Operating and Maintaining Physical and Logical Cloud Security

Part 2 - Services

Dr. Lyron H. Andrews

CISSP/CCSP/SSCP/CRISC/CISM/CCSK

https://www.profabula.com/whyprofabula

Overview

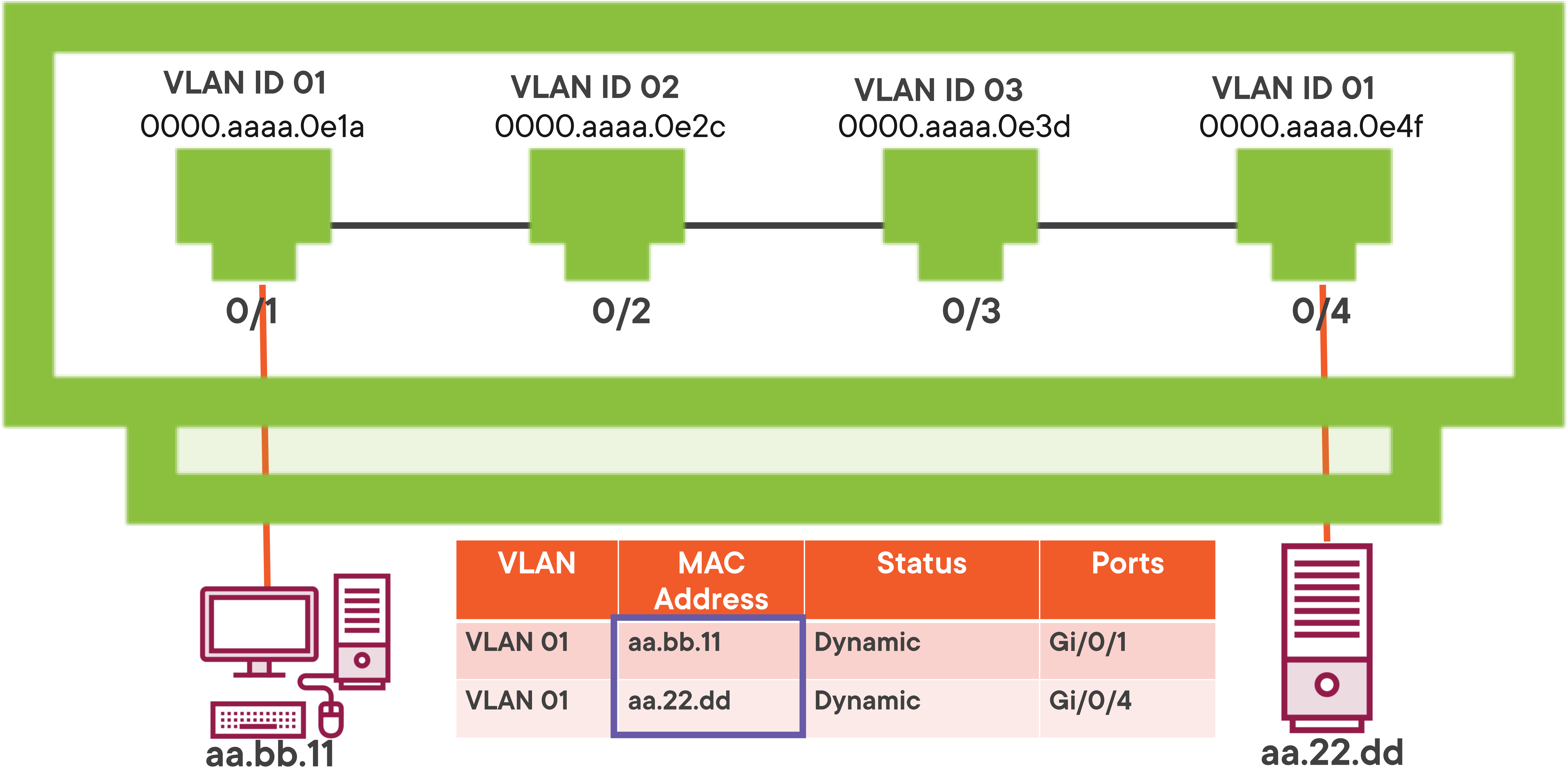
Enumerate the major systems that provide physical and logical security

Review the configuration options of the systems

Demonstrate use-cases for system consumption

VXLAN

MAC Table Physical to Logical Mapping

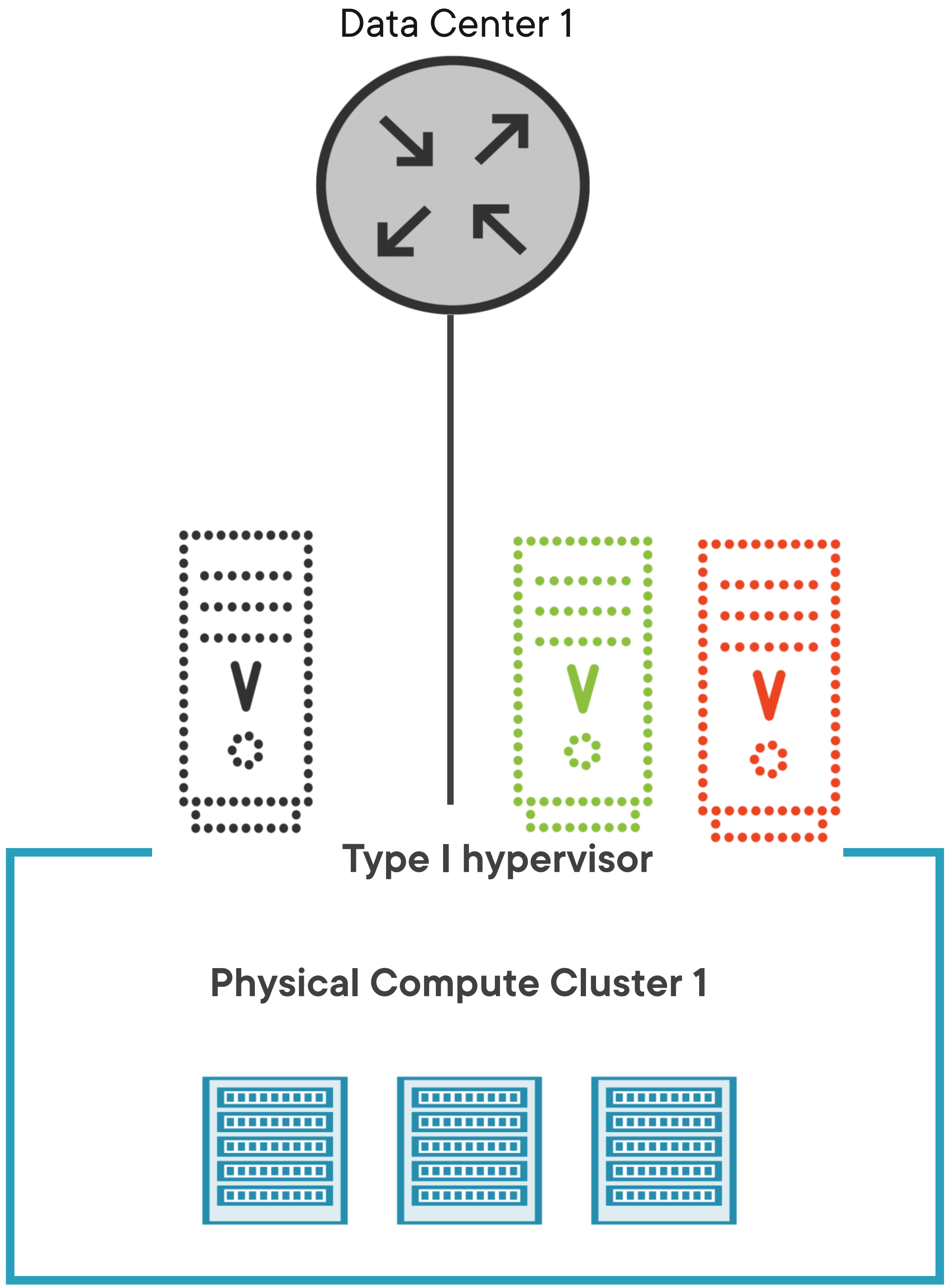


VLAN	MAC Address	Status	Ports
VLAN 01	aa.bb.11	Dynamic	Gi/0/1
VLAN 01	aa.22.dd	Dynamic	Gi/0/4

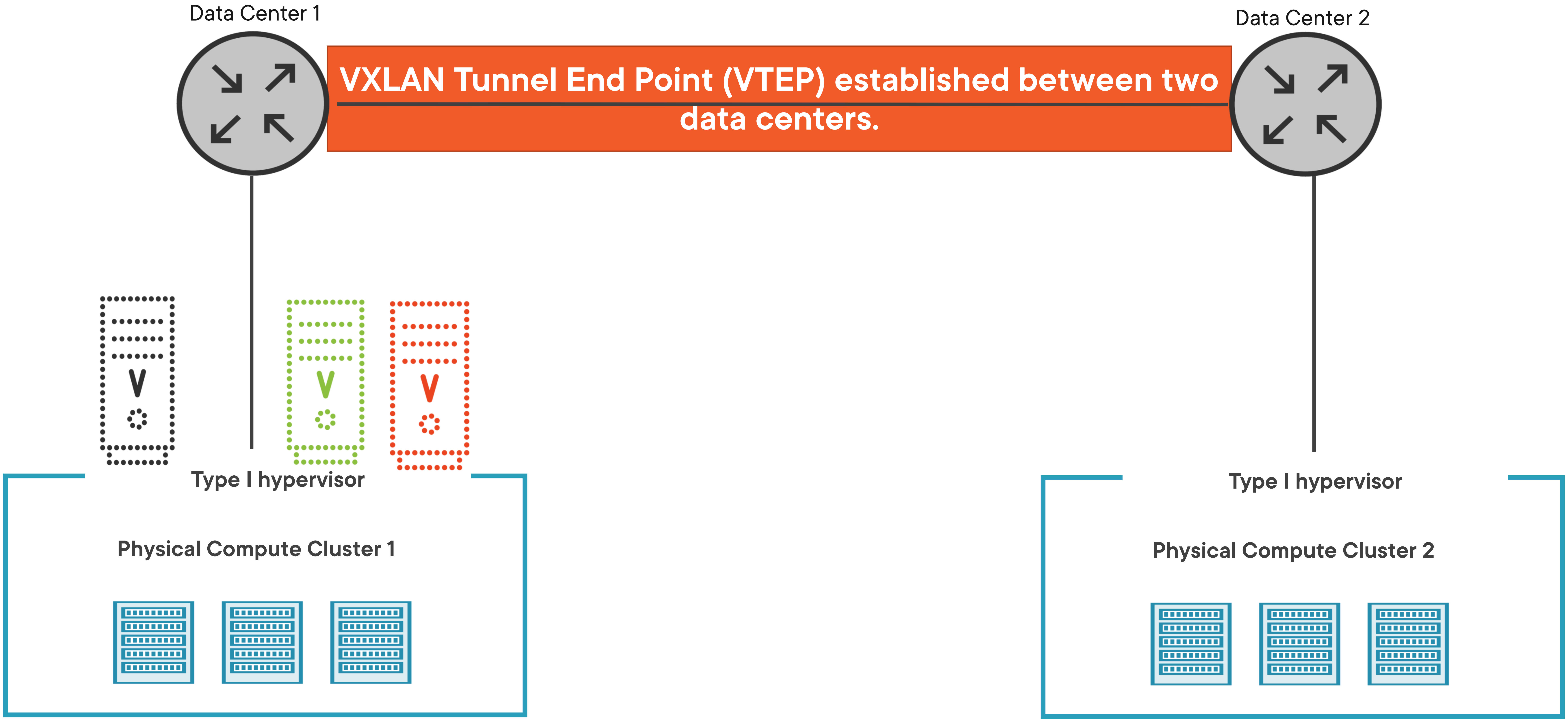
VXLANs have different network size and functions from VLANs

VLANs can create 4096 LANs in an administrative domain.
VXLAN can create 16 million.
VXLANs communicate with VTEP.

VXLAN Use Case



VXLAN Use Case



Data Center 1

Data Center 2

VXLAN Tunnel End Point (VTEP) established between two data centers.

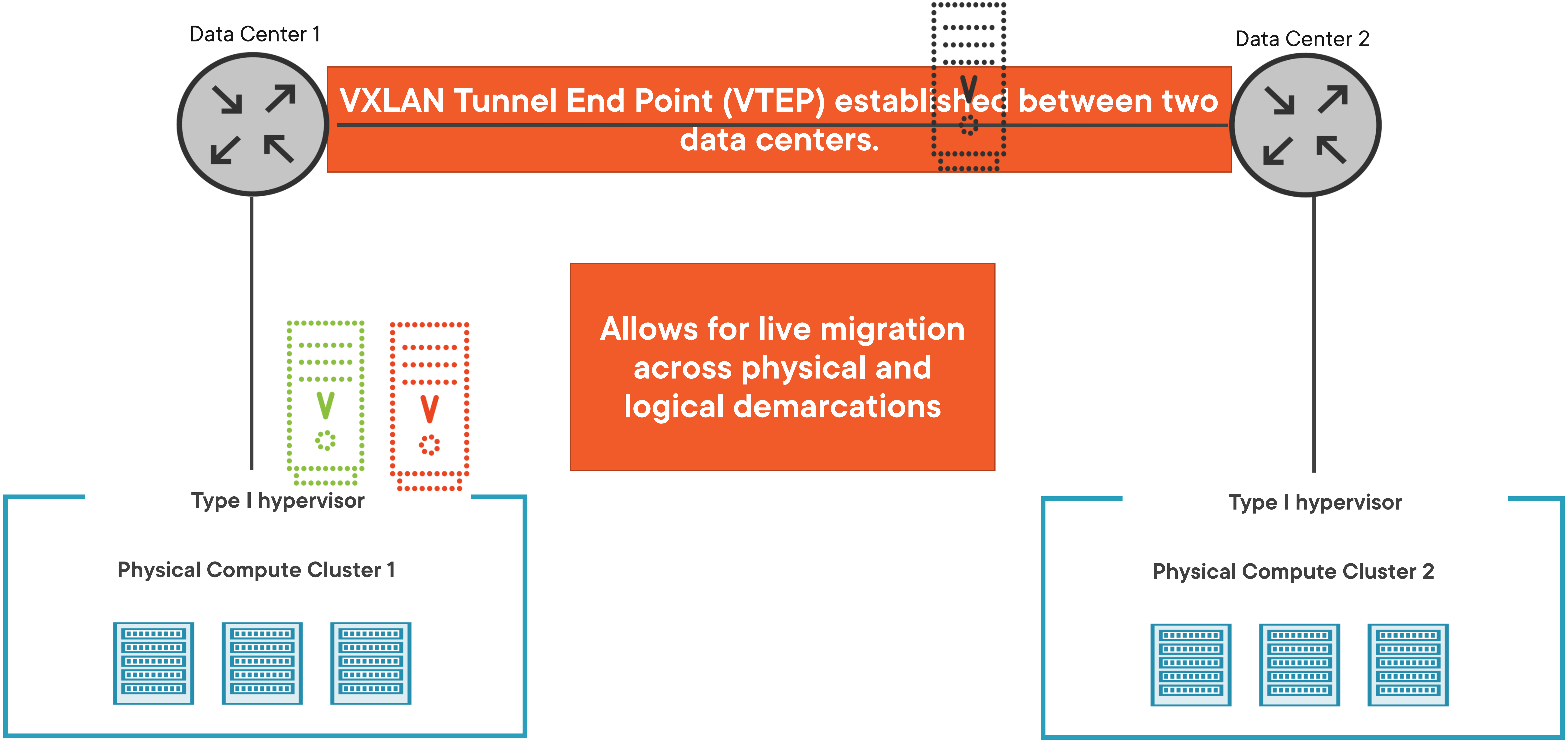
Type I hypervisor

Physical Compute Cluster 1

Type I hypervisor

Physical Compute Cluster 2

VXLAN Use Case



VXLAN Tunnel End Point (VTEP) established between two data centers.

Allows for live migration across physical and logical demarcations

DHCP and Security Issues

DHCP Specifications

- Client/Server Protocol
- IP, subnet mask, gateway
- Pools of pre-allocated address
- Port 67/68

DHCP Options

DNS settings

Domain name

NTP servers

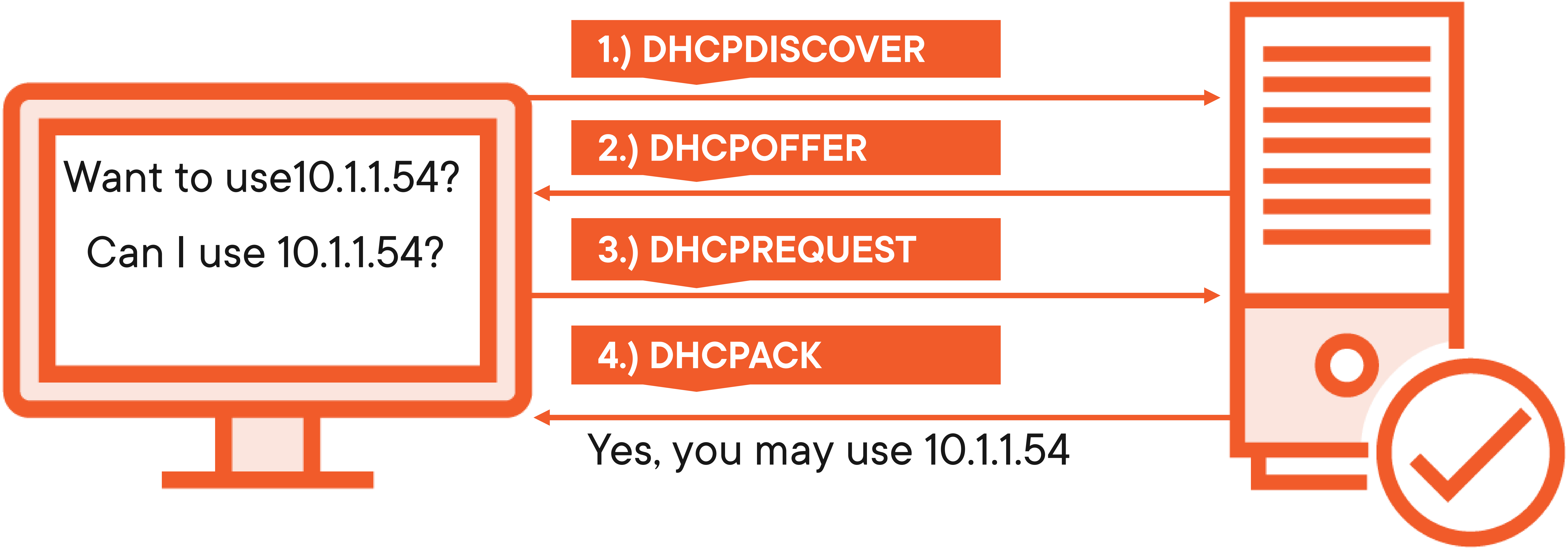
Rouge DHCP systems

No native encryption of traffic

Interception or manipulation

DHCP Security Issues

DHCP Process



1.) DHCPDISCOVER

2.) DHCPOFFER

3.) DHCPREQUEST

4.) DHCPACK

Want to use10.1.1.54?

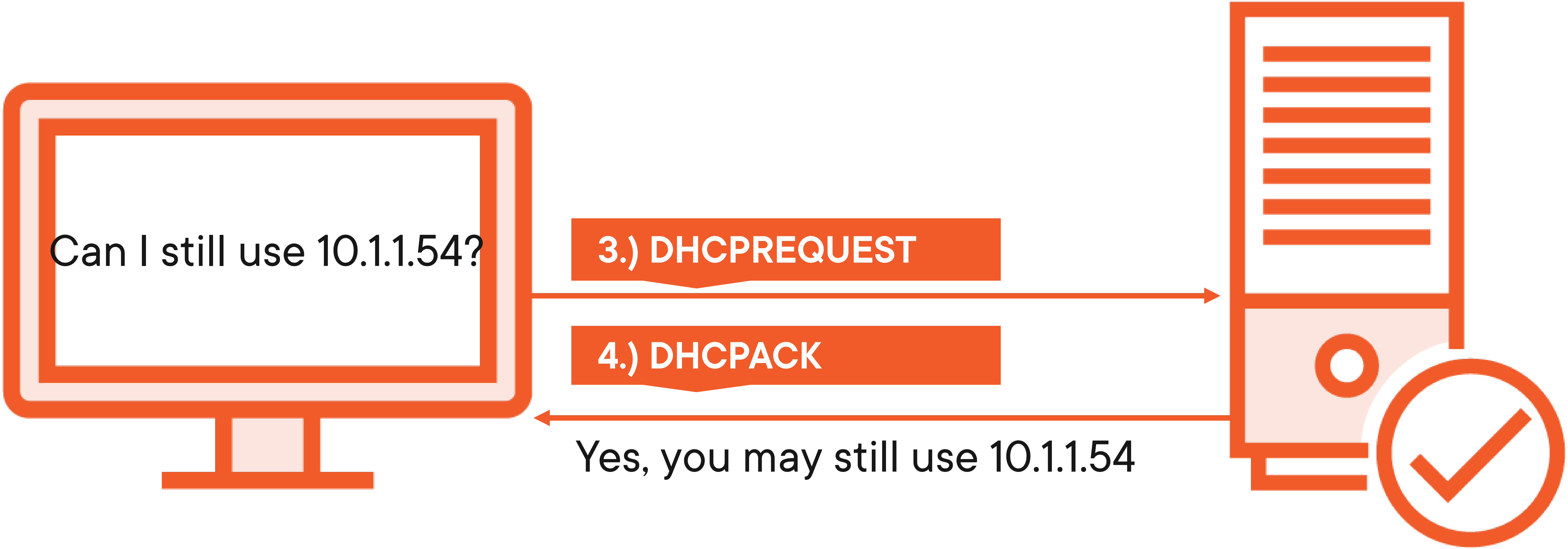
Can I use 10.1.1.54?

Yes, you may use 10.1.1.54

DHCP Client

DHCP Server

DHCP Process Halfway Through Lease



Can I still use 10.1.1.54?

3.) DHCPREQUEST

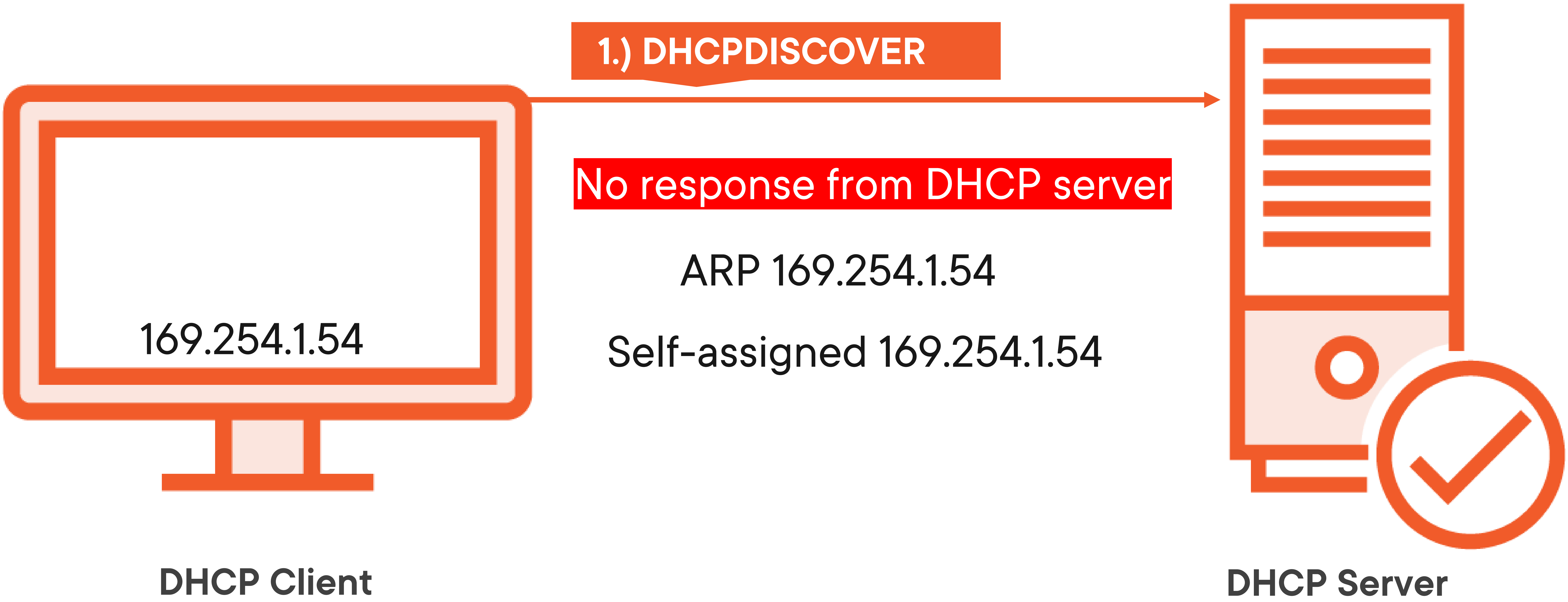
4.) DHCPACK

Yes, you may still use 10.1.1.54

DHCP Client

DHCP Server

Automatic Private IP Address



1.) DHCPDISCOVER

No response from DHCP server

ARP 169.254.1.54

Self-assigned 169.254.1.54

DNS and Security Issues

DNS Specifications

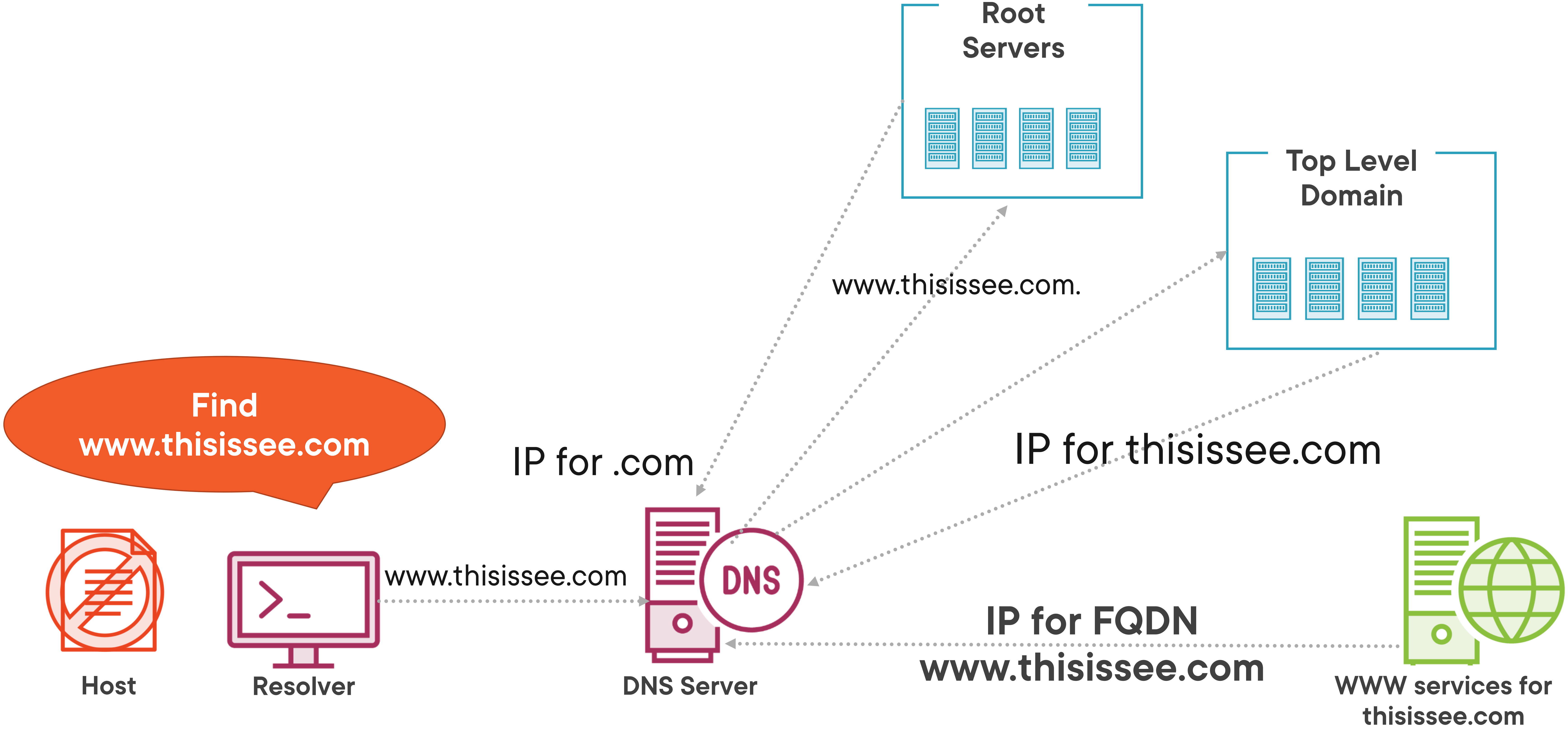
Resolves FQDN to IP

Client known as resolver

Root servers resolve external

Additional extensions

DNS Lookup Process



Essential DNS Records

Host

Start of authority

Name server

Pointer

Mail exchange

DNS Security Issues

- Lacking integrity/confidentiality
- DNS shadowing
- Amplification/reflection
- Traffic interception and surveillance

Securing DNS

DNSSEC

DMARC/SPF/DKIM

DNS over HTTPS (DoH)

Log review

Password process

MFA only

DNSSEC Records

RRSIG

Cryptographic signature

DNSKEY

Public signing key

DS

Hash of DNSKEY

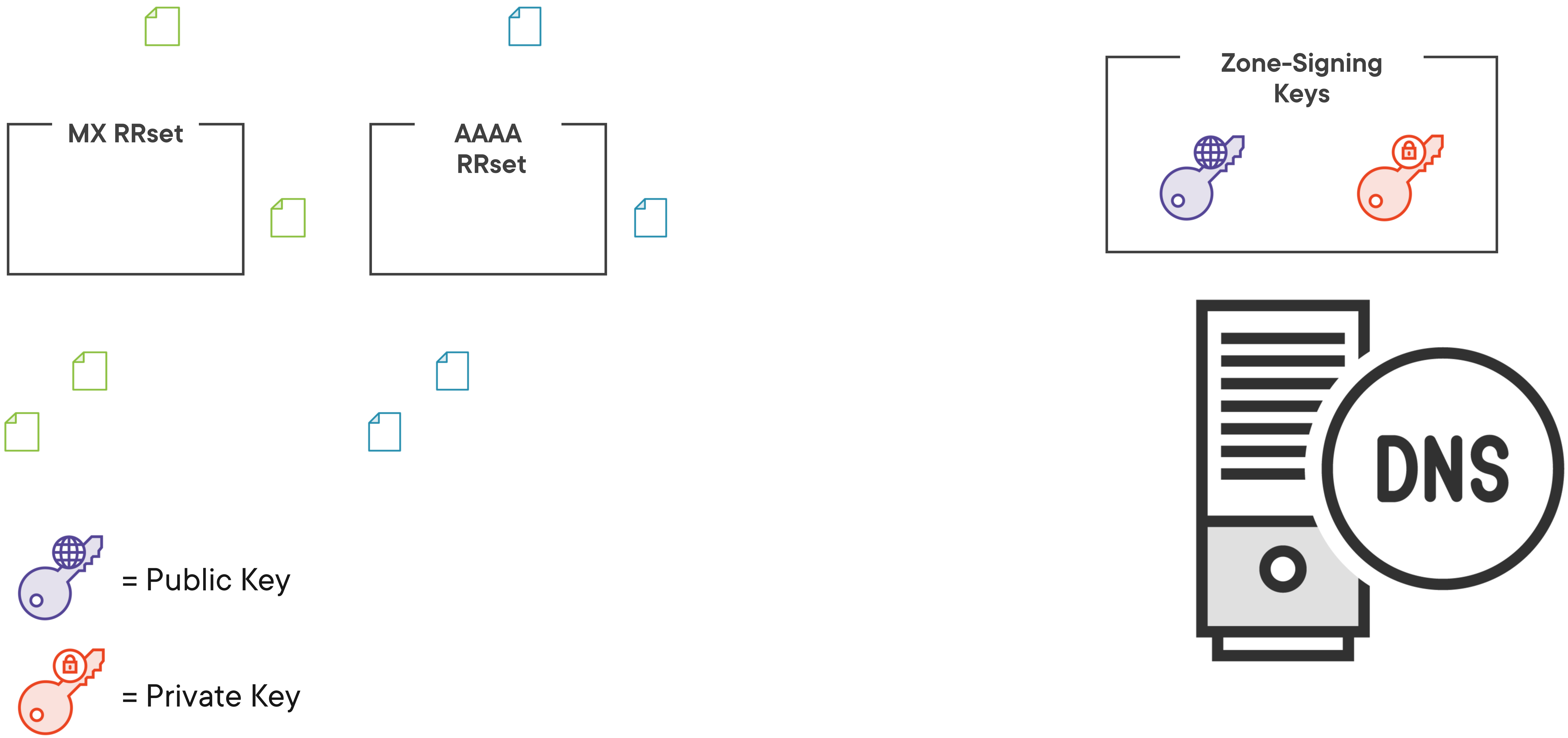
NSEC and NSEC3

Denial-of-existence

CDNSKEY and CDS

Child to parent zone update request

DNSSEC Process



MX RRset

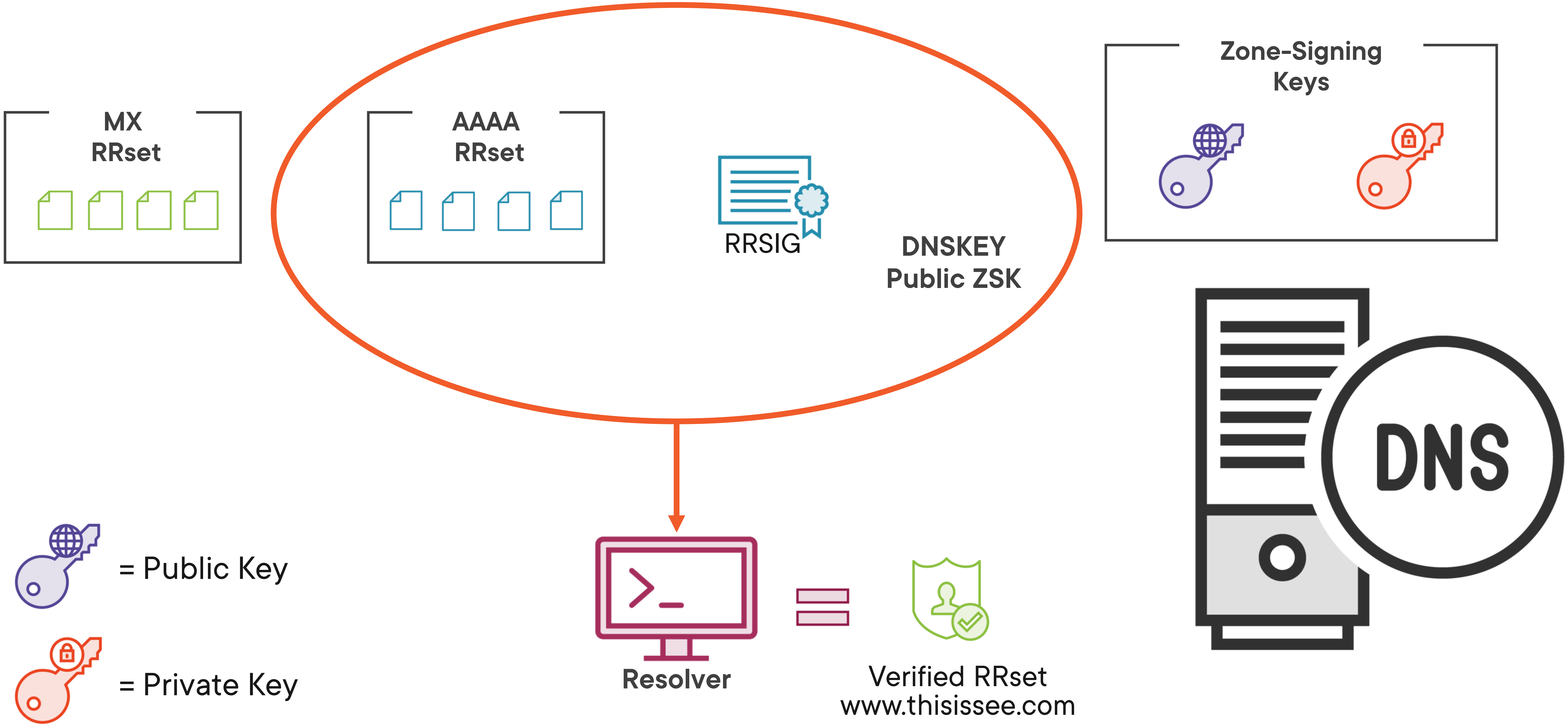
AAAA RRset

Zone-Signing Keys

= Public Key

= Private Key

DNSSEC Process



MX
RRset

AAAA
RRset

RRSIG

DNSKEY
Public ZSK

Zone-Signing
Keys

= Public Key

= Private Key

Resolver

Verified RRset
www.thisissee.com

Internet Protocol Security (IPsec) VPN

Planning and establishment of ZTA reduce or eliminate the need for VPNs.

IPSEC Main Components

Authentication Header (AH)

Proves identity of source IP

Encapsulating Security Payload (ESP)

Encrypts IP packets and ensures integrity

Encapsulating Security Payload (ESP)

ESP header

ESP payload

ESP trailer

Authentication

IPSEC Main Components

Authentication Header (AH)

Proves identity of source IP

Encapsulating Security Payload (ESP)

Encrypts IP packets and ensures integrity

Security Association (SA)

Endpoint communications

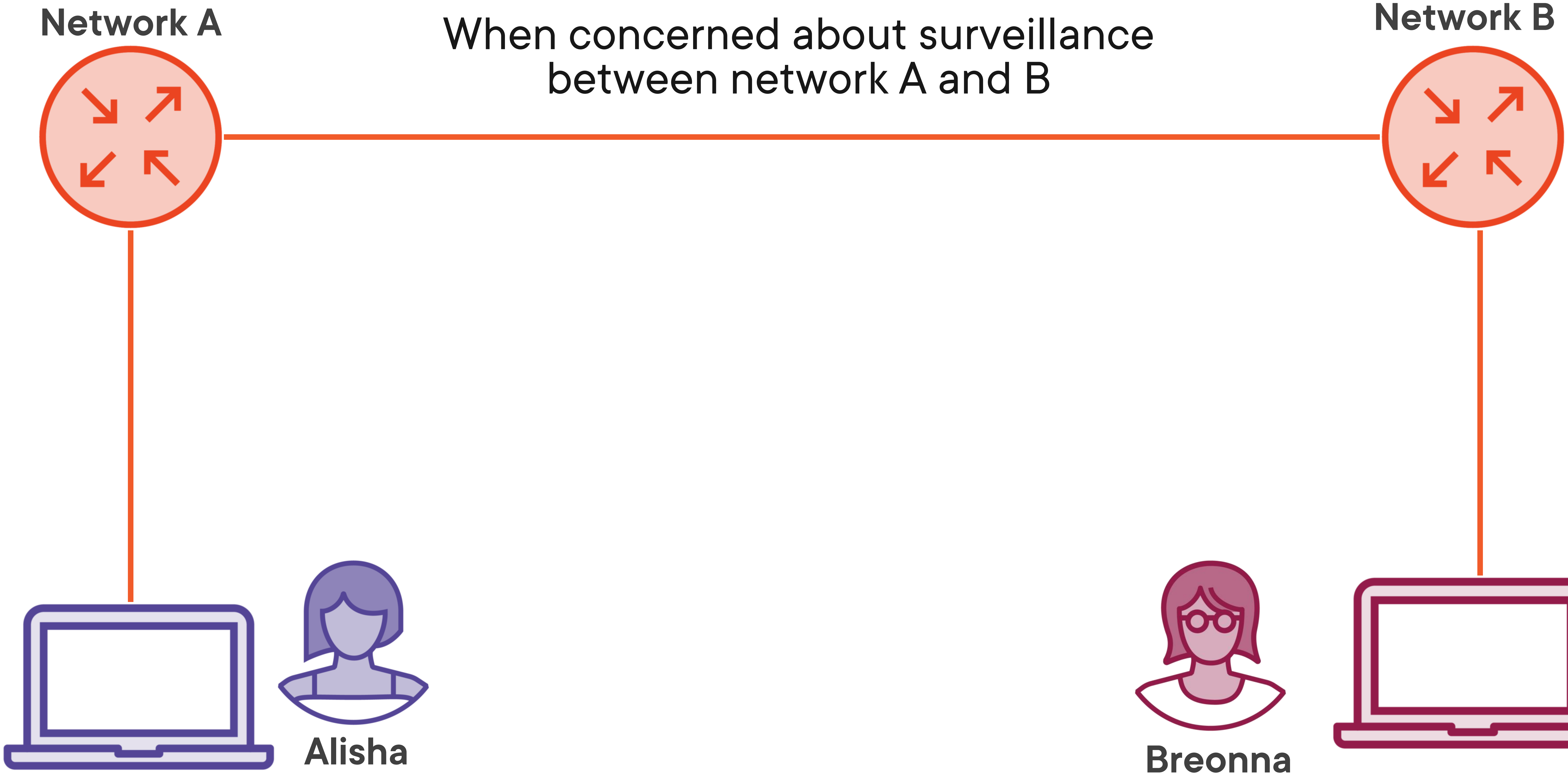
Internet Key Exchange (IKE)

Enables exchange of cryptographic information

Transport and Tunnel Mode

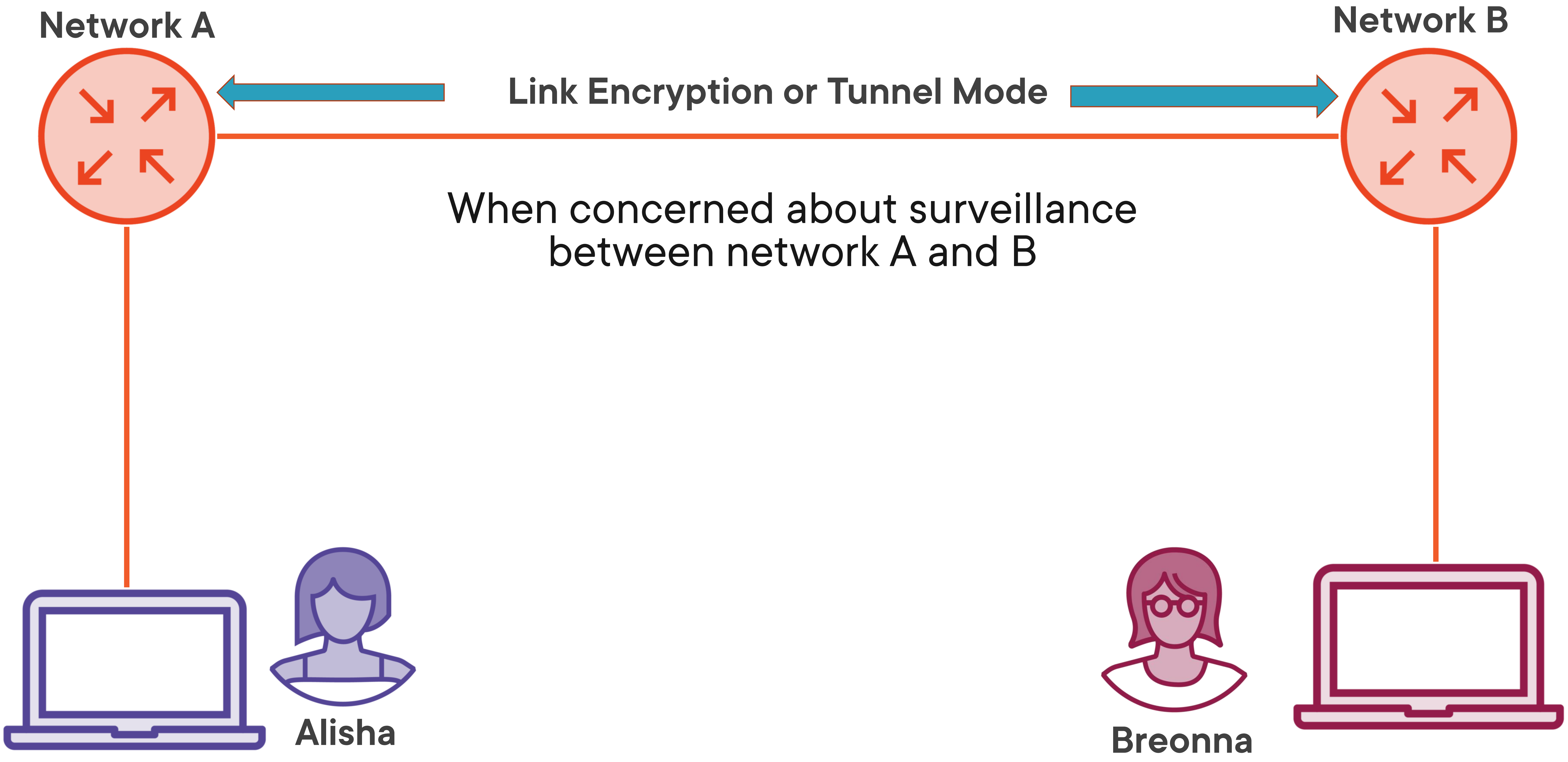
End-to-end or link encryption

IPSEC Transport and Tunnel Mode



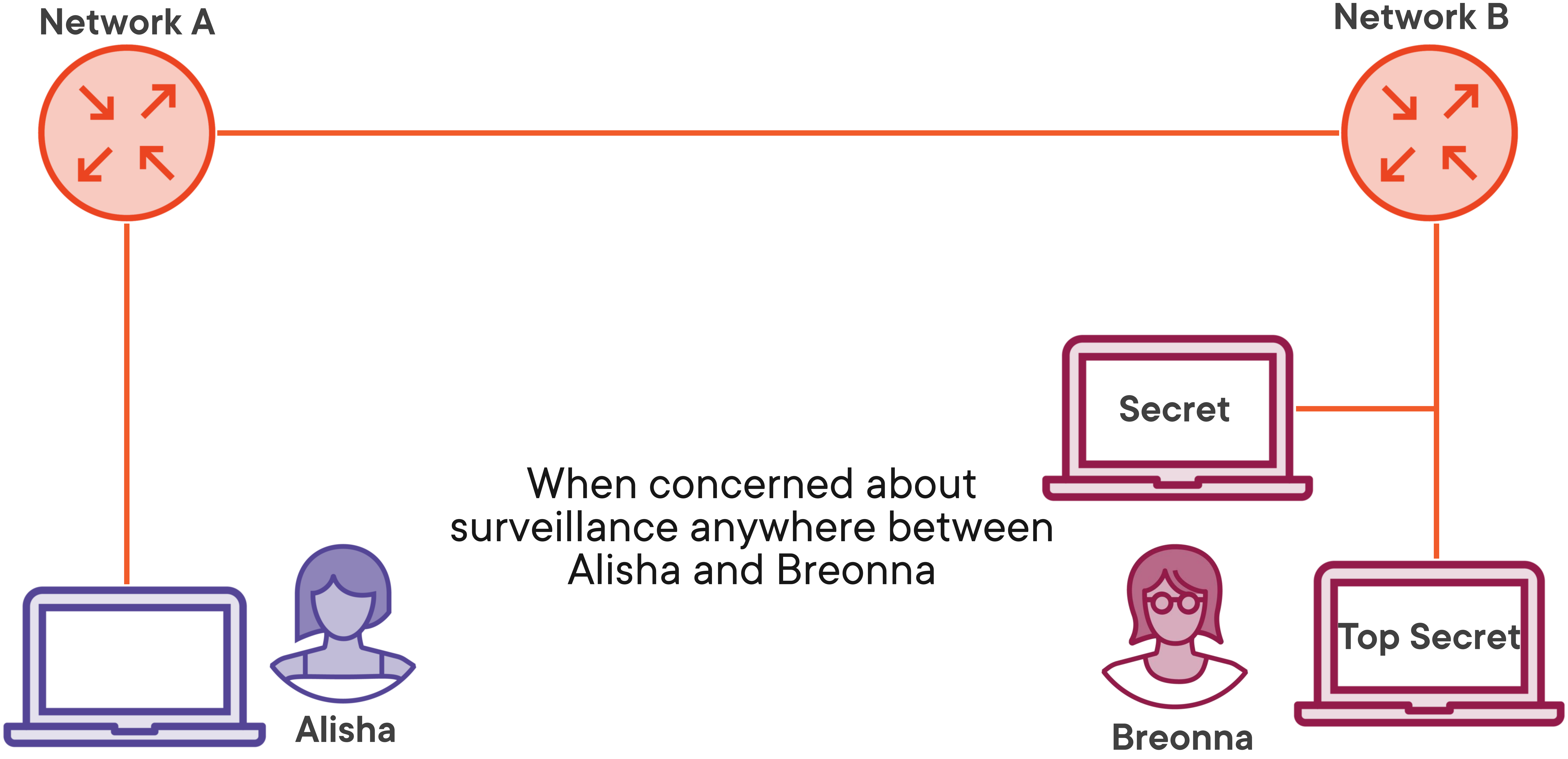
When concerned about surveillance between network A and B

IPSEC Transport and Tunnel Mode



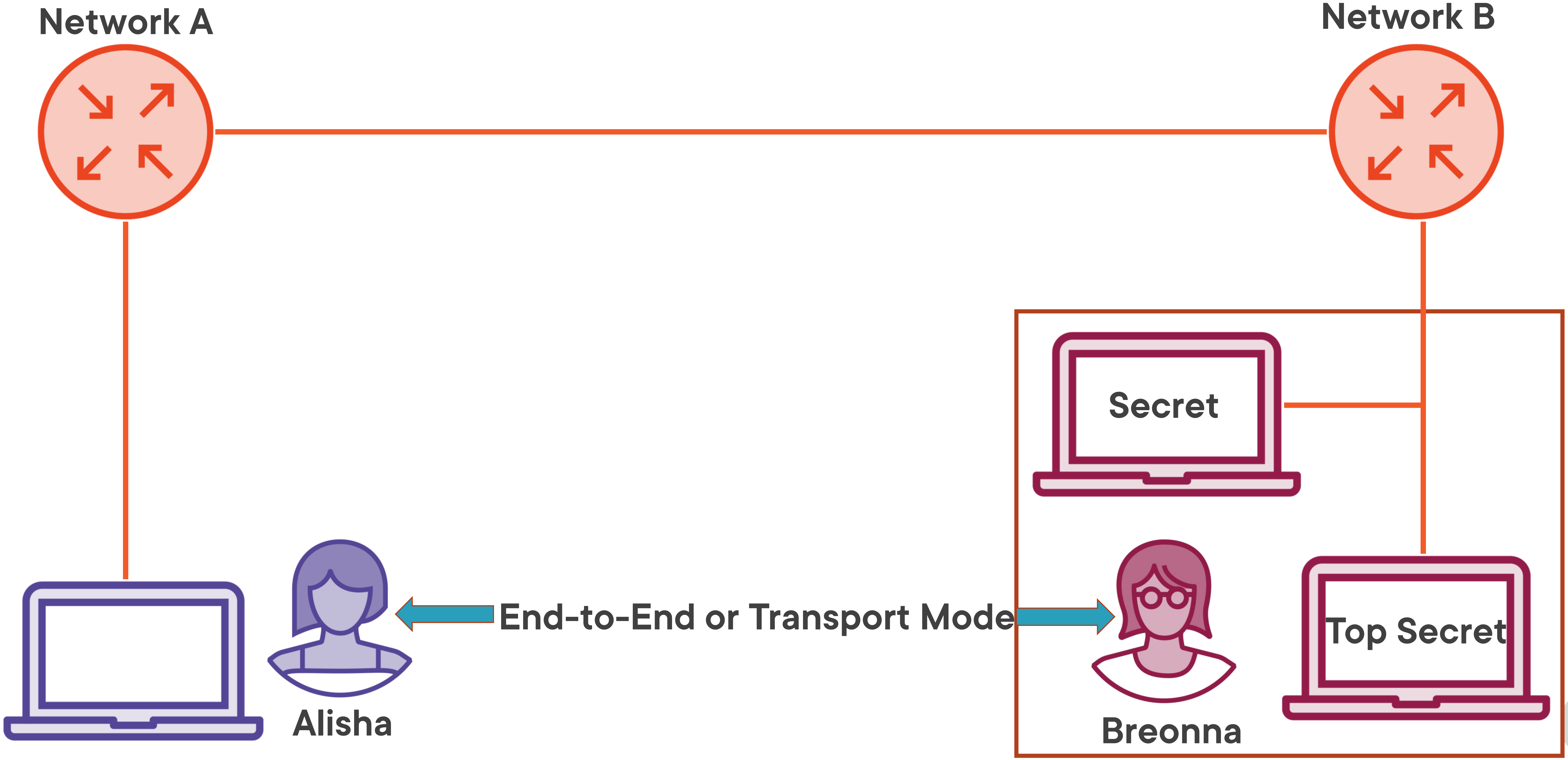
When concerned about surveillance between network A and B

IPSEC Transport and Tunnel Mode



When concerned about surveillance anywhere between Alisha and Breonna

IPSEC Transport and Tunnel Mode



Transport Layer Security (TLS) VPN

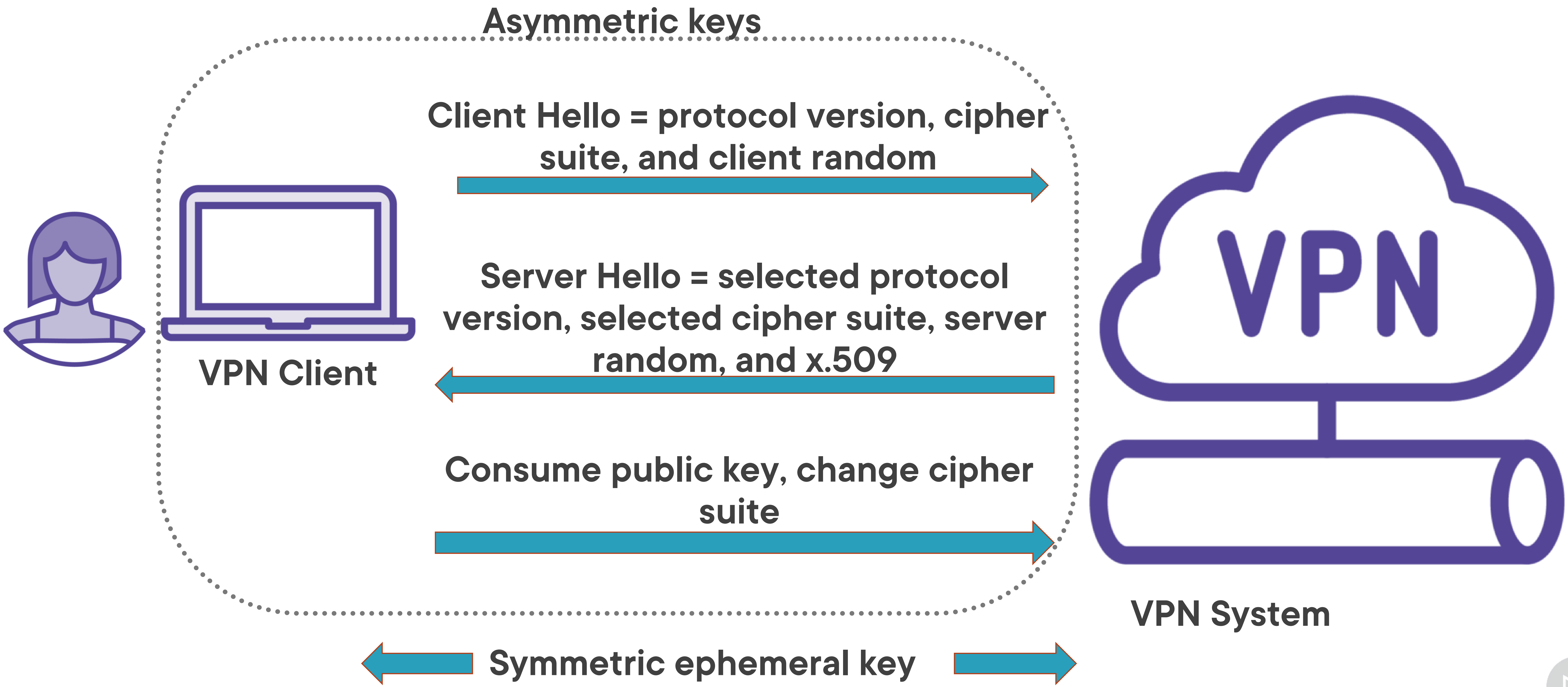
Started as SSL 2.0

TLS 1.0 and SSL 3.0

TLS 1.1, 1.2, and 1.3

History of SSL/TLS

Transport Layer Security (TLS 1.2)



Asymmetric keys

Client Hello = protocol version, cipher suite, and client random

Server Hello = selected protocol version, selected cipher suite, server random, and x.509

Consume public key, change cipher suite

VPN Client

VPN System

Symmetric ephemeral key

Legacy symmetric encryption reduced

AEAD included

Cipher suite modification

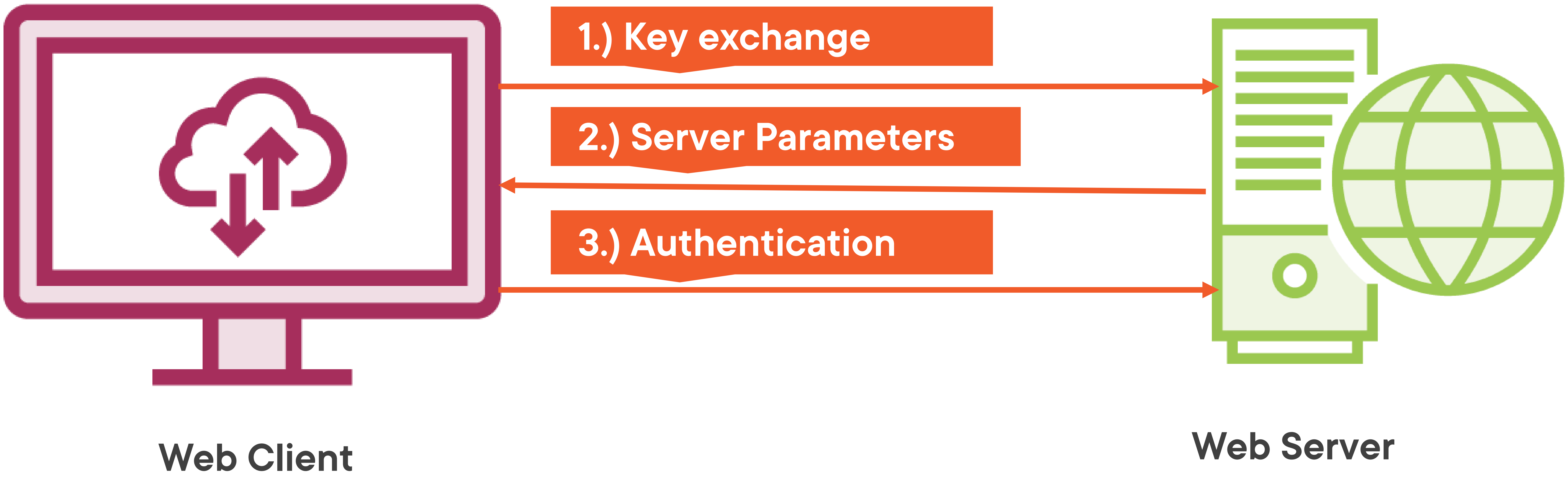
0-RTT added

Static Asymmetric removed

ECC added

Transport Layer Security 1.3 (TLS)

TLS 1.3 Handshake Process



1.) Key exchange

2.) Server Parameters

3.) Authentication

Web Client

Web Server

VM OS Vulnerability Monitoring and Hardening

Demo

We will use AWS Inspector as a vulnerability assessment tool

We will log in to the AWS console and connect to an existing instance

- We will have vulnerabilities that haven’t been addressed to see the detection process
- We will create a target assessment for the virtual network review vulnerabilities then run an update to address

Demo

We will take a snapshot of an image to exemplify a baseline in AWS

First login to the management console and go to EC2

- All snapshot services can be used for forensics and restores
- Select the VM with image we need and choose snapshot.

Maintain Cloud Infrastructure as Code (IaC)

Demo

We will use AWS CloudFormation to examine and execute a template to create a Stack

We will log in to the AWS console and import the template

- We will review the template settings
- We will execute the IaC template

Summary

What systems in the physical and logical infrastructure are at most risk for you?

How are you mitigating the risks you are responsible for in the shared responsibility model?

Where are your areas of control in the share responsibility model?

Up Next:

Implementing Administrative Operational Controls