

Understanding some key communication concepts

4 important ones.....

Un-hiding network resources

IP addresses, hostnaming & DNS

Control information flow

Data packet flow

AppGateSDP
Access, evolved.

Cyxtera proprietary

Un-hiding network resources

AppGateSDP
Access, evolved.

Single Packet Authorization (SPA) – Client Connections

- SPA - allows ONLY the Client to open a TCP connection with the AppGate system because it has been pre-SEEDDED with a specific key
- SPA is enabled by default
- New systems use a General 'key'
 - it should be deleted and replaced with a new SPA key
- Multiple keys may be used
- CA fingerprint is included in the key
- Option of QR code for seeding the Clients

Global Settings MFA for Admins **Client Connections** Client Auto-Update CA License Utilities

Client Connections

SPA mode

- ☒ Disable
- ☐ TCP (as TLS extension)
- ☐ UDP-TCP (SPA-DNS on port 53/SPA-DTLS on port 443 + SPA-TCP)

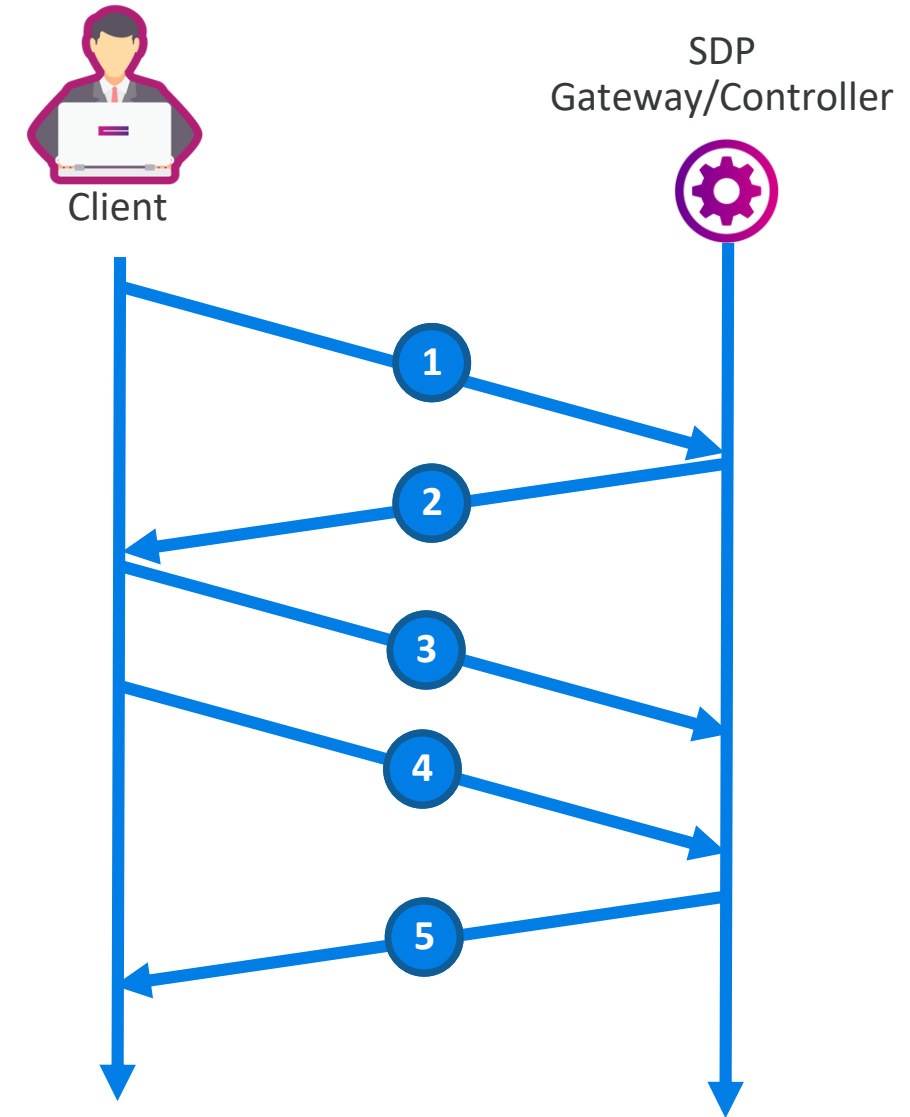
Manage client URLs [Add new](#)

Key hellospa1234 URL		includes Fingerprint			
----------------------	--	----------------------	--	--	--

[Download QR code](#)

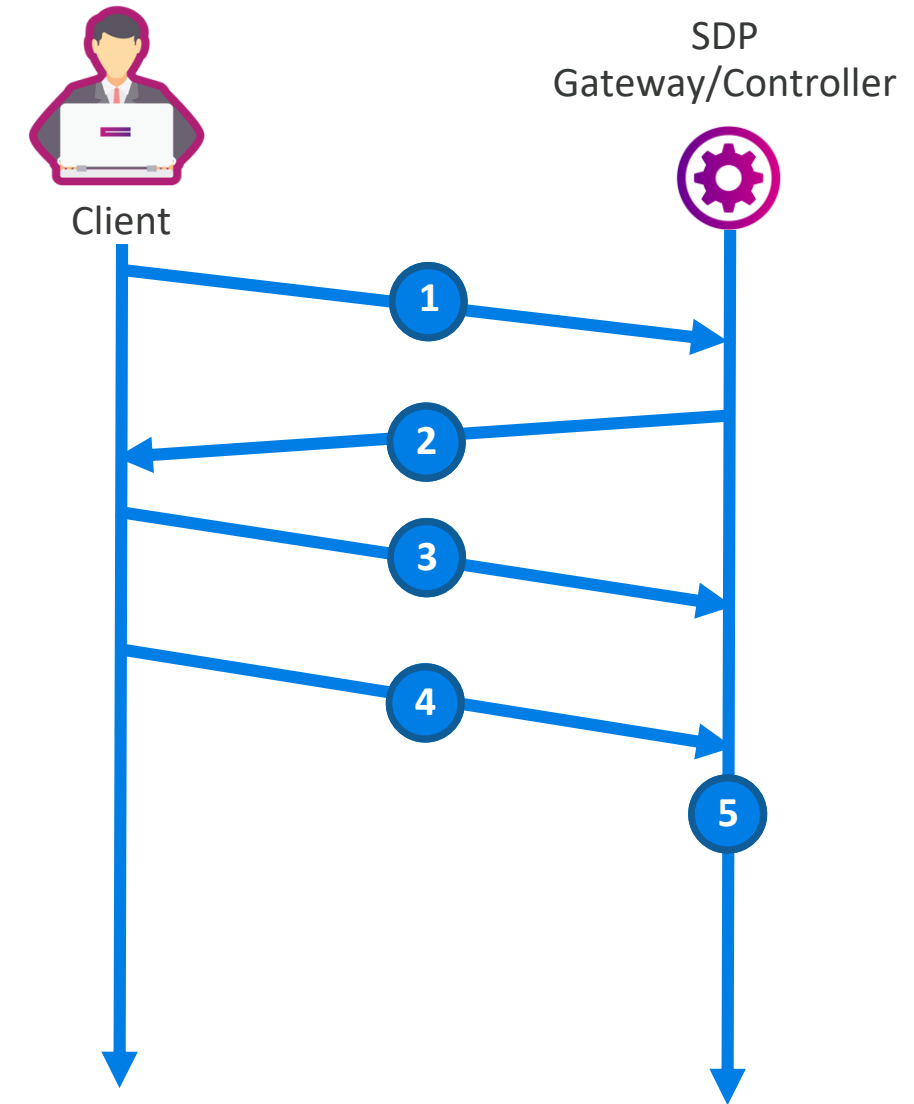
Normal SSL/TLS traffic, no SPA

1. Client sends TCP SYN to Gateway/Controller on 443
2. SDP answers with TCP SYN ACK to acknowledge the first packet
3. Client sends TCP ACK to acknowledge previous packet
 - There is now an established TCP session on port 443, and SSL/TLS layer is **NOW** accessible
4. If Client ask for SSL/TLS (TLS/SSL client Hello packet)
5. SDP responds with server Hello packet



SSL/TLS traffic, with TCP SPA

1. Client sends TCP SYN to Gateway/Controller on 443
2. SDP answers with TCP SYN ACK to acknowledge the first packet
3. Client sends TCP ACK to acknowledge previous packet
 - There is now an established TCP session on port 443, but SSL/TLS layer is NOT accessible
4. Client will send a TCP SPA packet, hidden as TLS Hello packet
5. If correct SPA packet, SDP is now ready to accept TLS traffic
6. TLS vulnerabilities are not exploitable before successful SPA packet !



SSL/TLS traffic, with TCP SPA

No.	Time	Delta	Source	Destination	Protocol	SEQ#	RTT	NEXTSEQ#	ACK#	Info
12	7.300157	0.007870000	10.0.2.15		TLSv1.2	1		268	1	Client Hello

> Frame 12: 321 bytes on wire (2568 bits), 321 bytes captured (2568 bits) on interface 0

> Ethernet II, Src: PcsCompu_d5:72:d1 (08:00:27:d5:72:d1), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)

> Internet Protocol Version 4, Src: 10.0.2.15, Dst: 212.16.176.166

> Transmission Control Protocol, Src Port: 50641, Dst Port: 443, Seq: 1, Ack: 1, Len: 267

Secure Sockets Layer

- TLSv1.2 Record Layer: Handshake Protocol: Client Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 262
 - Handshake Protocol: Client Hello
 - Handshake Type: Client Hello (1)
 - Length: 258
 - Version: TLS 1.2 (0x0303)
 - Random: e7656777870bc8deb35fa9b25acb133ad2a5dd4f248512af...
 - Session ID Length: 0
 - Cipher Suites Length: 4
 - Cipher Suites (2 suites)
 - Compression Methods Length: 1
 - Compression Methods (1 method)
 - Extensions Length: 213
 - Extension: server_name (len=26)
 - Extension: ec_point_formats (len=4)
 - Extension: supported_groups (len=28)
 - Extension: SessionTicket TLS (len=0)
 - Extension: signature_algorithms (len=32)
 - Extension: heartbeat (len=1)
 - Extension: Unknown type 67 (len=94)
 - Type: Unknown (67)
 - Length: 94
 - Data: 014275696c742d696e2d6265383533363038393532343200...

SPA Demo

AppGateSDP
Access, evolved.

IP addresses, Hostname & DNS

Care needs to be taken when setting up a distributed system to make sure all the elements can communicate!

Setting hostnames in AppGate

Because AppGate is a distributed system, there are several options when configuring 'hostnames':

System/Appliance/General>

This will identify the system in the UI, and be used by the appliance internally.

Appliance /Networking>Interfaces

Eth0 would normally be configured with the same hostname as above

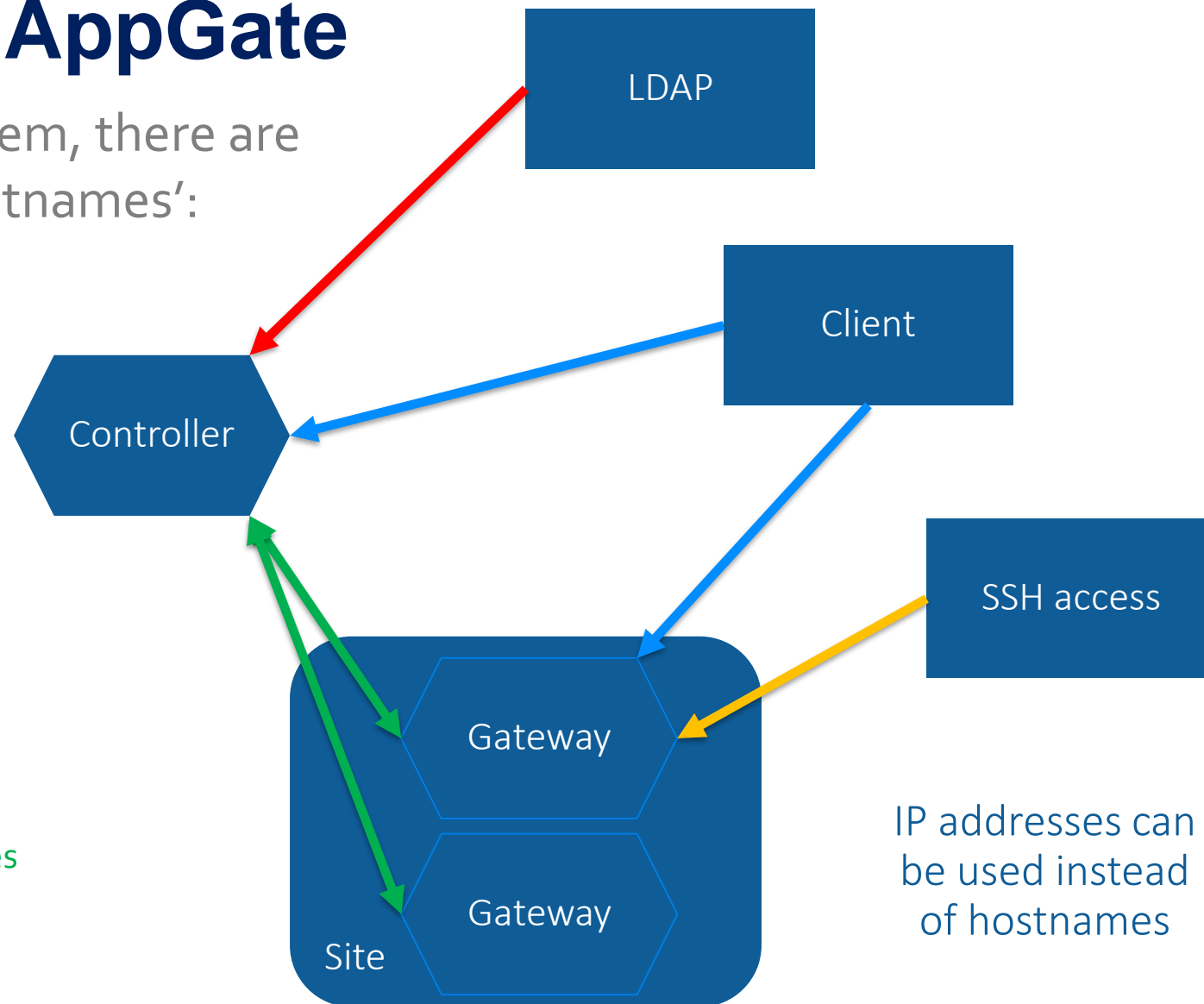
Eth1,2,3,etc would be other (internal?) interface names

Appliance/>Client Interface

You can change the hostname the client will try to resolve/connect to.

Appliance/>Peer Interface

You can change the hostname the other appliances in the collective will try to resolve/connect to.



Setting up DNS – done in 3 places

Identity providers

Used by the Client to resolve hostnames in entitlements.
These will typically be an internal DNS server through the tunnel - so add DNS entitlement!

Configured by IdP so that it is easy to configure for multiple tenants

Sites (one of the Name Resolver options)

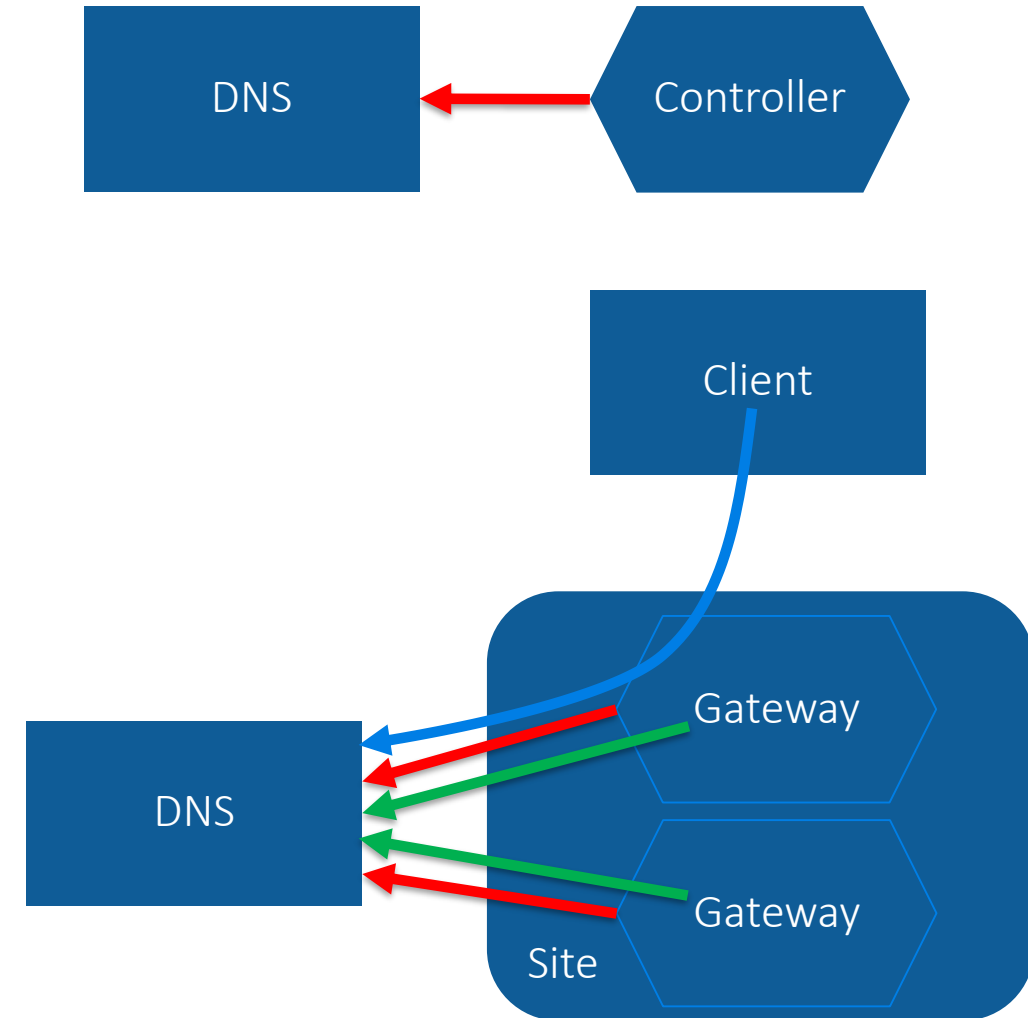
DNS settings used by the Gateway's firewall engine to resolve the hostnames in the Entitlements

Configured by Site so that DNS services are where the protected hosts actually reside

Appliances>Basic Settings>Networking

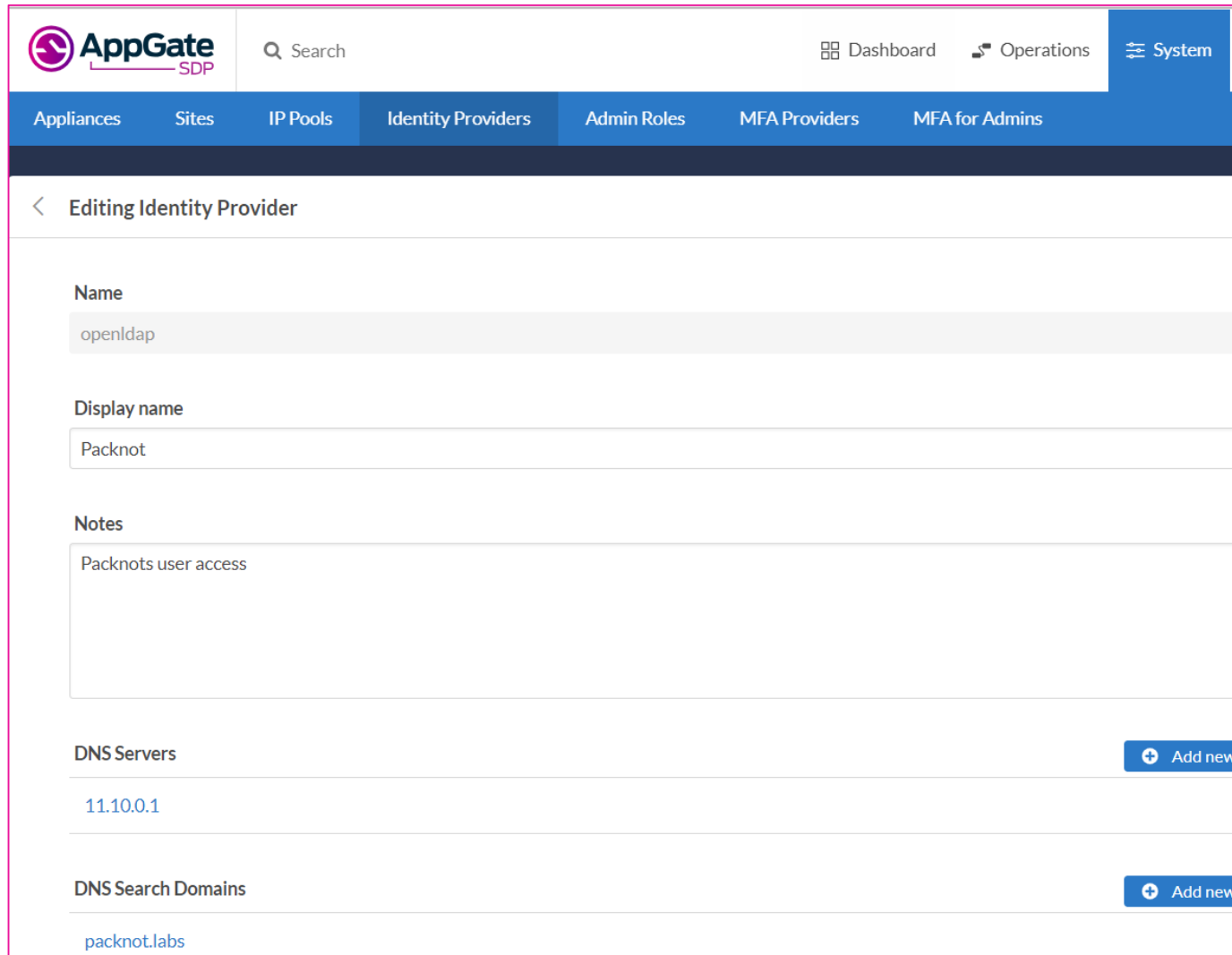
DNS settings used by the appliance operating system to resolve hostnames

Configured by appliance so that local services (RADIUS etc) can be resolved



Setting up DNS – cont'd

1. IdP



The screenshot shows the 'Editing Identity Provider' configuration page in the AppGate SDP interface. The page has a top navigation bar with the AppGate SDP logo, a search bar, and links to Dashboard, Operations, and System. Below this is a secondary navigation bar with tabs for Appliances, Sites, IP Pools, Identity Providers (selected), Admin Roles, MFA Providers, and MFA for Admins. The main content area is titled 'Editing Identity Provider' and contains several sections: 'Name' with the value 'openldap', 'Display name' with the value 'Packnot', 'Notes' with the value 'Packnots user access', 'DNS Servers' with the value '11.10.0.1' and an 'Add new' button, and 'DNS Search Domains' with the value 'packnot.labs' and an 'Add new' button.

AppGate SDP Search Dashboard Operations System

Appliances Sites IP Pools **Identity Providers** Admin Roles MFA Providers MFA for Admins

< Editing Identity Provider

Name
openldap

Display name
Packnot

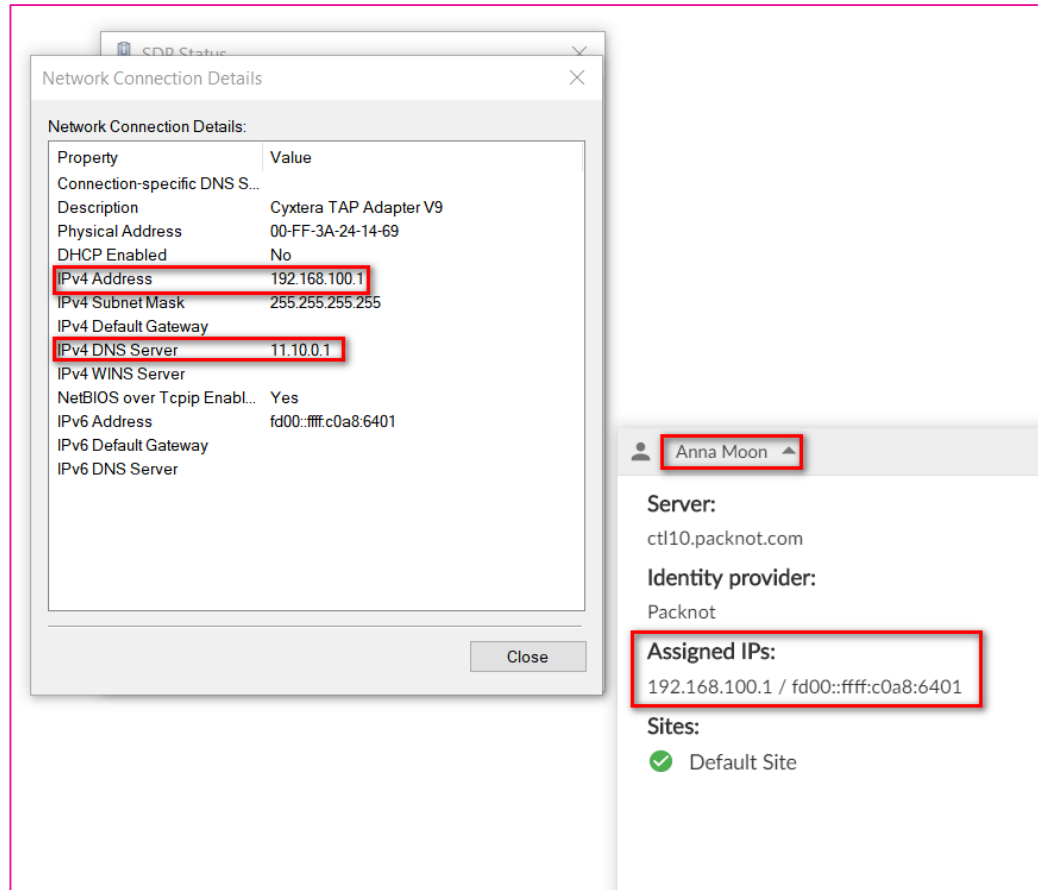
Notes
Packnots user access

DNS Servers + Add new
11.10.0.1

DNS Search Domains + Add new
packnot.labs

Setting up DNS – cont'd

1. IdP



Setting up DNS – cont'd

2. Site

The screenshot shows the AppGate SDP web interface. The top navigation bar includes the AppGate SDP logo, a search bar, and links to Dashboard, Operations, System, and Scripts. Below this is a secondary navigation bar with tabs for Appliances, Sites, IP Pools, Identity Providers, Admin Roles, MFA Providers, and MFA for Admins. The 'Sites' tab is active, and the page title is 'Editing Site - Name Resolvers'. The main content area has three tabs: General, Client Routing, and Name Resolvers. The 'Name Resolvers' tab is selected. Under the 'Hosts File (Appliance)' section, the 'Use Hosts File' checkbox is unchecked. Below this is the 'Name Resolvers' section, which contains a table with one entry: 'AWS Resolver 1'. To the right of this entry are edit and delete icons. An 'Add new' button is located to the right of the table. At the bottom of the page are buttons for 'Delete', 'Clone', 'Cancel', and 'Save'.

AppGate SDP

Search

Dashboard Operations System Scripts

Appliances Sites IP Pools Identity Providers Admin Roles MFA Providers MFA for Admins

< Editing Site - Name Resolvers

General Client Routing Name Resolvers

Hosts File (Appliance)

☐ Use Hosts File

Name Resolvers

+ Add new

AWS Resolver 1

Delete Clone Cancel Save

Setting up DNS – cont'd

3- Appliance

The screenshot displays the AppGate SDP web interface. At the top, the AppGate SDP logo is on the left, and a search bar is in the center. On the right, there are navigation links for Dashboard, Operations, System (which is highlighted), and Scripts. Below this is a blue navigation bar with links for Appliances, Sites, IP Pools, Identity Providers, Admin Roles, MFA Providers, and MFA for Admins. The main content area is titled 'Editing Appliance - Networking' with a back arrow. It features four tabs: General, Networking (selected), Client Interface, and Peer Interface. Under the Networking tab, there are four sections: Interfaces, Routes, DNS Servers, and DNS Search Domains. Each section has an 'Add new' button. The Interfaces section shows 'eth0 - Addresses: DHCP'. The Routes section has a link 'Click here or Add new to populate the list'. The DNS Servers section shows '10.10.0.2'. The DNS Search Domains section shows 'packnot.lab'.

AppGate SDP Search

Dashboard Operations **System** Scripts

Appliances Sites IP Pools Identity Providers Admin Roles MFA Providers MFA for Admins

< Editing Appliance - Networking

General **Networking** Client Interface Peer Interface

Interfaces + Add new

eth0 - Addresses: DHCP

Routes + Add new

Click here or Add new to populate the list

DNS Servers + Add new

10.10.0.2

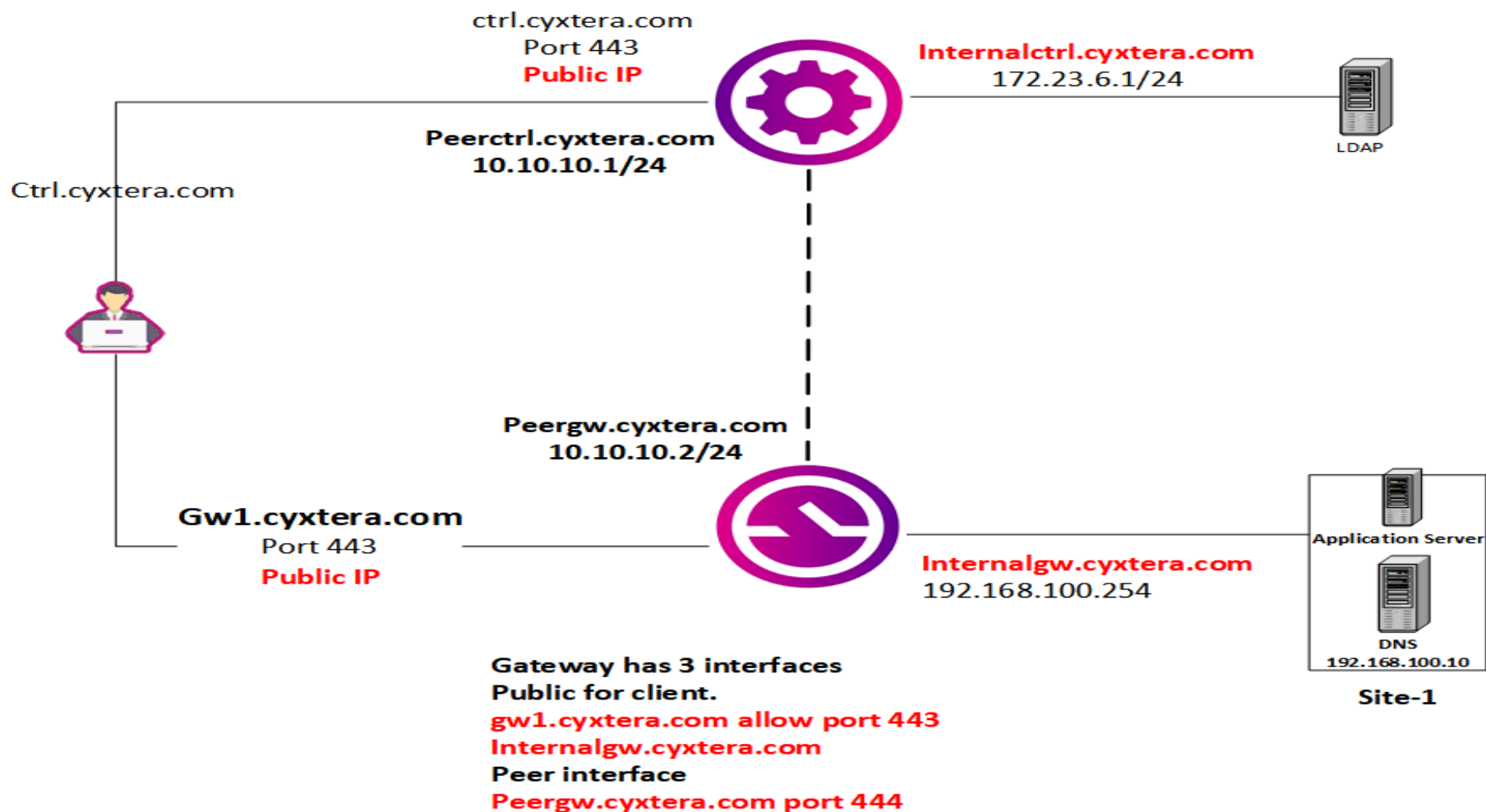
DNS Search Domains + Add new

packnot.lab

Controller has 3 interfaces

- 1- **ctrl.cyxtera.com** public for client connection
- 2- **internalctrl.cyxtera.com** for internal servers such as LDAP
- 3- **peerctrl.cyxtera.com** for AppGate collective appliances such as GW , another Log server and another controller

IP pool for client is 192.168.100.0/24
DNS 192.168.100.10



Control flow in AppGate

Almost all interactions between elements in the AppGate system are tokenized

AppGateSDP
Access, evolved.

Security & the token based model

The Controller is the **Certificate Authority** and uses a self-signed CA certificate.

When any appliance is configured, all the hostnames and IP addresses are added to the appliance certificate.

- These certificates are used to establish trusted (TLS) communications between appliances (peer-interface) and between client and appliance (client-interface).

The CA certificate is also used for creating signed tokens.

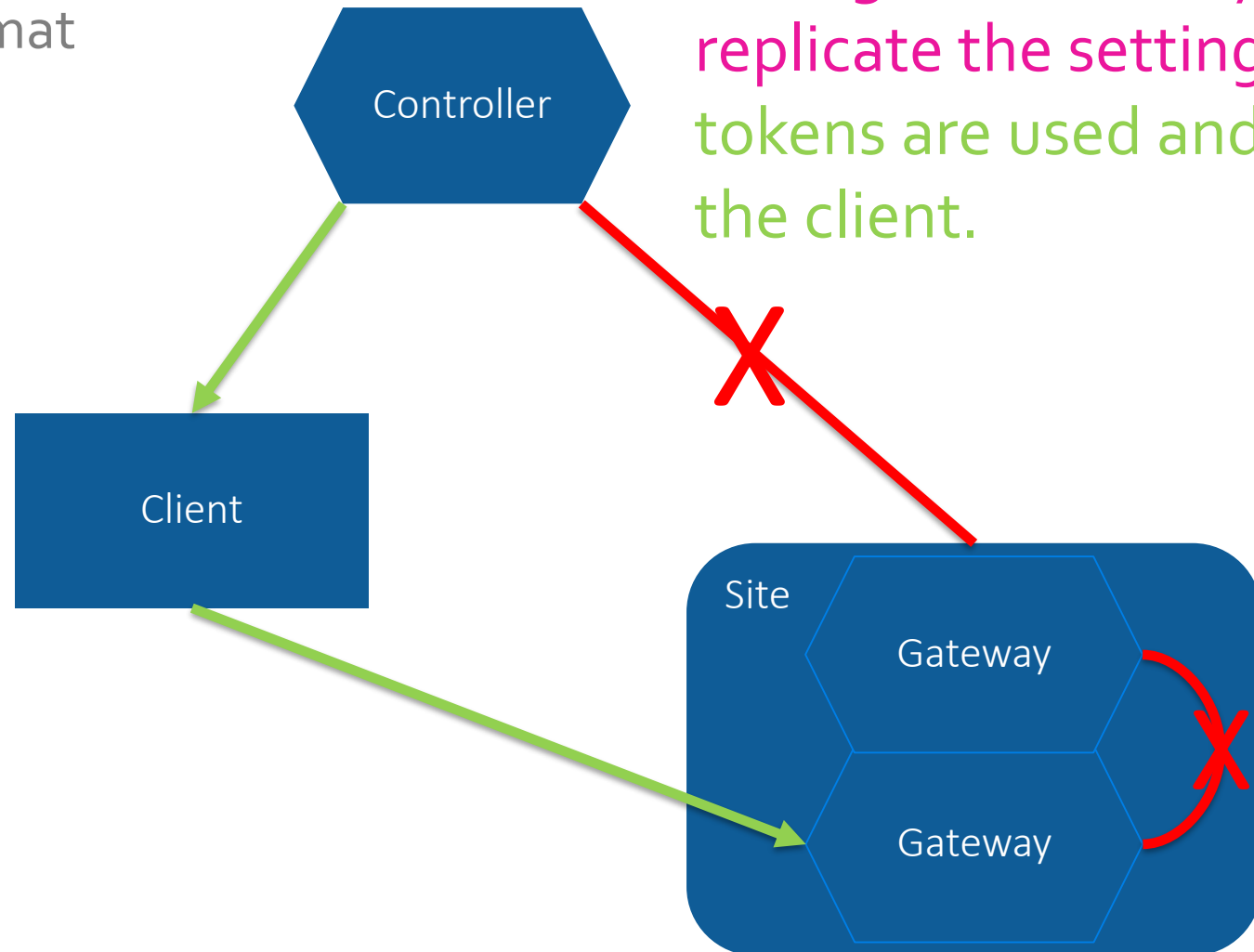
- The Client is responsible for acquiring the necessary Claims and Entitlement tokens from the Controller and for pushing them to the Gateway.
- The Gateway uses the tokens for each user to configure firewall rules and control access on a per-user basis.

The CA cert can be renewed – a new license is required!

- Required when built in one expires.
- Replacing CA cert for security reasons

Tokens


- The control flow uses “Tokens”
 - JSON Web Token format
- Two Tokens:
 - Claims
 - Entitlements
- One x509 cert:
 - VPN Certificate





Instead of the Controller 'writing' to the Site and having the Gateways replicate the settings, tokens are used and sent via the client.


Managing tokens using *User and Devices*


- AppGate adapts to changes in the environment automatically. To push any changes made within the AppGate itself.....
- Use the Users and Devices console to renew Users' or all tokens


AppGateSDP


Dashboard


Operations

System

Scripts

Users & Devices

Settings




Active Devices

Blacklisted Users


Licensed Users


On-boarded Devices

Audit Logs 

Active Devices (24H)

Total Active Devices (24H) 2

Renew All

Blacklist User

Username	Identity Provider	Hostname	Device Id	Last Token ↓
zahir	local	CYXSELP0001	820aac81-6b61-4b4c-80a4-bd8b19c48278	6/1/2018, 1:13:46 PM
admin	local		2f19de9e-5a17-4b69-97b6-130041d21a44	6/1/2018, 12:15:07 PM

Data flow in AppGate

AppGateSDP
Access, evolved.

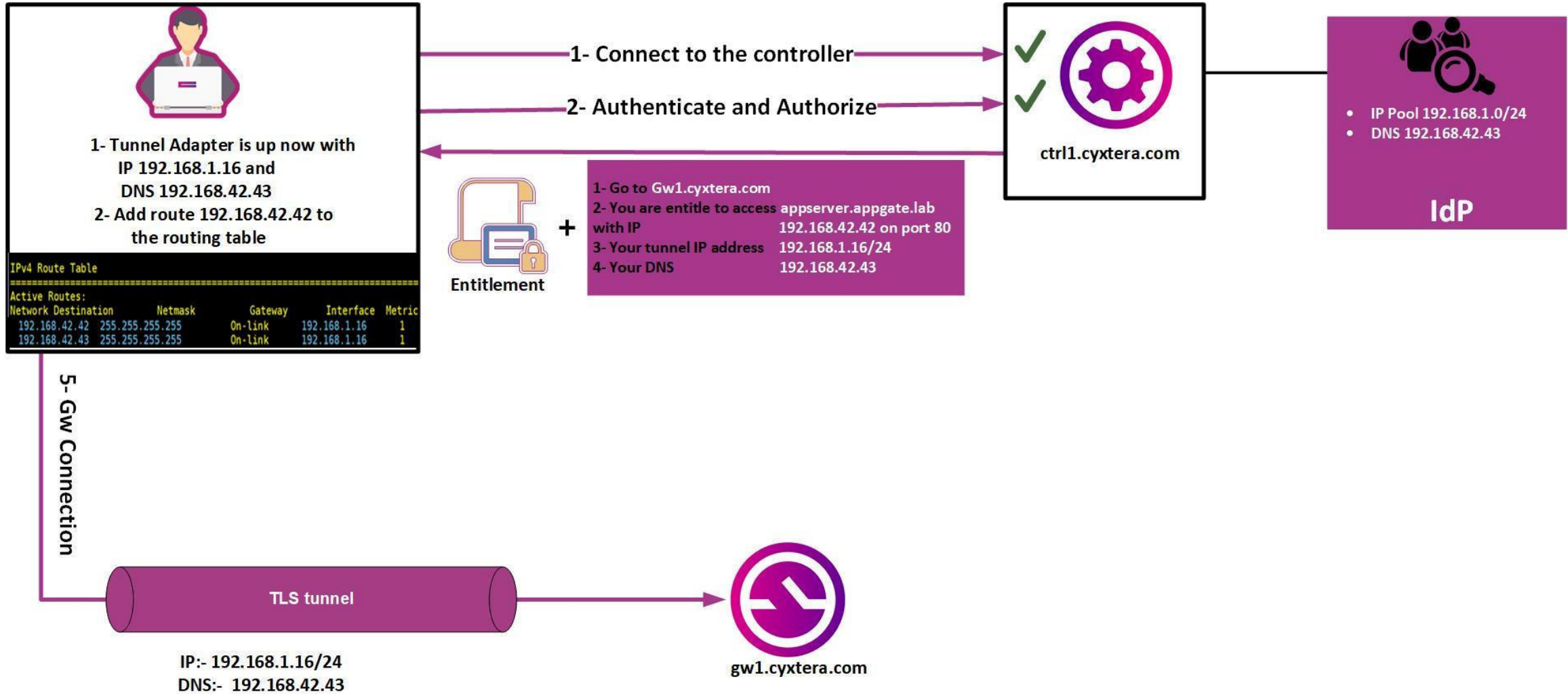
IP pool management

- Every device is allocated its own IP address from the pool – same user connecting from two devices will consume 2 IP's
- If multiple Identity Providers are configured, every time a user connects using a different IdP, another unique IP address will be consumed
- The IP address will remain reserved until the lease time (30 days default) has expired – lease time can be set per pool
- IP Pools console – stats on *currently used* and *reserved* IP's
- Health check warning when any pool's *currently used* and *reserved* IPs reach 90% of the Total size

Host routing and IP Pools

- Client creates a **tun** device: a virtual NIC
- Controller registers an IP (tun-ip) from the IP Pool and assigns it to the client after authorization
- tun-ip is given to the tun device on client
- Host routes are added (based on Entitlements and/or Sites)
- Applications resolve hosts using DNS
- The packets in the tunnel are sent from the tun-ip

Host routing and IP Pools cont'd



SNAT

No SNAT

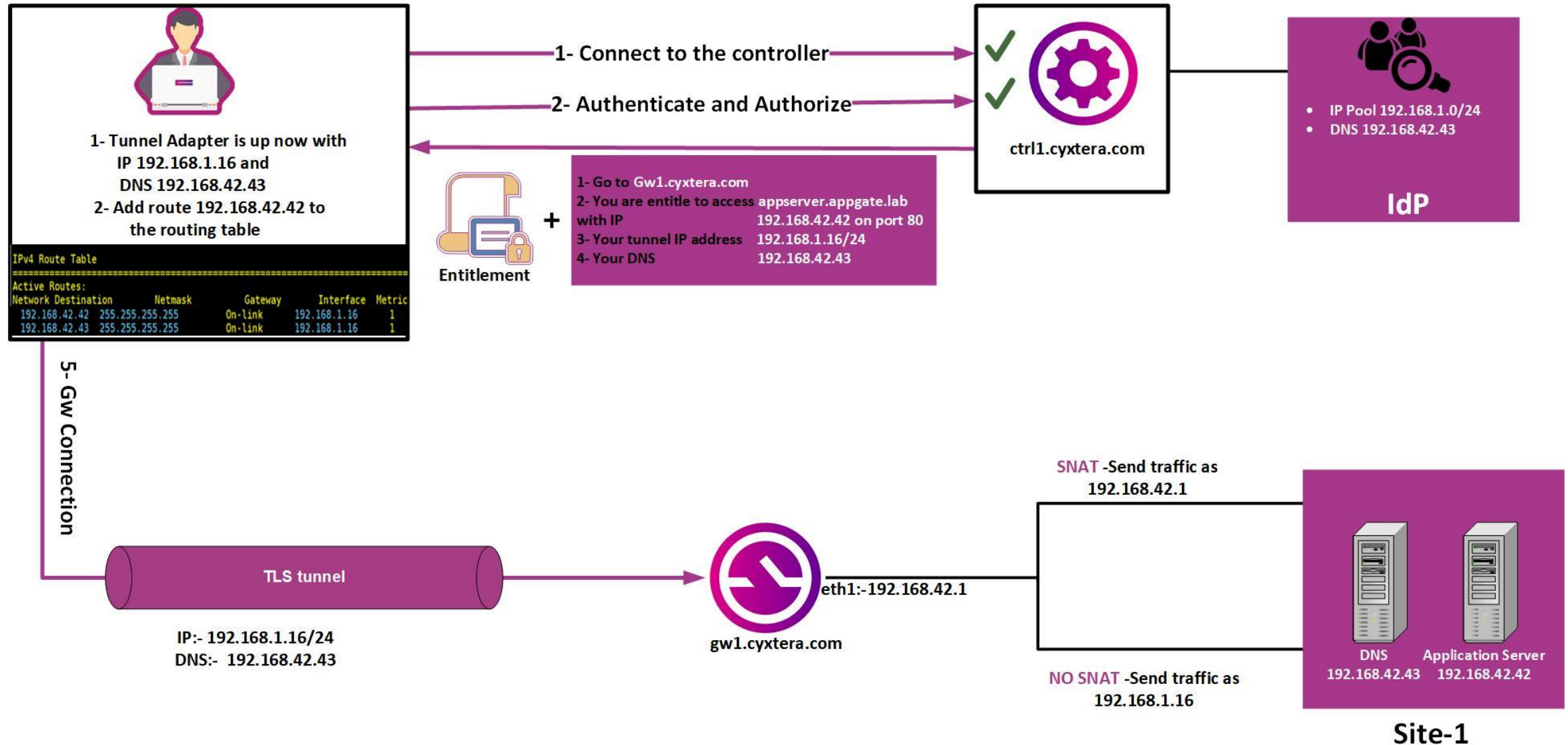
This is the Question



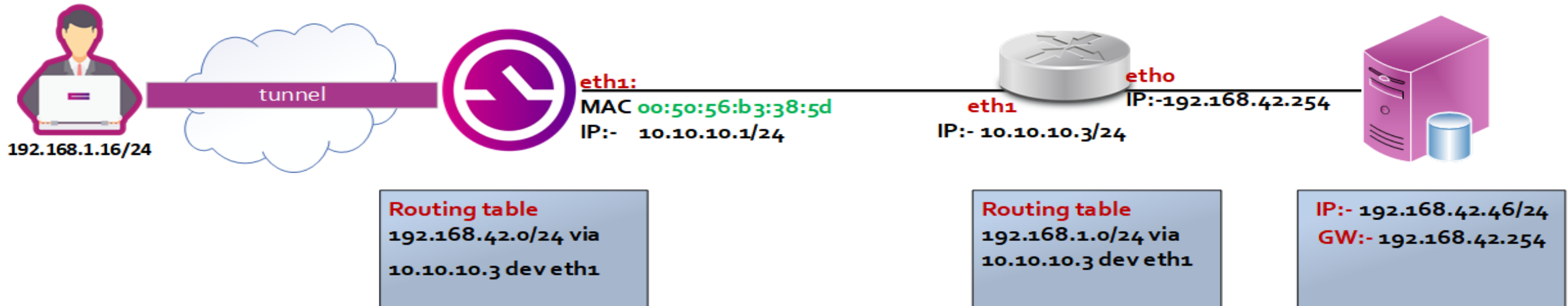
Firewalling and Source NAT

- VPN traffic hits the gateway and is firewallled on a per-user basis.
- When the traffic is forwarded over the network there are two options:
 1. Gateway sends the packet to the network as-is
 - Routers needs to be configured to forward tun-ip range
 - Endpoints receive and send to the individual tun-ips
 2. Gateway does a Source-NAT (replaces the tun-ip with the Gateway-ip)
 - No need for router configuration in the network
 - Endpoints receive and send to the Gateway IP

Firewalling and Source NAT cont'd



No-SNAT (ARP Proxy)



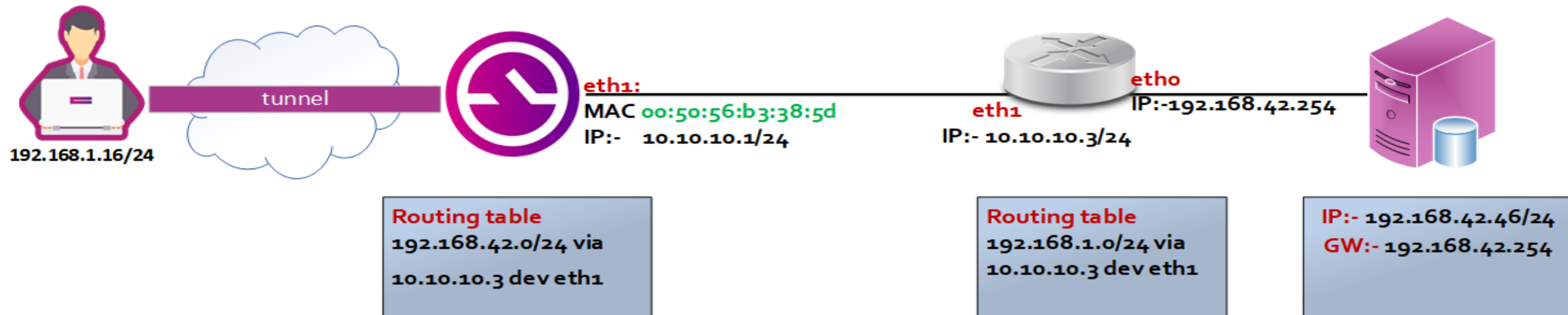
```
Broadcast ARP Who has 192.168.1.16? Tell 10.10.10.3 Router ARP request
Vmware_b3:40:8d ARP 192.168.1.16 is at 00:50:56:b3:38:5d AppGate GW ARP answer

> Frame 18: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: Vmware_b3:38:5d (00:50:56:b3:38:5d), Dst: Vmware_b3:40:8d (00:50:56:b3:40:8d)
✓ Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: Vmware_b3:38:5d (00:50:56:b3:38:5d)
  Sender IP address: 192.168.1.16
  Target MAC address: Vmware_b3:40:8d (00:50:56:b3:40:8d)
  Target IP address: 10.10.10.3
```

No SNAT

- Good: Great auditing
- Good: Track packets over the internal network
- Good: Can separate tenant traffic by IP
- Good: Allows stateful Failover
- Bad: Requires network configuration on the infrastructure
 - Return routes need defining.
- Bad: limited use in Cloud deployments

SNAT



Broadcast	ARP	Who has 10.10.10.1? Tell 10.10.10.3	Router ARP request
Vmware_b3:40:8d	ARP	10.10.10.1 is at 00:50:56:b3:38:5d	AppGate GW ARP answer

```
> Frame 4: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: Vmware_b3:38:5d (00:50:56:b3:38:5d), Dst: Vmware_b3:40:8d (00:50:56:b3:40:8d)
✓ Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: Vmware_b3:38:5d (00:50:56:b3:38:5d)
  Sender IP address: 10.10.10.1
  Target MAC address: Vmware_b3:40:8d (00:50:56:b3:40:8d)
  Target IP address: 10.10.10.3
```

SNAT

- Good: Requires NO network configuration on the infrastructure
- Good: Most compatible, works everywhere
- Good: Ideal for Cloud
- IP pool changes have no impact
- Bad: Packets lost the original source IP
- Bad: No full state-full failover is possible

What you have learnt

- SPA – what it is and how to ensure users can connect
- Hostnaming & DNS - Because SDP is a distributed system care needs to be taken when setting up networking
- Tokens – are the backbone of AppGate's control system and allow all the elements in the system to work independently of one another
- Data packet flow – How to connect with applications/servers on (multiple) protected sites

Lab 5 &6

AppGateSDP
Access, evolved.

Cyxtera proprietary