

Adding a Gateway

AppGateSDP
Access, evolved.

Cyxtera proprietary

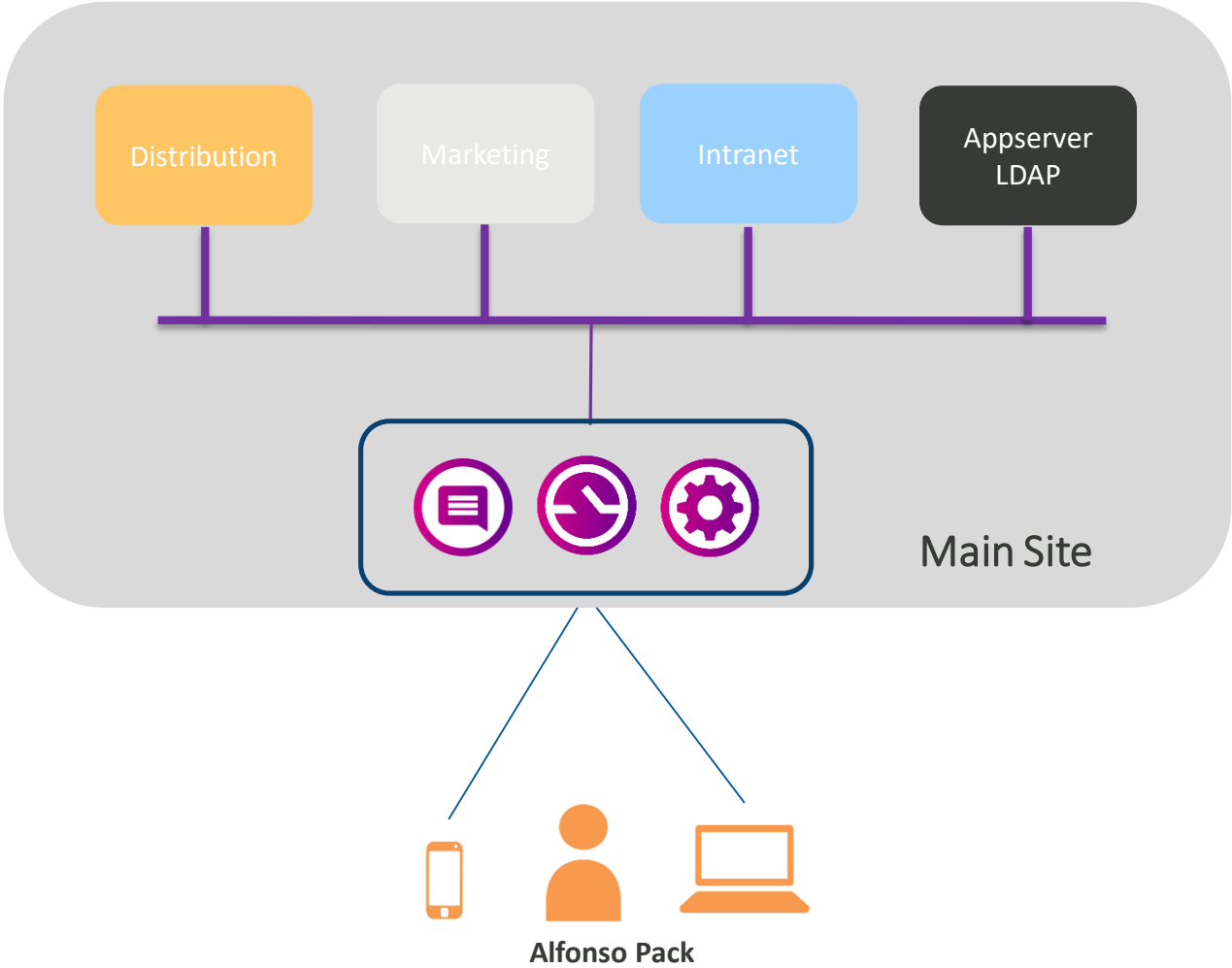
You will learn

- How you configure a multi-Site/multi-tunnel in AppGate
- How to create a Site and Appliance on the Controller
- How to seed an additional Gateway to be added to the Collective
- Create proper Policy to verify the connection to the resources behind the Gateway

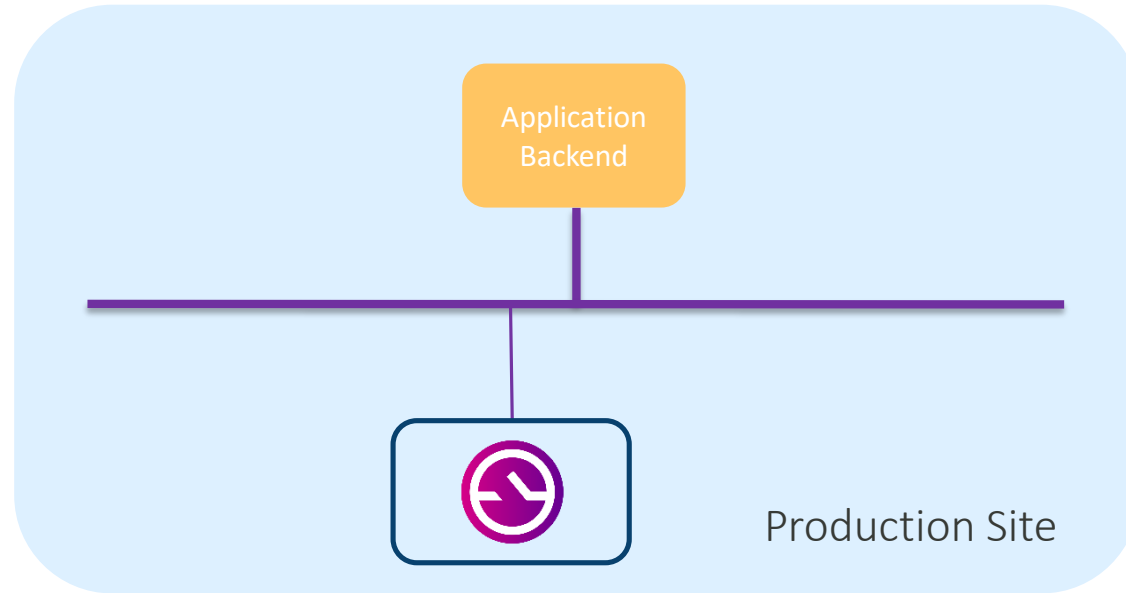
Scenario: Provisioning access to Application Backend

AppGateSDP
Access, evolved.

Current setup

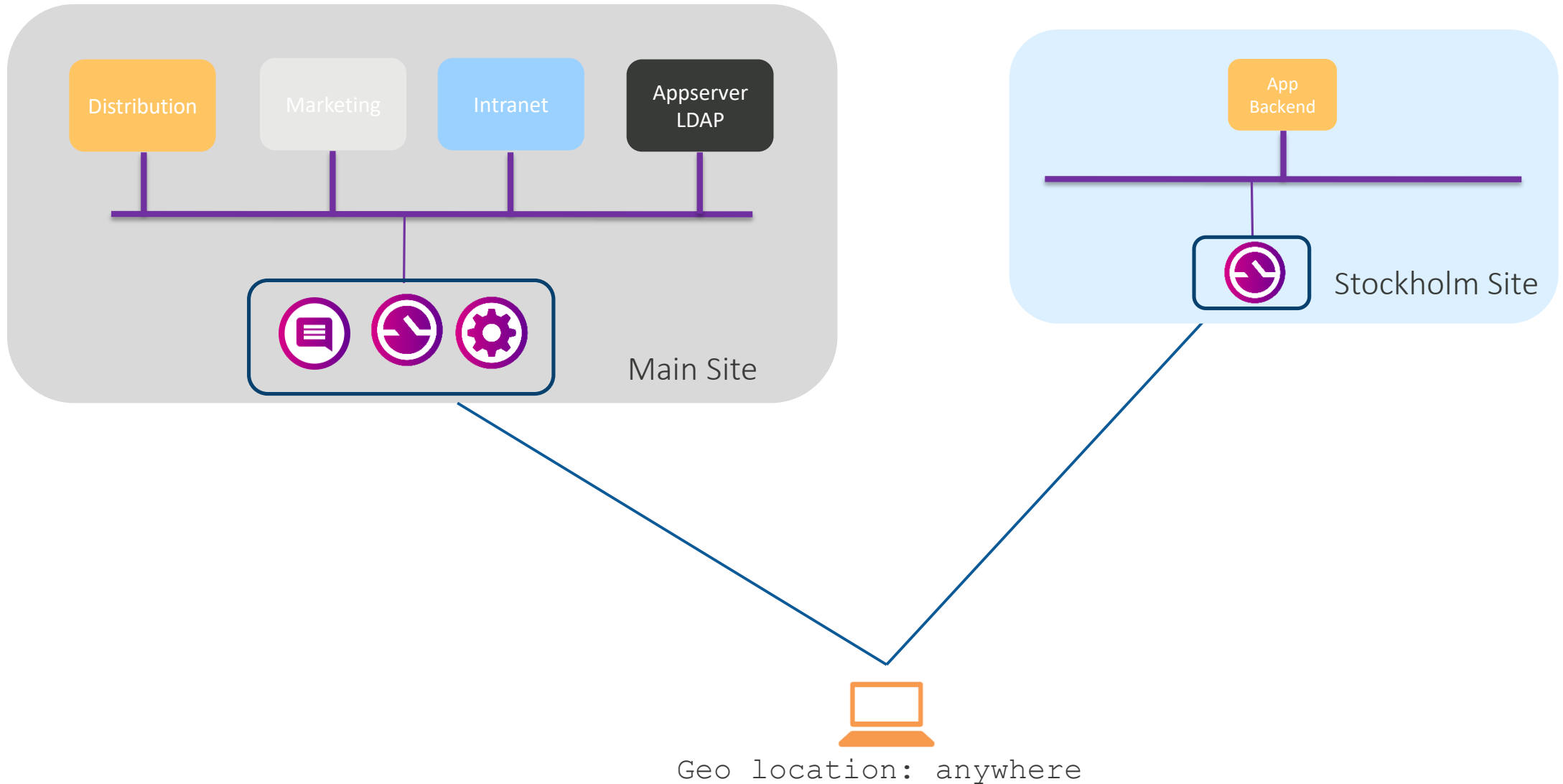


Application Site located in Stockholm



- The Site is an existing production site, hosting the web application backend.
- The appliance to be seeded (to become a Gateway) is up and running.

Desired outcome



Step by step

AppGateSDP
Access, evolved.

Overall process

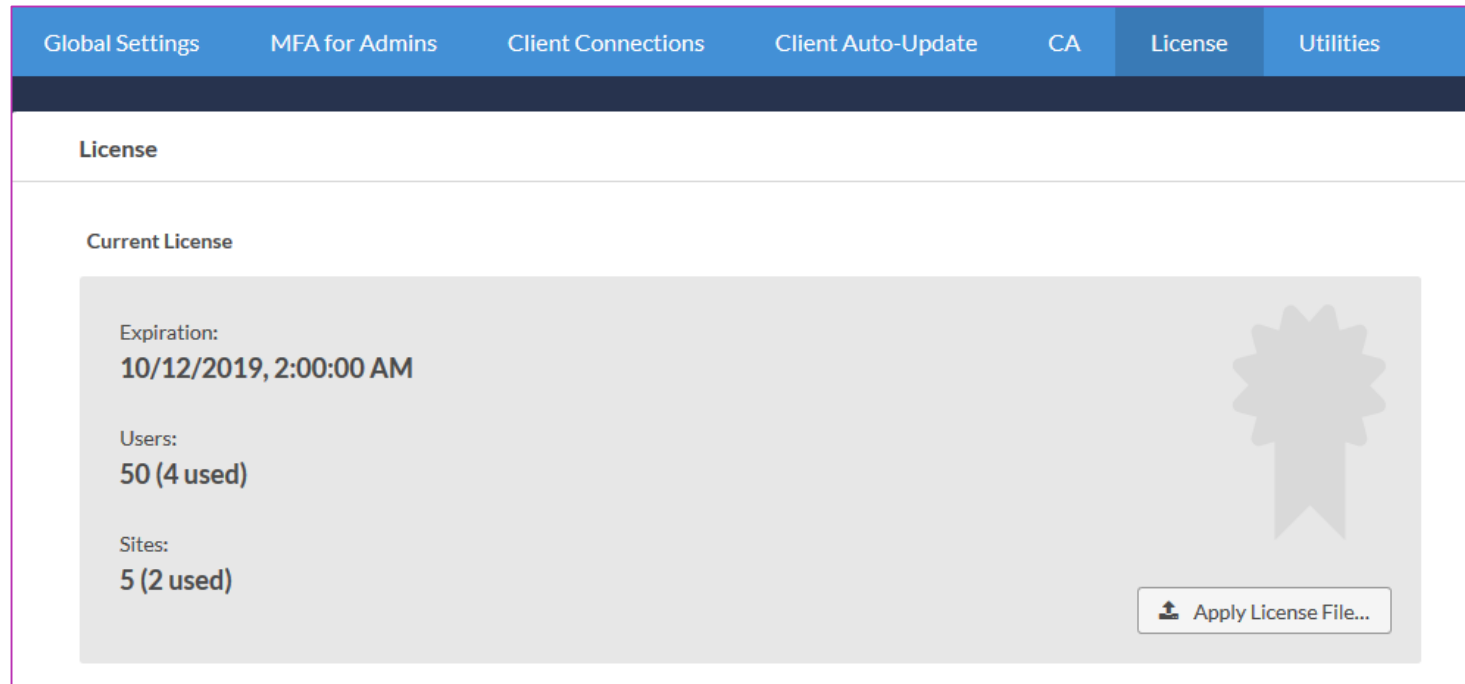
1. Assure you have licenses for additional sites
2. Create a new Site called "Stockholm" in the Controller
3. Create a new appliance in the Controller
 - Download and save the seed file
4. Seed the appliances
 - We copy the seed file (JSON) to the already existing appliance
5. Verify in Controller new Gateway works properly
6. Test the scenario works as expected

Step-by-Step walkthrough

- Have a read under [trent-documentation](#), you find all the information:
 - Site information
 - IP addresses
 - Appliance settings
 - Etc.

Step 1: Check license

- Additional Sites require additional licensing
- Check on the Controller's Dashboard for your license



- You need to request a new license if sites-count < 2

Step 2: Create new Site

<

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

<

Editing Site - Client Routing

General

Client Routing

Name Resolvers

☒ Entitlement Based Routing

☐ Subnet Based Routing

☐ Route all traffic through tunnel (Default Gateway)

<

Editing Site - Name Resolvers

General

Client Routing

Name Resolvers

Hosts File (Appliance)

☐ Use Hosts File

Name Resolvers

+ Add new

AWS Resolver 1

Step 3: Create new Appliance (1)

<

Editing Appliance - General

General

Networking

Client Interface

Peer Interface

Name

Stockholm

Notes

Appliance Hostname

gw6.packnot.com

Roles

☐ Controller

☐ LogServer

☒ Gateway

Site

Stockholm

User Tunneling - Load Balancing Weight

100

User Tunneling - Allow Destinations

nic eth0

+ Add new

<

Editing Appliance - Networking

General

Networking

Client Interface

Peer Interface

Interfaces

eth0 - Addresses: DHCP

+ Add new

Routes

Click here or Add new to populate the list

+ Add new

DNS Servers

10.10.0.2

+ Add new

DNS Search Domains

Click here or Add new to populate the list

+ Add new

NTP Servers

0.ubuntu.pool.ntp.org

+ Add new

Advanced Settings

Delete

Clone

Cancel

Save

Step 3: Create new Appliance (2)

< Editing Appliance - Client Interface

General

Networking

Client Interface

Peer Interface

Hostname

gw6.packnot.com

TLS Port

443

DTLS Port

443

☐ Enable Proxy Protocol

Allow Sources

+ Add new

0.0.0.0 nic Any

:: nic Any

Delete

Clone

Cancel

Save

< Editing Appliance - Peer Interface

General

Networking

Client Interface

Peer Interface

Hostname

gw6.packnot.com

TLS Port

444

Allow Sources

+ Add new

0.0.0.0 nic Any

:: nic Any

Delete

Clone

Cancel

Save

Step 4: Seed the Appliance

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

☐ Use password

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

Cancel

Export Seed

Appliances						
Appliances						
Total Appliances 2 Search Add New						
Name ↑	Hostname	Site	State	Tags		Modified
ctl6_packnot_com	ctl6.packnot.com	Default Site	Active	managed-by-trent	first-appliance	2/27/2019, 1:41:29 PM
Stockholm	gw6.packnot.com	Stockholm	Not active			3/7/2019, 11:04:52 AM

Export Seed File/ISO

Step 4: Seed the appliance

- Copy the seed file to the Appliance:

```
scp -i ~/keys/mykey ~/Desktop/newgateway_seed.json cz@newgateway.wherever.com:/home/cz
```

```
C:\Users\lfteris.chairetakis>scp -i C:\Users\lfteris.chairetakis\Downloads\ing.pem C:\Users\lfteris.chairetakis\Downloads\stockholm-seed.json cz@gw6.packnot.com:/home/cz
The authenticity of host 'gw6.packnot.com (13.53.35.74)' can't be established.
RSA key fingerprint is SHA256:/55e1cKy4gyX3I584gNwqfG7SC54etaCPB7ba7mK/Qo.
Are you sure you want to continue connecting (yes/no)?
Warning: Permanently added 'gw6.packnot.com,13.53.35.74' (RSA) to the list of known hosts.
Authorized uses only. All activity may be monitored and reported.
stockholm-seed.json                                100%   11KB 736.5KB/s   00:00
```

```
Authorized uses only. All activity may be monitored and reported.
Last login: Thu Mar  7 10:18:48 2019 from 212.16.176.132
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.15.0-43-generic x86_64)
AppGate 4.2.2-12675-release (image1)
Hint: run 'sudo cz-setup' for appliance management.
cz@ec2-13-53-35-74:~$
Appliance seed configuration file picked up at /home/cz/stockholm-seed.json
```

- Wait until the Appliance appears on the Dashboard

Step 5: Verify in Controller the new Gateway

Admin Messages

Total Admin Messages 3

i

From Appliance: Appliance 'Stockholm' joined to the collective. This appliance operates as Gateway.
This message has appeared once. Last time: 3/7/2019, 11:24:05 AM.

!

From Controller: Identity provider 'Packnot' has failed to authenticate a user. Details: ERR_04110_CANNOT_CONNECT_TO_SERVER Cannot connect to the server: Connection refused
This message has appeared once. Last time: 2/27/2019, 2:06:10 PM.

i

From Appliance: Appliance 'ctl6_packnot_com' joined to the collective. This appliance operates as LogServer and Controller.
This message has appeared once. Last time: 2/27/2019, 1:39:46 PM.

Connectivity errors during appliance configuration changes or upgrades are expected.

Admin Guide

2 Appliances

2 Gateways

1 Controller

1 LogServer

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
ctl6_packnot_com	healthy	healthy	healthy	healthy	1%	59%	4.66 Kbps/3.49 Kbps	3%	4.2.2-12675-release

Step 6: Test the scenario works as expected

1. Create Entitlement to give access to the production services described in <http://intranet.packnot.lab/doc>
2. Add the Entitlement to the distribution policy
3. Login with a user belonging to the distribution group and verify access to the services
4. Can you access all services and links on the production site?

Result

http://192.168.10.200/

**PACKNOT PRODUCTION**
Site Stockholm

PRODUCTION

PRODUCTION-INFO

ADMIN

WELCOME TO STOCKHOLM PRODUCTION INFO

Training material


By [Alfonso Pack](#)

Application hosting Stockholm

The vault release hosting environment for the Asian market is mainly hosted out of Stockholm. Most of the customers are also from Japan.

Packnot.com

Twitter



Route print on user machine

IPv4 Route Table

=====

Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	192.168.10.1	192.168.10.176	40
	10.10.0.0	255.255.0.0	On-link	192.168.100.1	1
10.10.255.255	255.255.255.255		On-link	192.168.100.1	257
13.231.89.80	255.255.255.255		192.168.10.1	192.168.10.176	40
35.158.84.20	255.255.255.255		192.168.10.1	192.168.10.176	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
192.168.10.0	255.255.255.0		On-link	192.168.10.176	296
192.168.10.1	255.255.255.255		On-link	192.168.10.176	40
192.168.10.176	255.255.255.255		On-link	192.168.10.176	296
192.168.10.200	255.255.255.255		On-link	192.168.100.1	1
192.168.10.255	255.255.255.255		On-link	192.168.10.176	296
192.168.100.1	255.255.255.255		On-link	192.168.100.1	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	192.168.100.1	257
224.0.0.0	240.0.0.0		On-link	192.168.10.176	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	192.168.100.1	257
255.255.255.255	255.255.255.255		On-link	192.168.10.176	296

=====

The end

AppGateSDP
Access, evolved.