
cisco Live!
Let's go

The bridge to possible

Secure Access with ISE in the Cloud

Eugene Korneychuk, Technical Leader

BRKSEC-2039

cisco Live!

#CiscoLive

About Eugene Korneychuk

- Security TAC Technical Leadership Team
- 15+ years of security and networking experience
- 20+ published documents
- On personal note:
  - Family time
  - Travel
  - Football
- Lives in Cary, North Carolina, US

Session Objective

The Goal of this session is to:

- Make you familiar with ISE Cloud deployments and designs
- Cover ISE automation techniques
- Explain the SAML Authentication functionality and its implementation on ISE
- Walk you through ROPC authentication with ISE and Azure Active Directory

Agenda

- ISE Architecture Concepts
- ISE in the Cloud
- ISE in AWS and Azure
- Migration and Upgrade
- AWS Partner Solution
- ISE SAML SSO
- ISE Azure Active Directory Authentication
- Conclusion

ISE Architecture Concepts

ISE Design Concepts

Policy Administration Node (PAN)
- Single plane of glass for ISE admin
- Owns ISE database and replicates it to other nodes

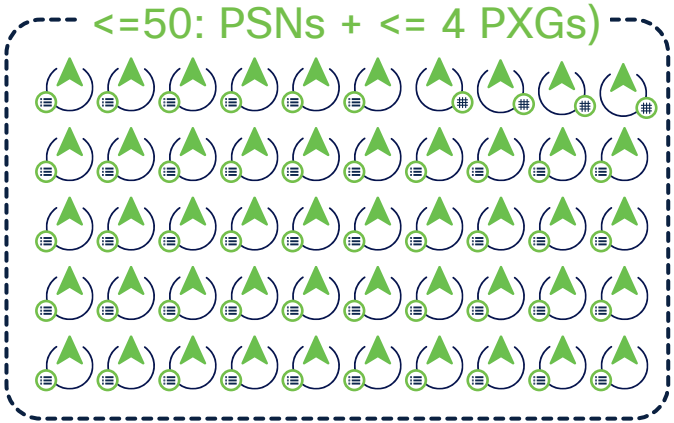
Monitoring & Troubleshooting Node (MnT)
- Reporting and logging node
- Collects health and log information from other nodes

Policy Services Node (PSN)
- Makes policy decisions
- RADIUS / TACACS+ Servers

pxGrid Controller
- Facilitates sharing of context

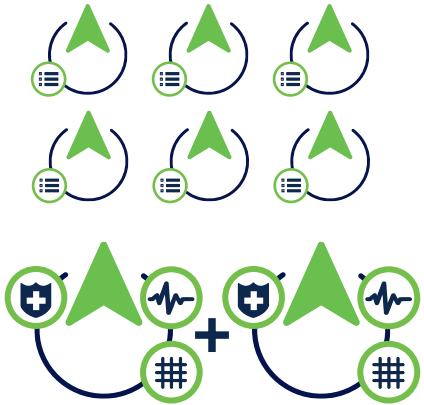
ISE Scaling

Lab and Evaluation



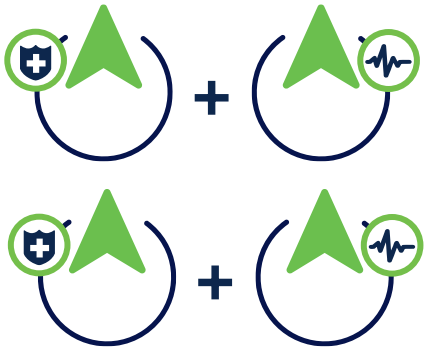
Small HA Deployment

2 x (PAN+MNT+PSN)+ Extra PSN



Medium Multi-node Deployment

2 x (PAN+MNT+PXG), <= 6 PSN



Large Deployment

2 PAN, 2 MNT, <=50: PSNs + <= 4 PXGs

PSN Maximum Concurrent Active Sessions

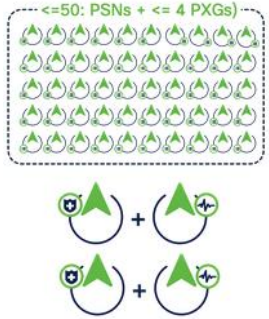
Cisco ISE

PSN Type	SNS 3615	SNS 3715	SNS 3595	SNS 3655	SNS 3755	SNS 3695	SNS 3795
Concurrent active endpoints supported by a dedicated PSN (ISE node has only PSN persona)	25,000	50,000	40,000	50,000	100,000	100,000	100,000
Concurrent active endpoints supported by a shared PSN (ISE node has multiple personas)	12,500	25,000	20,000	25,000	50,000	50,000	50,000

Small Deployment

Medium Deployment

Large Deployment



Total Maximum Concurrent Active Sessions

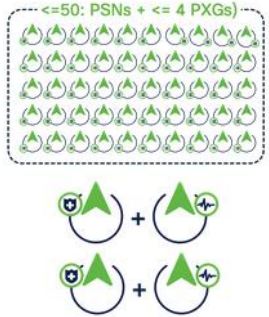
Cisco ISE

Deployment Type	SNS 3615	SNS 3715	SNS 3595	SNS 3655	SNS 3755	SNS 3695	SNS 3795
Large deployment	Unsupported	Unsupported	500,000	500,000	750,000	2,000,000	2,000,000
Medium deployment	10,000	75,000	20,000	25,000	150,000	50,000	150,000
Small deployment	10,000	25,000	20,000	25,000	50,000	50,000	50,000

Small Deployment

Medium Deployment

Large Deployment



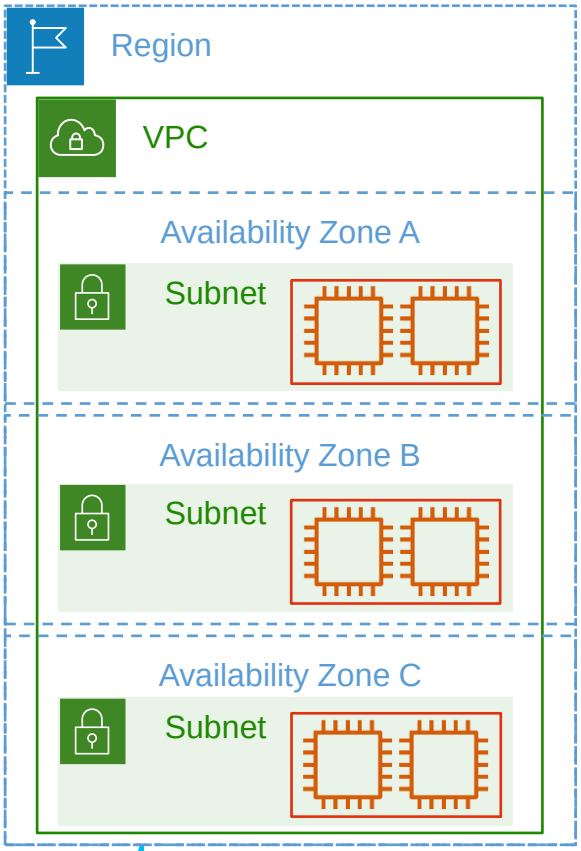
Cisco Cloud Platforms Sizing

Models	SNS 3615	SNS 3595	SNS 3655	SNS 3695
VM Appliance	16 vCPU 32 GB	16 vCPU 64 GB	24 vCPU 96 GB	24 vCPU 256 GB
AWS	c5.4xlarge*	m5.4xlarge	c5.9xlarge* m5.8xlarge	m5.16xlarge
Azure	Standard_F16s_v2*	Standard_D16s_v4	Standard_F32s_v2* Standard_D32s_v4	Standard_D64s_v4
OCI	Optimized3.Flex* (8 OCPU** and 32 GB)	Standard3.Flex (8 OCPU and 64 GB)	Optimized3.Flex* (16 OCPU and 64 GB) Standard3.Flex (16 OCPU and 128 GB)	Standard3.Flex (16 OCPU and 256 GB)

* This instance is compute-optimized and provides better performance compared to the general purpose instances.
** In OCI, you choose CPU in terms of Oracle CPU (OCPU). Each OCPU equals two hardware execution threads known as vCPUs.

ISE in the Cloud

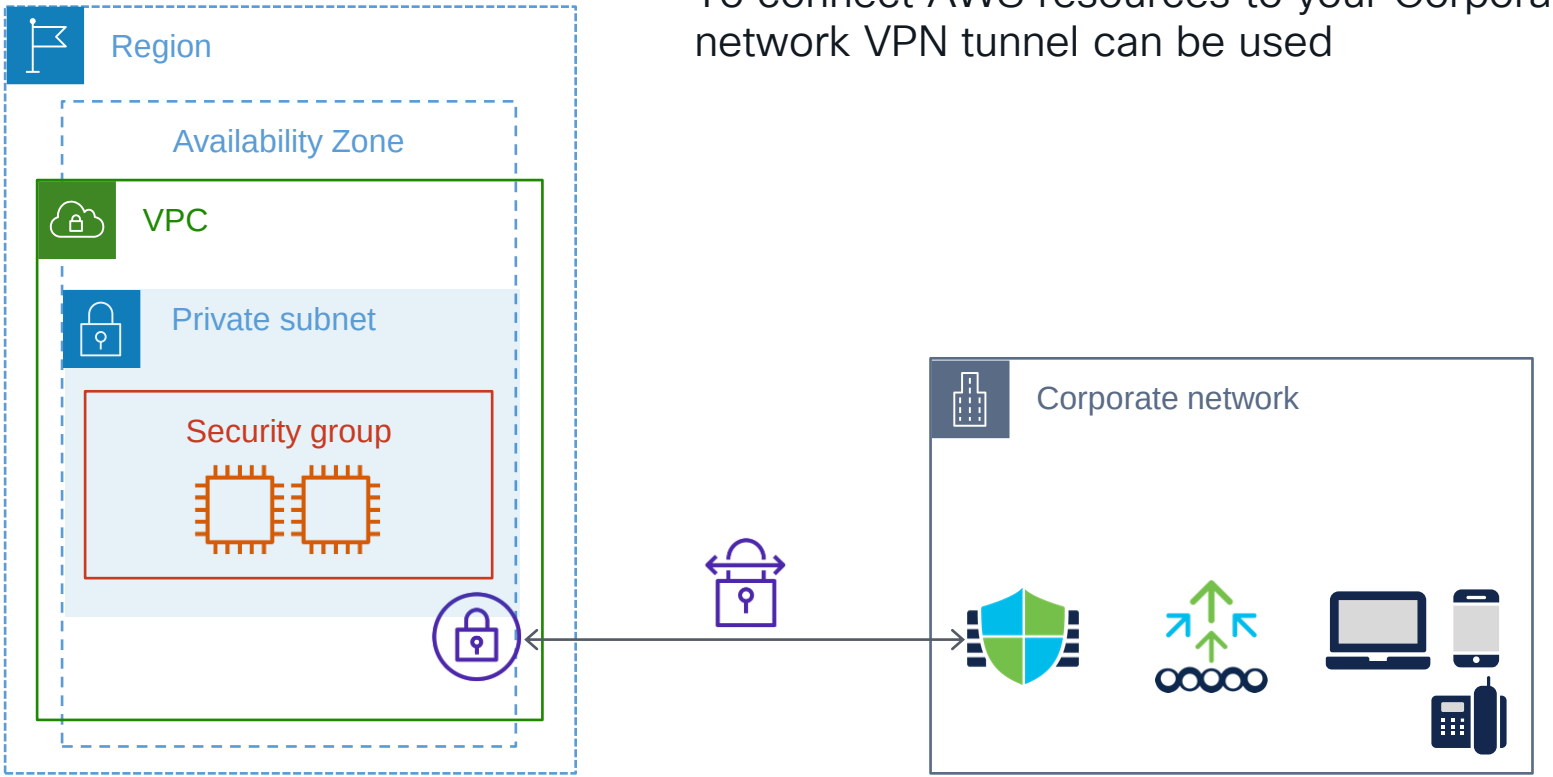
AWS basics



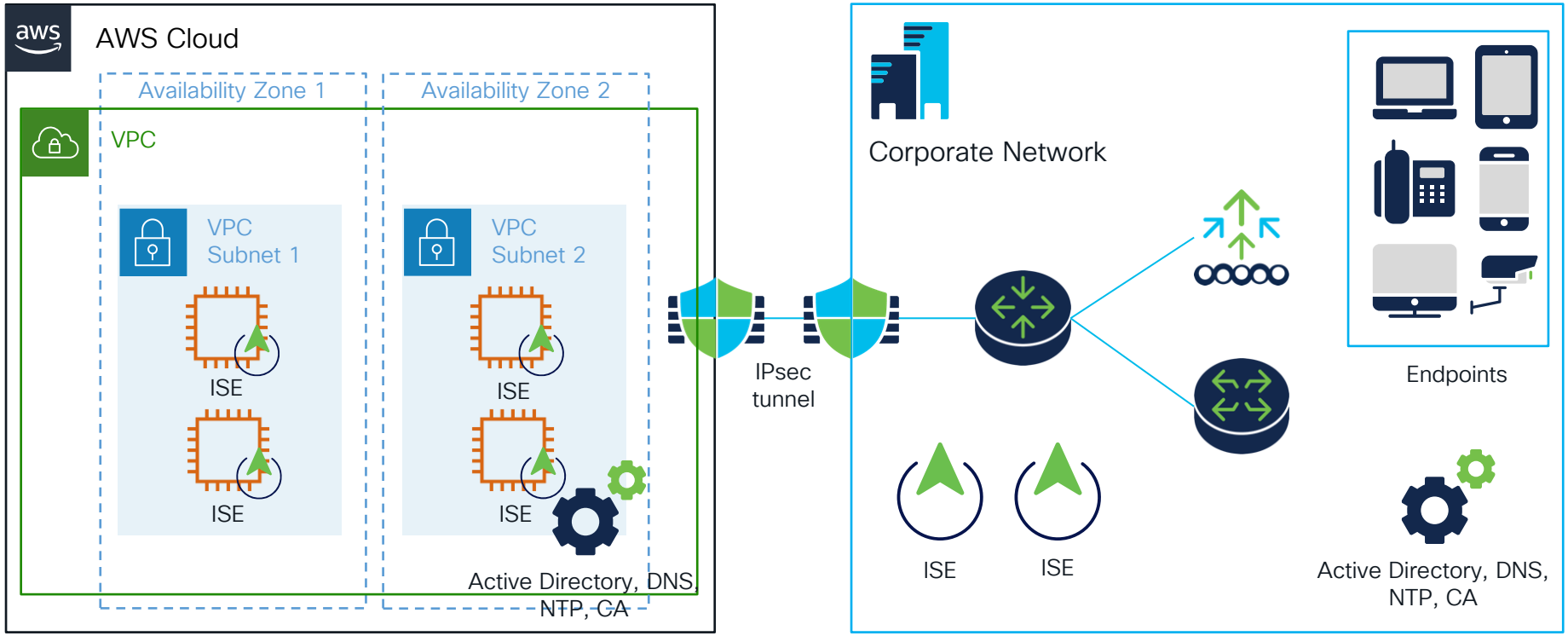
- Each Region is fully isolated from another region to achieve fault tolerance.
  - us-east-2 (Ohio)
  - eu-central-1 (Frankfurt)
  - ap-south-1 (Mumbai)
- Each Region has multiple isolated locations known as Availability Zones. The code for Availability Zone is its Region code followed by a letter identifier.
  - us-east-1a
  - us-east-1b
- VPC is a Virtual Network which spans all of the Availability Zones in the Region.
  - After creating a VPC you can add one or more subnets in each Availability Zone
- Security Group acts like virtual firewall, controlling the traffic which is allowed to reach and leave the resources associated with it.

AWS basics

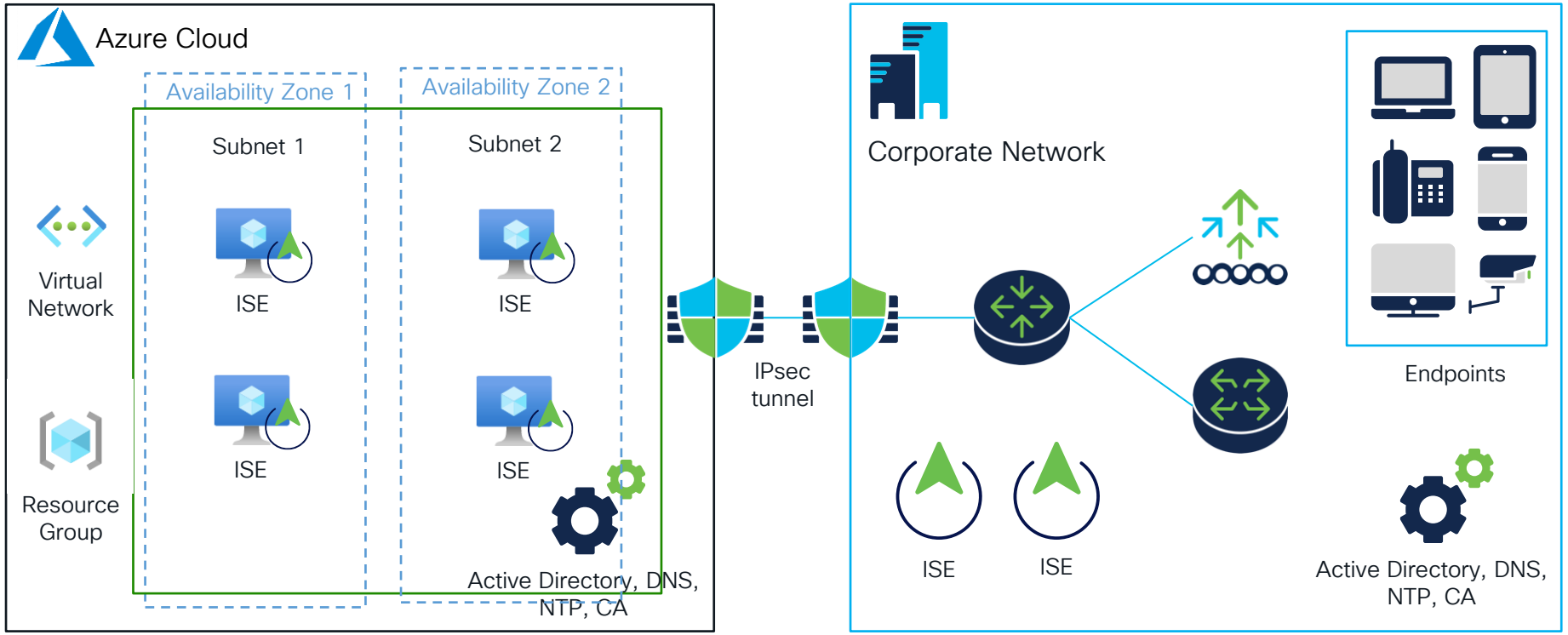
- To connect AWS resources to your Corporate network VPN tunnel can be used



Design Scenarios – AWS



Design Scenarios – Azure



Know Before You Go- Azure

Problem: EAP-TLS Authentications might fail due to the fragmentation issue.

Failure Reason: 5440 Endpoint abandoned EAP Session and started new

Failure Reason 5411 Supplicant stopped responding to ISE

Technical Background and Solution:

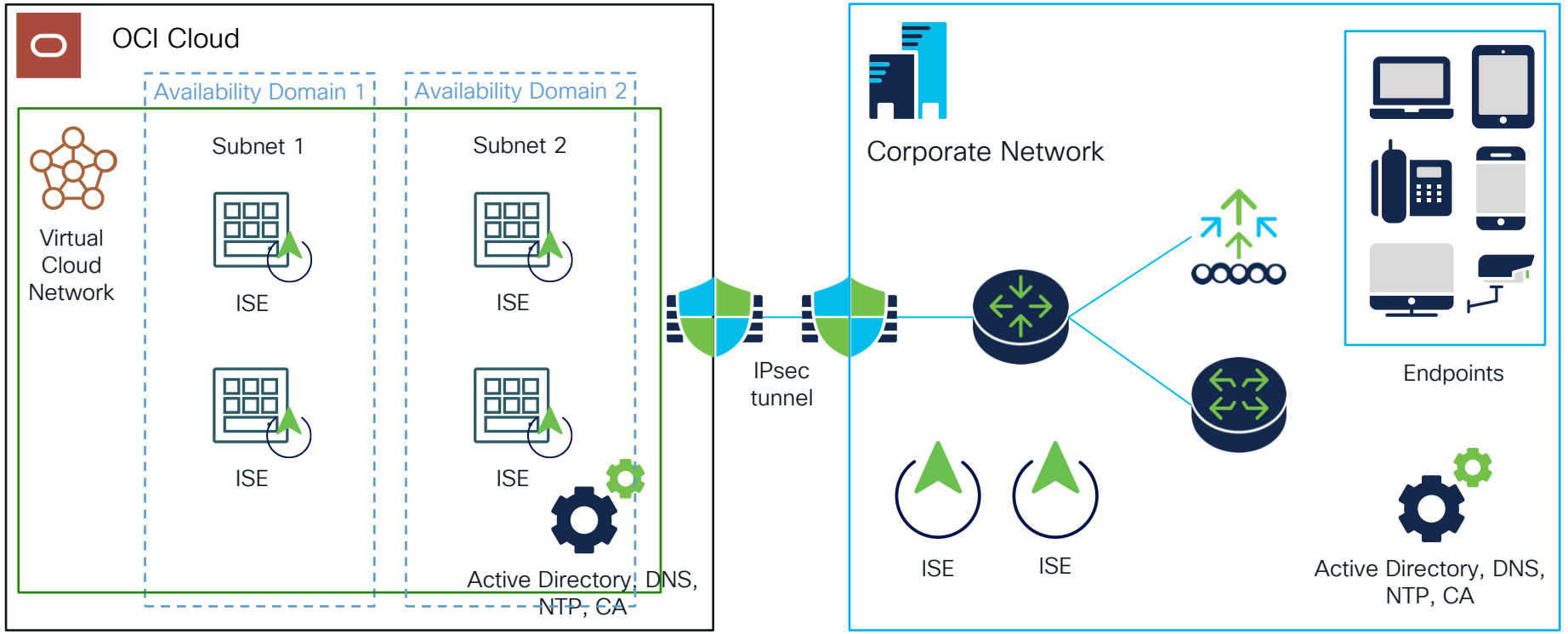
There is a bug in the Azure fragmentation reassembly code. While Microsoft plans to address this issue, a temporary solution has been proposed for Cisco ISE customers utilizing Azure instances.

To implement the short-term fix, ISE customers are advised to raise an Azure support ticket. Microsoft has committed to:

1. Pinning the subscription to ensure that all instances within that subscription are deployed on Gen7 hardware.

2. Allowing out-of-order fragments to pass to the destination instead of being dropped.

Design Scenarios – OCI



ISE in AWS

ISE Setup Options

AWS Marketplace

Amazon Elastic Compute Cloud (Amazon EC2)

AWS CloudFormation

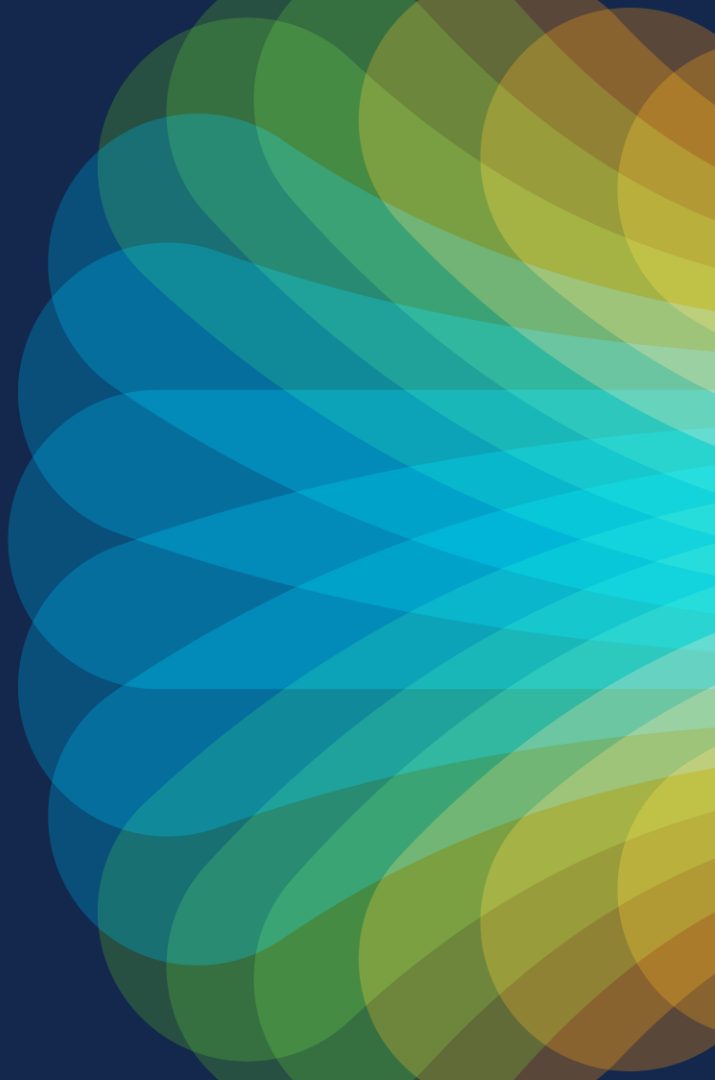
Setup ISE Manually

Automate ISE deployment

Checklist for ISE setup on AWS

1. Decide on Region and Availability Zone
2. Create a VPC and Subnet
3. Create a Security Group
4. Setup VPN between AWS and On-Prem Network
5. Create a Key Pair for SSH
6. Keep ISE setup information handy (hostname, DNS, Domain, NTP, Timezone, credentials)

Demo. ISE installation on AWS using CloudFormation



Console Home Info

Reset to default layout | + Add widgets

Introducing the new Managed instances, Ops summary, and Patch compliance widgets. View new widgets

Recently visited Info

- CloudFormation
- EC2
- Route 53
- AWS Marketplace Subscriptions
- VPC
- Kinesis
- IoT SiteWise
- IAM
- Key Management Service
- API Gateway
- CloudWatch

View all services

Welcome to AWS

Getting started with AWS
Learn the fundamentals and find valuable information to get the most out of AWS.

Training and certification
Learn from AWS experts and advance your skills and knowledge.

What's new with AWS?
Discover new AWS services, features, and Regions.

AWS Health Info

Open issues

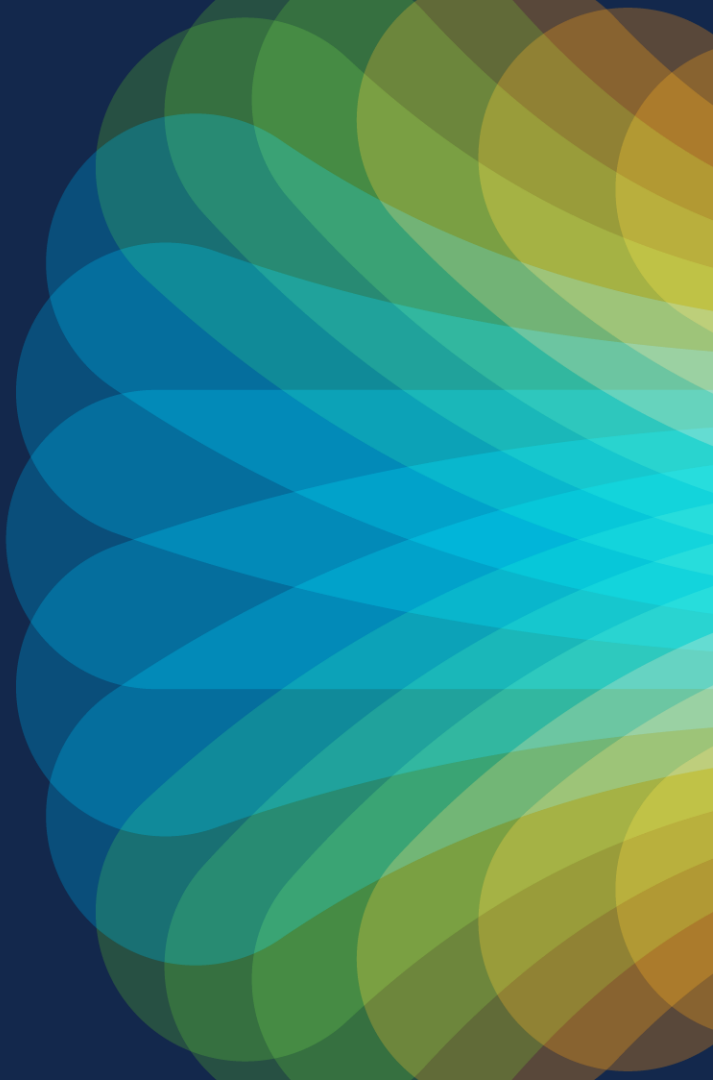
0 Past 7 days

Build a solution Info

Start building with simple wizards and automated workflows.

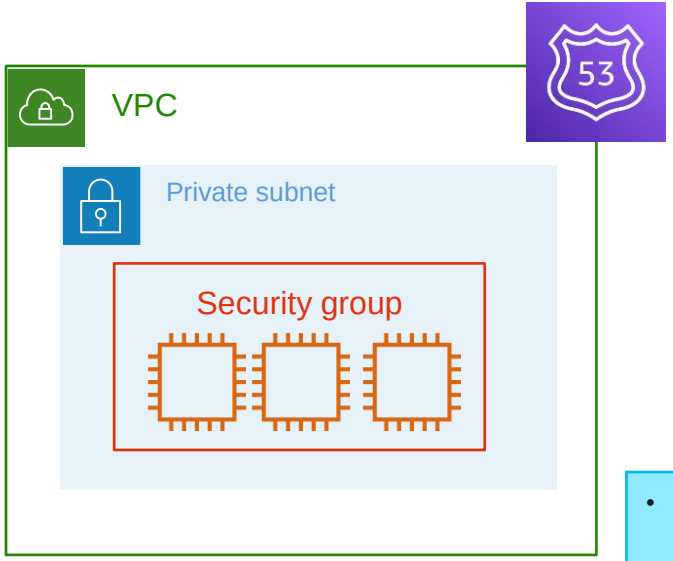
- Launch a virtual machine
  With EC2 (2 mins)
- Register a domain
  With Route 53 (3 mins)

What if you would like to install whole infrastructure?



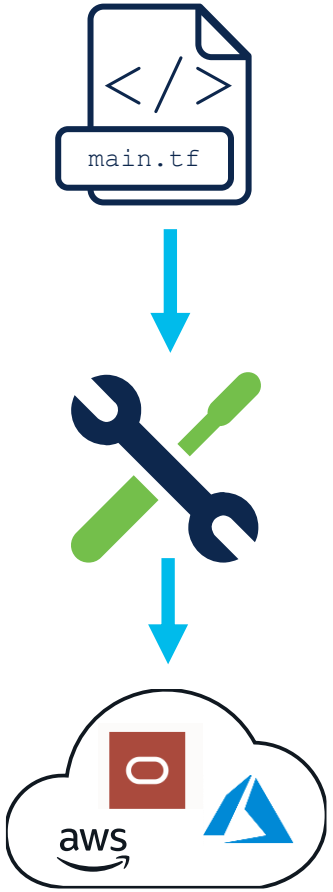
Terraform

- Infrastructure as a Code to automate the provisioning of your infrastructure resources

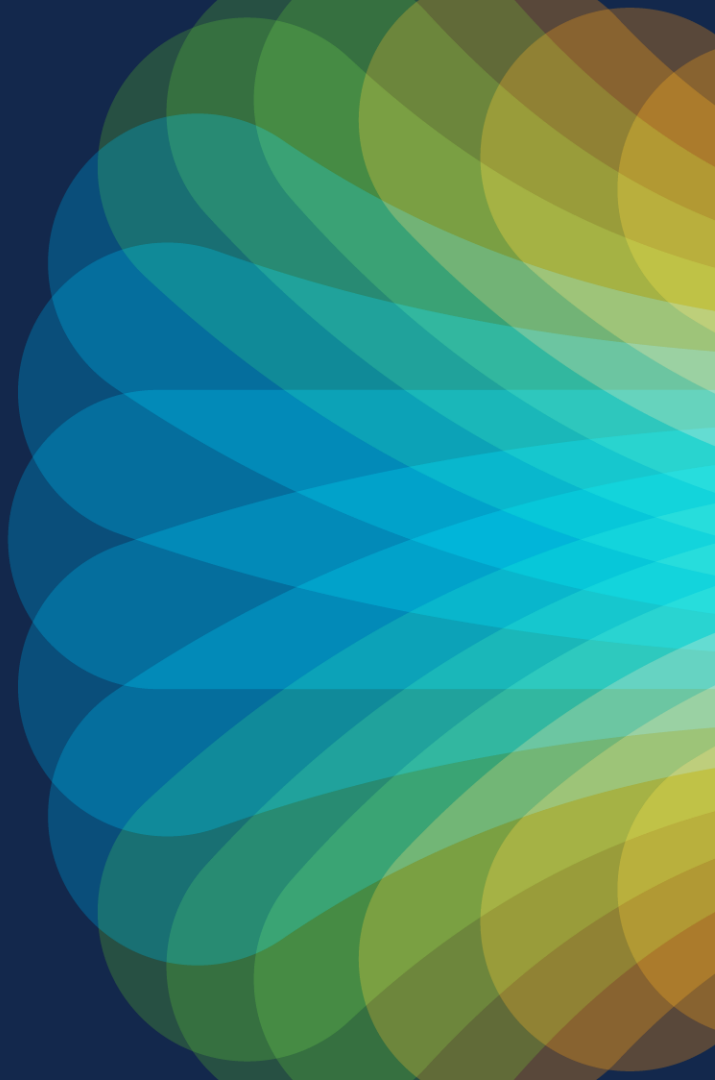


- Create VPC
- Create a Subnet
- Create Security Group
- Create EC2 Instances
- Create DNS records

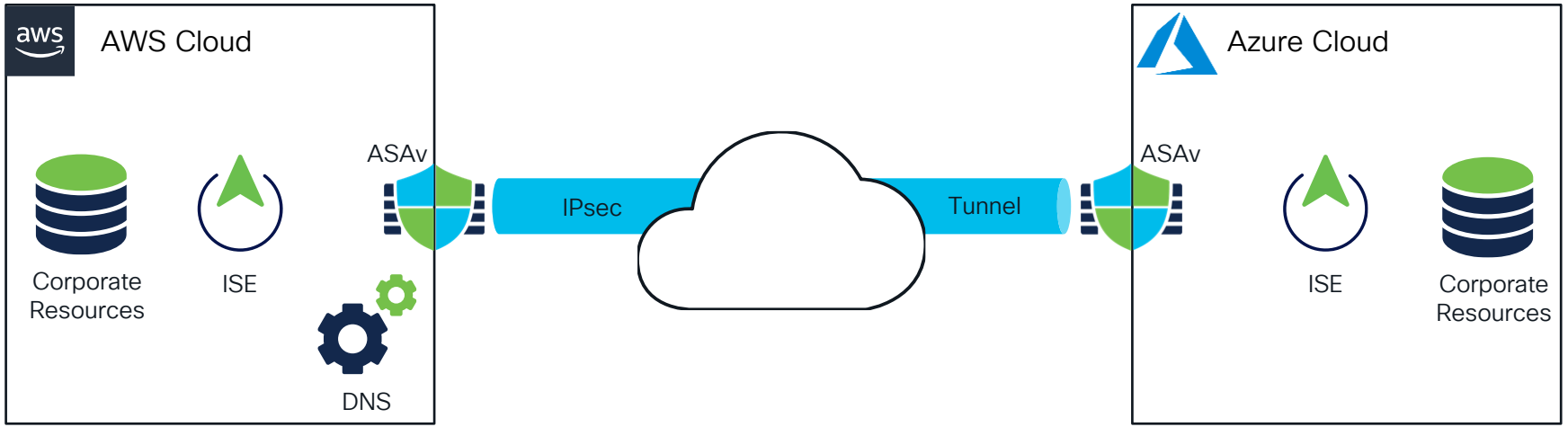
- Relies on the main.tf (terraform config) file to provision resources
- Terraform keeps the state of the infrastructure, compare the end result to what the current state is and provisions resources accordingly



Demo. ISE installation on AWS and Azure using Terraform



Deployment Topology



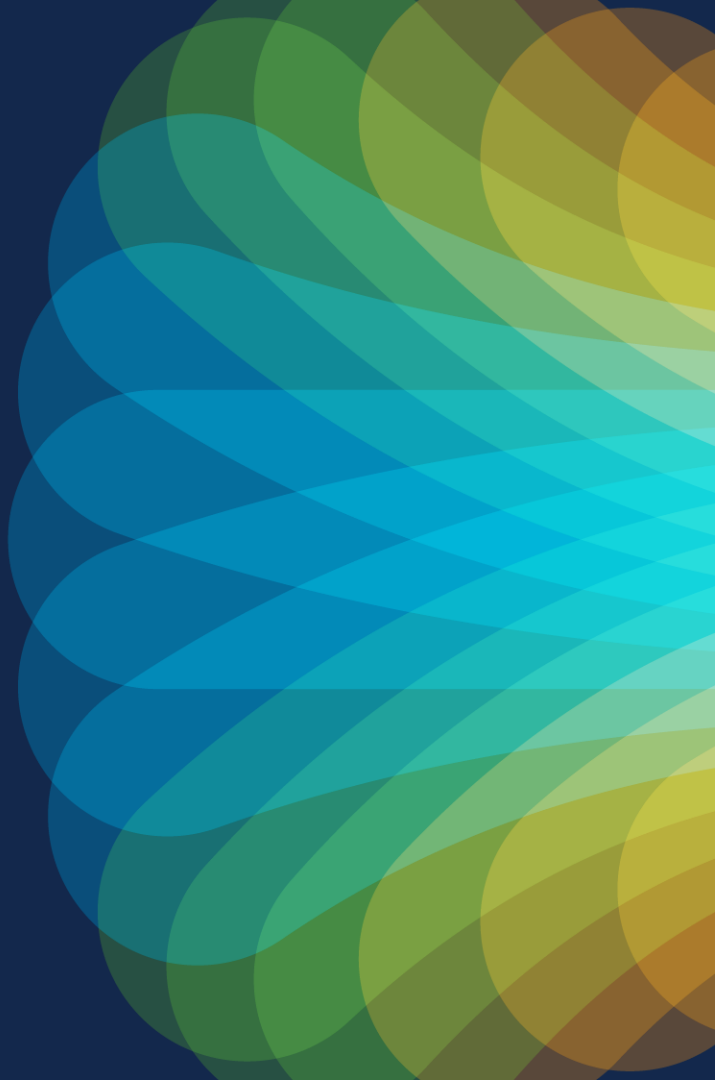
```
ekorneyc@EKORNEYC-M-20GN Terraform % terraform apply

Terraform used the selected providers to generate the following execution plan. Resource actions are indicated w
following symbols:
  + create

Terraform will perform the following actions:

  # aws_instance.ise1 will be created
  + resource "aws_instance" "ise1" {
      + ami                                  = "ami-08c545c5ef3cacced"
      + arn                                  = (known after apply)
      + associate_public_ip_address          = (known after apply)
      + availability_zone                    = (known after apply)
      + cpu_core_count                       = (known after apply)
      + cpu_threads_per_core                 = (known after apply)
      + disable_api_termination              = (known after apply)
      + ebs_optimized                        = (known after apply)
      + get_password_data                    = false
      + host_id                              = (known after apply)
      + id                                   = (known after apply)
      + instance_initiated_shutdown_behavior = (known after apply)
      + instance_state                       = (known after apply)
      + instance_type                        = "c5.4xlarge"
      + ipv6_address_count                   = (known after apply)
      + ipv6_addresses                       = (known after apply)
      + key_name                             = "AWS2"
```

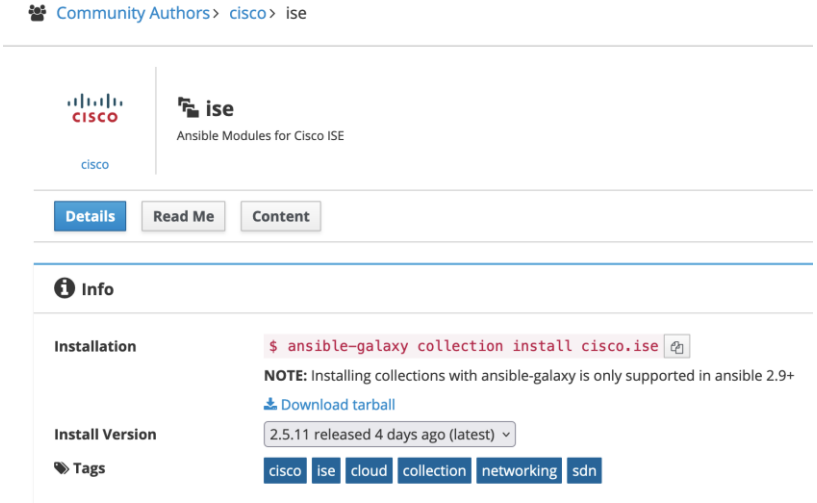
That’s not it, you need to configure things...



Ansible

- Ansible playbooks are written in YAML
- Ansible playbooks consist of plays, which are sets of Tasks

galaxy.ansible.com



Play (set of tasks)

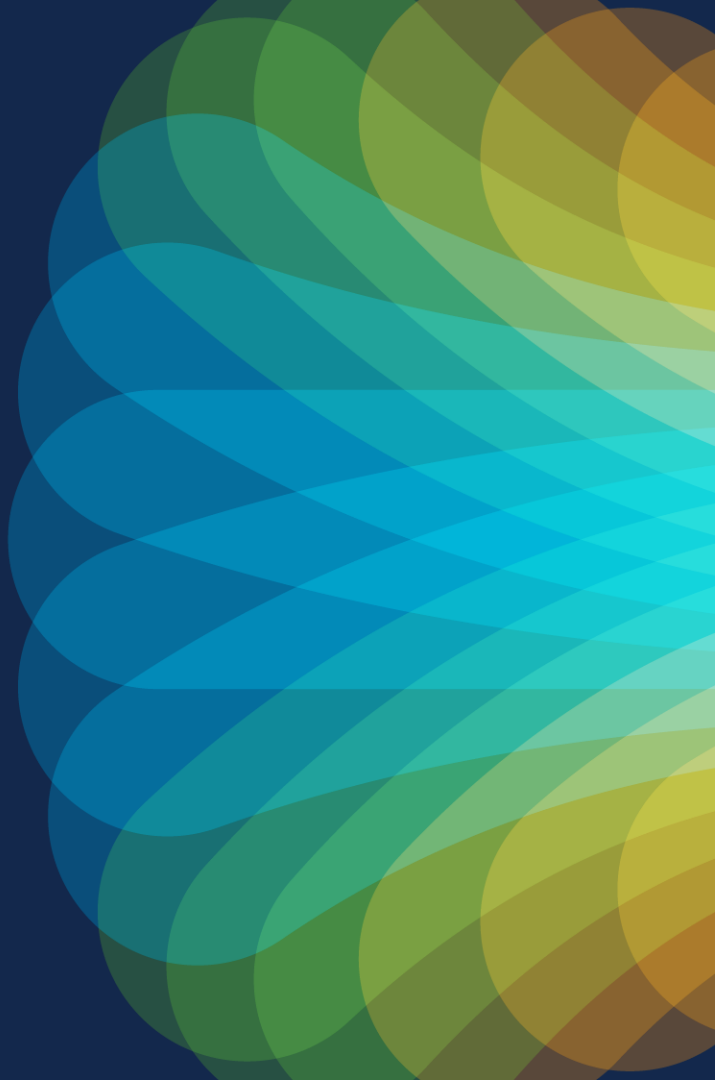
Task

```yaml
- hosts: ise_servers
  vars_files:
    - credentials_emea.yml
  gather_facts: no
  tasks:

  - name: Create or update ASAv
    cisco.ise.network_device:
      ise_hostname: "{{ise_hostname}}"
      ise_username: "{{ise_username}}"
      ise_password: "{{ise_password}}"
      ise_verify: "{{ise_verify}}"
      state: present
      name: ASAv2
      NetworkDeviceIPList:
      - ipaddress: 172.31.108.43
        mask: 32
      authenticationSettings:
        radiusSharedSecret: 'cisco'
        networkProtocol: 'RADIUS'
      description: 'ASAv in AWS'
    register: result
```

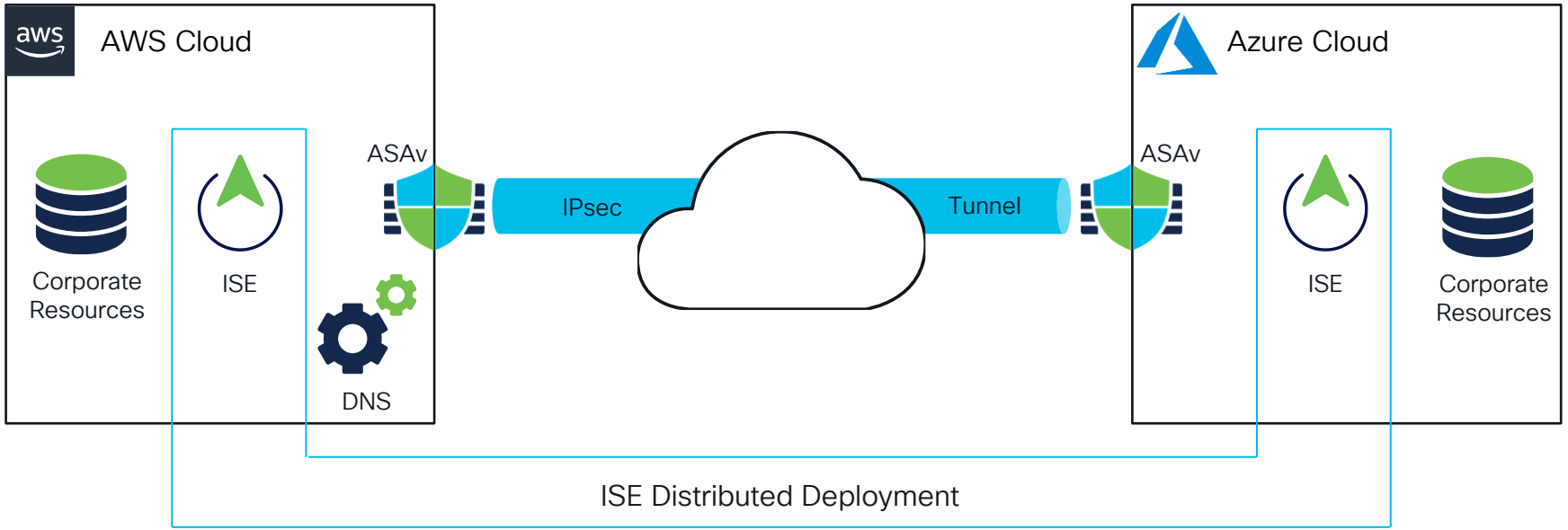
Playbook (set of plays)

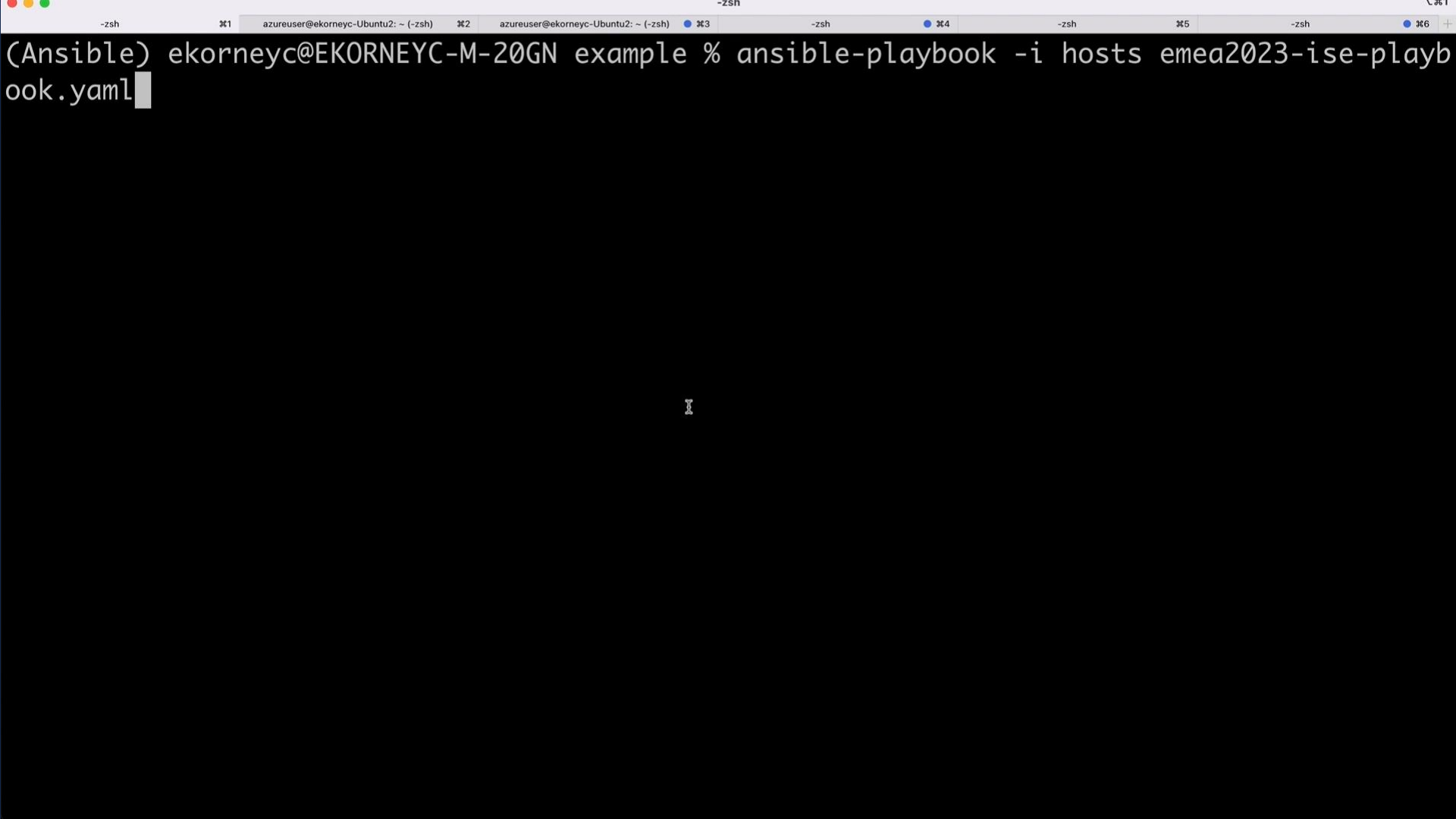
Demo. ISE configuration using Ansible



Deployment Topology

ISE Configuration




-zsh
-zsh ⌘1
azureuser@ekorneyc-Ubuntu2: ~ (-zsh) ⌘2
azureuser@ekorneyc-Ubuntu2: ~ (-zsh) ⌘3
-zsh ⌘4
-zsh ⌘5
-zsh ⌘6
(Ansible) ekorneyc@EKORNEYC-M-20GN example % ansible-playbook -i hosts emea2023-ise-playbook.yaml

AWS Partner Solution – Cisco ISE

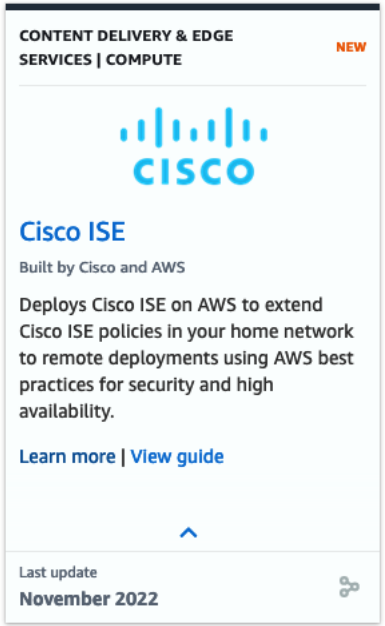
Partner Solutions Overview (formerly Quick Starts)

Automated Deployments built by Amazon Web Services solutions Architects and AWS Partners

Helps customers deploy popular technologies on AWS according to AWS Best Practices

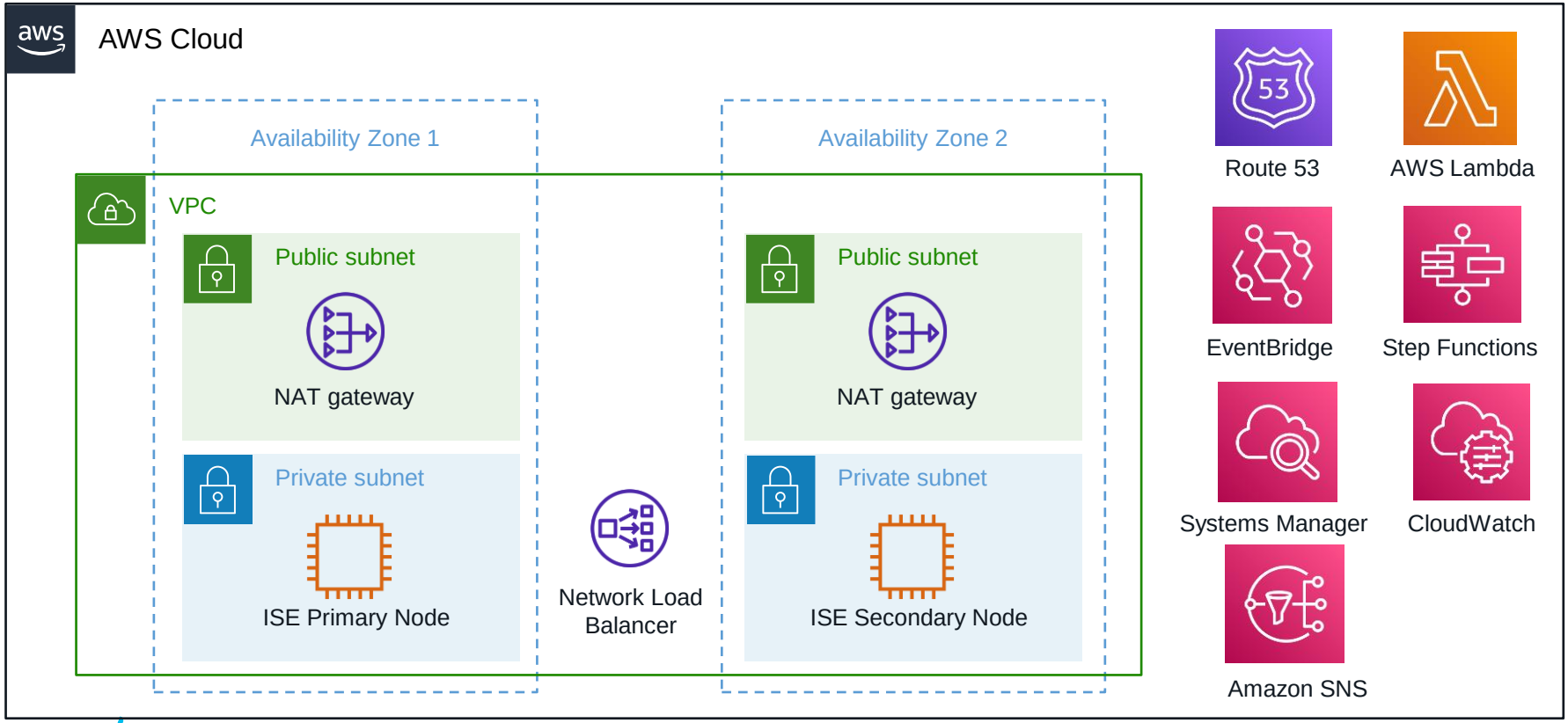
Reduces hundreds of manual procedures into just few steps, so AWS customers can build production environments quickly

Automate deployments to the AWS Cloud



https://aws.amazon.com/quickstart/

AWS Partner Solution – Cisco ISE Architecture



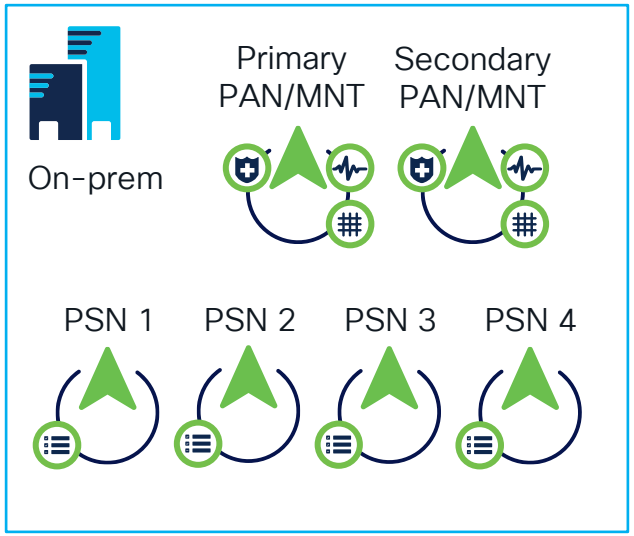
ISE in the Cloud. Licensing

Cisco ISE leverages the Bring Your Own License (BYOL)

- ISE Comes with 90-days Evaluation License
- Use the Common VM License to enable Cisco ISE on cloud platforms, in addition to the other Cisco ISE licenses that you need for the Cisco ISE features you want to use.

ISE Migration and Upgrade

Migration



Scenario: ISE 3.2 patch 4 Medium Deployment Migration to Cloud Infrastructure

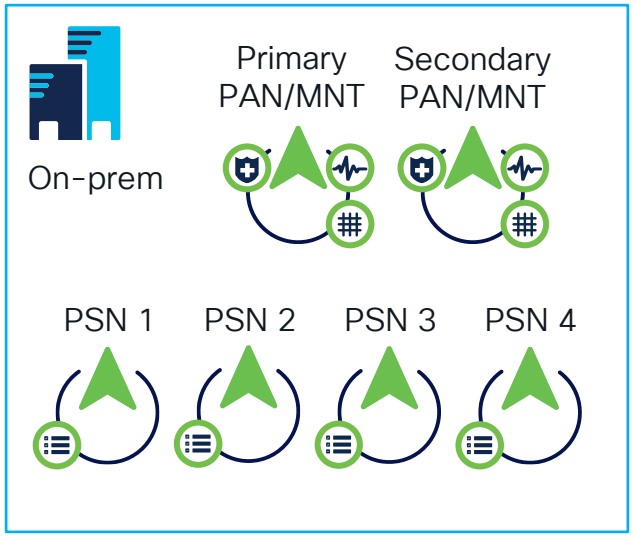
--- === Phase 0 === ---

- Plan
  - Take a Backup
  - Run Health Checks
  - FQDN's of ISE Nodes to be used
  - IP addresses of ISE Nodes to be used
  - End to End connectivity with the Cloud Providers
  - Test Infrastructure
  - Time and Date for MW

aws AWS Cloud

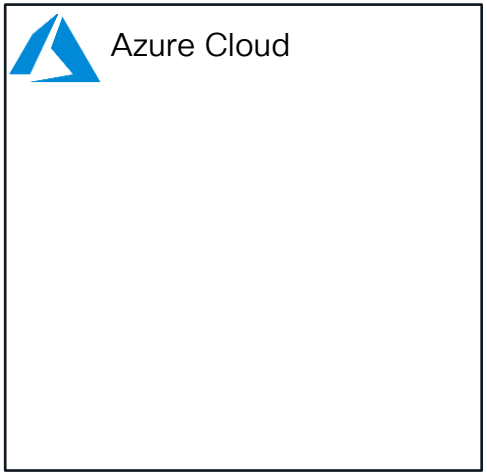
Azure Cloud

Migration



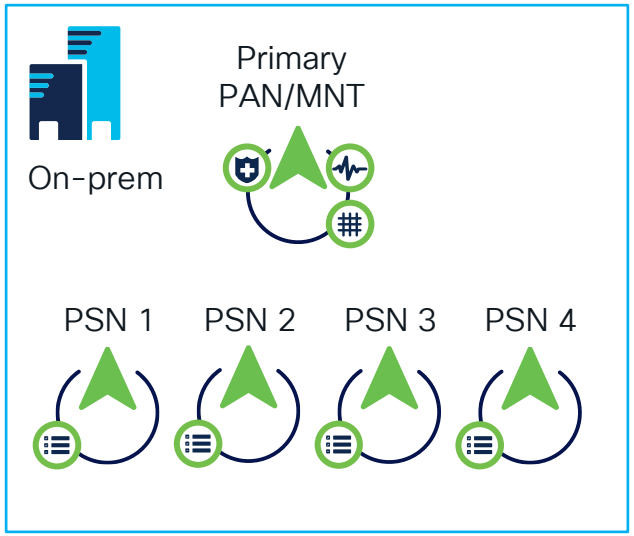
--- === Phase 1 === ---

1. Deregister Secondary PAN/MNT
2. Deploy Cloud Instance
3. Install Patch
4. Add Node to the Deployment



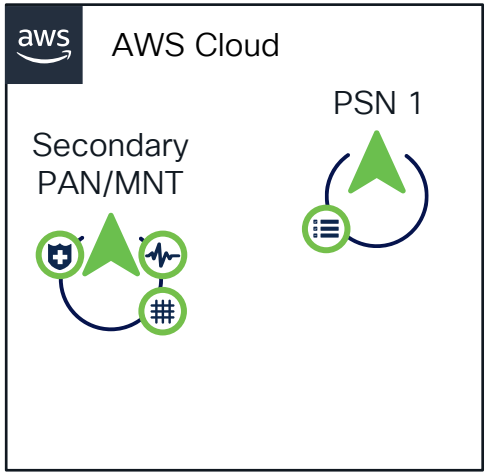
Considerations:
- (Optional) Certificates to be exported prior Deregistration of Secondary PAN, imported before adding Node to the Deployment

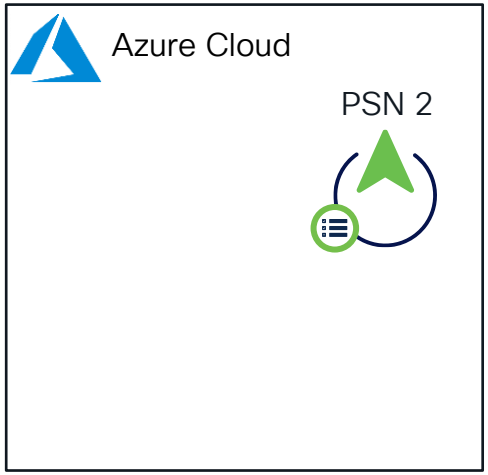
Migration



--- === Phase 2 === ---

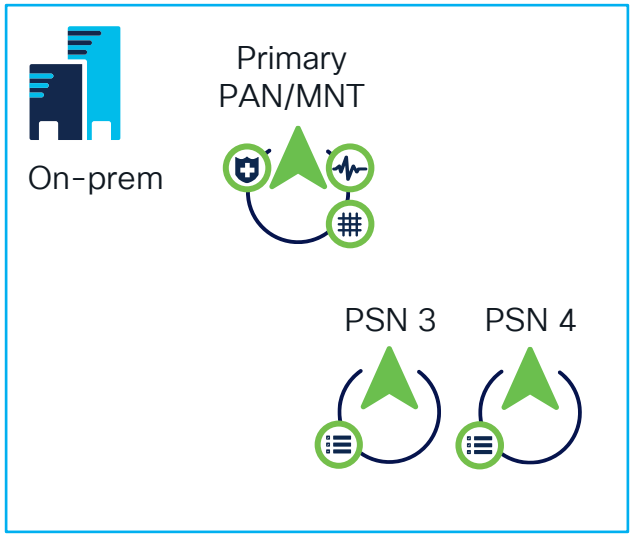
1. Deregister PSN1, PSN2
2. Deploy Cloud Instances
3. Install Patch
4. Add Nodes to the Deployment
5. Test





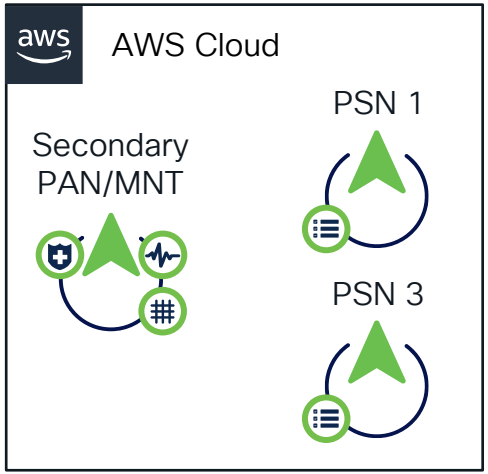
Considerations:
- (Optional) Certificates to be exported prior Deregistration, imported before adding Nodes to the Deployment
- NAD's configuration should be evaluated prior to Phase 2. Exclude PSN1 and PSN2 from LB Groups or ensure that high availability configuration includes PSN3 and PSN4

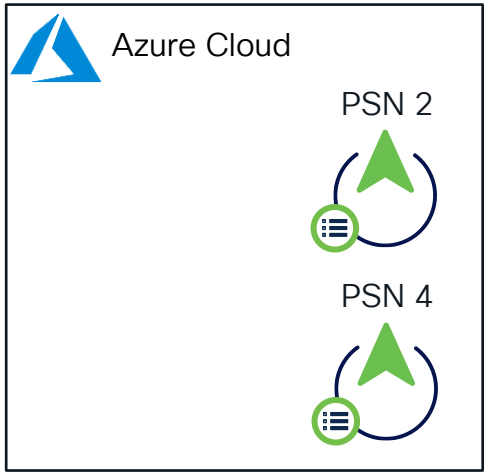
Migration



--- === Phase 3 === ---

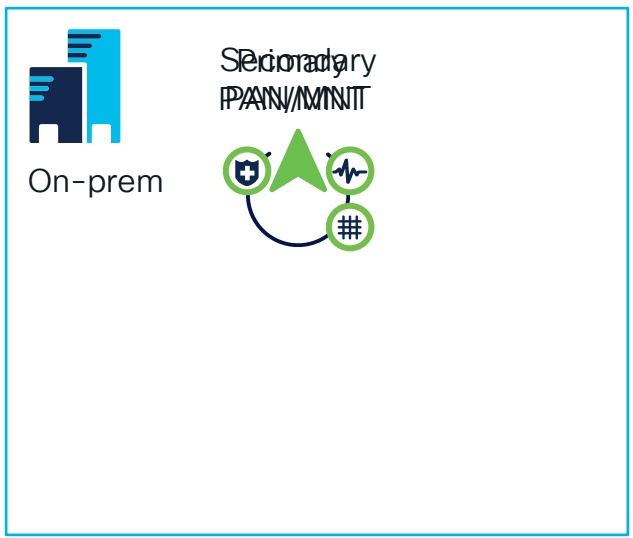
1. Deregister PSN3, PSN4
2. Deploy Cloud Instances
3. Install Patch
4. Add Nodes to the Deployment
5. Test





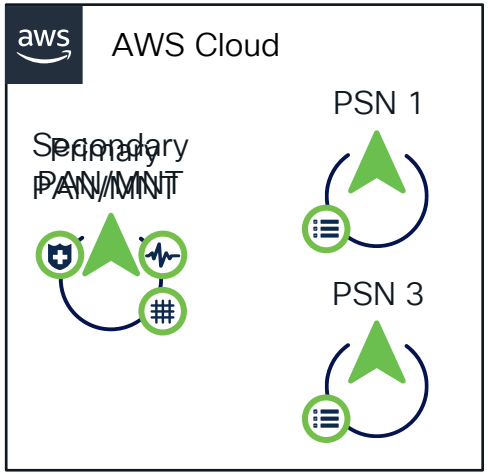
Considerations:
- (Optional) Certificates to be exported prior Deregistration, imported before adding Nodes to the Deployment
- NAD's configuration should be evaluated prior to Phase 3. Exclude PSN3 and PSN4 from LB Groups or ensure that high availability configuration includes PSN1 and PSN2

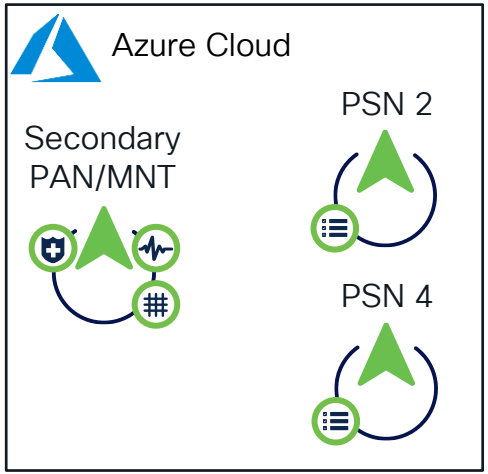
Migration



--- === Phase 4 === ---

1. Promote Secondary PAN/MNT to Primary
2. Remove Secondary PAN/MNT
3. Deploy Cloud Instance
4. Install Patch
5. Add Node to the Deployment





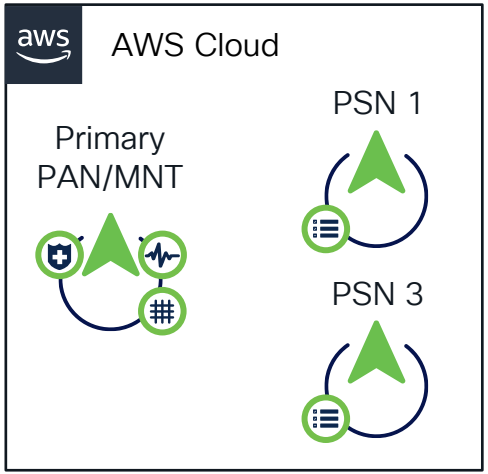
Considerations:
- (Optional) Certificates to be exported prior Removal of PAN, imported before adding Node to the Deployment

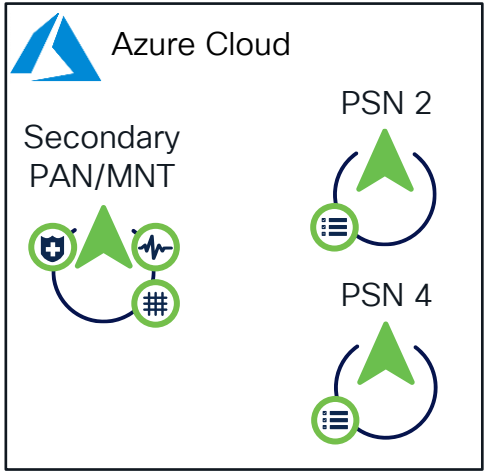
Upgrade

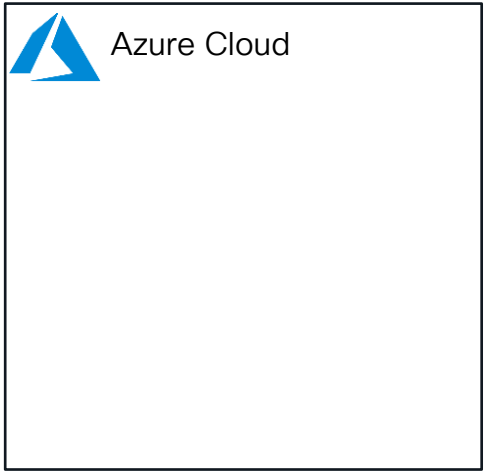
--- === Phase 0 === ---

- Plan
  - Review the Upgrade Guide
  - Take a Backup
  - Test Infrastructure
  - Time and Date for MW
  - Run Health Checks

Scenario: ISE 3.2 patch 4 Medium Deployment Upgrade to ISE 3.3 patch 1





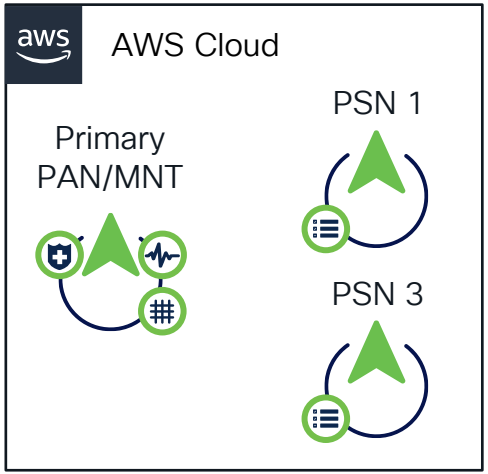


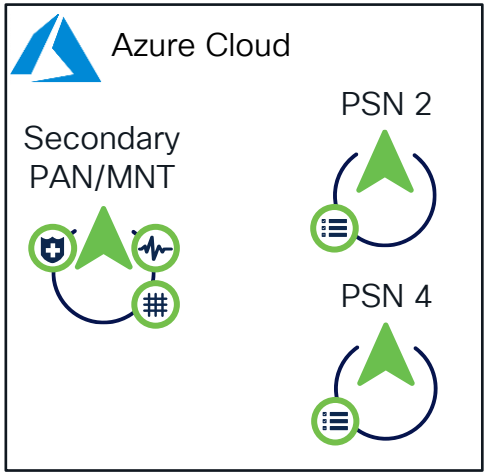
Upgrade

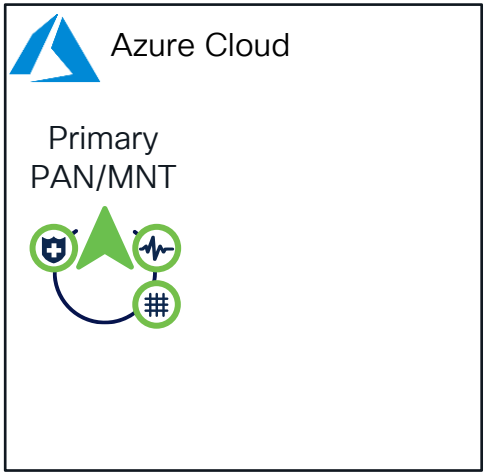
--- === Phase 1 === ---

- Deregister Secondary PAN/MNT and delete the instance
- Deploy the new instance to destination ISE release.
- Install the patch
- Restore the Backup
- Promote the Standalone Node to Primary PAN/MNT

Considerations:
- (Optional) Certificates to be exported prior Deregistration of Secondary PAN, imported after the Backup Restore





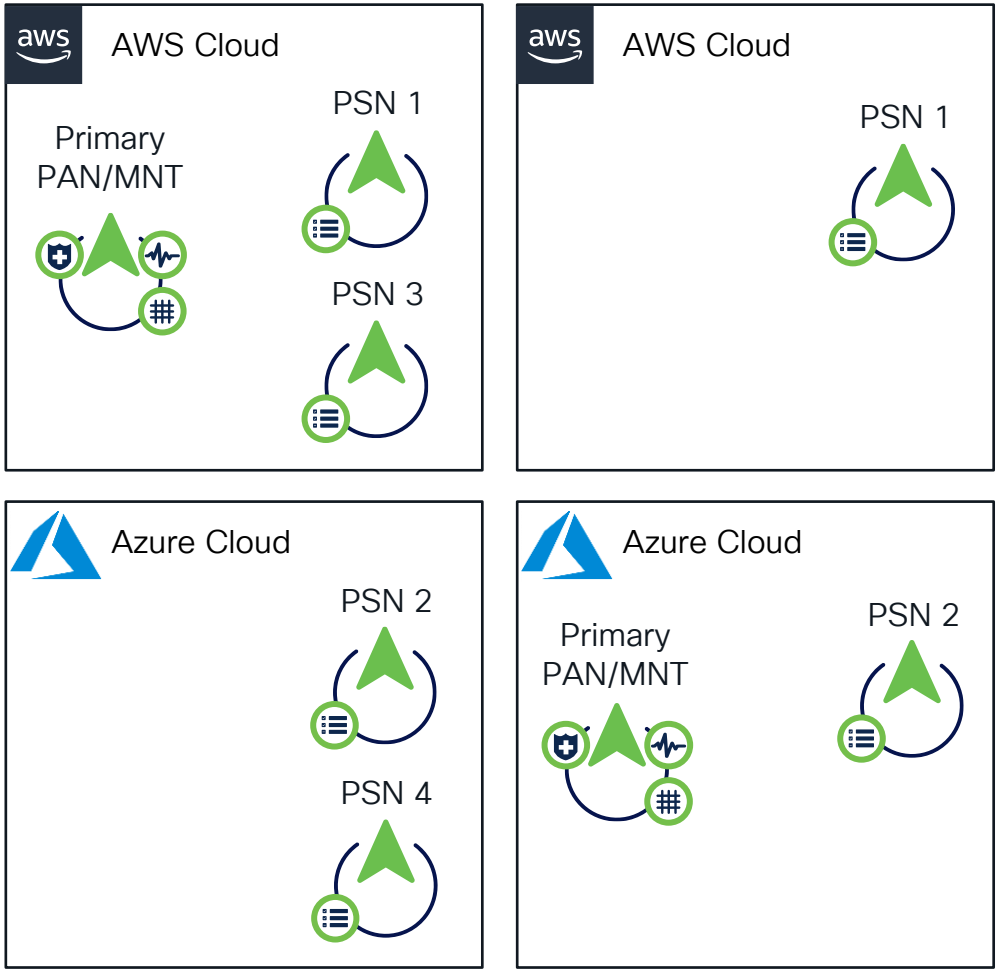


Upgrade

--- === Phase 2 === ---

- Deregister PSN1 and PSN2 and delete the instances
- Deploy the new instances to destination ISE release.
- Install the patch
- Join the new deployment
- Test

Considerations:
- (Optional) Certificates to be exported prior Deregistration of PSN1 and PSN2, imported before Joining the Deployment
- NAD's configuration should be evaluated prior Deregistration. Exclude PSN1 and PSN2 from LB Groups or ensure that high availability configuration includes PSN3 and PSN4

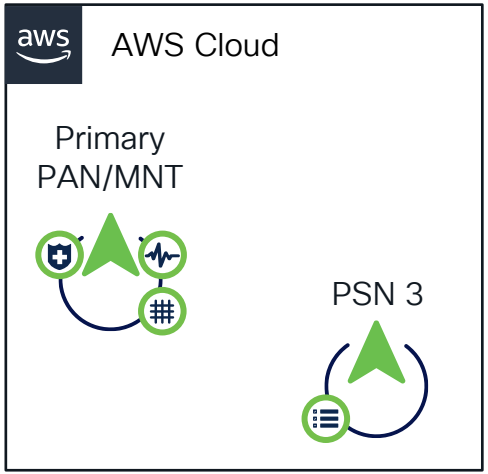


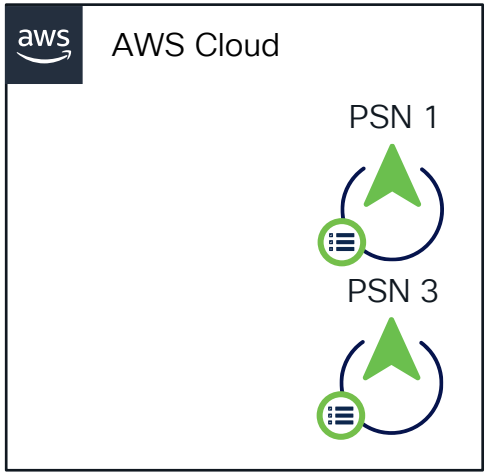
Upgrade

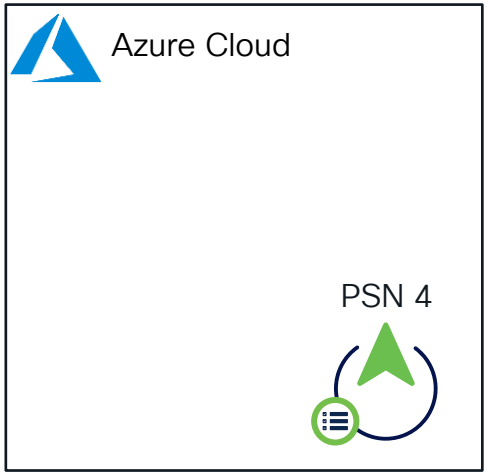
--- === Phase 3 === ---

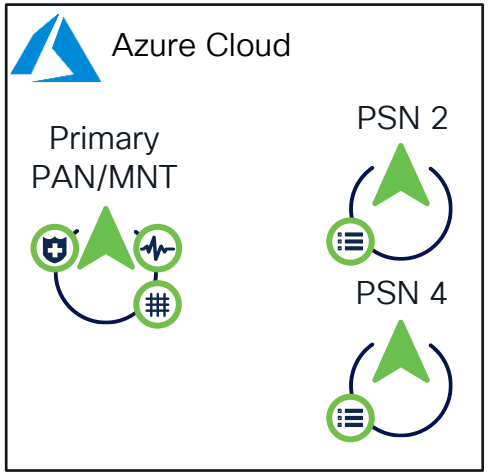
- Deregister PSN3 and PSN4 and delete the instances
- Deploy the new instances to destination ISE release.
- Install the patch
- Join the new deployment
- Test

Considerations:
- (Optional) Certificates to be exported prior Deregistration of PSN3 and PSN4, imported before Joining the Deployment
- NAD's configuration should be evaluated prior Deregistration. Exclude PSN3 and PSN4 from LB Groups or ensure that high availability configuration includes PSN1 and PSN2







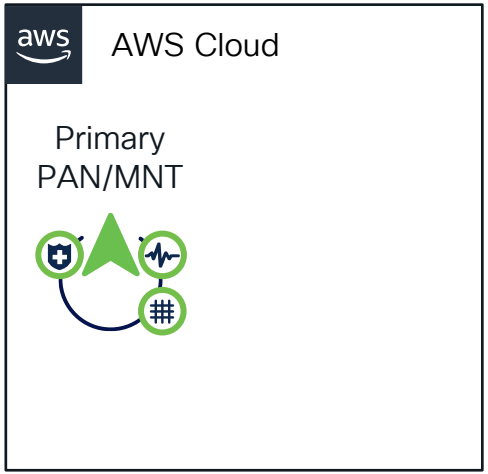


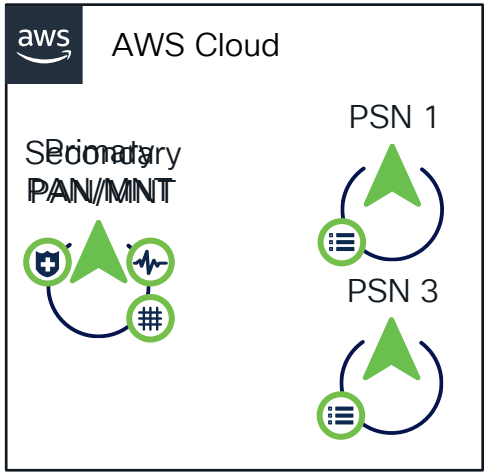
Upgrade

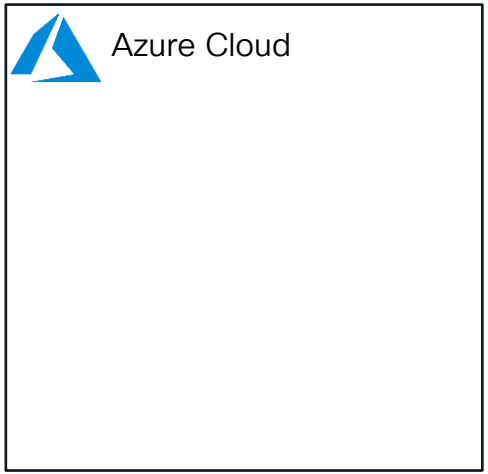
--- === Phase 4 === ---

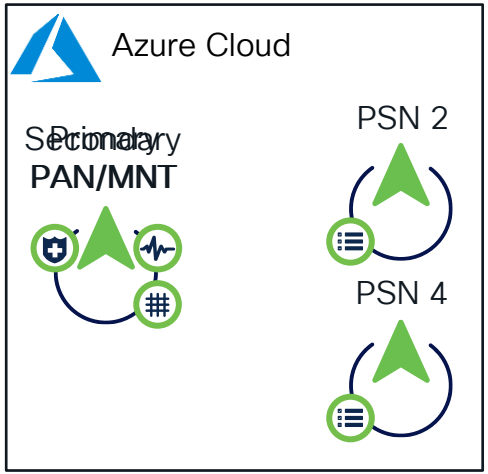
- Delete Primary PAN/MNT of old deployment
- Deploy the new instance to destination ISE release.
- Install the patch
- Join the new deployment
- Promote Secondary PAN/MNT to Primary PAN/MNT
- Test

Considerations:
- (Optional) Certificates to be exported prior Deregistration of Primary PAN, imported before joining the deployment









ISE in the Cloud. Design Considerations

- Upgrade workflow is not supported. Only fresh installs are supported. However, you can carry out backup and restore of configuration data

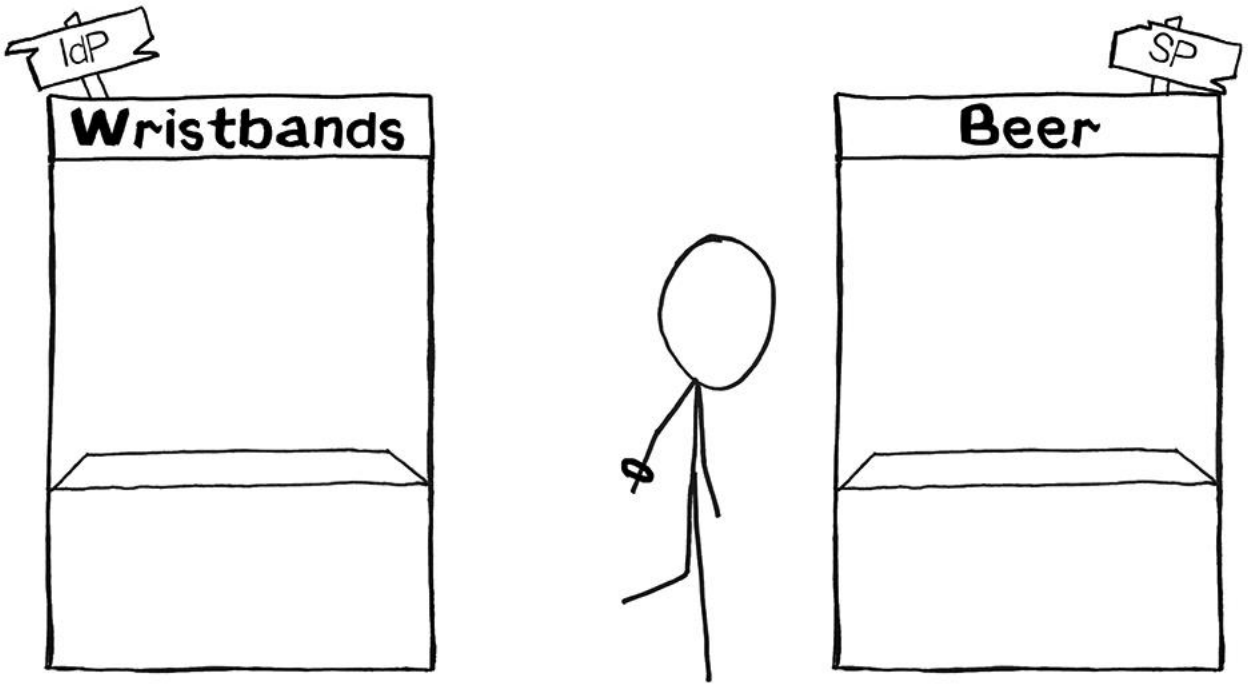
- SSH access to Cisco ISE CLI using password-based authentication is not supported. You can only access the Cisco ISE CLI through a key pair

- Latency should be below 300 msec

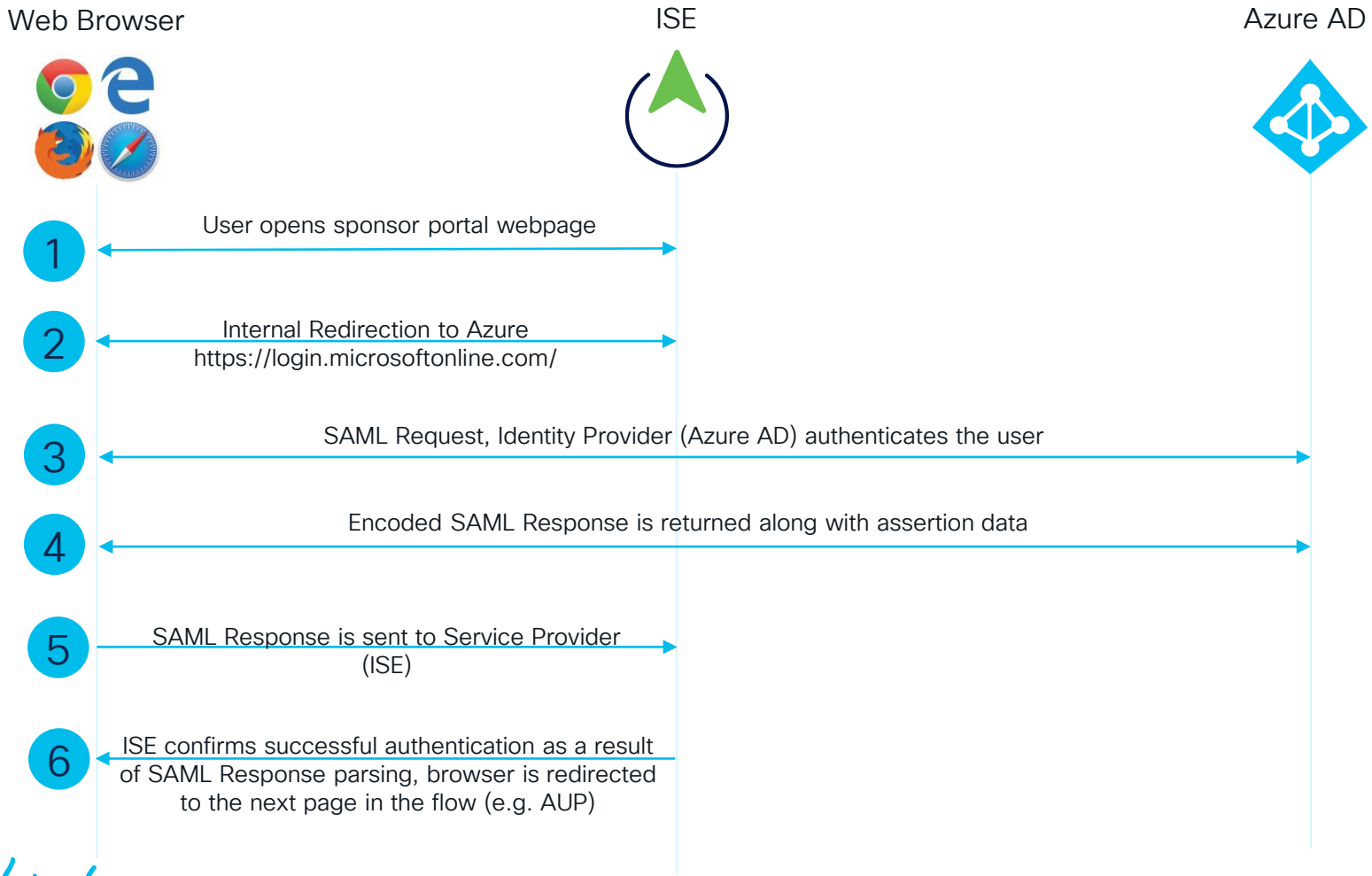
- Starting ISE 3.2 default GUI username is “iseadmin”

ISE SAML SSO

What is SAML?

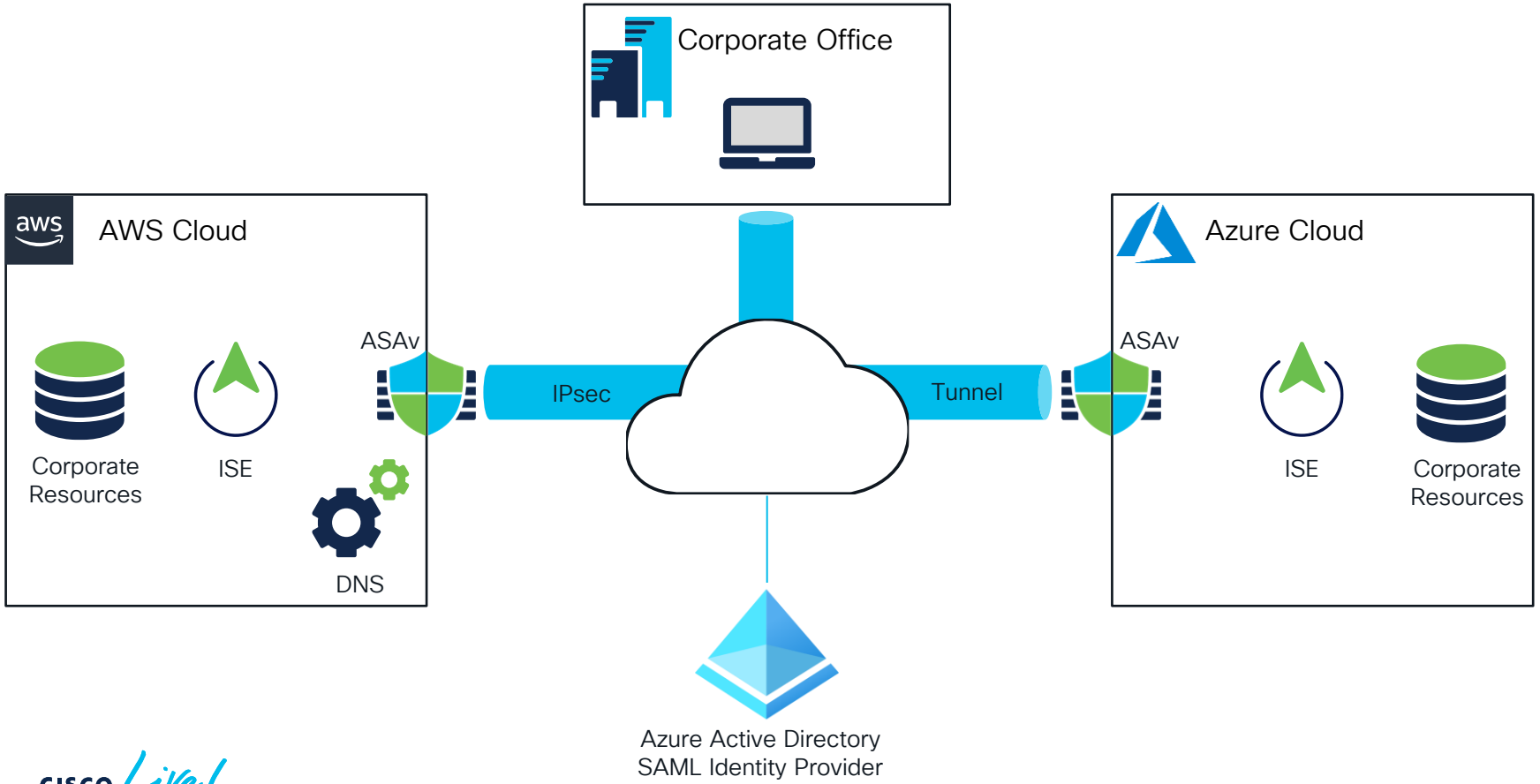


The Beer Drinker's Guide to SAML



Demo. ISE Sponsor Portal Authentication with SAML

Deployment Topology



Route 53 Console Hosted Zones | Identity Services Engine

https://54.80.78.237/admin/#home

Cisco ISE

Dashboard

Evaluation Mode 89 Days

Summary | Endpoints | Guests | Vulnerability | Threat

Manage

Total Endpoints	Active Endpoints	Rejected Endpoints	Anomalous Behavior	Authenticated Guests	BYOD Endpoints	C
1	0	0	0	0	0	

AUTHENTICATIONS

Identity Store | Identity Group | Network Device | Failure Reason

NETWORK DEVICES

Device Name | Type | Location

ENDPOINTS

Profile | Logical Profile

BYOD ENDPOINTS

Type | Profile

ALARMS

Severity	Name	Occu...	Last Occurred
	Name		
⚠	ISE Authentication In...	75	less than 1 min ...

SYSTEM SUMMARY

2 node(s)

All | 24HR

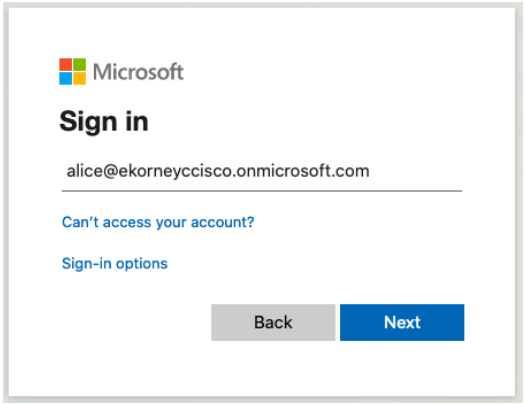
ISE31-aws1

62

ISE Azure Active Directory Authentication

cisco Live!

802.1x Authentication Problem with SAML



Endpoint

SAML

802.1x

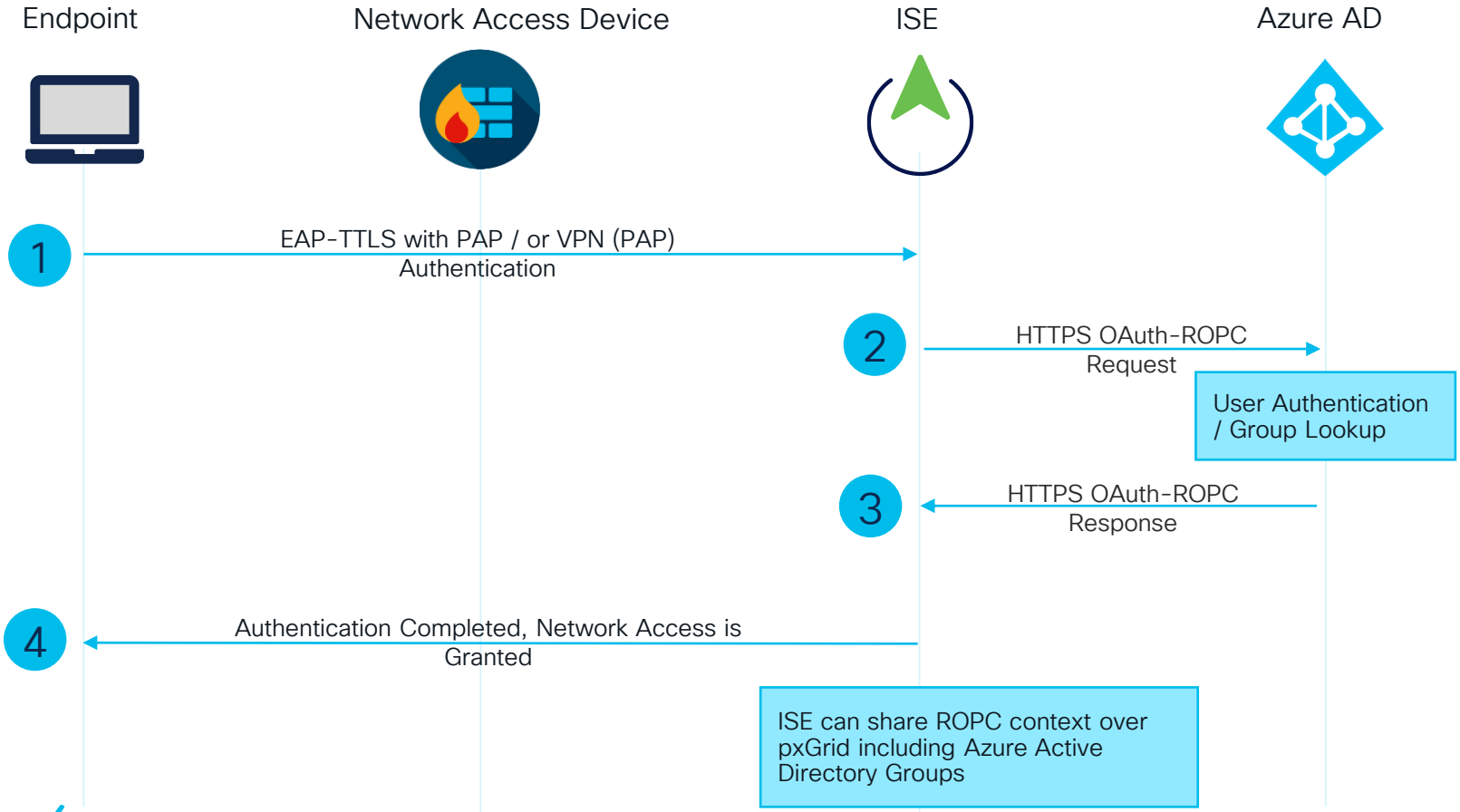
Azure AD

SAML assumes network connectivity, so the Endpoint can reach Identity Provider

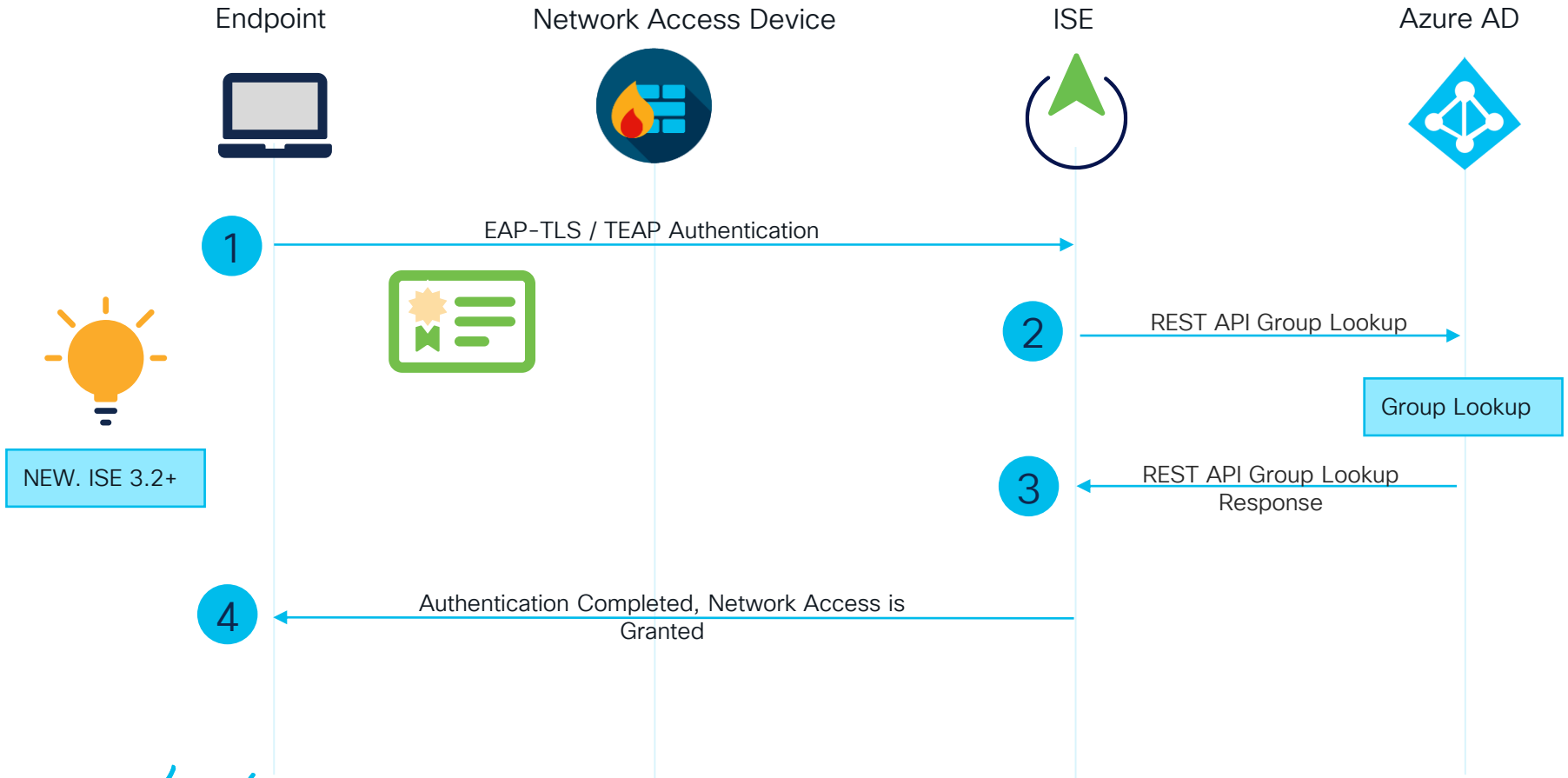
802.1x being a Layer 2 authentication protocol, will grants Network Access after Authentication is completed

No Access Before Authentication

ROPC Flow Diagram



EAP-TLS Authorization with Azure Active Directory

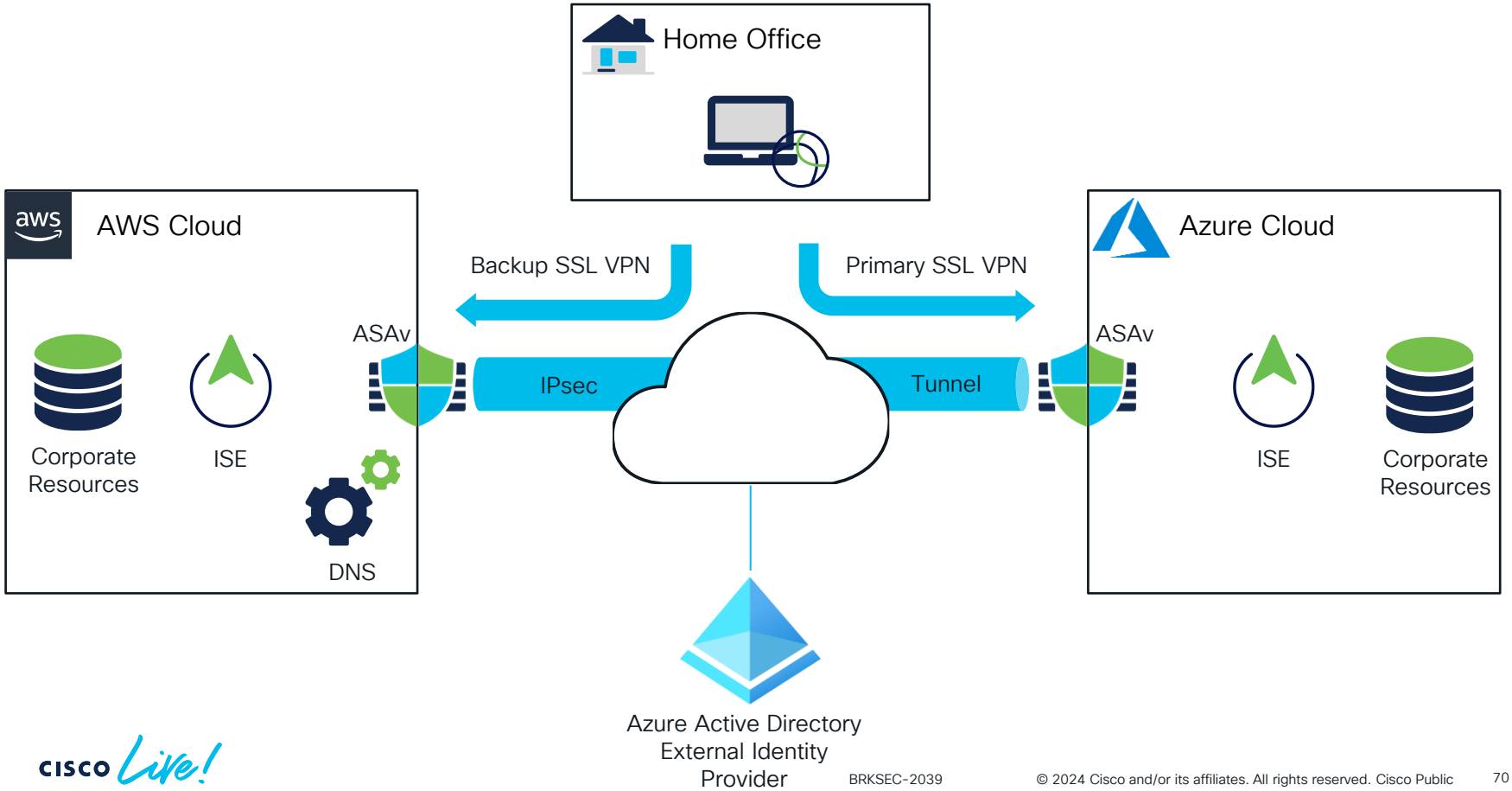


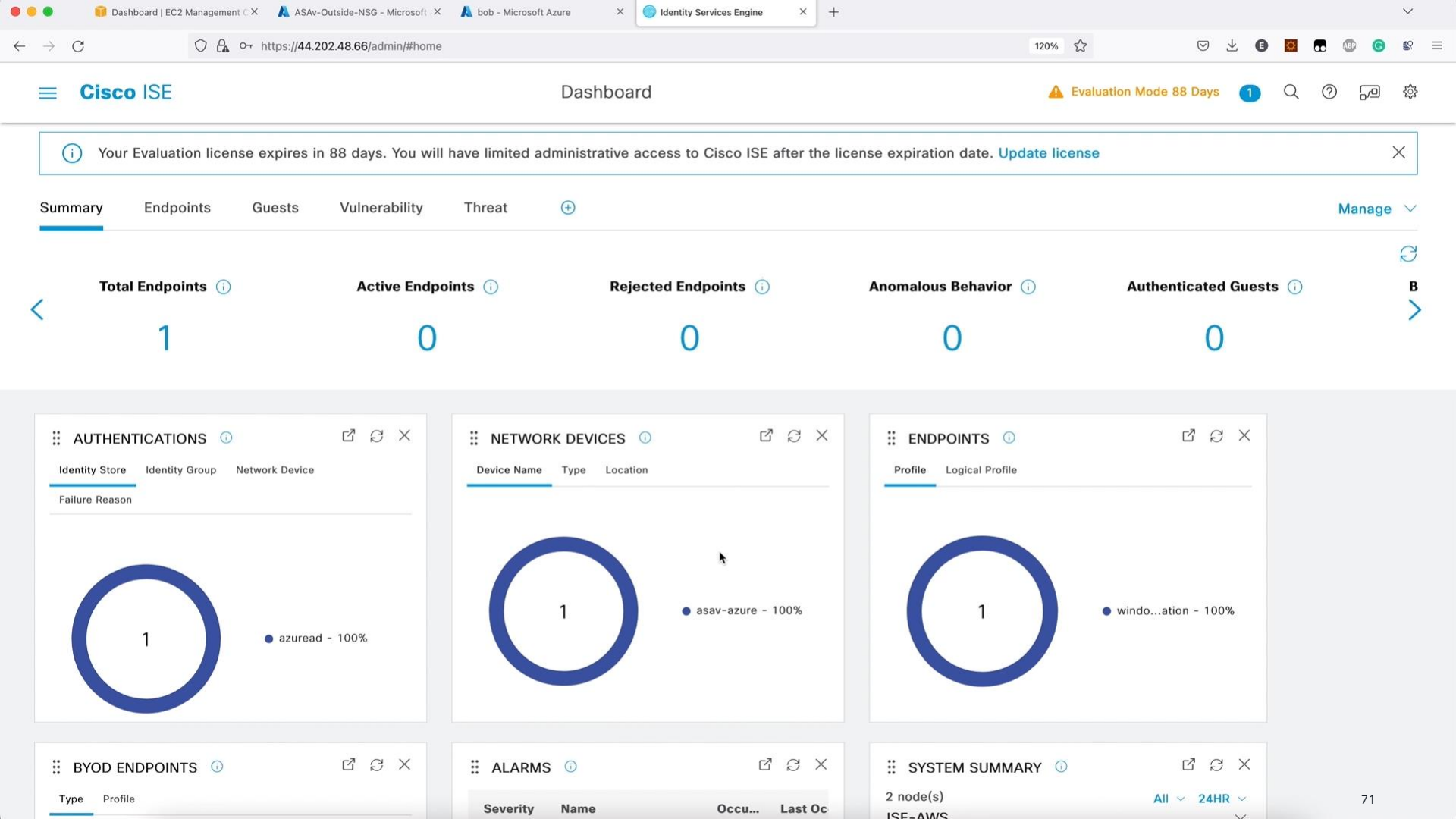
ROPC Limitations

- No user interactions allowed for password changes, MFA, or AUPs
- No new accounts that have not yet changed the default password
- Azure AD tenants and accounts only. No invited personal accounts or federated IdPs like Microsoft, Google+, Twitter, AD-FS, Facebook
- Only user authentication is supported

Demo. Remote Access VPN Authentication with Azure Active Directory

Deployment Topology




Dashboard | EC2 Management
ASAv-Outside-NSG - Microsoft
bob - Microsoft Azure
Identity Services Engine
https://44.202.48.66/admin/#home
120%
Cisco ISE
Dashboard
Evaluation Mode 88 Days
1
Your Evaluation license expires in 88 days. You will have limited administrative access to Cisco ISE after the license expiration date. Update license
Summary
Endpoints
Guests
Vulnerability
Threat
Manage
Total Endpoints
1
Active Endpoints
0
Rejected Endpoints
0
Anomalous Behavior
0
Authenticated Guests
0
AUTHENTICATIONS
Identity Store
Identity Group
Network Device
Failure Reason
1
azuread - 100%
NETWORK DEVICES
Device Name
Type
Location
1
asav-azure - 100%
ENDPOINTS
Profile
Logical Profile
1
windo...ation - 100%
BYOD ENDPOINTS
Type
Profile
ALARMS
Severity
Name
Occu...
Last Oc
SYSTEM SUMMARY
2 node(s)
All
24HR
ISE-AWS

Conclusion

Key Takeaways

- ISE can be deployed natively on AWS, Azure, OCI
- SAML SSO is available on ISE for Portals (Admin, Guest, Sponsor, etc.)
- 802.1X authentications, RA VPN authentications are possible with Azure Active Directory as an External Identity Store


cisco
The bridge to possible
Thank you
cisco Live!


cisco Live!
Let's go