

AppGate SDP Basic Training Labs

Lefteris Chairetakis

Zahir Alli

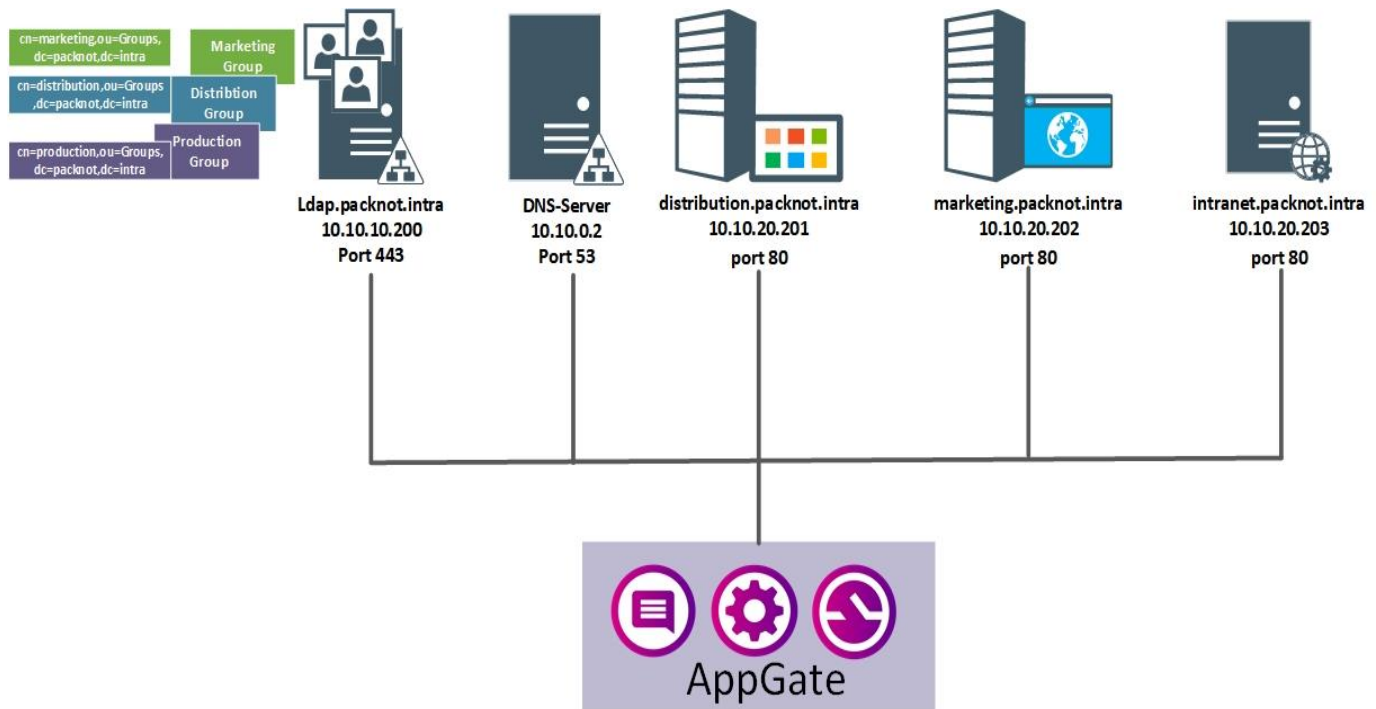
October 2019

Singapore

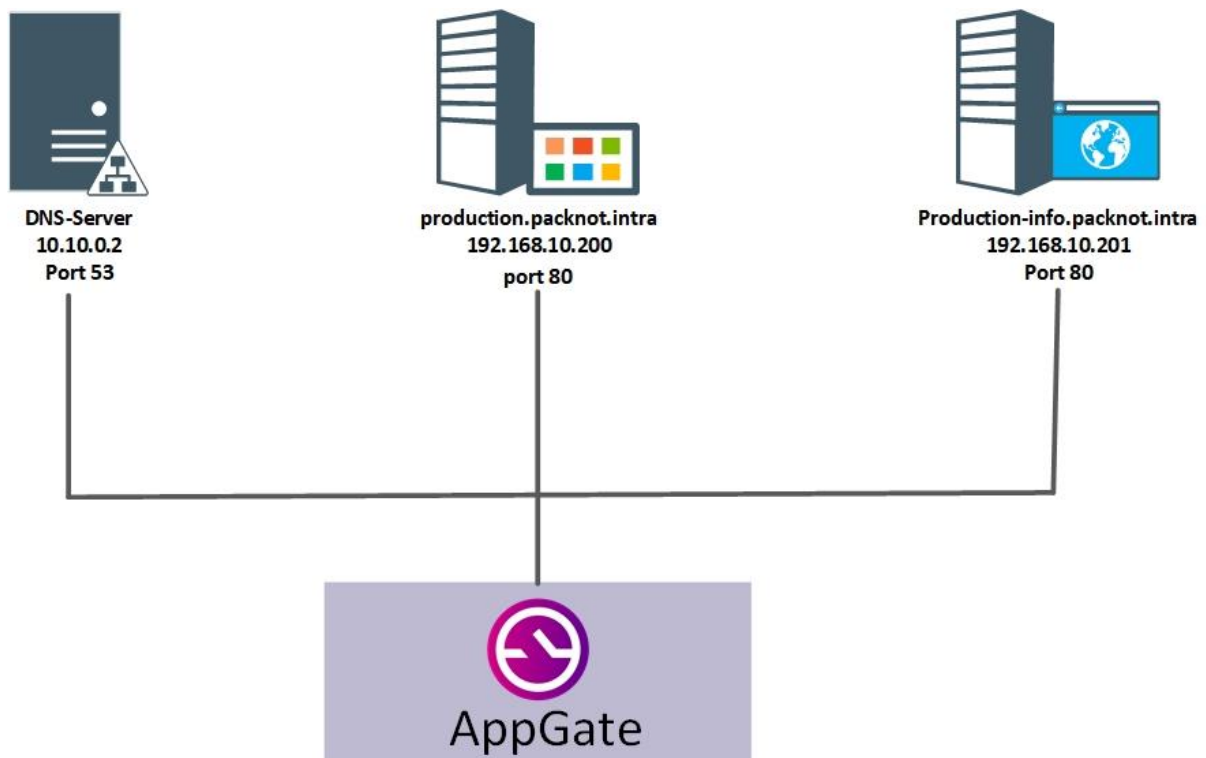
Table of Contents

Packnot HQ Infrastructure	3
Packnot Production-Site Infrastructure	3
Lab 1. Provisioning access for employees working within distribution	4
Lab 2. Allow access to the distribution web site only during business hours.....	6
Lab 3. Add a User Interaction (Remedy Method) to access the distribution web site outside business hours.....	7
*Lab 4. Add periodic re-evaluation of the configured Condition	8
Lab 5. Provision additional access for distribution employees to the marketing application	8
Lab 6. Allow Distribution user to enter OTP once for all resources	9
Lab 7. Create Stockholm Gateway Step-by-Step walkthrough	10
Step 1. Check the License	10
Step 2. Create a new Site	11
Step 3. Create a new Appliance	14
Step 4. Seed the appliance	19
Step 5. Verify Stockholm Gateway in the Controller dashboard	23
Step 6. Test the scenario works as expected	24
Lab 8a. Set a Login Banner Message and Message of the Day	25
Lab 8b. Configuring Admin access with MFA	25
Lab 9. Create a delegated admin role for distribution employees' access.....	25

Packnot HQ Infrastructure

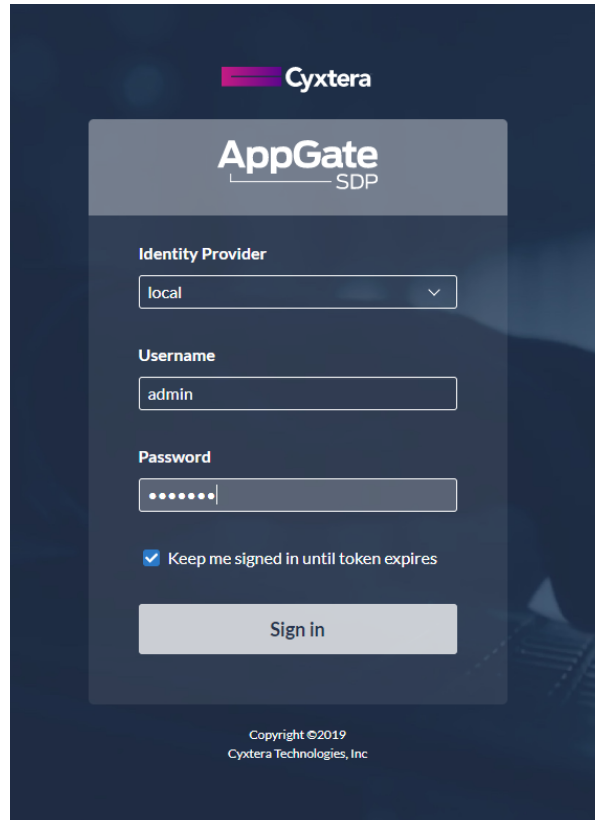


Packnot Production-Site Infrastructure

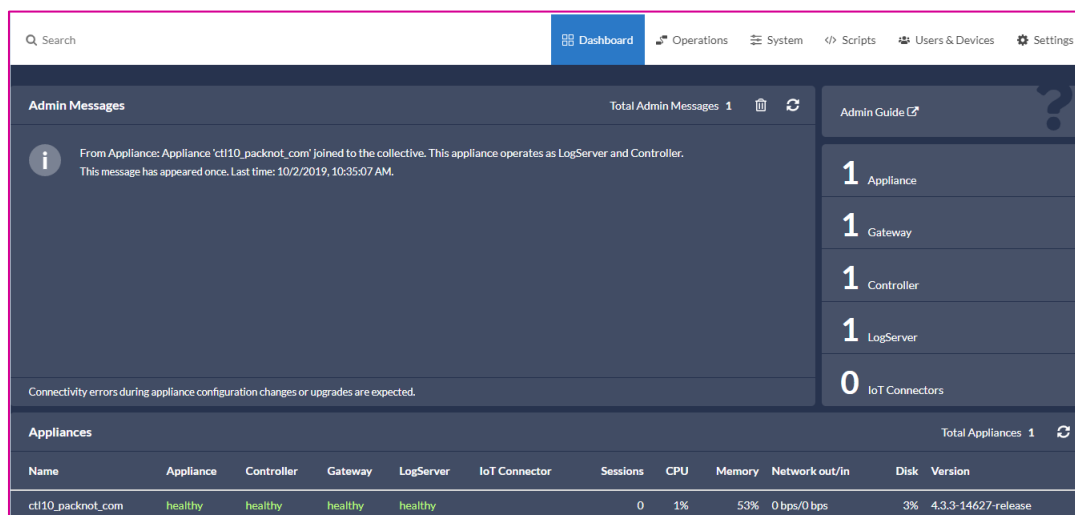


Lab 1. Provisioning access for employees working within distribution

- Open your browser and login to the admin UI, on the following link:
<https://ctlX.packnot.com:444>, where **X** is your number from **1-100**
Ex:- ctl1.packnot.com, ctl2.packnot.com, ctl3.packnot.com...etc.
- Pick "local" as the Identity Provider. Use username **admin** and password **rosebud**



The image shows the AppGate SDP login interface. At the top is the Cyxtera logo. Below it is the AppGate SDP logo. The main form has three input fields: 'Identity Provider' with a dropdown menu showing 'local', 'Username' with the text 'admin', and 'Password' with masked dots. Below the password field is a checkbox labeled 'Keep me signed in until token expires' which is checked. A 'Sign in' button is at the bottom of the form. At the very bottom, there is a copyright notice: 'Copyright ©2019 Cyxtera Technologies, Inc.'



The image shows the AppGate SDP Admin Dashboard. The top navigation bar includes a search bar and tabs for Dashboard, Operations, System, Scripts, Users & Devices, and Settings. The main content area is divided into two sections. The left section, 'Admin Messages', shows a message from an appliance 'ctl10.packnot.com' that has joined the collective. The right section, 'Appliances', shows a summary of appliance counts: 1 Appliance, 1 Gateway, 1 Controller, 1 LogServer, and 0 IoT Connectors. Below this is a table of appliances.

Name	Appliance	Controller	Gateway	LogServer	IoT Connector	Sessions	CPU	Memory	Network out/in	Disk	Version
ctl10.packnot.com	healthy	healthy	healthy	healthy		0	1%	53%	0 bps/0 bps	3%	4.3.3-14627-release

- Once you are successfully signed in, from the admin UI navigate to Operations -> Entitlements.
- Click on **Add New** and create a new Entitlement as below:

Name	Distribution
Display Name	Distribution Access
Notes	Access for employees working with deliveries in the field
Site	Default site
Actions -Rule	ALLOW
Protocol	TCP up
Network Resources	distribution.packnot.intra
Ports	80
Condition	Always
Tags	distribution

Press Save

- Next step is to create the Policy where distribution employees are assigned the above Entitlement for access to the distribution web site.
- From the admin UI, navigate to Operations -> Policies. Click on Add New to create a new Policy:

Name	Distribution
Notes	People working in the field such as airports, transport, etc.
Select Assignment Criteria	Group
Match	cn=distribution,ou=Groups,dc=packnot,dc=intra
Entitlements (by name)	Distribution
Tags	distribution

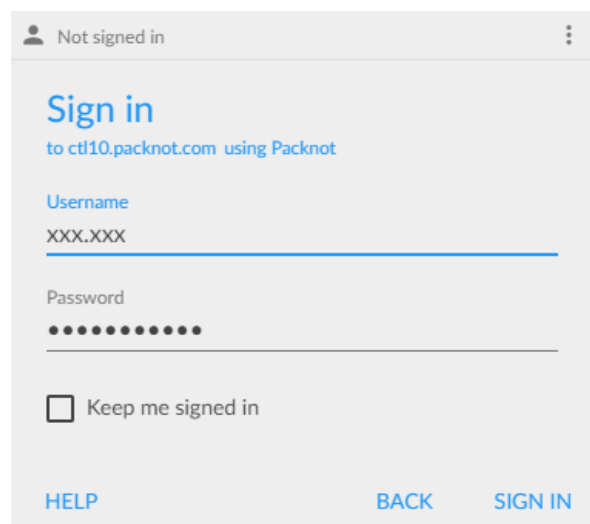
Press Save

Now pick any user that is in the distribution group and login with the AppGate client to **the same Controller that you logged in the first step.**

Browse to:

<http://distribution.packnot.intra/>

All users belonging to the distribution group should now be able to access the distribution web site.



Lab 2. Allow access to the distribution web site only during business hours

Steps:

1. From the admin UI, navigate to **Operations → Conditions**
2. Click Add New and create a new Condition with Name **"Distribution Access only during business hours"**
3. The Notes field is optional and meant for documentation purposes
4. Under Access Criteria, click Add New and from the Select Access Criteria drop-down list choose **"Time is between"** and set the time range accordingly.
5. Press **Save**.
6. Once you have created the Condition, you will have to attach it to the relative Entitlement, in this case the **"Distribution"** Entitlement, for it to take effect.
7. Go back to Entitlements, pick the Distribution Entitlement and add the Condition you just created: Under Condition, **delete the "Always" Condition**, click on **Add New** and add the **"Distribution Access only during business hours"** Condition. Press **Save**
8. Pick a user who is supposed to have access to distribution, log in via the client as that user and try to access again <http://distribution.packnot.intra> log- make sure you have logged out from your client from the previous lab, so that the change takes effect

Note:- Play with the time range set in the Condition and make sure that it is working as expected – i.e. forbidding access outside the hours you have set above.

Lab 3. Add a User Interaction (Remedy Method) to access the distribution web site outside business hours

If the Condition set in Lab 2 is not met, users should be still able to access the distribution resource as long as they provide a valid **OTP (One-Time Password)**.

For this Lab to work you need to have **Google Authenticator** installed on your mobile which is the default built-in time-based OTP Provider for AppGate.

Note:- You can install *Microsoft Authenticator* on your machine instead to do above.

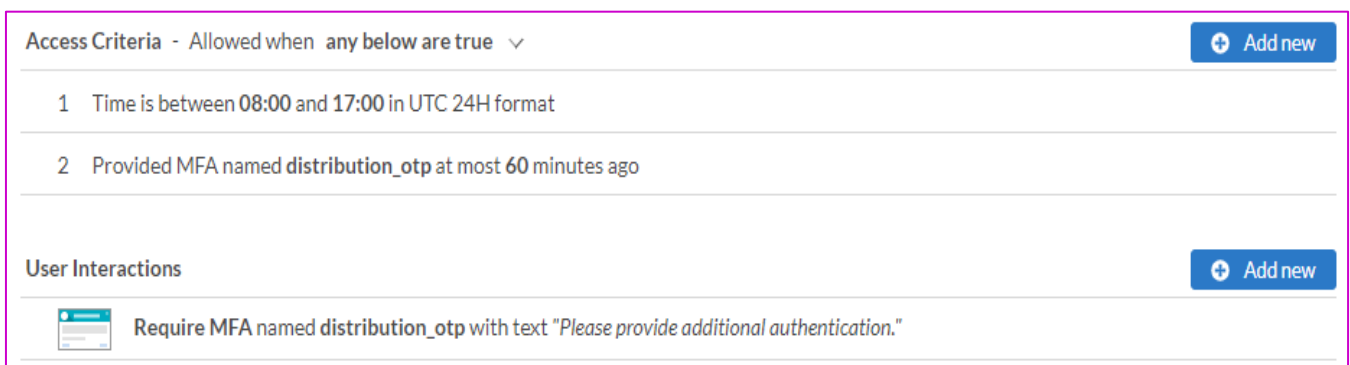
Steps:

1. Go to the **"Distribution Access only during business hours"** Condition you created in the previous Lab. Click Add new in the User Interactions section and fill in as per below:

Type of Interaction	Require MFA
Message	The text the user will be presented with, e.g. "Please provide additional authentication"
Claim Suffix	distribution_otp
MFA Provider	Default Time-Based OTP Provider

2. Under Access Criteria, along with the **"Time is between"** access criterion, we will now add a new Condition statement checking the User Interaction we just configured: Click Add new and choose **"Provided MFA"** from the drop-down list. Fill in the claim suffix field with the same value you entered when configuring the User Interaction section, i.e. **distribution_otp**. Set the time period to **1 minute** for the purpose of this lab only. Don't forget to change the "Allowed when" statement to **"any below are true"**.

Your Condition should look similar to the following:



The screenshot shows the configuration interface for a condition. At the top, it says "Access Criteria - Allowed when any below are true" with a dropdown arrow and an "Add new" button. Below this, there are two criteria listed: "1 Time is between 08:00 and 17:00 in UTC 24H format" and "2 Provided MFA named distribution_otp at most 60 minutes ago". Below the criteria, there is a section for "User Interactions" with an "Add new" button. Under "User Interactions", there is one entry: "Require MFA named distribution_otp with text 'Please provide additional authentication.'".

3. Make sure to have set the **"Time is between"** range in the Condition above as such that this will fail, and the User Interaction will be triggered.

4. **Click Save.** Log off and then back on to your client as a distribution user to test access. You should now be prompted for an OTP *once you try accessing the distribution server* and upon valid entry, you will be granted access to the distribution application.

*Lab 4. Add periodic re-evaluation of the configured Condition

Users should be asked every hour for re-entering an OTP when accessing the distribution application outside the business hours.

Steps:

1. Go to the **Condition** and under **"Re-evaluate periodically based on UTC"**, check a reasonable time interval – **on the quarters** is suggested. Save changes.
2. Log off and back on your client and access the distribution application. What you will experience from now on is that every hour you will be asked for a new OTP.

***The purpose of this lab is for the trainee's education and supposed to be completed outside the class due to the time limitations of the training. For more information in setting real-time re-evaluations, please check: [https://sdphelp.cyxtera.com/adminguide/v4.3/real-time-\(re\)evaluations.html](https://sdphelp.cyxtera.com/adminguide/v4.3/real-time-(re)evaluations.html)**

Lab 5. Provision additional access for distribution employees to the marketing application

The employees working within distribution should be provisioned with access to the marketing application as well, the exact same way they access the distribution application – i.e. access during normal working hours and request for OTP if out of normal hours

Steps:

1. To give the distribution users access to the marketing app, as admin you will have to add the Entitlement called **"Marketing Server"** to the **"Distribution"** Policy. You can do that either by name or by tag (marketing). Click **Save** when you are done.
2. The easiest way to create the relevant Condition for access to the marketing app would be to clone the already existing Condition **"Distribution Access only during business hours"**. Get to that Condition and click the **Clone** button at the bottom of the page. Make sure to change the name to **"Marketing Access only during business hours"** and also **give a different name to the one-time password claim** that is under the **Access Criteria** and **User Interactions**, something like **"marketing_otp"**. Click **Save**.
3. Add the new Condition to the **"Marketing Server"** Entitlement (**do not forget to delete the "Always by trent" Condition that already is there**) and click **Save**. No further action is needed within the Distribution Policy itself.

4. Test with your distribution user and make sure everything is working as expected when users try to access the marketing site:

<http://marketing.packnot.intra/>

At this point, what a distribution user should experience when trying to access either the distribution or the marketing application should be the following:

- If logging in during normal working hours, access should be straightforward
- If outside normal working hours, MFA (Multi Factor Authentication) will be required

Lab 6. Allow Distribution user to enter OTP once for all resources

Let's say now that we want our distribution users to enter an OTP once for all the resources they are entitled to access without having to enter an OTP every time they need to access a specific resource.

Steps:

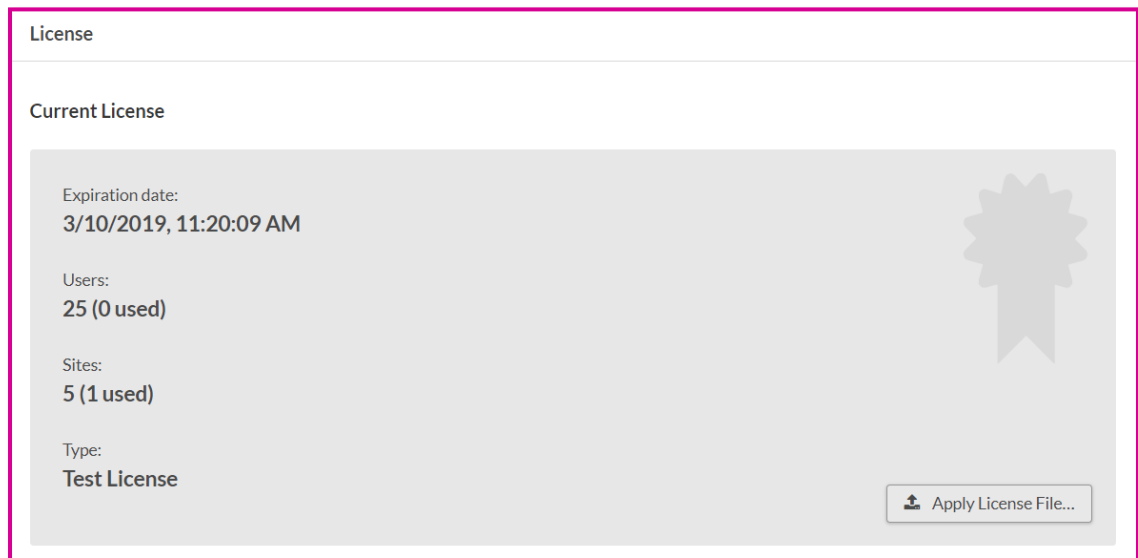
1. Go to **Conditions** and either create a new Condition or clone one of the existing ones ("**Distribution or Marketing Access only during business hours**"). Give it the name "**Distribution-Marketing Access only during business hours**" and make sure you change the claim suffix that is in the **Condition** and **User Interaction** to something like "**distrib_market_otp**". Click **Save**.
2. Go to **Entitlements**. Remove any Conditions in the "**Distribution**" and "**Marketing Server**" Entitlements and add the Condition you just created to both. No change is required within the "**Distribution**" Policy
3. What distribution users should experience now is that they will be asked for an OTP only once
 - i.e. once they access the marketing application and enter their OTP, access to the distribution app will be direct. Sign out and back in your client and test.

This way we have created a generic remedy method applied to a number of Entitlements instead of having a specific remedy method for each Entitlement.

Lab 7. Create Stockholm Gateway Step-by-Step walkthrough

Step 1. Check the License

1. Additional Sites require additional licensing
2. From the admin UI, navigate to Settings and check the License:



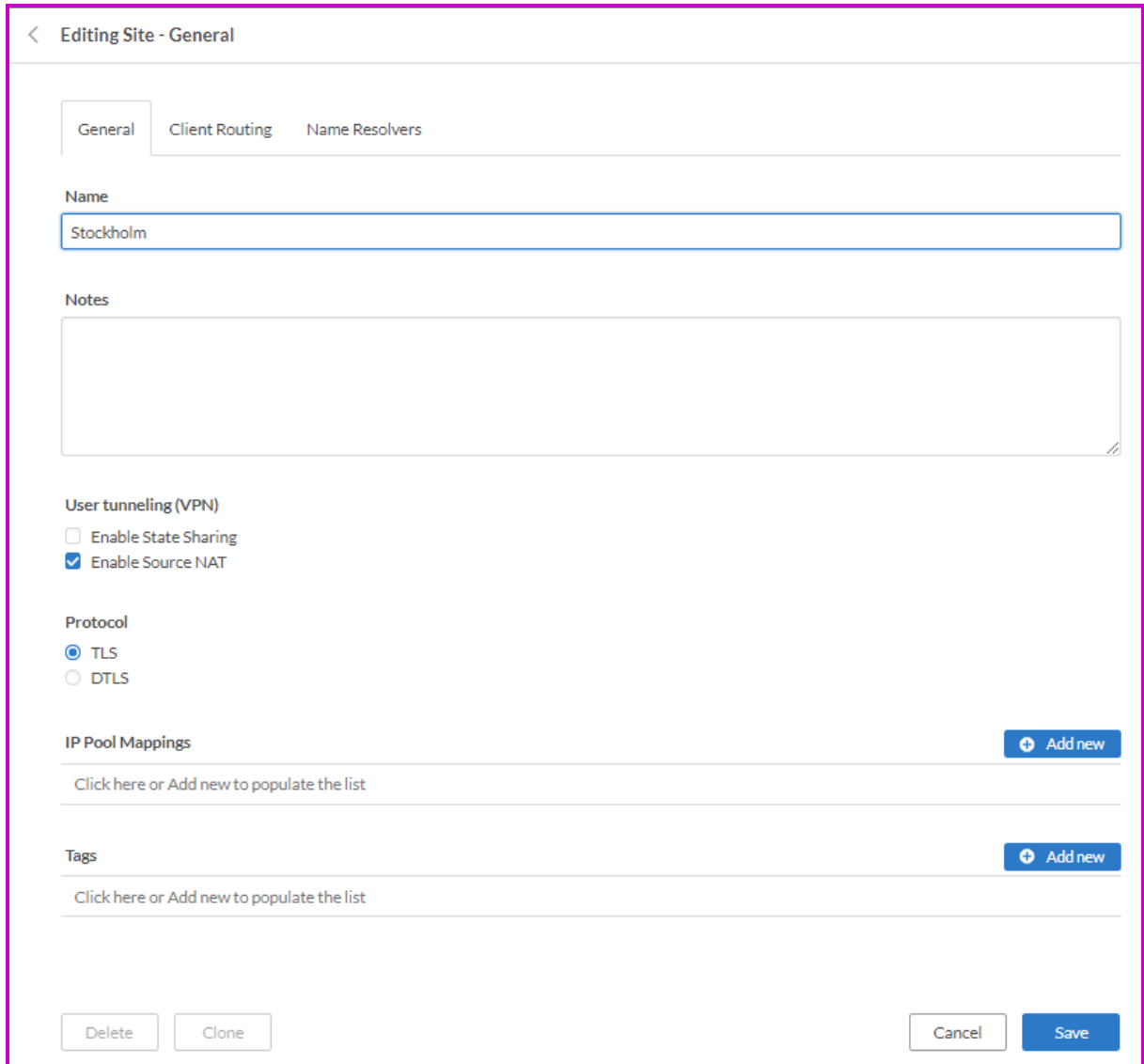
3. You need to request a new License if Sites-count < 2

Step 2. Create a new Site

Navigate to **System** → **Sites**, click **Add New** and fill in as below:

***Remember to click Save once you have entered the necessary information in all tabs.**

1- General



< Editing Site - General

General Client Routing Name Resolvers

Name

Stockholm

Notes

User tunneling (VPN)

☐ Enable State Sharing

☒ Enable Source NAT

Protocol

☒ TLS

☐ DTLS

IP Pool Mappings [Add new](#)

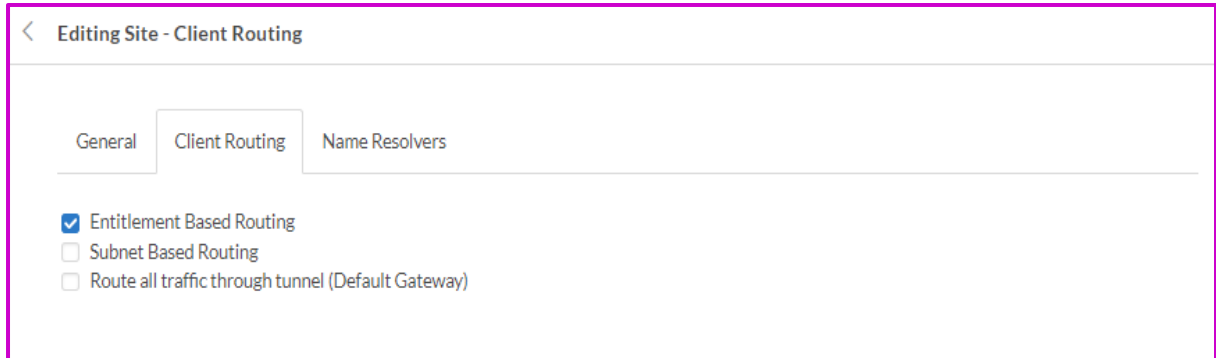
Click here or Add new to populate the list

Tags [Add new](#)

Click here or Add new to populate the list

Delete Clone Cancel Save

2- Client Routing



< Editing Site - Client Routing

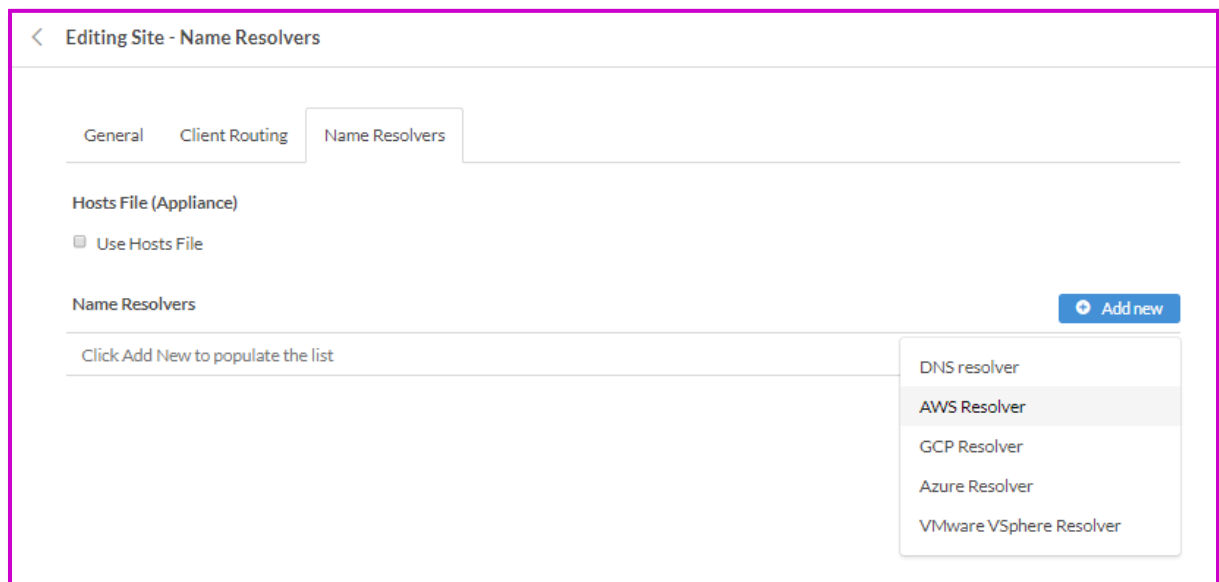
General Client Routing Name Resolvers

☒ Entitlement Based Routing

☐ Subnet Based Routing

☐ Route all traffic through tunnel (Default Gateway)

3- Name Resolvers



< Editing Site - Name Resolvers

General Client Routing Name Resolvers

Hosts File (Appliance)

☐ Use Hosts File

Name Resolvers [Add new](#)

Click Add New to populate the list

- DNS resolver
- AWS Resolver
- GCP Resolver
- Azure Resolver
- VMware VSphere Resolver

AWS Resolver

Name

Update Interval (seconds)

Access Method

☒ Use IAM Role
☐ Use Access Key

Regions [Add new](#)

[Click here or Add new to populate the list](#)

☐ Use Assumed Roles
☐ Disable VPC Auto Discovery
☐ Use Https Proxy

[Delete](#) [Cancel](#) [Done](#)

Press **Done**

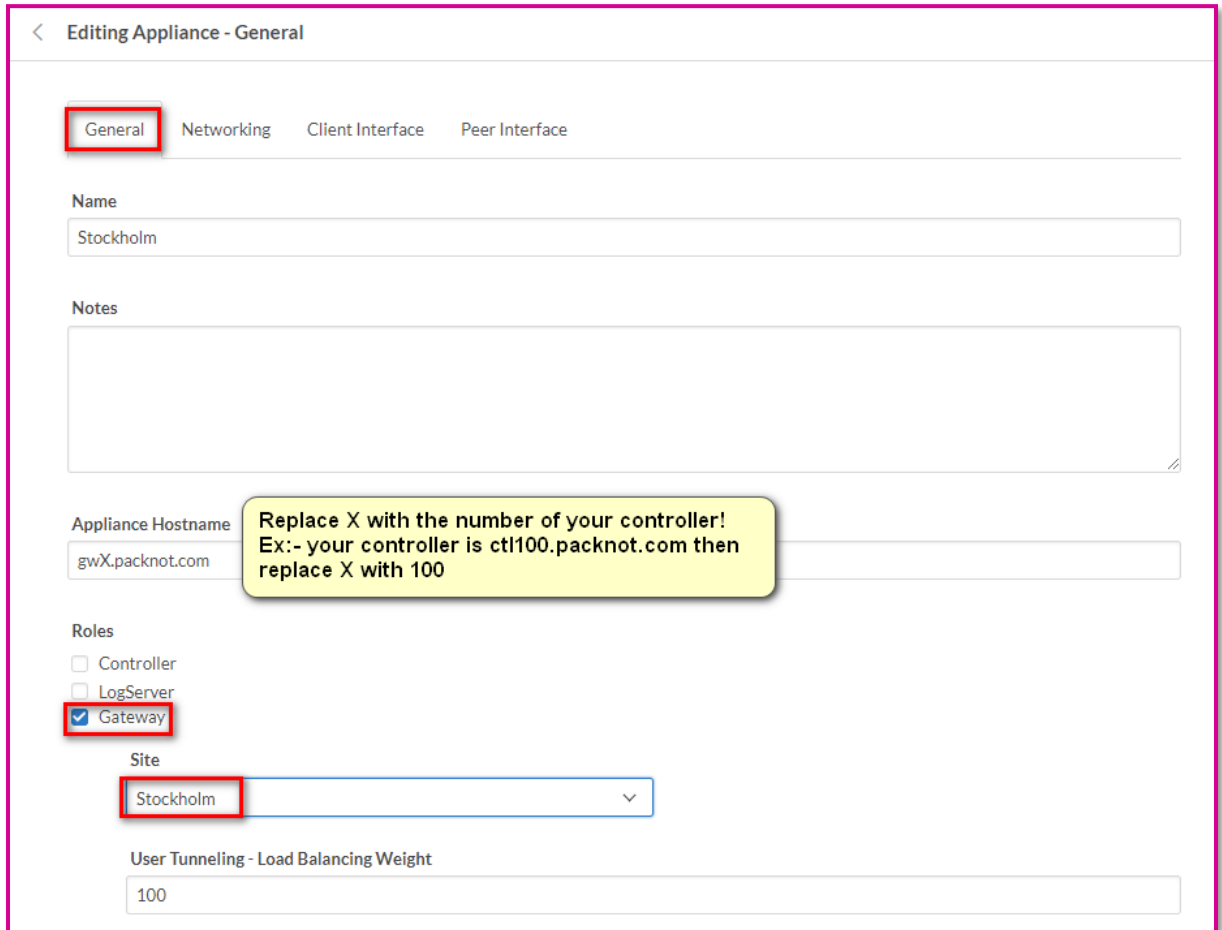
And then press **Save**

Step 3. Create a new Appliance

Navigate to **System** → **Appliances**, click **Add New** and fill in as below

*Remember to click Save once you have entered the necessary information in all tabs.

1- General



< Editing Appliance - General

General Networking Client Interface Peer Interface

Name
Stockholm

Notes

Appliance Hostname
gwX.packnot.com

Replace X with the number of your controller!
Ex:- your controller is ctl100.packnot.com then
replace X with 100

Roles

☐ Controller

☐ LogServer

☒ Gateway

Site
Stockholm

User Tunneling - Load Balancing Weight
100

- User Tunneling → **Add New** and fill as below

Target

Address

Netmask Length

Network Interface

eth0

Delete

Cancel

Done

Press **Done** so you end up as below:

User Tunneling - Allow Destinations

+ Add new

nic eth0

2- Networking

Interfaces → Add new and fill as below

Interface

☒ Enabled

Interface Name

IPv4 DHCP
☒ Enabled
☒ DNS
☒ Default Gateway
☐ NTP

Static IPv4 addresses [+ Add new](#)

[Click here or Add new to populate the list](#)

Press Done and back in the Networking tab add DNS **10.10.0.2**

Press Save

Networking Tab should look as below:

< Editing Appliance - Networking

General

Networking

Client Interface

Peer Interface

Interfaces

+ Add new

eth0 DHCP

Routes

+ Add new

Click here or Add new to populate the list

DNS Servers

+ Add new

10.10.0.2

DNS Domains

+ Add new

Click here or Add new to populate the list

NTP Servers

+ Add new

0.ubuntu.pool.ntp.org

Advanced Mode

Delete

Clone

Cancel

Save

3- Client Interface

< Editing Appliance - Client Interface

General Networking **Client Interface** Peer Interface

Hostname gwX.packnot.com

TLS Port 443

DTLS Port 443

☐ Enable Proxy Protocol

Allow Sources [+ Add new](#)

0.0.0.0 nic Any

:: nic Any

**Replace X with the number of your controller!
Ex:- If your controller ctl100.packnot.com
then replace X with 100**

4- Peer Interface

< Editing Appliance - Peer Interface

General Networking Client Interface **Peer Interface**

Hostname gwX.packnot.com

TLS Port 444

Allow Sources [+ Add new](#)

0.0.0.0 nic Any

:: nic Any

**Replace X with the number of your controller!
Ex:- If your controller ctl100.packnot.com
then replace X with 100**

Press Save

Now under Appliances you should have 2 Appliances as below:

Appliances							Total Appliances 2	Search	Add New
Name ↑	Hostname	Site	State	Tags		Modified			
ctl7_packnot_com	ctl7.packnot.com	Default Site	Active	managed-by-trent	first-appliance	2/27/2019, 1:41:29 PM			
Stockholm	gwX.packnot.com	Stockholm	Not active			3/5/2019, 10:55:53 AM			

Note: The numbers for the two Appliances will be according to your Controller number
e.g. you may have

ctl100.packnot.com as Controller

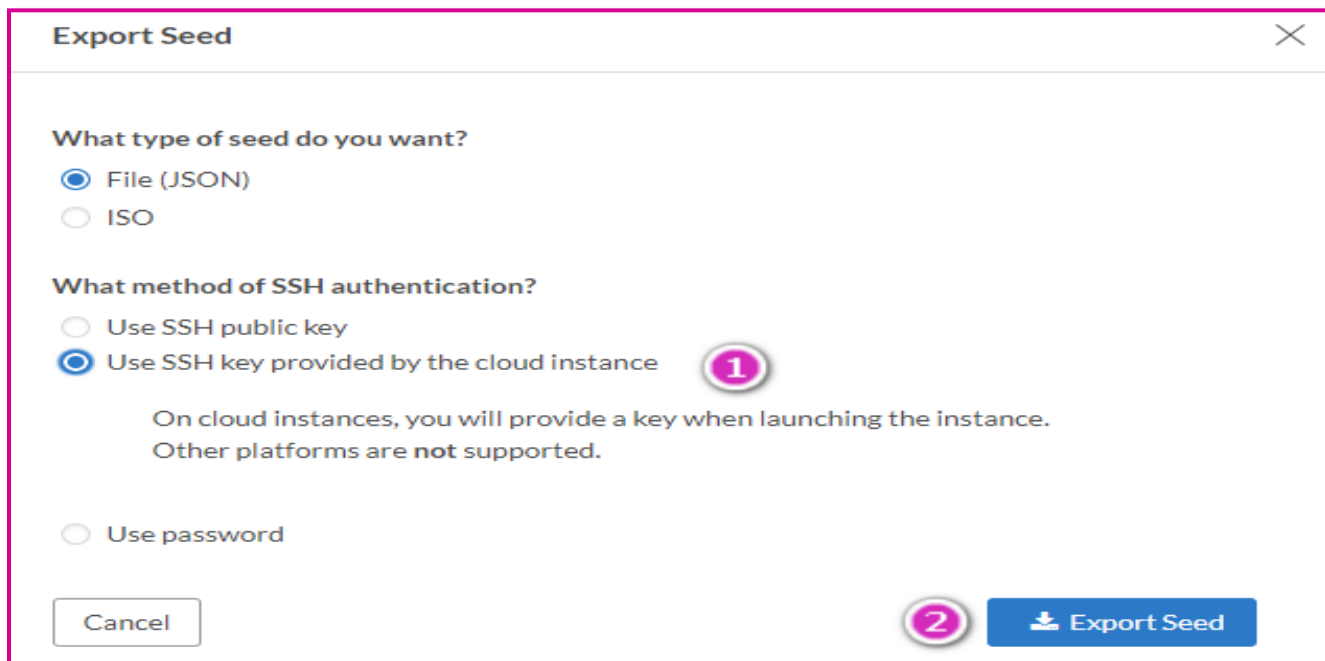
and

gw100.packnot.com as GW

Step 4. Seed the appliance

Under Appliances download the **seed.json** file and choose SSH key provided by the cloud instance

Appliances							Total Appliances 2	Search	Add New
Name ↑	Hostname	Site	State	Tags		Modified			
ctl7_packnot_com	ctl7.packnot.com	Default Site	Active	managed-by-trent	first-appliance	2/27/2019, 1:41:29 PM			
Stockholm	gwX.packnot.com	Stockholm	Not active			3/5/2019, 10:55:53 AM			



The image shows a dialog box titled "Export Seed" with a close button (X) in the top right corner. It contains two sections of radio button options. The first section, "What type of seed do you want?", has "File (JSON)" selected. The second section, "What method of SSH authentication?", has "Use SSH key provided by the cloud instance" selected, which is also marked with a circled "1". Below this option is a note: "On cloud instances, you will provide a key when launching the instance. Other platforms are not supported." At the bottom left is a "Cancel" button, and at the bottom right is an "Export Seed" button with a download icon, marked with a circled "2".

Export Seed

What type of seed do you want?

☒ File (JSON)

☐ ISO


What method of SSH authentication?

☐ Use SSH public key

☒ Use SSH key provided by the cloud instance **1**

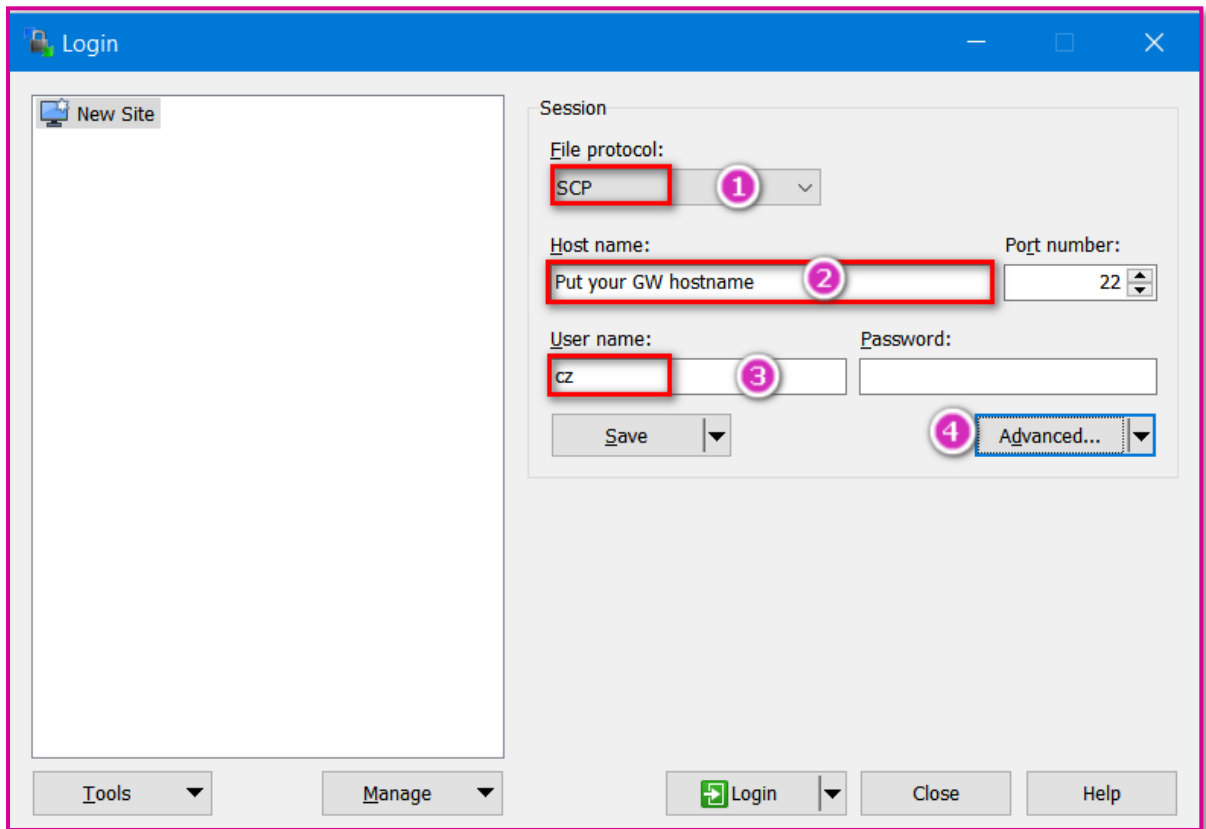
On cloud instances, you will provide a key when launching the instance.
Other platforms are **not** supported.

☐ Use password

Cancel **2**  Export Seed

After downloading the **seed.json** file, you need to copy it to Stockholm GW so it can talk to your Controller. To do so, follow the below instructions:

- Copy the seed file to the appliance by using **winscp** as below. Login with AppGate client to your Controller, you can use any username from the distribution group. Browse to <http://intranet.packnot.intra/files/course/>
- Download the private key and WinSCP portable as well.
- Open WinSCP and do as below:



Login

New Site

Session

File protocol: SCP (1)

Host name: Put your GW hostname (2)

Port number: 22

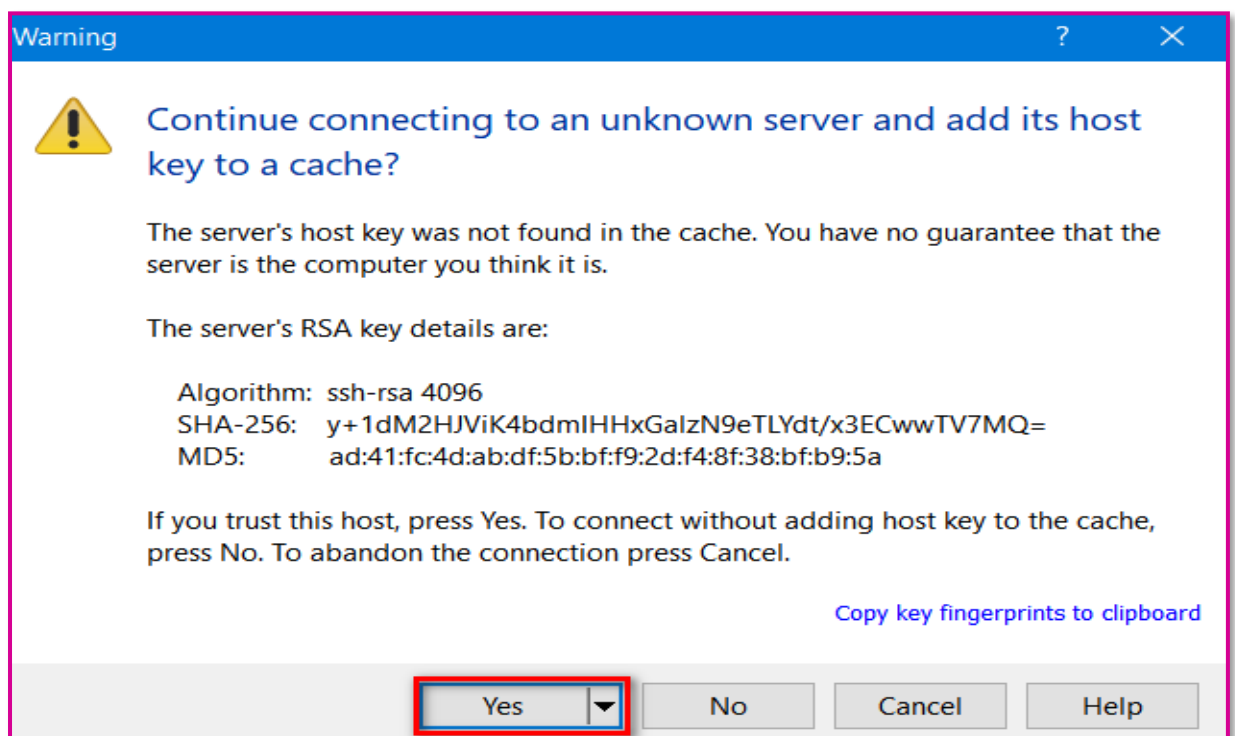
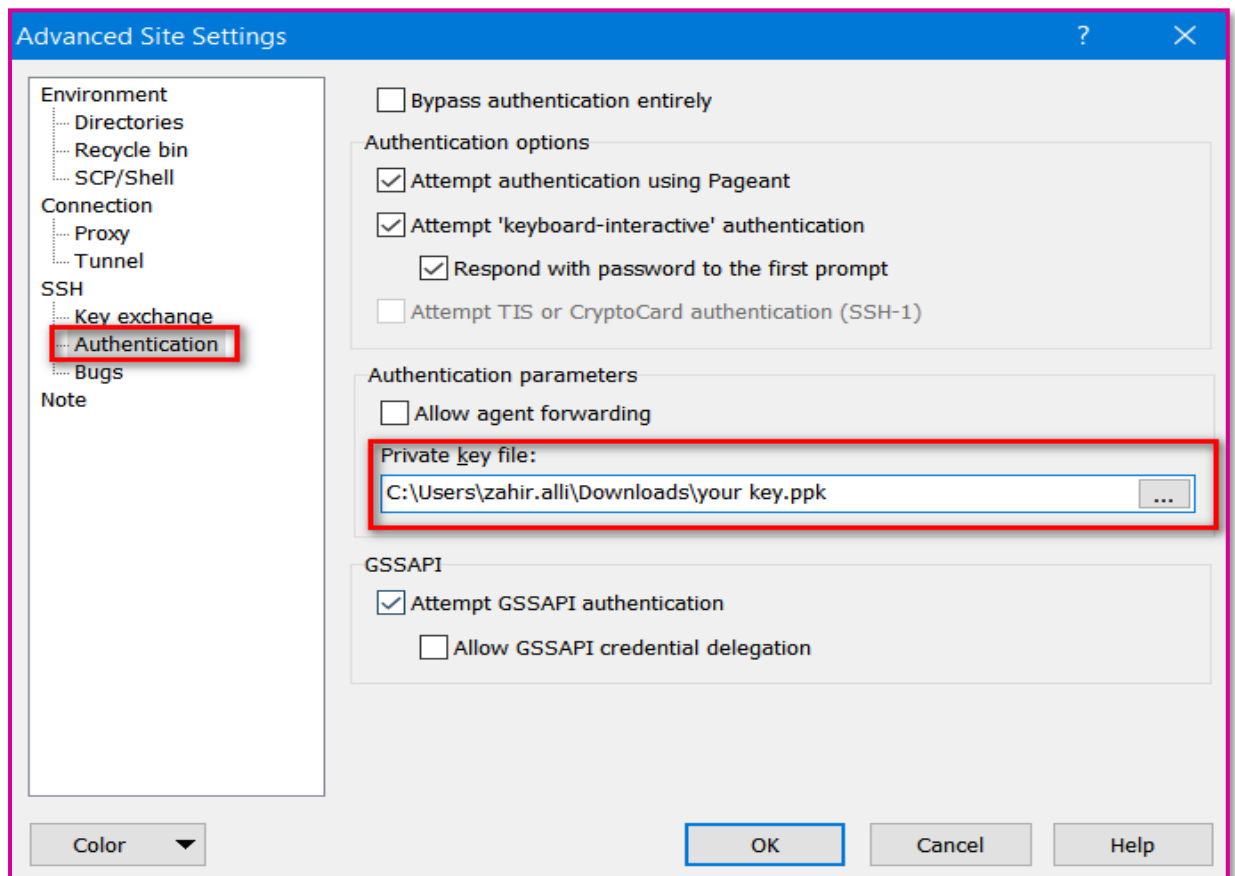
User name: cz (3)

Password:

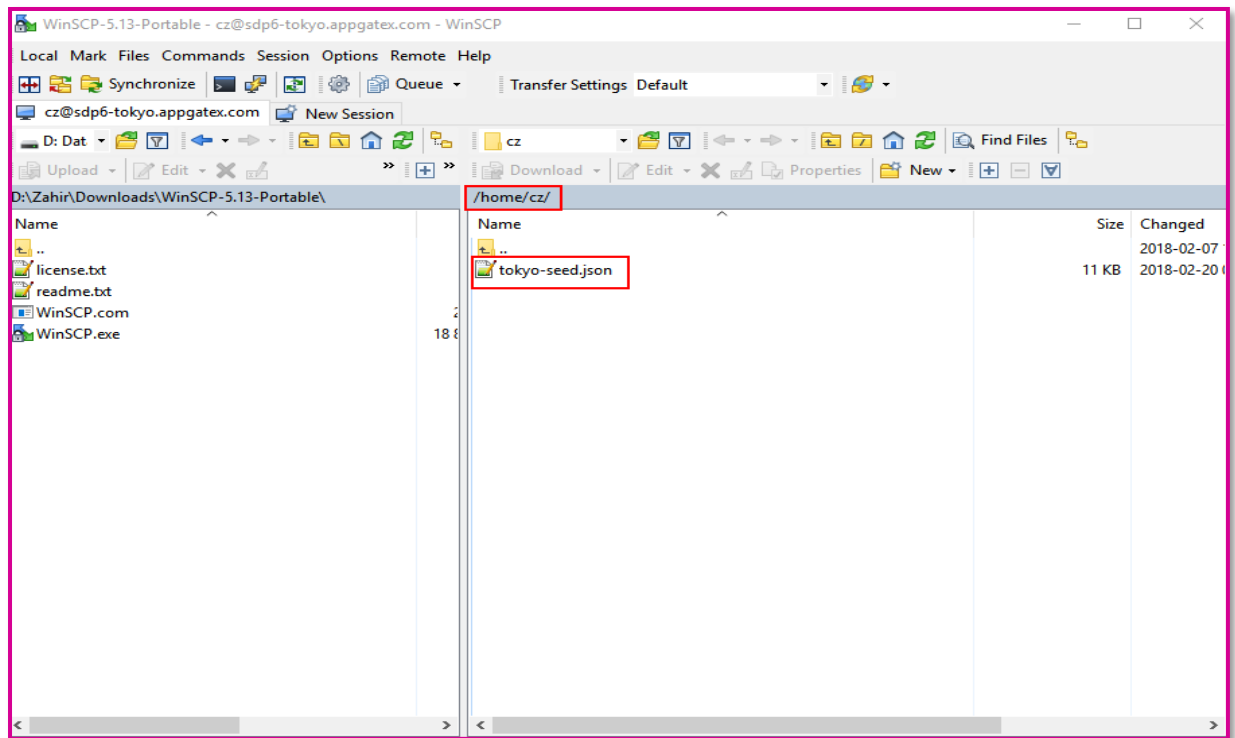
Save

Advanced... (4)

Tools Manage Login Close Help



Now you just need to copy **seed.json** file to home/cz



Step 5. Verify Stockholm Gateway in the Controller dashboard

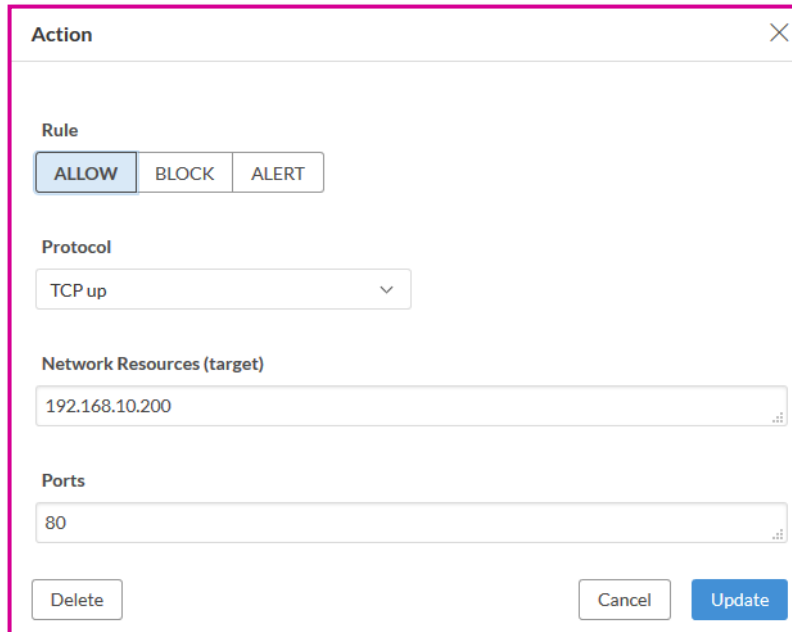
Appliances					Total Appliances 2				
Name	Appliance	Controller	Gateway	LogServer	CPU	Memory	Network out/in	Disk	Version
Stockholm	healthy		healthy		1%	24%	3.74 Kbps/4.94 Kbps	2%	4.2.2-12675-release
ctl7_packnot_com	healthy	healthy	healthy	healthy	0%	55%	4.66 Kbps/3.49 Kbps	3%	4.2.2-12675-release

If Stockholm GW is not activated, SSH to it and run

journalctl -u cz-configd --since "15 min ago"

Step 6. Test the scenario works as expected

1. Create an Entitlement with following Action – Site should be **Stockholm** and Condition “Always”:



Action

Rule

Protocol

Network Resources (target)

Ports

2. Add the Entitlement to the distribution policy
3. Login with any user in the distribution group and browse to **192.168.10.200** or <http://production.packnot.intra/> and check the result.
4. Can you access all services and links on the production-info link? If not, how to fix that?

Lab 8a. Set a Login Banner Message and Message of the Day

A *Login Banner Message* can be configured and will appear on the sign-in form of the admin UI. This should be used for any warning you might want to have about improper use, monitoring, etc.

In this lab, you will notify your admins that login will require MFA based on the security requirements.

From the admin UI, go to Settings → **Global Settings** and set an **Administration Banner Message**, e.g. "MFA is required for access to the admin UI"

Log out and back in your admin UI and confirm you can see the message.

Lab 8b. Configuring Admin access with MFA

We would like to force administrators to use two factor authentications for accessing the admin UI of AppGate.

Steps:

1. From the admin UI, navigate to System → MFA for Admins
2. Enable the Multi-factor authentication Mode
3. As an MFA Provider, choose the default Time-Based OTP Provider and make sure you have Google/Microsoft Authenticator installed on your mobile.
4. Note that you could also specify any exempted admin users.
5. Log out the admin UI and log back in. You should be now prompted for an OTP.

Lab 9. Create a delegated admin role for distribution employees' access

We would like to create a limited admin role that will be able to only view all Conditions and Sites and view/edit/delete Entitlements that should do only with distribution.

Steps:

1. From the admin UI, navigate to **System → Admin Roles**
2. Click **Add New** and create a **new Administrative Role**. Give it the name "**Distribution Administrator**"
3. Once you enter the new Admin Role "Name" and any "Notes", click on the "Add new" button to add Privileges to the role. Use the drop-down menu under "Privilege Type" to select which admin action will be allowed – note that you can only select one option at a time. For our lab, we will need the View, Edit and Delete privileges.
4. Under the "**Target Item**" drop-down menu you can select the entities that the administrator will be allowed to access – for our example we are going for "**Conditions**" and "**Entitlements**". Just like for Privileges you can only select one option at a time.
5. The "**Scope of Privilege**" section allows you to further restrict which targets the relevant privilege applies to. Keep in mind that this is only configurable if a specific privilege action

and target have been selected. For our Lab, we want the Scope of Privilege to restrict the administrator to only viewing all Conditions and Sites and viewing/editing/deleting only those Entitlements that have to do with distribution access – i.e. Entitlements with the tag “distribution”. Add that under the “Entitlements by Tag” section

6. The privileges of the new admin Role should look like below:



Privileges
View all Sites
View all Conditions
View all Entitlements tagged with distribution
Delete all Entitlements tagged with distribution
Edit all Entitlements tagged with distribution

7. **Save the changes**
8. Once the admin role has been created and defined, we will need to create a Policy in order to assign the specific Admin Role to a delegated administrator
9. Let's first create a new local user that will have the role of the distribution admin and be assigned the role we created above.
10. Go to System --> Identity Providers and pick the local one. At the bottom of the page, click on "Manage Users". Create a new local user and select "**d_admin**" as username – this will be used for the Policy Assignment Criteria we will create below – and fill-in the rest of the required fields. **Save the changes**
11. Navigate to Operations --> Policies and create a new Policy. Give it a relevant name, e.g. Distribution Administration Policy. For simplicity reasons, we create a Policy Assignment Criterion like this one: username is "**d_admin**"
12. Finally, under Administrative Roles (Admin UI Access) add the admin role "**Distribution Administrator**" you created in the beginning. **Save the changes.**
13. Now log in to the admin UI as the delegated admin **d_admin** you created in the Local Database. Confirm that you have access as a delegated admin to only what your admin role allows you.

Right now, no info/stats should be available to your delegated admin on the Dashboard. Let's say that the distribution admin should be also able to view the Active Sessions on the Dashboard.

Steps:

1. Log in the admin UI as the built-in admin and edit the "**Distribution Administration**" Role to include "**View**" Privileges on "**Session Info**".
2. Log out and log back in again as **d_admin** and confirm that you are now able to see the active sessions on your Dashboard and the Session Details

Note: Please remember to disable Multi-Factor Authentication for access to the Admin UI that was configured in Lab 8 at the end of the labs