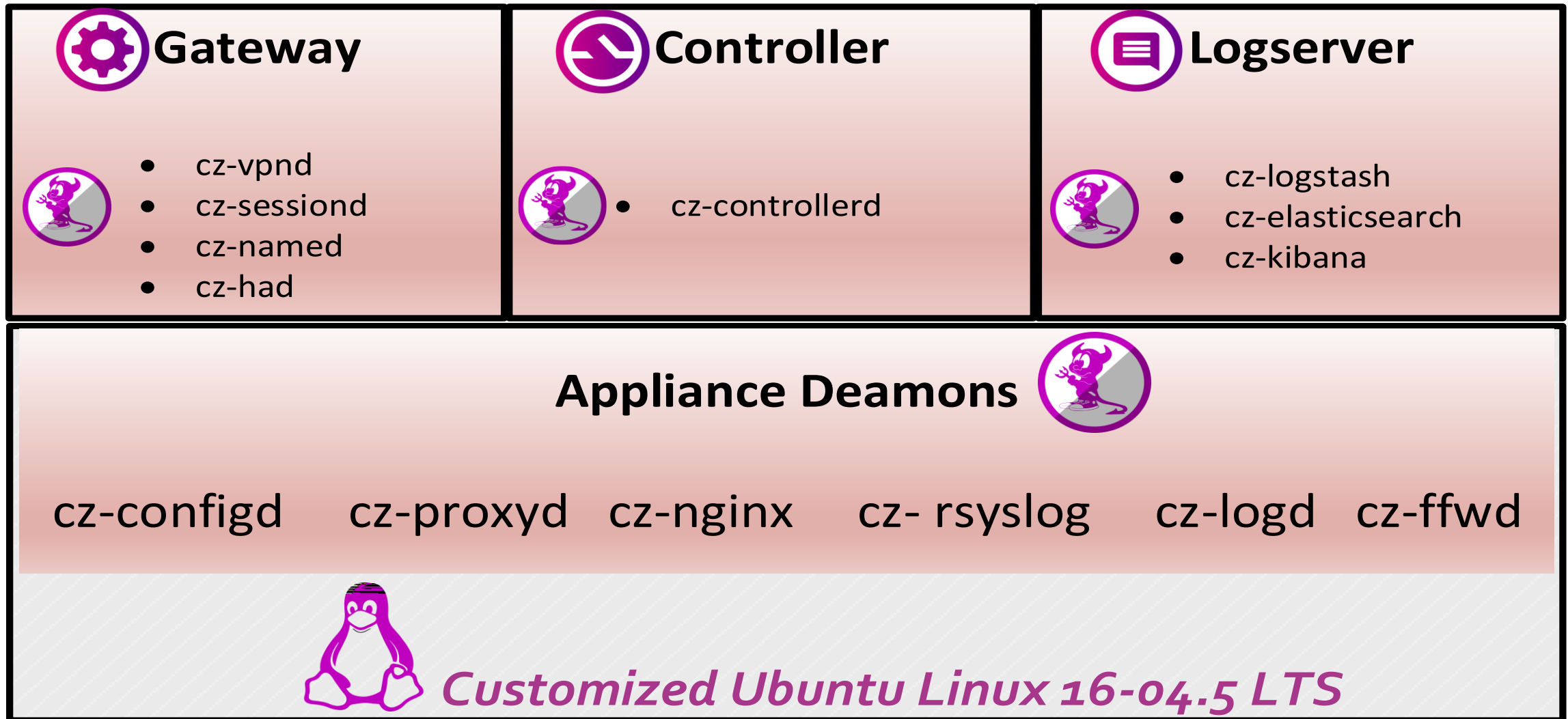
# Troubleshooting at the Appliance Level

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

# Part 1: Appliance components

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

# Appliance architecture



# Daemons



- Daemons are functional components, running on Linux Ubuntu
- Every daemon has a functional task in the overall system
- Self contained programs (C++, Java, python)
- Decoupled
- Communicate locally over sockets (TCP ports),
- Communicate **between** appliances over TLS+TCP



# Appliance Daemons –in general

- **cz-configd**: Manages and applies the appliance configuration
- `journalctl -u cz-configd.service -f`

```
Feb 27 13:32:59 appgate.example.com systemd[1]: Started AppGate appliance configuration daemon.
```

```
Feb 27 13:33:02 appgate.example.com cz-configd[635]: INFO [networking] Waiting for DHCP configuration to be applied on the following NICs: eth0 ...
```

```
Feb 27 13:33:22 ec2-13-48-24-163.eu-north-1.compute.amazonaws.com cz-configd[635]: WARNING [status] System status changed from busy to healthy
```

```
Mar 05 10:29:48 gw7.packnot.com cz-configd[635]: INFO [ActivateApplianceAction] Activating appliance...
```

```
Mar 05 10:29:48 gw7.packnot.com cz-configd[635]: INFO [ActivateApplianceAction] Appliance activated.
```

- **cz-proxyd**: Listens for TCP connections and forwards to the correct component depending on the connection type (HTTPS or VPN traffic).

```
Mar 05 10:59:14 ctl7.packnot.com cz-proxyd[4129]: INFO [2019-03-05T10:59:14.080Z] [M 7f63f0244cc0] [7] SPA-TCP message from 82.100.100.100:42545 has been authorized by using the key with name "Built-in-be85360895242"
```

```
Mar 05 10:59:14 ctl7.packnot.com cz-proxyd[4129]: INFO [2019-03-05T10:59:14.080Z] [M 7f63f0244cc0] [7] Not a VPN connection, passing to /run/czd/cz-nginx.socket [redacted]:42545
```



# Appliance Daemons –in general

- **cz-ffwd**: Forwards logs from rsyslog securely to the AppGate log server, also receives logs securely on the AppGate log server.
- **nginx**: Frontend for all the HTTPS traffic, routes it to the correct daemon and the admin UI.

```
43 "https://ctl7.packnot.com:444/ui/active-users" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36"
Mar 05 10:57:53 ctl7.packnot.com nginx[6622]: [REDACTED] - - [05/Mar/2019:10:57:53 +0000] "PUT /admin/token-records/revoked/by-dn/CN=820aac816b614b4c80a4bdbb19c48278,CN=Anna.Moon,OU=openldap HTTP/2.0" 200 911 "https://ctl7.packnot.com:444/ui/active-users" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36"
Mar 05 10:57:53 ctl7.packnot.com nginx[6622]: 127.0.1.1 - - [05/Mar/2019:10:57:53 +0000] "POST /sessions/revocations HTTP/1.1" 201 0 "-" "cz-controllerd (appliance-connector)"
```

# Appliance Daemons –in general

- **cz-logd:** Gathers the audit-logs from all the daemons running on the Appliance, and forwards them to rsyslog and logserver.
- **rsyslog:** Receives the audit-logs from cz-logd, gathers logs from all the daemons running on the Appliance and forwards them to external log systems.

```
Mar 17 16:35:19 gw7.packnot.com cz-proxyd[12865]: ERR [2019-03-17T16:35:19.784Z] [M 7f9db0af8cc0] [7] Dropping nginx connection
Mar 17 06:39:44 ctl7.packnot.com cz-controllerd[3733]: INFO [AdminMessageCleanupService] Cleaning up admin messages.
Mar 17 06:39:44 ctl7.packnot.com cz-controllerd[3733]: INFO [LdapConnectionPoolCache] Cleaning up LDAP connection cache.
Mar 17 06:40:38 ctl7.packnot.com systemd-journald[341]: Forwarding to syslog missed 2 messages.
Mar 17 07:41:32 ctl7.packnot.com cz-sessiond[6730]: INFO [2019-03-17T07:41:32.923Z] [AppDiscoveryCollection] No old appDiscoverys to cleanup, still exists: 0
Mar 17 09:55:08 ctl7.packnot.com cz-appliance: [AUDIT] {"username":"alvin","version":9,"timestamp":"2019-03-17T09:55:08Z","event_type":"ssh_access_failed","client_ip":"73.70.13.247","collective_id":"7c24581a-8fce-4bd2-be2d-ead5de1572b2"}
Mar 17 09:55:36 ctl7.packnot.com cz-appliance: [AUDIT] {"username":"test","version":9,"timestamp":"2019-03-17T09:55:35Z","event_type":"ssh_access_failed","client_ip":"198.199.66.10","collective_id":"7c24581a-8fce-4bd2-be2d-ead5de1572b2"}
```

- **ssh:** Handles SSH connections to the Appliance.

# Daemons – Controller feature

- **cz-controllerd:**
  - Manages appliances, sites and the dashboard.
  - Handles authentication, claims tokens
  - Handles authorization, entitlements, policies, condition expression, entitlement and administration
  - Handles communications with identity

```
Mar 18 12:17:20 ctl7.packnot.com cz-controllerd[3733]: ERROR[DefaultLdapConnectionFactory] ERR_04102_UNABLE_TO_BIND_CONNECTION unable to bind connection:  
Mar 18 12:17:20 ctl7.packnot.com cz-controllerd[3733]: WARN [LdapConnector] LDAP failure on 'openldap'. Details:
```

```
Mar 18 12:21:36 ctl7.packnot.com cz-controllerd[3733]: {"id":"1aa17738-dc31-4fee-b248-495c8aabf433","timestamp":"2019-03-18T12:21:36.288Z","version":9,"distinguished_name":"CN=820aac816b614b4c80a4bdbb19c48278,CN=Anna.Moon,OU=openldap","claims_token_id":"1b56e828-92d1-4b80-ad69-b0f49f2a00ff","authentication_type":"Client","client_ip":"[REDACTED]","user_claims":{"firstName":"Anna","lastName":"Moon","ag":{"loginTime":"2019-03-18T12:21:36.284Z","distinguishedName":"CN=820aac816b614b4c80a4bdbb19c48278,CN=Anna.Moon,OU=openldap"},"identityProviderId":"ffffffff-a0a0-a0a0-a0a0-000000000022"},"ldapOU":"clevel,office,distribution,production-site","userId":"Anna.Moon","username":"Anna.Moon","group":["cn=clevel,ou=Groups,dc=packnot,dc=ing","cn=office,ou=Groups,dc=packnot,dc=ing","cn=distribution,ou=Groups,dc=packnot,dc=ing","cn=production-site,ou=Groups,dc=packnot,dc=ing"]},"event_type":"authentication_succeeded"}
```

# Daemons - Gateway feature

- **cz-sessiond**: Handles the client claims and entitlement tokens and generates the firewall rules that it sends to vpnd.

```
Mar 18 12:26:36 gw7.packnot.com cz-sessiond[13226]: INFO [2019-03-18T12:26:36.960Z] [PolicyEnforcer] [CN=820aac816b614b4c80a4bdbb19c48278,CN=Anna.Moon,OU=openldap] Entitlement result: Stockholm success
Mar 18 12:26:36 gw7.packnot.com cz-sessiond[13226]: INFO [2019-03-18T12:26:36.961Z] [AuditJsonEventLogger] {"id":"204c1bb6-a0b3-4e80-b42c-64e29ddac966","timestamp":"2019-03-18T12:26:36.952Z","version":9,"distinguished_name":"CN=820aac816b614b4c80a4bdbb19c48278,CN=Anna.Moon,OU=openldap","session_id":"45491640-5cda-4682-9271-7d2640cd1460","successful_condition_names":["Always"],"entitlement_token_id":"93be4e6e-800f-4be7-9f12-a2dd88b762ea","successful_entitlement_names":["Stockholm"],"execution_ms":9,"event_type":"entitlement_token_evaluated","entitlement_token_available":true}
Mar 18 12:29:25 gw7.packnot.com cz-sessiond[13226]: INFO [2019-03-18T12:29:25.523Z] [VpndUnsubscribeEvent] [CN=820aac816b614b4c80a4bdbb19c48278,CN=Anna.Moon,OU=openldap] vpnd->unsubscribe, vpnd id: 13302
Mar 18 12:29:25 gw7.packnot.com cz-sessiond[13226]: INFO [2019-03-18T12:29:25.523Z] [VpndUnsubscribeEvent] [CN=820aac816b614b4c80a4bdbb19c48278,CN=Anna.Moon,OU=openldap] no subscribers left on session, will remove in 300000 milisec
Mar 18 12:29:25 gw7.packnot.com cz-sessiond[13226]: INFO [2019-03-18T12:29:25.523Z] [Session] [CN=820aac816b614b4c80a4bdbb19c48278,CN=Anna.Moon,OU=openldap] Starting inactivity timer, will remove session at 2019-03-18T12:34:25.523Z
```

- **cz-vpnd**: Handles the actual VPN traffic and has the firewall engine.

```
Mar 18 12:32:15 gw7.packnot.com cz-vpnd@0[13302]: INFO [2019-03-18T12:32:15.909Z] [C 7f0c34eec700] CN=820aac816b614b4c80a4bdbb19c48278,CN=Anna.Moon,OU=openldap TUN device 'tun0' has been created: 13
```

```
Mar 18 12:32:35 gw7.packnot.com cz-vpnd@0[13302]: INFO [2019-03-18T12:32:35.954Z] [C 7f0c34eec700] CN=820aac816b614b4c80a4bdbb19c48278,CN=Anna.Moon,OU=openldap TLS connection has been terminated: "SSL_read(): the TLS/DTLS connection has been closed by peer"
Mar 18 12:32:35 gw7.packnot.com cz-vpnd@0[13302]: INFO [2019-03-18T12:32:35.975Z] [R 7f0c356ed700] Forwarding unsubscription of "CN=820aac816b614b4c80a4bdbb19c48278,CN=Anna.Moon,OU=openldap" to sessiond from connection thread [C 7f0c34eec700]
```

# Daemons - Gateway feature

- **cz-named:** Resolves names to IPs using various resolvers (DNS, AWS, ...).

```
Mar 06 10:17:33 gw7.packnot.com systemd[1]: Stopped AppGate appliance name resolution daemon.  
Mar 06 10:17:33 gw7.packnot.com systemd[1]: Started AppGate appliance name resolution daemon.  
Mar 06 10:17:36 gw7.packnot.com cz-named[12385]: [INFO] [AWSResolver] AWSResolver creating, regions None vpcs None vpc auto discovery True, caching time 900  
Mar 06 10:17:36 gw7.packnot.com cz-named[12385]: [INFO] No DNS resolver was defined, adding a default name resolver using the hosts file and system dns servers  
Mar 06 10:17:36 gw7.packnot.com cz-named[12385]: [INFO] Hostname resolver "Default hostname resolver" started using the following DNS server(s): 192.168.0.2, 10.10.0.2
```

- **cz-had:** Handles client failover via the ARP (ipv4) and NDP protocol (ipv6). It is also used to handle **ARP** and **NDP** requests sent over the local network so that the router and/or endpoints can find where to send back traffic to the clients through the tunnel.

```
Mar 15 22:29:54 asdemo5.cryptzone.com cz-had[1746]: Log "Broadcasted Gratuitous ARP reply via interface eth1 for IPv4 address 192.168.1.16" wrapped 2 times  
Mar 15 22:29:54 asdemo5.cryptzone.com cz-had[1746]: INFO [2019-03-15T22:29:54.518Z] Proxy ARP stopped for IP 192.168.1.16  
Mar 16 20:16:46 asdemo5.cryptzone.com cz-had[1746]: INFO [2019-03-16T20:16:46.346Z] Starting Proxy ARP for IP 192.168.1.16  
Mar 16 20:16:46 asdemo5.cryptzone.com cz-had[1746]: INFO [2019-03-16T20:16:46.346Z] Broadcasted Gratuitous ARP reply via interface eth1 for IPv4 address 192.168.1.16  
Mar 16 20:22:02 asdemo5.cryptzone.com cz-had[1746]: Log "Broadcasted Gratuitous ARP reply via interface eth1 for IPv4 address 192.168.1.16" wrapped 2 times  
Mar 16 20:22:02 asdemo5.cryptzone.com cz-had[1746]: INFO [2019-03-16T20:22:02.520Z] Proxy ARP stopped for IP 192.168.1.16
```

# Daemons – Log Server feature

- Logd: Collects and parses audit logs and sends them to elasticsearch.
- Elasticsearch: Log database used for audit logs.
- Kibana: Log viewer used to view audit logs.



# Troubleshooting on appliance level

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

# Appliance Logs

- To see live logs:

```
journalctl -f
```

- To show specific service

```
journalctl -u cz-configd
```

```
journalctl -u cz-vpnd@o (vpnd instance number o)
```

```
journalctl -u "cz-vpnd@*" (vpnd all instances)
```

- To only show logs from a certain importance

```
journalctl -p warning
```

- To show logs in a certain time range

```
journalctl --since="2017-06-01 12:17:16" --until="2017-06-02"
```



# Download \*any\* appliance logs via UI

Appliances

Sites

IP Pools

Identity Providers

MFA Providers

Admin Roles

Appliances

Total Appliances 2

Search

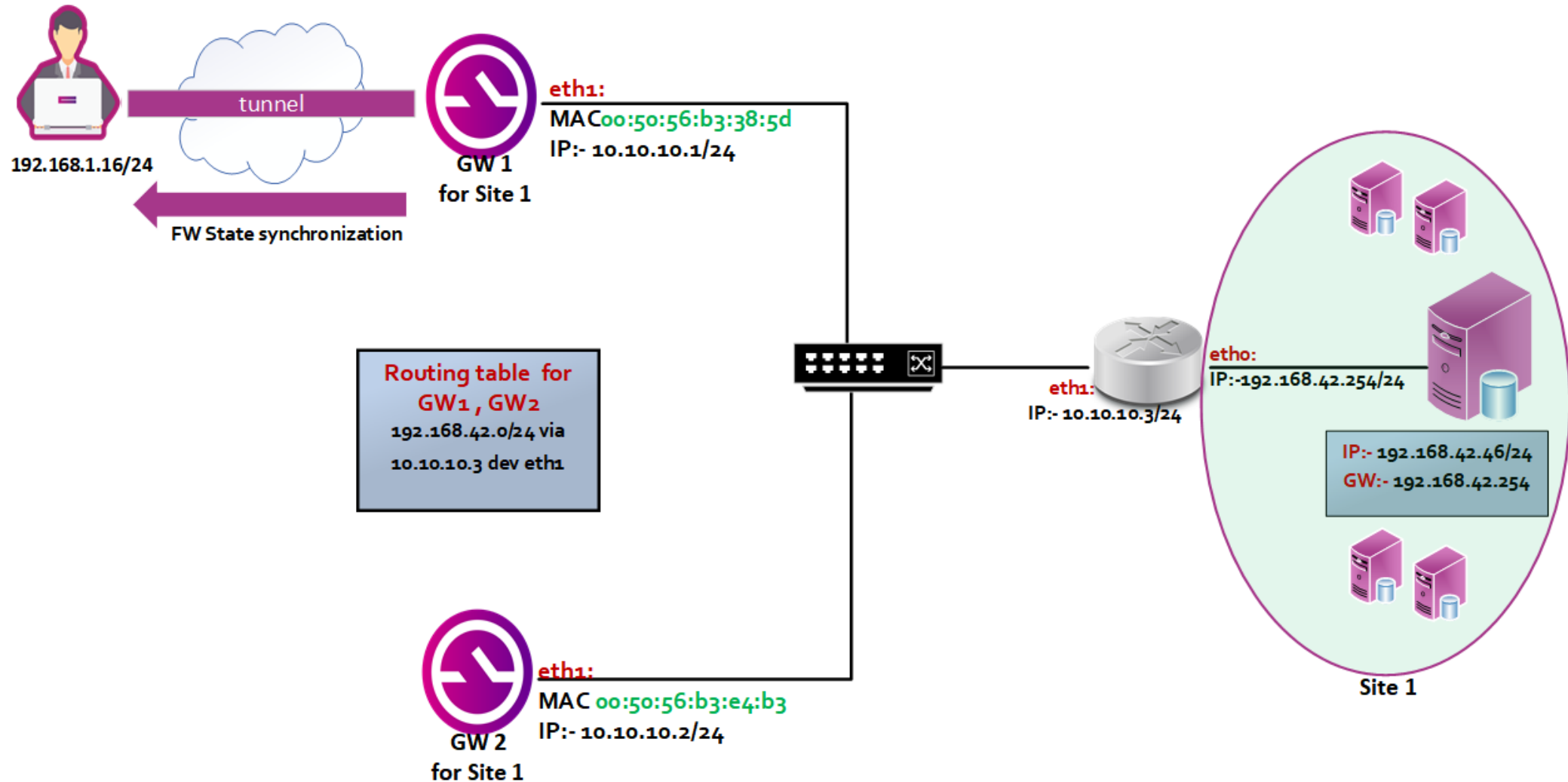
Add New

Name ↑	Hostname	Site	State	Tags	Modified	
<a href="#">sdps2_appgatex.com</a>	sdps2.appgatex.com	<a href="#">Main site</a>	Active	<div>managed-by-trent</div> <div>first-appliance</div>	11/12/2018, 3:48:26 PM	<div><div></div><div></div><div></div></div>
Tokyo	sdps3-gw-tk.appgatex.com	Tokyo	Active		11/16/2018, 2:07:01 PM	<div><div></div></div>

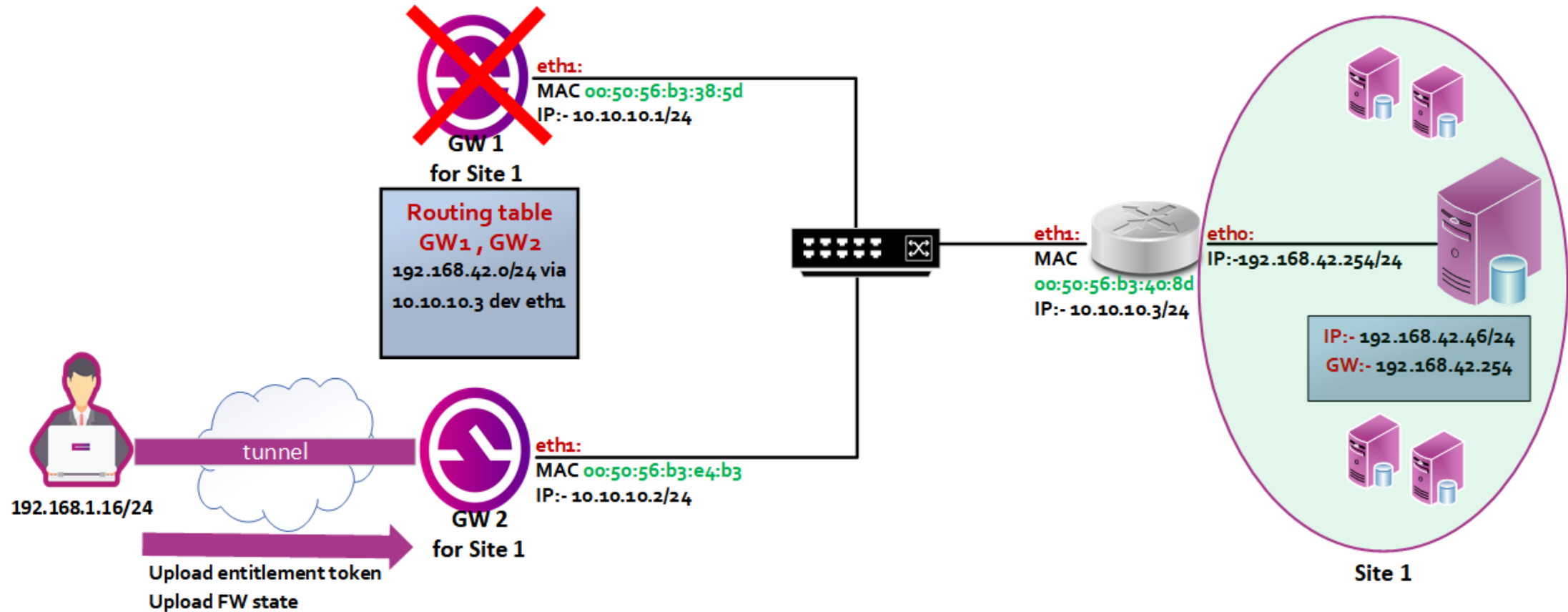
# High Availability – Gateways

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

# Stateful Failover & Linear Scaling



# Stateful Failover & Linear Scaling



```
cz-had[1778]: INFO [2018-10-04T12:10:24.895Z] Broadcasted Gratuitous ARP reply via interface eth1 for IPv4 address 192.168.1.16
cz-had[1778]: INFO [2018-10-04T12:54:48.358Z] An ARP request has been received from 0:50:56:b3:40:8d via interface eth1 for IP 192.168.1.16
cz-had[1778]: INFO [2018-10-04T12:54:48.358Z] Sent ARP reply to 0:50:56:b3:40:8d via interface eth1 for IPv4 address 192.168.1.16
```

# Debug Log

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

# Run cz-setup

Appliance setup

This appliance has already been seeded.

Change log levels

Reassign network interfaces

Exit

# Change Log Level to Debug

Change log levels	
Daemon	Log level
configd	INFO
controllerd	INFO
had	INFO
healthcheckd	INFO
named	INFO
nginx	INFO
proxyd	INFO
sessiond	INFO
vpnd	INFO
Apply changes	

Set log level for configd

DEBUG

INFO

WARNING

ERROR

CRITICAL

Arrow keys to move, RETURN to select, ESC to leave

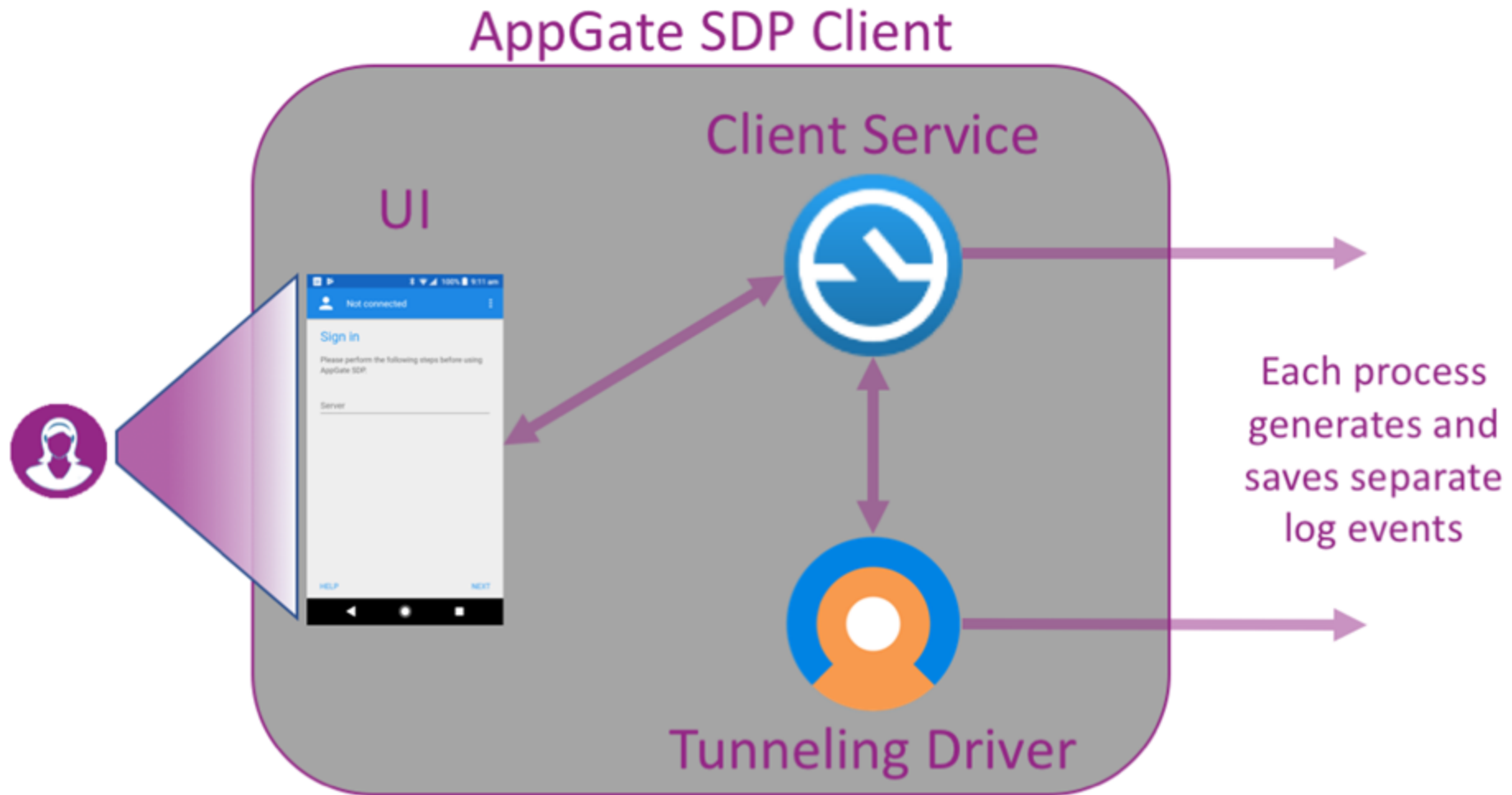


# Client-side Troubleshooting

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



# Remember



# Client Components Cont'd

- Client Daemon

AppGate SDP Driver	0,2%	1,7 MB	0 MB/s	0 Mbps
AppGate SDP Service (32 bit)	0%	15,0 MB	0 MB/s	0 Mbps

- User Interface

Not signed in

Sign in

Please perform the following steps before using AppGate SDP.

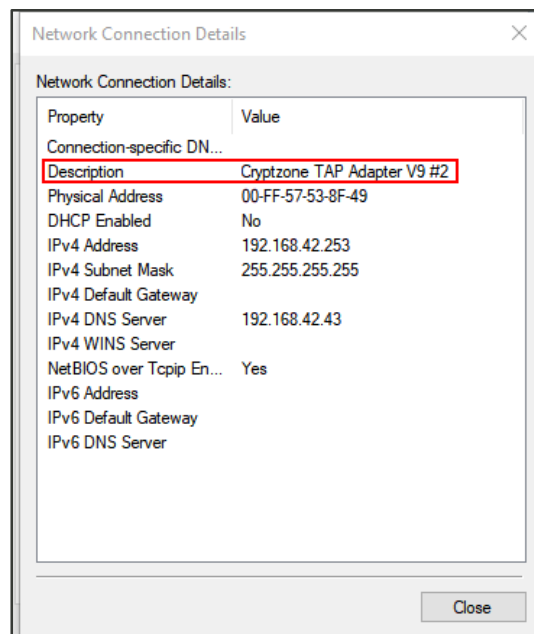
Server  
sdp.appgate.lab

HELP CANCEL NEXT

# Client Components Cont'd

- Tunneling service (runs with root privileges)
  - Shuffles IP packets, connects to Gateways (vpnd, sessiond), ships tokens
  - Provides a virtual network adapter (tun-device)


> AppGate IP Tunneling Driver Service (32 bit)	0%	0,1 MB	0 MB/s	0 Mbps
AppGate SDP (32 bit)	0%	31,3 MB	0 MB/s	0 Mbps
AppGate SDP (32 bit)	0%	32,7 MB	0 MB/s	0 Mbps



# Client Access Steps

1. SPA Network Layer
2. On-Boarding First connection only
3. Authentication Client receives Claims Token
4. Authorization Client receives Entitlements Tokens
5. Gateway conn One connection per Site

# Client Access Steps

 zahir - none connected ▲

Server:






Identity provider:

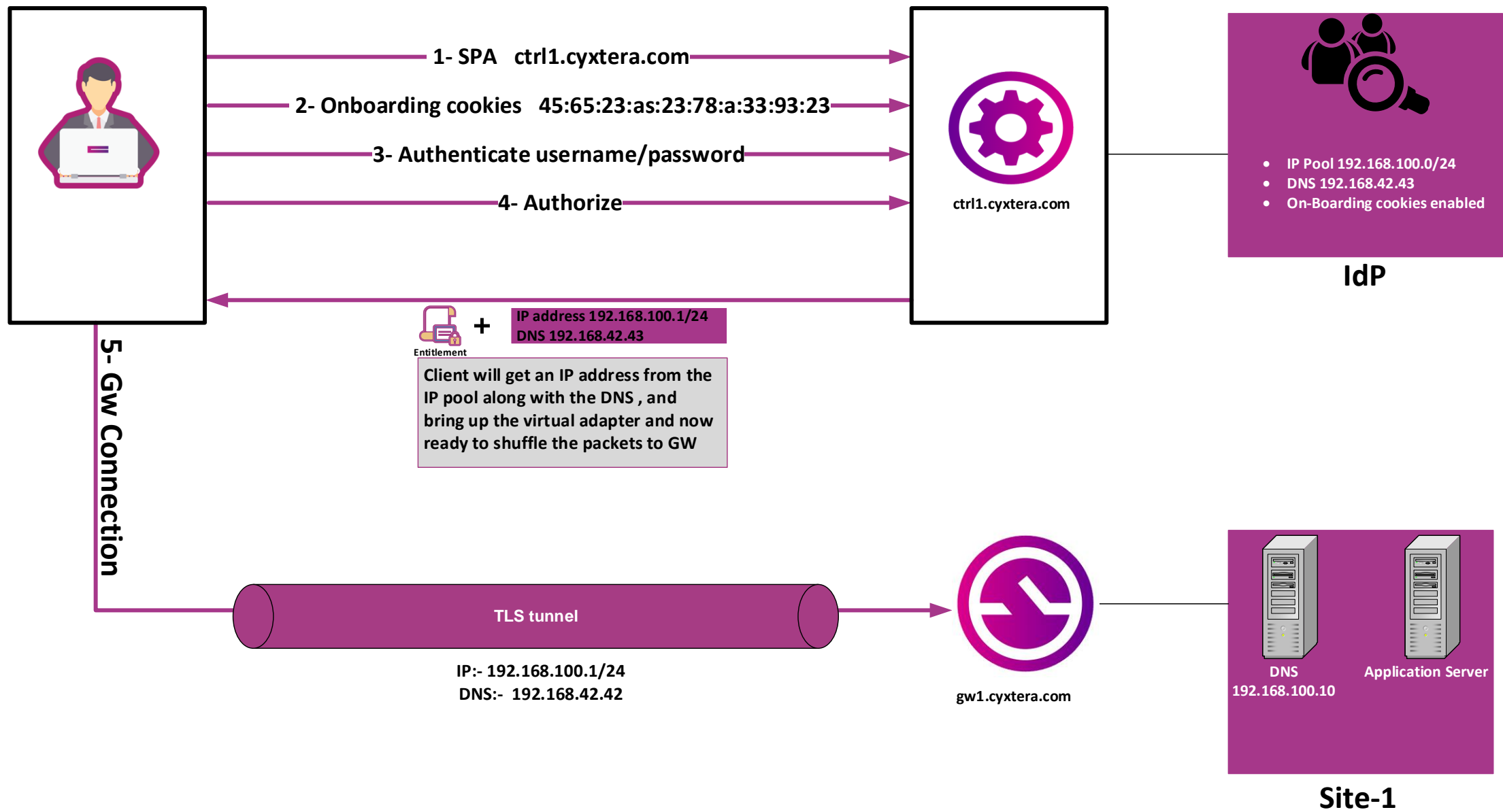
LDAP Certificate

Assigned IPs:

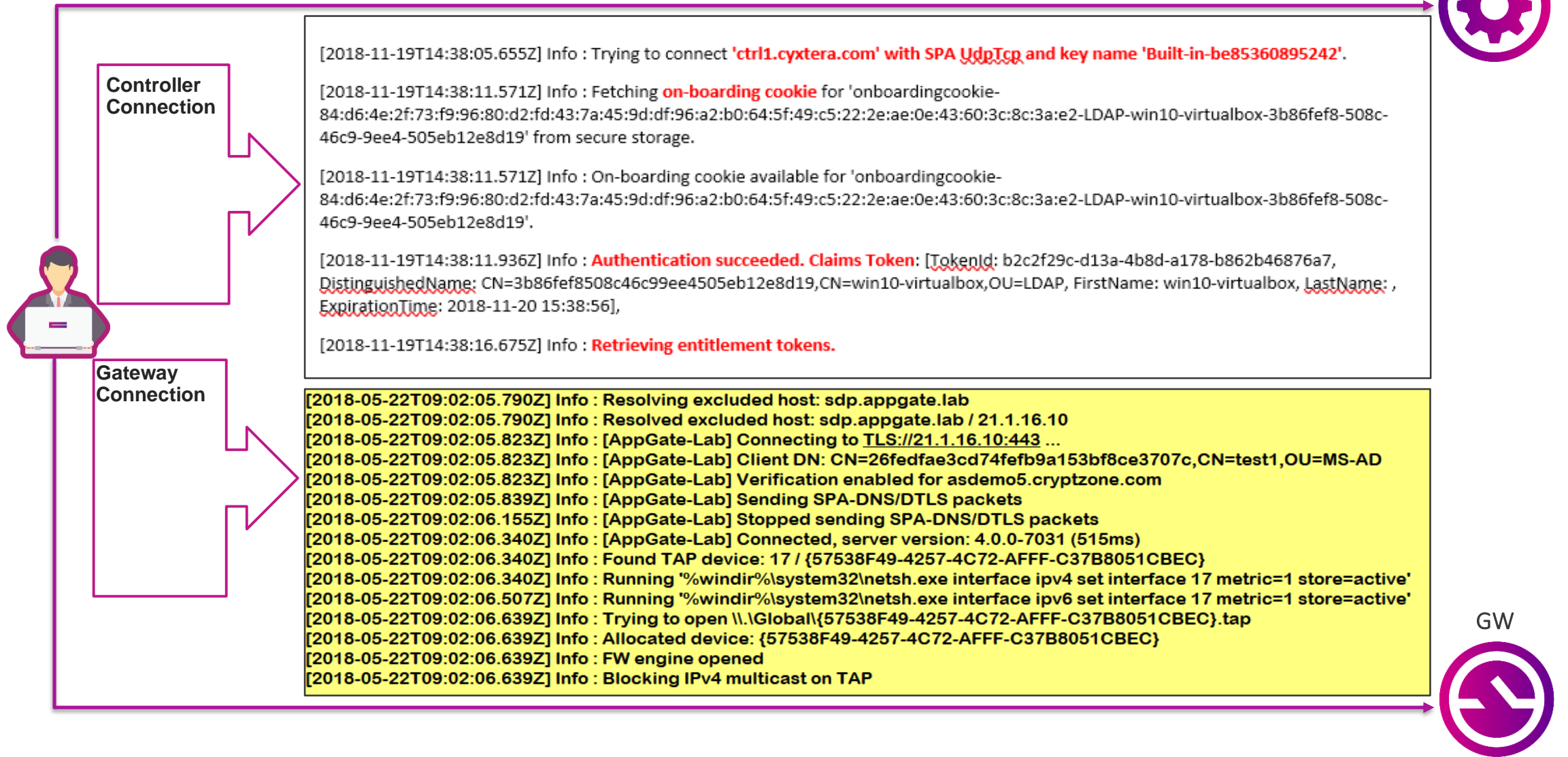
Sites: [Reconnect](#)

-  42\_Network
-  52\_Network
-  62\_Network

0 of 3 connected



# Log Files



# Log files Cont'd

- **Windows:**

- C:\Users\<username>\AppData\Roaming\AppGate\Logs
- %ProgramData%\AppGate\driver.log

- **MacOS:**

- /users/<username>/.appgatesdp/log/
- /var/log/appgate/tun-service.log

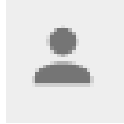
- **Linux**

- ~/.appgate/log/
- journalctl -u appgatedriver.service

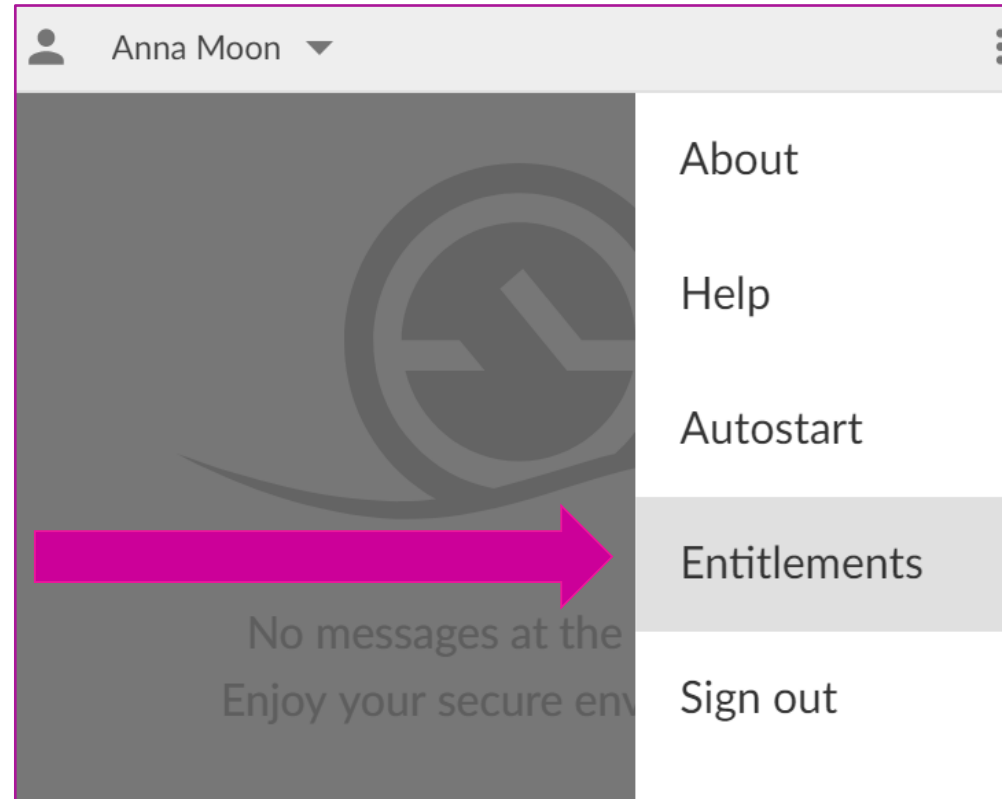


# Hidden menu for the admin



- Click 5s on avatar







- Then use the menu




# Entitlement View - Client


 Anna Moon 




 All Sites 


 Mai


Distribution Access




 Mai


DNS for default site




 Mai

Intranet access



 Tok

tokyo action



# Rollback to a fresh install (1/2)

- Remove all passwords and certificates. Remember:
  - Windows: Cert store
  - MacOSX: Key chain

Errors are in red

A screenshot of a 'Connect' dialog box. At the top, it says 'not connected' next to a user icon and a gear icon. The title 'Connect' is in blue. Below it, the text says 'Please perform the following steps in order to connect.' There is a 'Server' label above a text input field. The input field contains a red error message: 'Invalid certificate. Please contact your administrator'. At the bottom, there are three buttons: 'HELP', 'CANCEL', and 'NEXT'.

# Rollback to a fresh install (2/2)

- Before you start, base-line:
  - Install matching/latest client version
  - Restart the machine
  - Verify connectivity: IP, DNS, default routing
- Check the error messages the user interface provides
- Replicate the issue:
  - Try a user who you know works
  - Try on another installation with the same user
  - Try another version of the client

# Other common errors

- Gateway internal network configuration issues
- SNAT disabled, allow sources configured wrong, arp...
- Time synchronization issues
- Google OTP, certificate validity etc.
- Hostname, DNS and certificate issues between appliances
- Ports and firewall configuration issues (443, 444, 5432)

# When out of options...

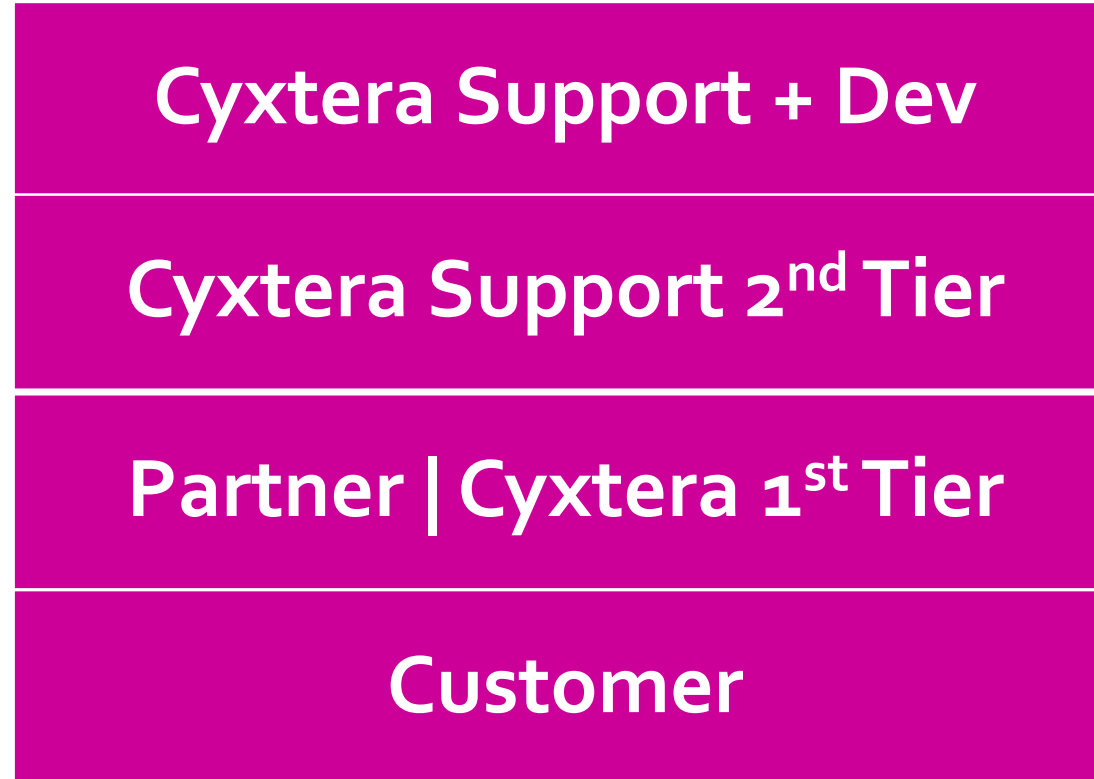
- On each OS, analyze:
  - Network interfaces, addresses, routes
  - DNS server and search domain settings
  - 3rd party firewalls, endpoint protections

# Support and Resources

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



# The Support Stack



# Resources

- Knowledgebase, Announcements & Ticketing System
  - Site: [AppGate SDP Support](#)
  - E-Mail: [appgatesdp.support@cyxtera.com](mailto:appgatesdp.support@cyxtera.com)
- Latest AppGate SDP Manuals
  - Admin Guide: <https://sdphelp.cyxtera.com/adminguide>
  - User Guide: <https://sdphelp.cyxtera.com/userguide>
  - Previous versions append /version (e.g., /v4.0)
- Downloads
  - [AppGate SDP v4.2 Download Center](#)
- Professional Services & Training

# Audit Logs and Simple Troubleshooting

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

Cyxtera proprietary