AppGate Training Environment TRENT

Training environment to learn the basics of the AppGate System

Table of Contents

Cyxtera Technologies Proprietary . . . 1
Introduction . . . 2
Packnot company . . . 3
Packnot organizational structure . . . 4
    Packnot users in the ldap directory . . . 5
        Service account for openldap bind . . . 7
Main Site infrastructure . . . 8
    Packnot’s internal network (Main Site) . . . 8
    Packnot’s internal applications (assets) . . . 9
AppGate provision access for Packnot’s employees . . . 10
Accessing AppGate and internal assets . . . 11
    Access the internal assets (enduser) . . . 12
    Access the administration interface . . . 13
    Access the log server . . . 14
The Production Site Infrastructure . . . 15
    Overview of the Production Site . . . 16
        Technical details . . . 16
    Packnot’s production applications (assets) . . . 18

Cyxtera Technologies Proprietary

NOTE All material provided in the traininging environment **Trent** are Cyxtera Properitary ©.

Introduction

The training environment (trent) should reflect real-world scenarios based on the Packnot company and its products, people, places etc. Everything you going to test or build in the training is based on this pre-built environment. Packnot is the red thread throughout your training, giving you a real story behind the labs and configurations.

In a nutshell, trent is a ready to use infrastructure with the following characteristics:

- AppGate Server(s) public available and setup ready to use.
- Protected internal web resources, such as intranet, application etc are provisioned through the AppGate.
- Users and groups and group membership are hosted in an openldap directory.
- The AppGate's are reachable on the on the `packnot.com` domain.
- Internal web resources on a zone `packnot.intra`.

The documentation is also available on the intranet in the form of:

- pdf
- docx

Packnot company

Packnot is a global company in the business: *fashion in transit life style*. Yep, that's right, this is a hip company to work for and hey it is not at all fake!

Packnot has a public site and is present on twitter:

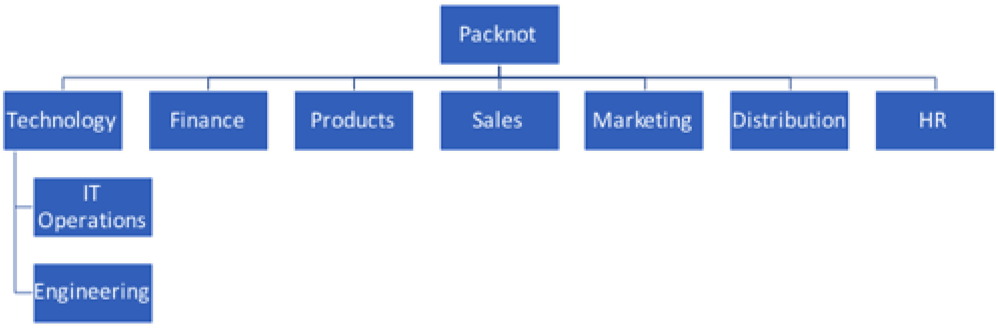
- packnot.com
- Packnot on twitter

Eventhough this is a very true-fake company, you would like to read up on these links get yourself a good picture what the company packnot feels like.

Packnot organizational structure

The Packnot organization looks as the following:

Packnot's organizational chart



Packnot counts around 25 employees. The directory service gives you an overview who these people in Packnot are and where they fit in the organization. The directory service is the primary `Identity Provider` in AppGate-- all the Packnot users (employees) reside in it.

Packnot users in the ldap directory

Table 1. Directory users

User ID	Password	Member of group	Description
Alfonso.Pack	Alfonso@govt	`clevel, office, finance, products, production-site, itoperations`	Founder and CEO
Bernhard.Wrankic	Bernhard@govt	`clevel, office, finance, sales`	CFO
Paul.Schiller	Paul@govt	`clevel, office, engineering`	CTO
Eugene.Bismarck	Eugene@govt	`clevel, office, products, production-site`	VP products
Anna.Moon	Anna@govt	`clevel, office, distribution, production-site`	Global manager HR. Note, Anna might not have access to certain internal systems eventhough she is the groups.
Chad.Jones	Chad@govt	`clevel, office, finance, products, production-site, itoperations`	The IT Administrator
Raymond.Reddington	Raymond@govt	`distribution, marketing, office`	Raymond, one of the first with the company now working with marketing and distribution in the field.
Elizabeth.Keen	Elizabeth@govt	`engineering, office, production-site`	Elizabeth is a test engineer, working in engineering.
Donald.Ressler	Donald@govt	`sales, office`	Donald works mainly with sales in the field.
Aram.Mojtabi	Aram@govt	`engineering, office, products, production-site`	Aram is a software engineer working in engineering.
Harold.Cooper	Harold@govt	`finance, office, clevel, production-site`	Harold assists with strategic decisions for the overall company.
Dembe.Zuma	Dembe@govt	`distribution`	Dembe works with the delivery of vaulted items first hand (oversees item security).
Tom.Keen	Tom@govt	`finance, office, products, sales`	Tom works with product placement and helps sales but also pulls together data from finance.
Samar.Navabi	Samar@govt	`office, marketing`	Samar works mainly with product marketing torwards the outside.

User ID	Password	Member of group	Description
agadmin	n/a	admin	The AppGate administrator has access to the entire infrastructure
Sara.Dator	Sara@govt	office, itoperations	IT operator and IT support
Petra.Krets	Petra@govt	office, itoperations	IT operator and IT support
Alpha.Packnot	Alpha@govt	office, itoperations	Dedicated user to log-in to their instance. This is one of the default accounts for training attendees.
Bravo.Packnot	Bravo@govt	office, itoperations	Dedicated user to log-in to their instance. This is one of the default accounts for training attendees.
Charly.Packnot	Charly@govt	office, itoperations	Dedicated user to log-in to their instance. This is one of the default accounts for training attendees.
Delta.Packnot	Delta@govt	office, itoperations	Dedicated user to log-in to their instance. This is one of the default accounts for training attendees.
External1	External1@govt	external	External (non-employee) user who should be given 3d party access.
External2	External2@govt	external	External (non-employee) user who should be given 3d party access.
External3	External3@govt	external	External (non-employee) user who should be given 3d party access.
External4	External4@govt	external	External (non-employee) user who should be given 3d party access.
Welcome	welcome@govt-08f26a6827a148acf	office	The end-user given to course participants prior to course start.

Table 2. Directory groups

Group	Description	Members
distribution	People working in the field such as airports, transport, and release agents.	Anna.Moon, Raymond.Reddington, Dembe.Zuma
finance	Access to finance back-end, invoicing and salary system.	Alfonso.Pack, Bernhard.Wrankic, Chad.Jones, Harold.Cooper, Tom.Keen
sales	CRM, databse backed systems for customer data.	Bernhard.Wrankic, Donald.Ressler, Tom.Keen

Group	Description	Members
`office`	Access to local infrastructure, intranet, printers etc.	Alfonso.Pack, Bernhard.Wrankic, Paul.Schiller, Eugene.Bismarck, Anna.Moon, Chad.Jones, Raymond.Reddington, Elizabeth.Keen, Donald.Ressler, Aram.Mojtabi, Harold.Cooper, Tom.Keen, Samar.Navabi, Sara.Dator, Petra.Krets, Alpha.Packnot, Bravo.Packnot, Charly.Packnot, Delta.Packnot, Welcome
`marketing`	Marketing material access, share point, graphic content etc.	Raymond.Reddington, Samar.Navabi
`products`	Access to different systems used in products group.	Alfonso.Pack, Eugene.Bismarck, Chad.Jones, Aram.Mojtabi, Tom.Keen
`clevel`	Management level clearence	Alfonso.Pack, Bernhard.Wrankic, Paul.Schiller, Eugene.Bismarck, Anna.Moon, Chad.Jones, Harold.Cooper
`admin`	Administrator with major privileges throughout the infrastructure.	agadmin
`itoperations`	Default group for the appgate operators. This is intended fortraining attendees initial accounts.	Alfonso.Pack, Chad.Jones, Sara.Dator, Petra.Krets, Alpha.Packnot, Bravo.Packnot, Charly.Packnot, Delta.Packnot
`engineering`	Engineers working with development systems, devops etc.	Paul.Schiller, Elizabeth.Keen, Aram.Mojtabi
`production-site`	Employees working with systems on the production sites.	Alfonso.Pack, Eugene.Bismarck, Anna.Moon, Chad.Jones, Elizabeth.Keen, Aram.Mojtabi, Harold.Cooper
`external`	3d party access such as consultants, regulators, maintenance etc. Short term and restricted access only.	External1, External2, External3, External4

Service account for openldap bind

Table 3. Service account

DN	Password
cn=binduser,ou=People,dc=packnot,dc=intra	zwiebel

Main Site infrastructure

The Main Site infrastructure can be divided into two zones, a public and an internal zone:

- Public:
  - `packnot.com` zone used by apps, web-sites etc.
  - `packnot.com` zone reserved for the appgate system, such as remote access and AppGate gateway communication.
- Internal:
  - `packnot.intra` is the internal zone and contains the mission critical infrastructure of the company.

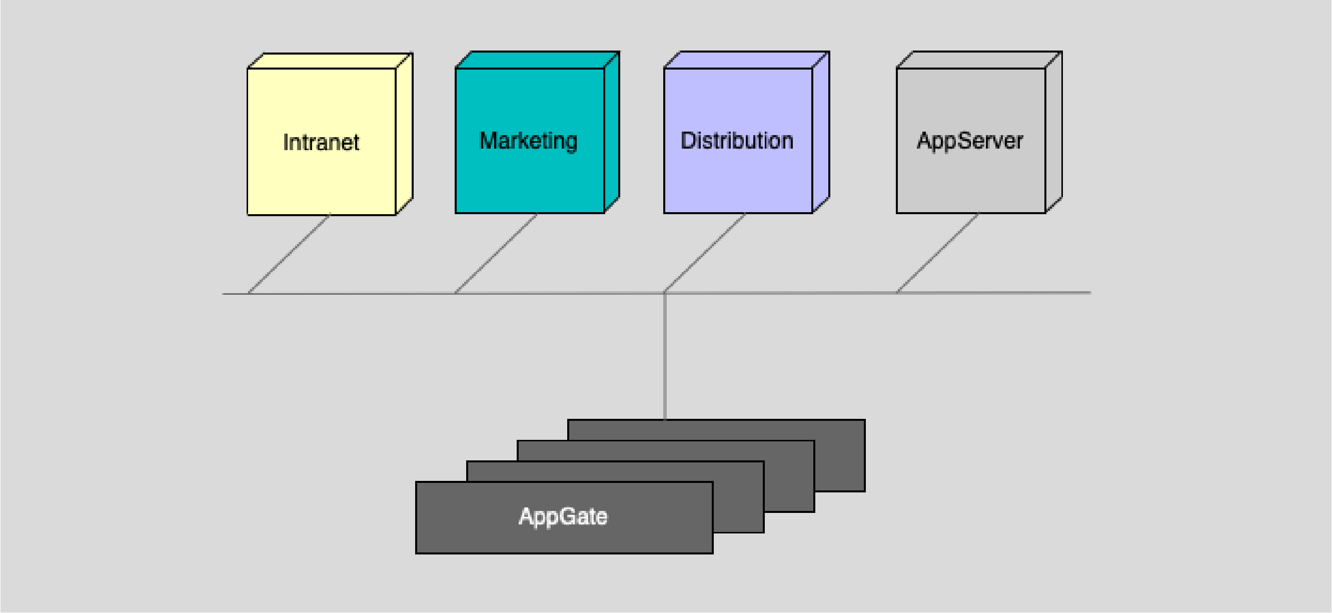


Figure 1. Infrastructure Overview

The applications in the internal zone, `appserver`, `marketing` and `distribution` are company assets. The `appserver` is reserved for the administration of the internal network, by the administrator `agadmin`. The appserver does also host the `openldap`.

Packnot’s internal network (Main Site)

The main site with the scope `govt` is hosted in Amazon AWS. The setup looks as the follow:

- Name of the environment (scope): `govt`
- Region: `ap-southeast-1` (Singapore)
- VPC CIDR block: `10.10.0.0/16`
- Subnets:
  - `10.10.10.0/24`, availability zone `ap-southeast-1a`
  - `10.10.20.0/24`, availability zone `ap-southeast-1b`
- DNS: `10.10.0.2`

Packnot's internal applications (assets)

Table 4. Applications

Name	Hostname	IP	Port	Protocol
appserver	ldap.packnot.intra	10.10.10.200	443	https
distribution	distribution.packnot.intra	10.10.20.201	80	http
marketing	marketing.packnot.intra	10.10.10.202	80	http
intranet	intranet.packnot.intra	10.10.10.203	80	http

Machine setup for assets

The internal assets can be setup in two different ways: either put all the assets on single machine and deploy multiple ip addresses for same machine referred to `mono setup`, or have the assets deployed each on a dedicated machine also referred as `split setup`. This environment \`govt \` is setup as:

- `split`

AppGate provision access for Packnot’s employees

The way how AppGate provisions access is tightly aligned with Packnots organizational structure. Do give you a fast forward introduction, consider the following diagram:

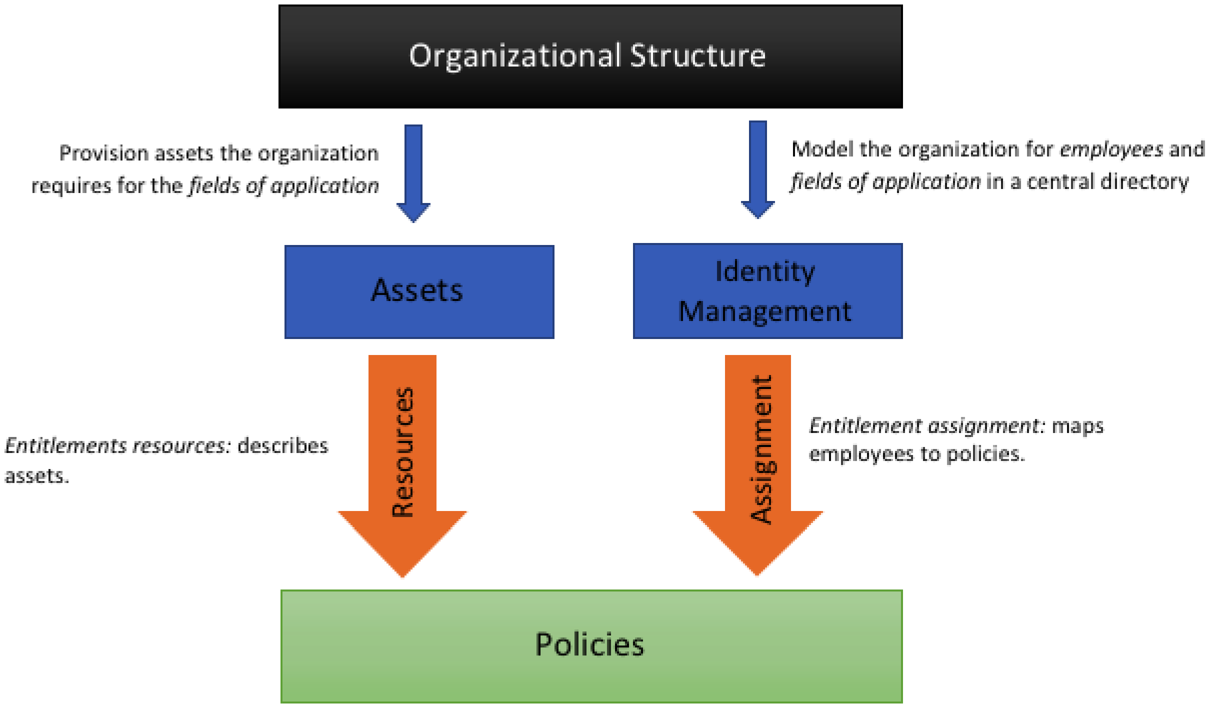

Organizational Structure
Provision assets the organization requires for the *fields of application*
Model the organization for *employees* and *fields of application* in a central directory
Assets
Identity Management
Resources
Assignment
Entitlements resources: describes assets.
Entitlement assignment: maps employees to policies.
Policies

Figure 2. The AppGate model

The model behind the configuration is straight forward. The organization’s structure is chosen as the ontology when the AppGate implementation was designed. This means the organization’s layout is chosen as the implementation model in AppGate. As you can see from the diagram, the organization already imposes a model in the openldap (Identity Management) as to its defacto existence. In openldap users are member of groups which correlate to the organization, so will for example the organizational group `marketing` become a group in openldap called `marketing`.

The assets in our context here are the entities the employees need to use for doing their job. This is the IT infrastructure with all the servers, services etc.

The aim with AppGate, in a simplified description, is to provision access to assets for their employees. In AppGate we model the user provisioned access to assets in the form of `policies`. A policy describes and groups assets. In AppGate, assets are modeled with the so called `entitlements`. In our infrastructure AppGate uses the openldap as the `identity provider` and hence inherits its data structure model and hence follows the organizational structure. With the help of `policy assignment` we can control what employee will have what policy assigned (mapping). In Packnot’s case, the mapping is generated from the openldap `group membership`.

`Policies` and `Entitlements` are concept of AppGate and allow us to implement the model as described above.

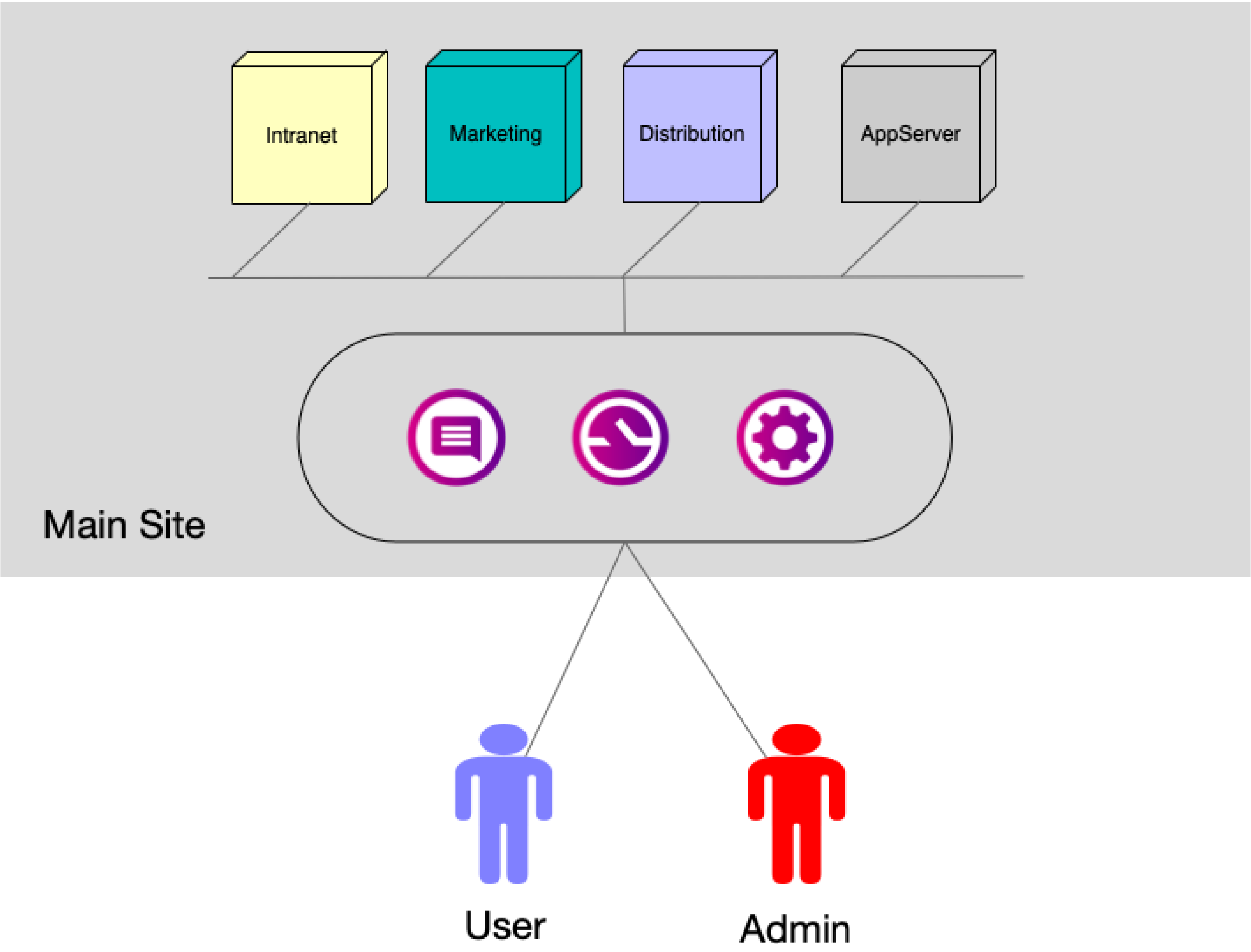
Accessing AppGate and internal assets

The AppGate server hosts three components:

- [controller] Controller
- [controller] Gateway
- [controller] Log Server

All three components are hosted on the same appliance. The `controller` is the AppGate authority and it also allows an administrator to administrate the system through the web based admin user interface. The `gateway` is the egress point of the user-tunneled traffic with the ingress point in the Appgate client. The log-server provides an audit trail of messages generated by user and system activities.

Big Picture



NOTE you will use the `AppGate Client` in the role of the end-user, and the `AppGate Administration User Interface` in the role of the administrator.

Access the internal assets (enduser)

[lclient_symbol] First, you need to install the client on your computer. The client will install the multi-tunnel driver, a user interface and a service. The client can be fetched here. To get started with the installation of the client and to understand how to client works continue reading on the User Guide. You can login with any user present in the directory service (see Packnot organizational structure below). Note that the access right to the assets depend on users group membership. Groups are directly mapped with the corresponding `filters` and `policies` in the AppGate system.

Start the `AppGate client` and the URL:

- ctl1.packnot.com
- ctl2.packnot.com
- ctl3.packnot.com
- ctl4.packnot.com
- ctl5.packnot.com
- ctl6.packnot.com
- ctl7.packnot.com
- ctl8.packnot.com
- ctl9.packnot.com
- ctl10.packnot.com
- ctl11.packnot.com
- ctl12.packnot.com
- ctl13.packnot.com

Log-in with any of the Packnot organizational structure users.

Access the administration interface

[controller_symbol] The administration of the AppGate is achieved through a web based application (User Interface/UI). You can access the UI with a web browser such as Chrome or IE. The administration UI for the govt environment is available on the following URL:

- https://ctl1.packnot.com:444/ui
- https://ctl2.packnot.com:444/ui
- https://ctl3.packnot.com:444/ui
- https://ctl4.packnot.com:444/ui
- https://ctl5.packnot.com:444/ui
- https://ctl6.packnot.com:444/ui
- https://ctl7.packnot.com:444/ui
- https://ctl8.packnot.com:444/ui
- https://ctl9.packnot.com:444/ui
- https://ctl10.packnot.com:444/ui
- https://ctl11.packnot.com:444/ui
- https://ctl12.packnot.com:444/ui
- https://ctl13.packnot.com:444/ui

Access the log server

[logserver_symbol] The log server is hosted under the same URL as the admin user interface. After logging into the admin user interface, choose on the left hand menu `Audit Logs`. This will bring you to the `kibana` log server interface.

The Production Site Infrastructure

Packnot runs a majority of its Vaulted Item Service in Asia, and therefore has a production site hosting application core for the asian market in Seoul.

Overview of the Production Site

As you can see, there is a single gateway fronting the production site. This gateway is currently used only to provision and control access for the Packnot employees. The Gateway is a leg of the entire Packnot infrastructure. At the moment, the gateway is not yet activated (or so called seeded), but will due to your help.

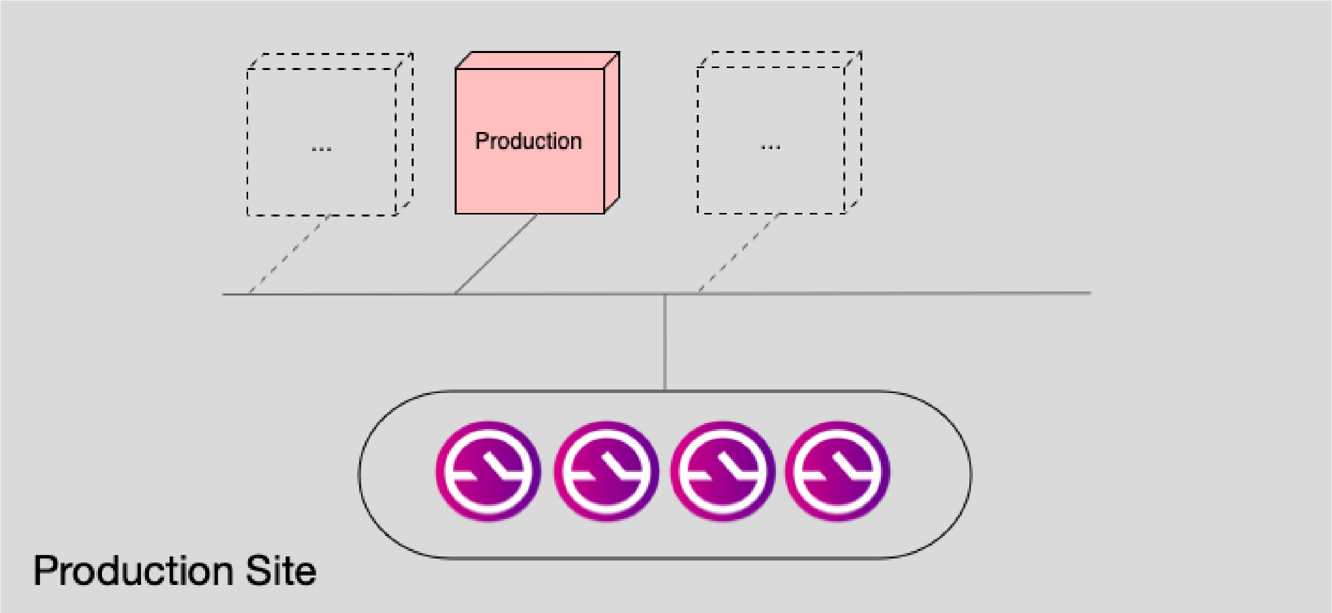


Figure 3. Production Site

The production site is reachable over the Internet on the following host names:

- gw1.packnot.com
- gw2.packnot.com
- gw3.packnot.com
- gw4.packnot.com
- gw5.packnot.com
- gw6.packnot.com
- gw7.packnot.com
- gw8.packnot.com
- gw9.packnot.com
- gw10.packnot.com
- gw11.packnot.com
- gw12.packnot.com
- gw13.packnot.com

Technical details

The production site with the scope `govt` is hosted in Amazon AWS. The setup looks as the follow:

- Name of the environment (scope): `govt`
- Region: `ap-northeast-2` (Seoul)
- VPC CIDR block: `192.168.0.0/16`
- Subnets:
  - `192.168.10.0/24`, availability zone `ap-northeast-2a`
  - `192.168.20.0/24`, availability zone `ap-northeast-2c`
- DNS: `10.10.0.2`

Packnot’s production applications (assets)

Table 5. Applications

Name	Hostname	IP	Port	Protocol
production	production.packnot.intra	192.168.10.200	80	http
production-info	production-info.packnot.intra	192.168.10.201	80	http