



The bridge to possible

Zero Touch Provisioning & Config Management of Cisco FTD in Azure using Terraform & Ansible

Madhuri Dewangan, Security Consulting Engineer
@madhuri_1507

Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated until February 24, 2023.

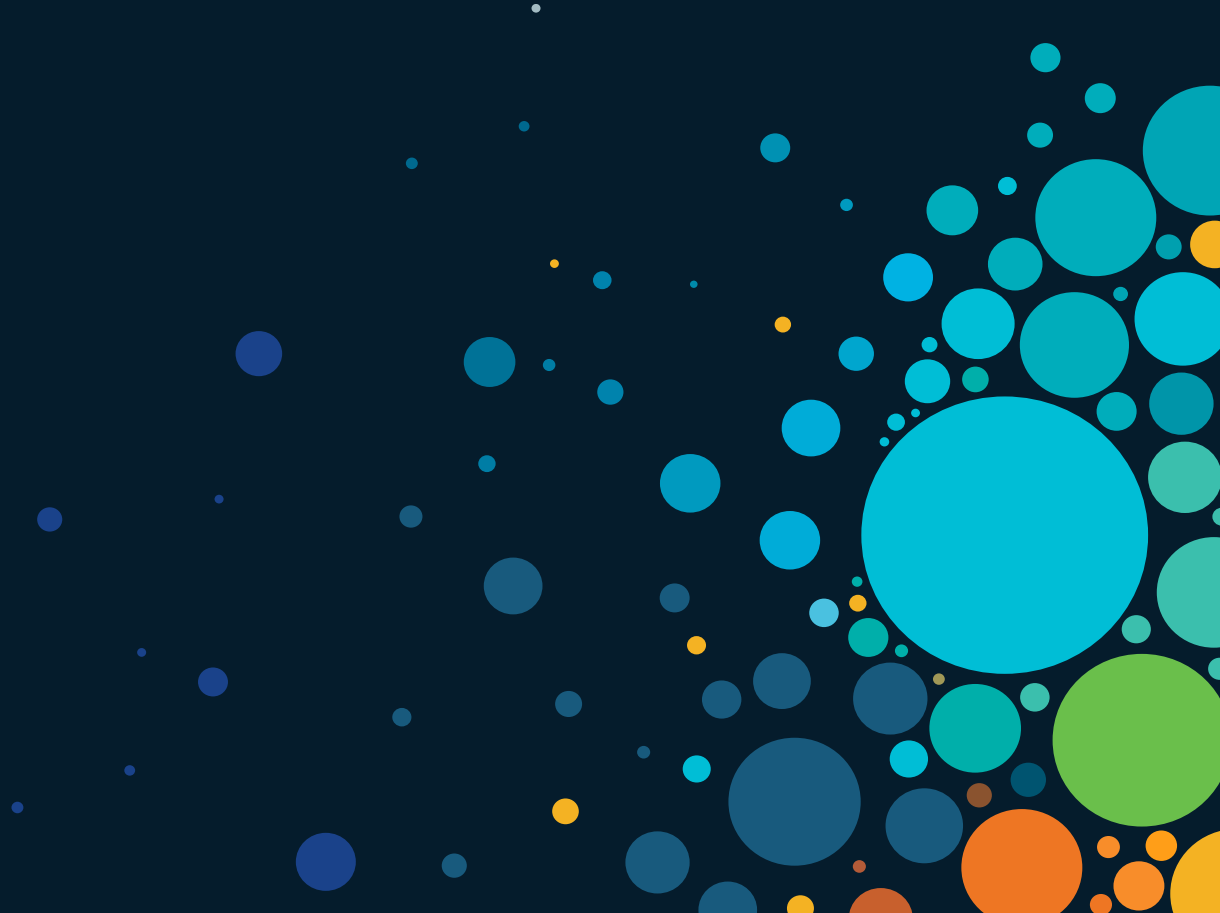




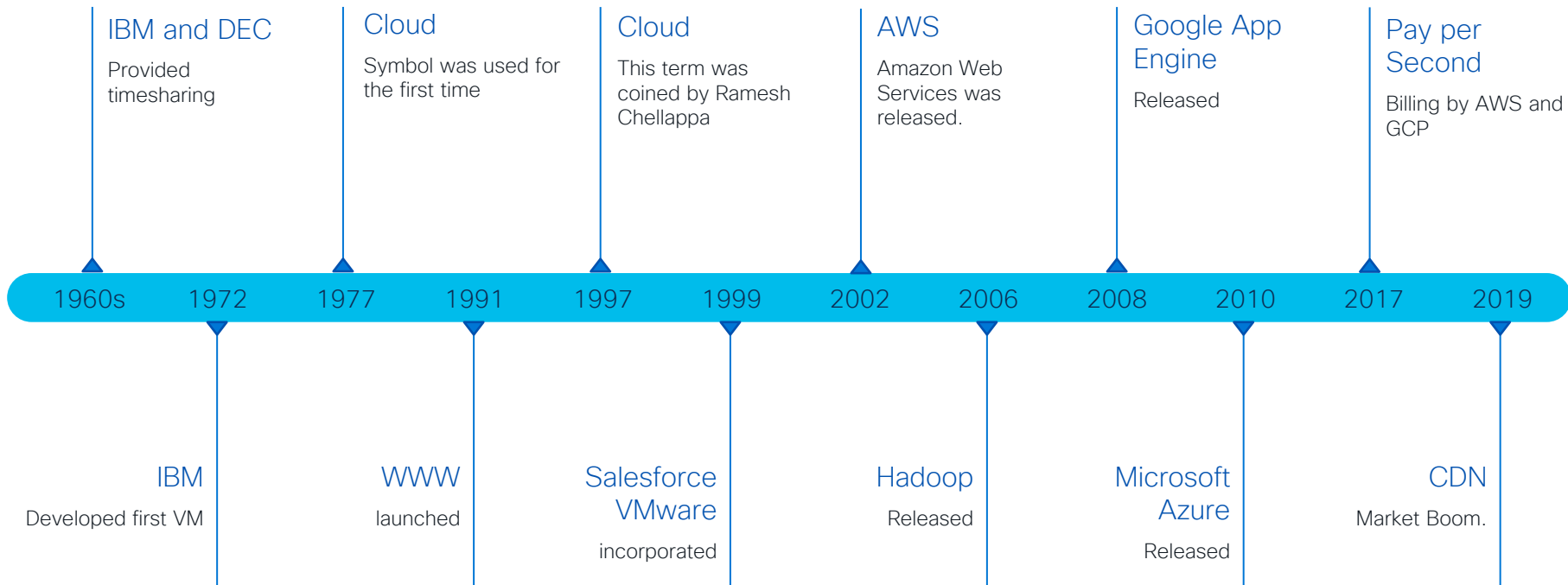
Agenda

- Evolution of Computing
- Introduction to Public Cloud
- Why Automation
- See the Difference
- Magic of Automation
- Conclusion

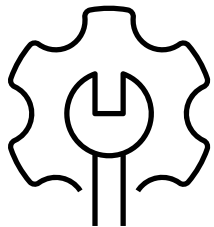
History of Computing



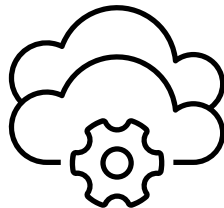
How Cloud Computing Evolved..



Why is Cloud needed?



Offload Resource
Maintenance



On-Demand
Scale-In and
Scale-Out

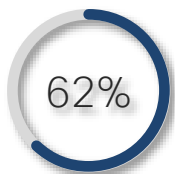


Cost Reduction

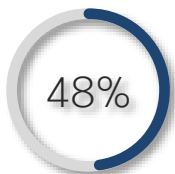
Market Trend & Benefits of Public Cloud



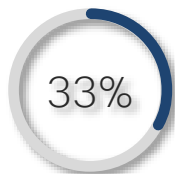
Trends of Cloud Movement in 2021



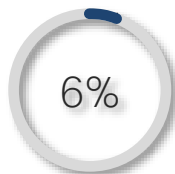
Amazon Web Service



Microsoft Azure



Google Cloud Platform



Oracle Cloud



IBM Cloud



Alibaba Cloud



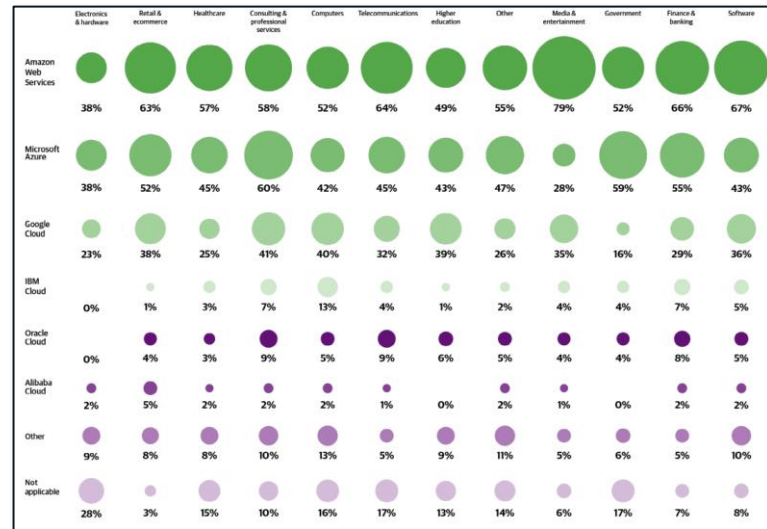
Others



Not Applicable

Market Research on Cloud Usage

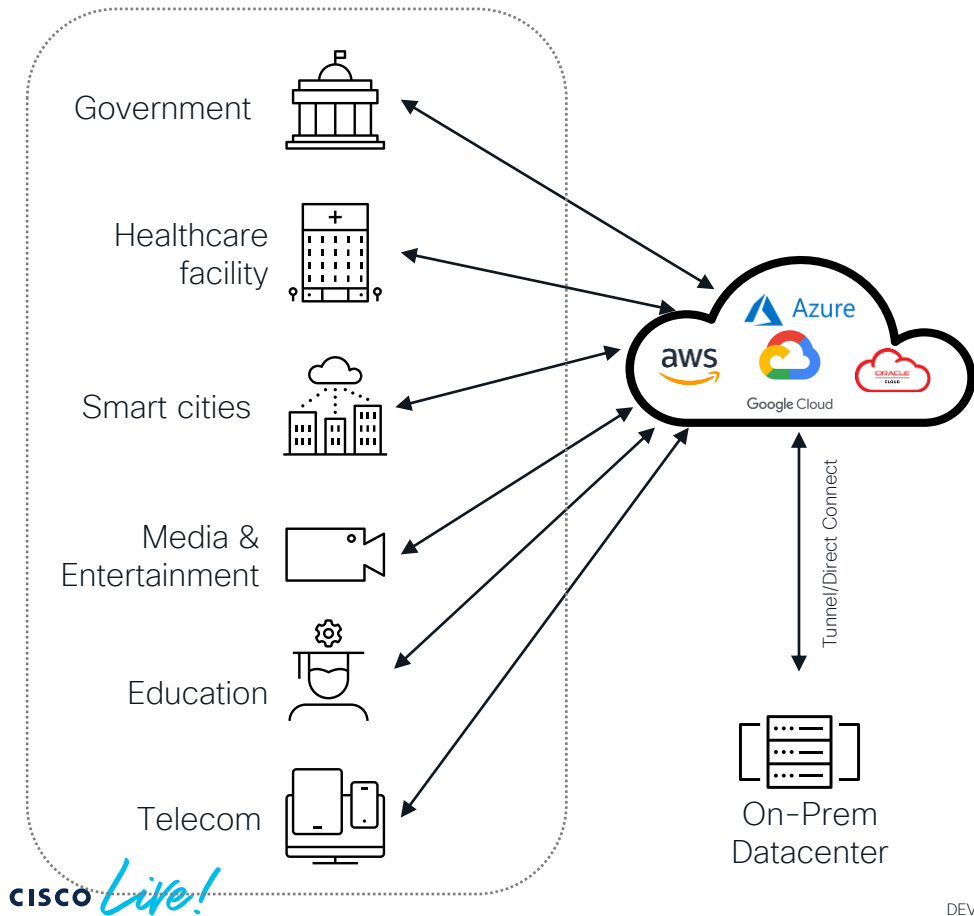
Usage of different cloud types in different vertical



Usage of various platforms in different vertical

Source : https://get.oreilly.com/content-team_signup.html?allid=eyJpIjoVWVwdGFTQXhWZINBanVic2UiLCJ0IjoVWVVFZmRCY1JxMkpcL0h5MnZhVn

Benefits of Public Cloud



Scalability

Scale-In and Scale-Out

Cost Reduction

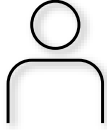
Pay per Use

Quick and Easy
Deployment

What is Quick and Easy Deployment?



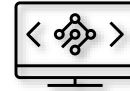
How we can deploy VMs in Cloud



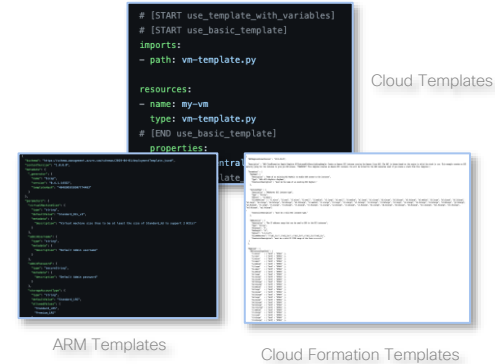
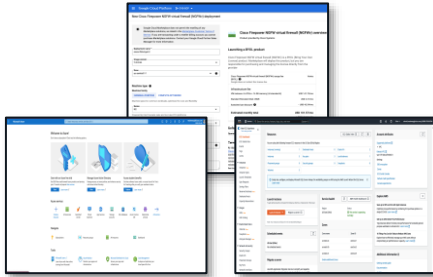
Manual



SDK



IaC



Pro & Cons of each Method

Manual

Pro

- Good for Learning
- Single VM build

Cons

- Multiple VM build is time consuming
- Design must be available
- Reverting back is difficult

SDK

Pro

- Fasten similar VM deployment
- Fastens VM edit

Cons

- Requires specialization
- Learning curve involved

laC

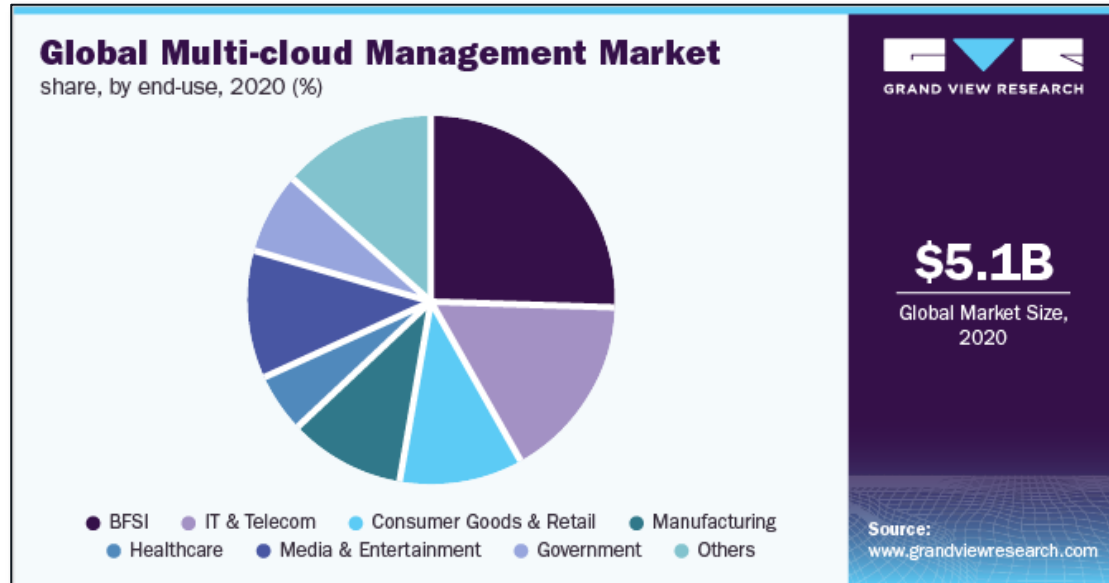
Pro

- Enable Re-use of code
- Fastens entire infra build
- Enables review & audit capability

Cons

- Every platform has its own laC format
- Requires specialization

Need for Multi-Cloud Reality Check



Source : <https://www.grandviewresearch.com>

Expectation from Infrastructure as Code

Reduced
Learning Curve

Single Template
Format

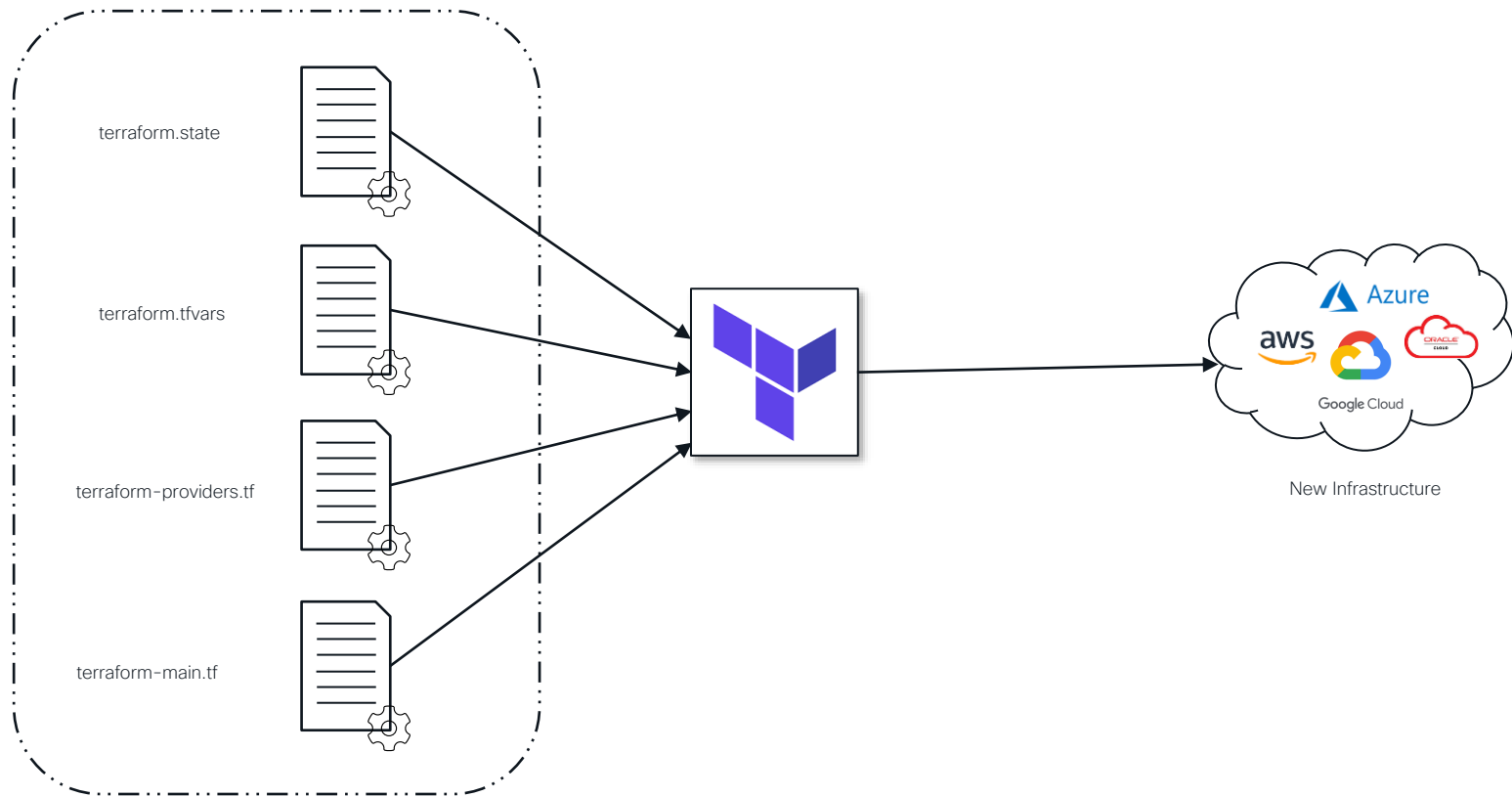
Enhanced
Productivity and
Accuracy

Ability to
Connect
Multiple Cloud

Versioned,
Review & Audit
Capability

Quick Build &
Destroy

Terraform



terraform.tfstate

- Store bindings between objects in a remote system and resource instances declared in configuration.
- Maintains state of managed infrastructure and configuration.
- Used to create plans and make changes.
- Refreshes on every operation.

```
{
  "version": 4,
  "terraform_version": "0.12.26",
  "serial": 370,
  "message": "705d9f6c-c425-405f-4395-c08ac46c23c",
  "outputs": {},
  "resources": [
    {
      "mode": "managed",
      "type": "aws_subnet",
      "name": "management",
      "provider": "provider.aws",
      "instances": [
        {
          "schema_version": 1,
          "attributes": {
            "arn": "arn:aws:ec2:us-east-2:366697986784:subnet/subnet-00276caa171bbefda",
            "assign_ipv6_address_on_creation": false,
            "availability_zone": "us-east-2a",
            "availability_zone_id": "use2-az1",
            "cidr_block": "10.50.2.0/24",
            "customer_owned_ipv4_pool": "",
            "id": "subnet-00276caa171bbefda",
            "ipv6_cidr_block": "",
            "ipv6_cidr_block_association_id": "",
            "map_customer_owned_ip_on_launch": false,
            "map_public_ip_on_launch": true,
            "outpost_arn": "",
            "owner_id": "366697986784",
            "tags": [
              {
                "Name": "Management"
              }
            ],
            "tags_all": [
              {
                "Name": "Management"
              }
            ],
            "timeouts": null,
            "vpc_id": "vpc-011ec5a1b2eeaa821b"
          }
        }
      ]
    },
    {
      "mode": "managed",
      "type": "aws_vpc",
      "name": "test-vpc",
      "provider": "provider.aws",
      "instances": [
        {
          "schema_version": 1,
          "attributes": {
            "arn": "arn:aws:ec2:us-east-2:366697986784:vpc/vpc-011ec5a1b2eeaa821b",
            "assign_generated_ipv6_cidr_block": false,
            "cidr_block": "10.50.0.0/16",
            "default_network_acl_id": "acl-0498cb17506a6668",
            "default_route_table_id": "rtb-06691bd813384e312",
            "default_security_group_id": "sg-03664b13d8ac3a52e",
            "dhcp_options_id": "dopt-094353910c2986e65",
            "enable_classiclink": false,
            "enable_classiclink_dns_support": null,
            "enable_dns_hostnames": true,
            "enable_dns_support": true,
            "id": "vpc-011ec5a1b2eeaa821b",
            "instance_tenancy": "default",
            "ipv6_association_id": "",
            "ipv6_cidr_block": "",
            "main_route_table_id": "rtb-06691bd813384e312",
            "owner_id": "366697986784",
            "tags": [
              {
                "Name": "test-vpc"
              }
            ],
            "tags_all": [
              {
                "Name": "test-vpc"
              }
            ],
            "private": "eyJzY2h8WFRlMmVyc2VubG9jEjQ=="
          }
        }
      ]
    }
  ]
}
```



Will initial execution of terraform operation have a state file?

terraform.tfvars

- Variable definition files
- **Consists of variable name assignments**
- Can be named as .tfvars, .tfvar.json, .auto.tfvars and .auto.tfvars.json

```
image_id = "ami-abc123"  
availability_zone_names = [  
    "us-east-1a",  
    "us-west-1c",  
]
```



Others ways of defining the variable in terraform

terraform-provider.tf

- Allows Interaction with Cloud providers, SaaS provider and other API endpoints
- Single template can have multiple providers

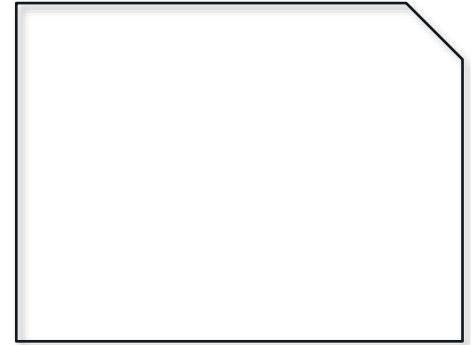
```
#####  
# Cloud Provider details; AWS  
#####  
provider "aws" {  
  profile  = "default"  
  region   = var.region  
  access_key = "XXXXXXX"  
  secret_key = "YYYYYYYY"  
}
```



If we don't define provider in template, how will terraform execute?

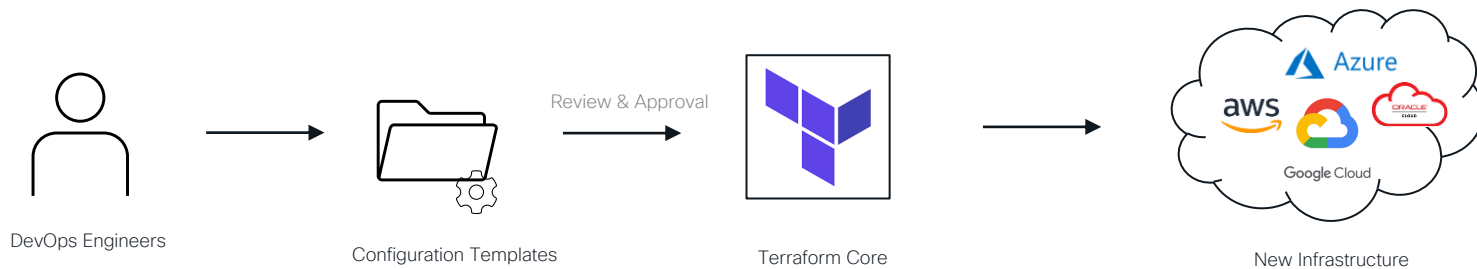
terraform-main.tf

- **Main set of configuration for module.**
- Defines the resources to be created.



If we don't define provider in template, how will terraform execute?

How this works?



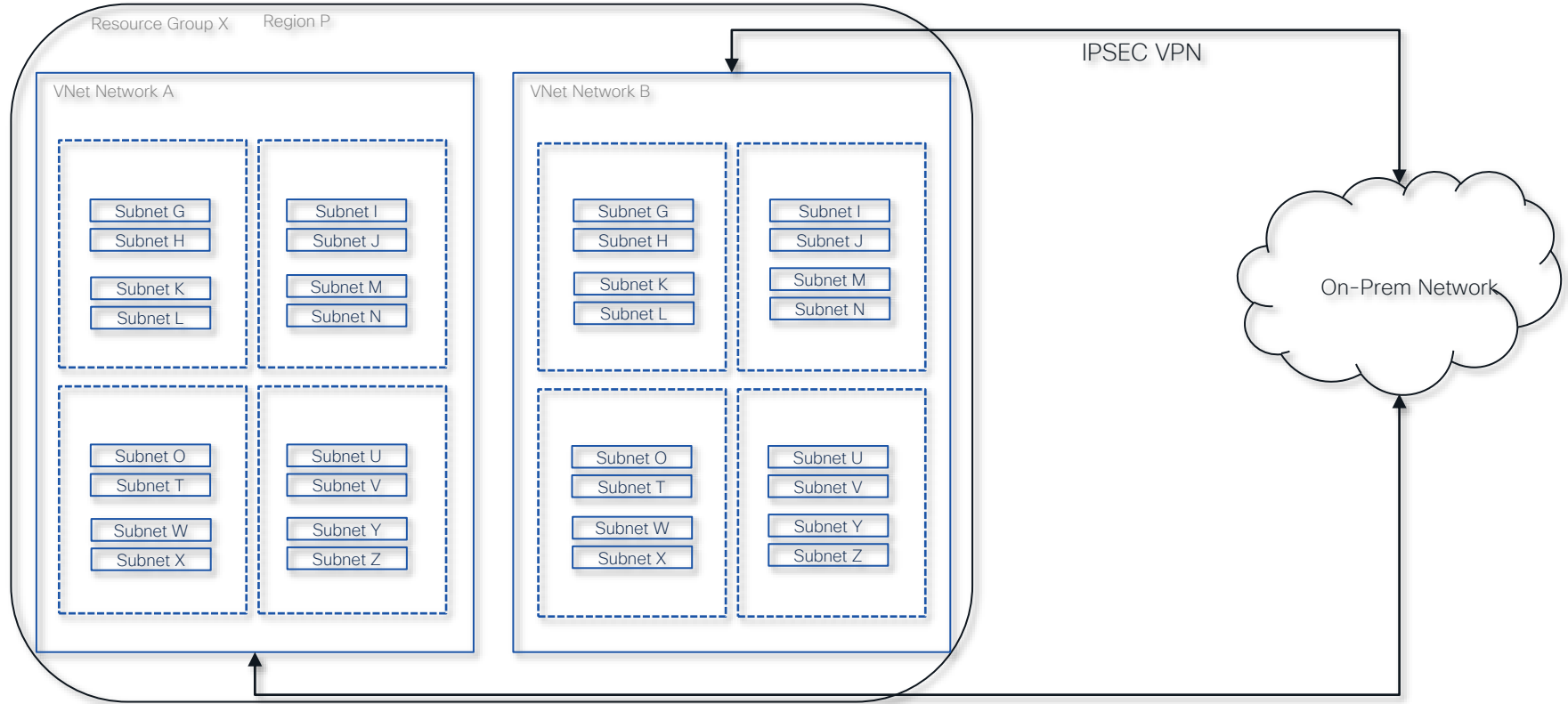
Basics of Public Cloud



Basic Terminology in Azure

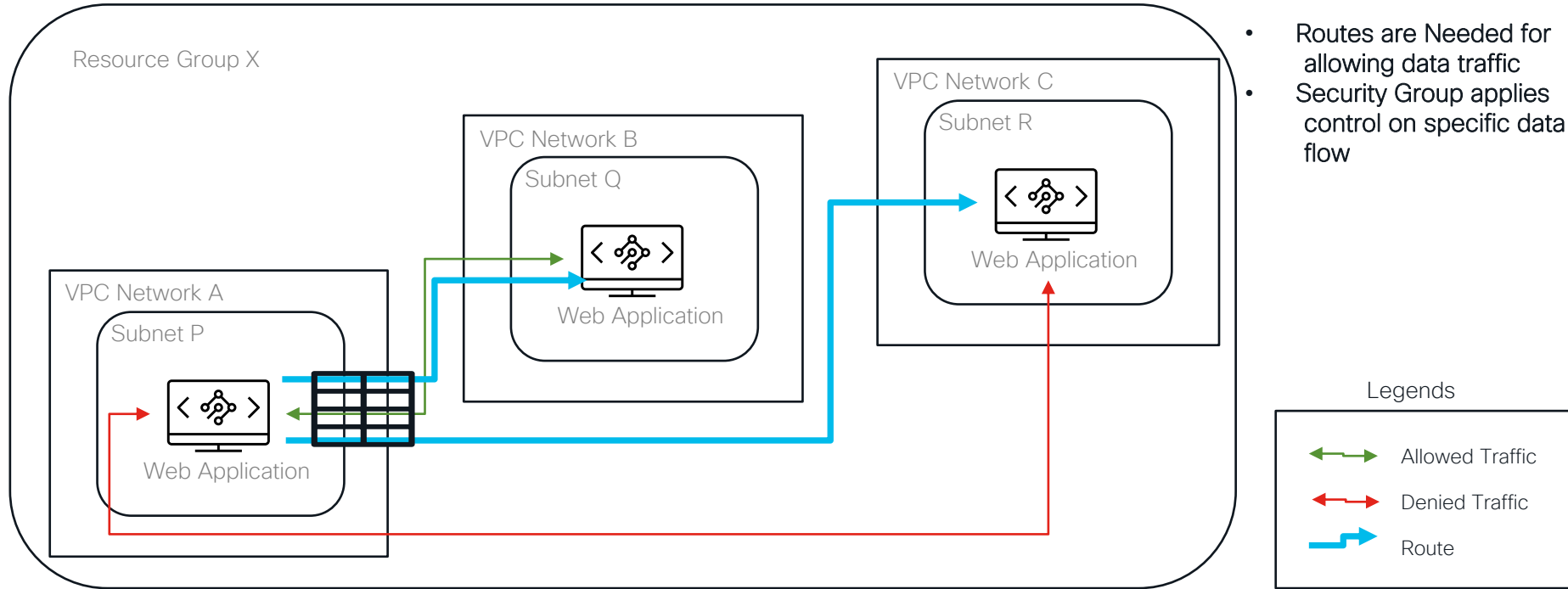
1. Subscription
2. Resource Group
3. VNet
4. Subnet
5. Security Group
6. Route

How is Public Cloud Networking is organized?



For Further Reading on On-Prem connectivity : <https://cloud.google.com/anthos/clusters/docs/on-prem/1.4/concepts/connect-on-prem-gcp>

What are Security Groups and Routes in Azure ?



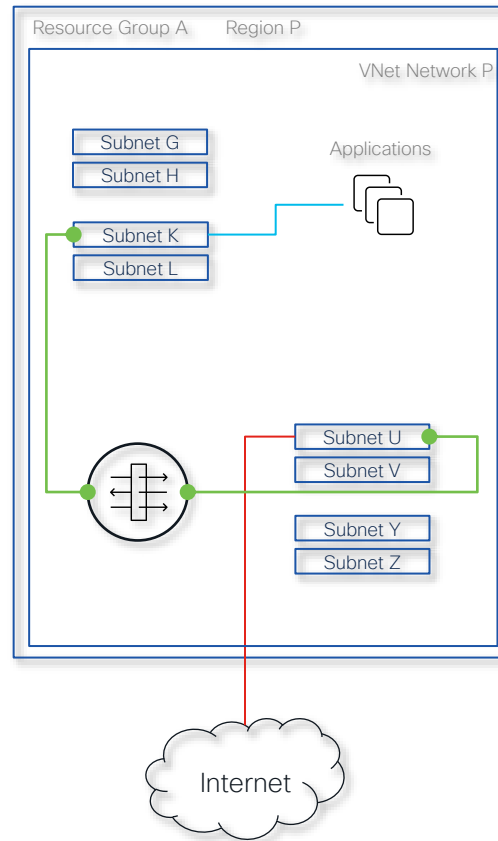
Secure Firewall in Azure and its Automation



Need to Build Secure Firewall in Azure

Use Cases:

- Next Generation Firewall Features
- URL Filtering/AMP Integrations
- RA VPN / S2S VPN
- Traffic Visibility



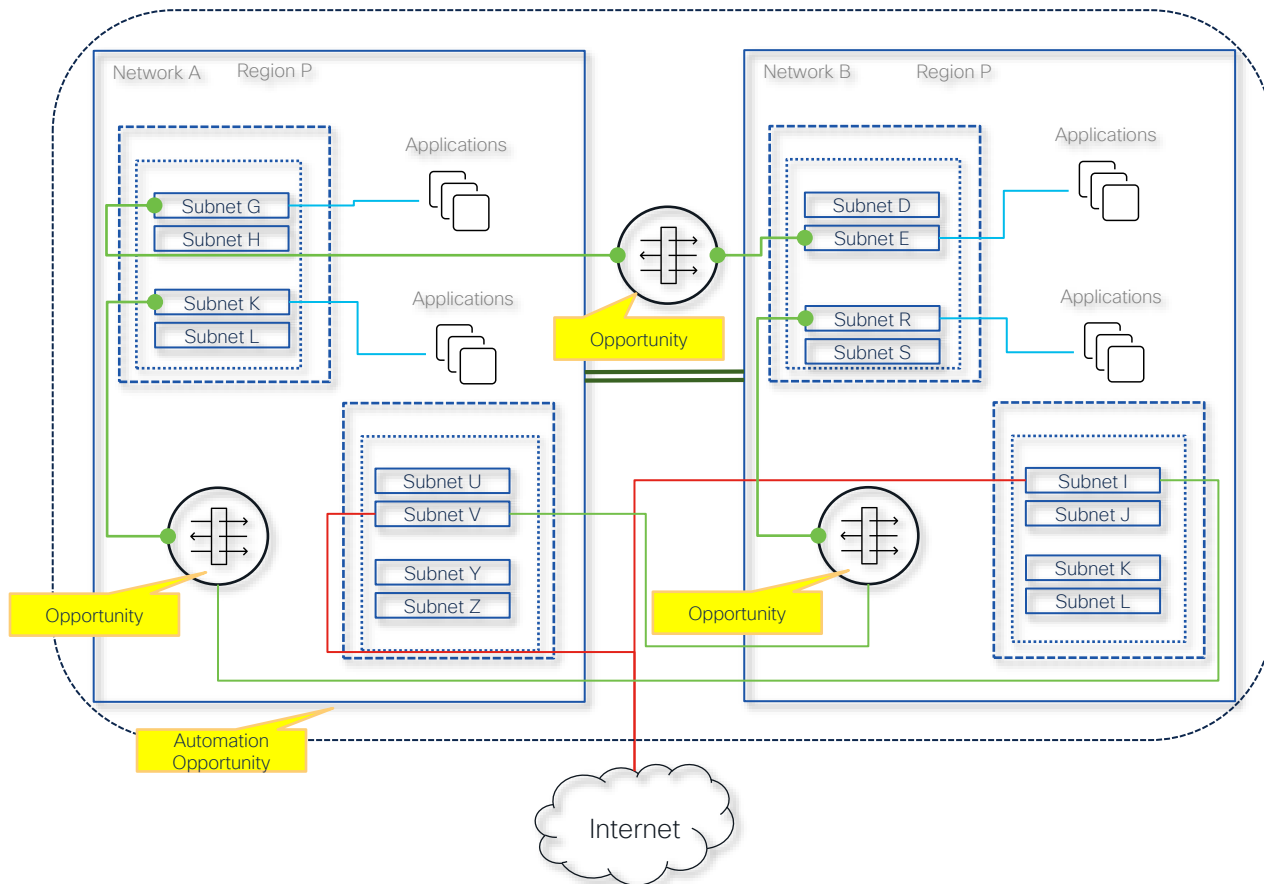
Role of Automation

Use Cases:

- Multiple Firewalls required
- Instant Build Requests
- Repeatable Activity
- Ensure Deployment Policy

Benefits:

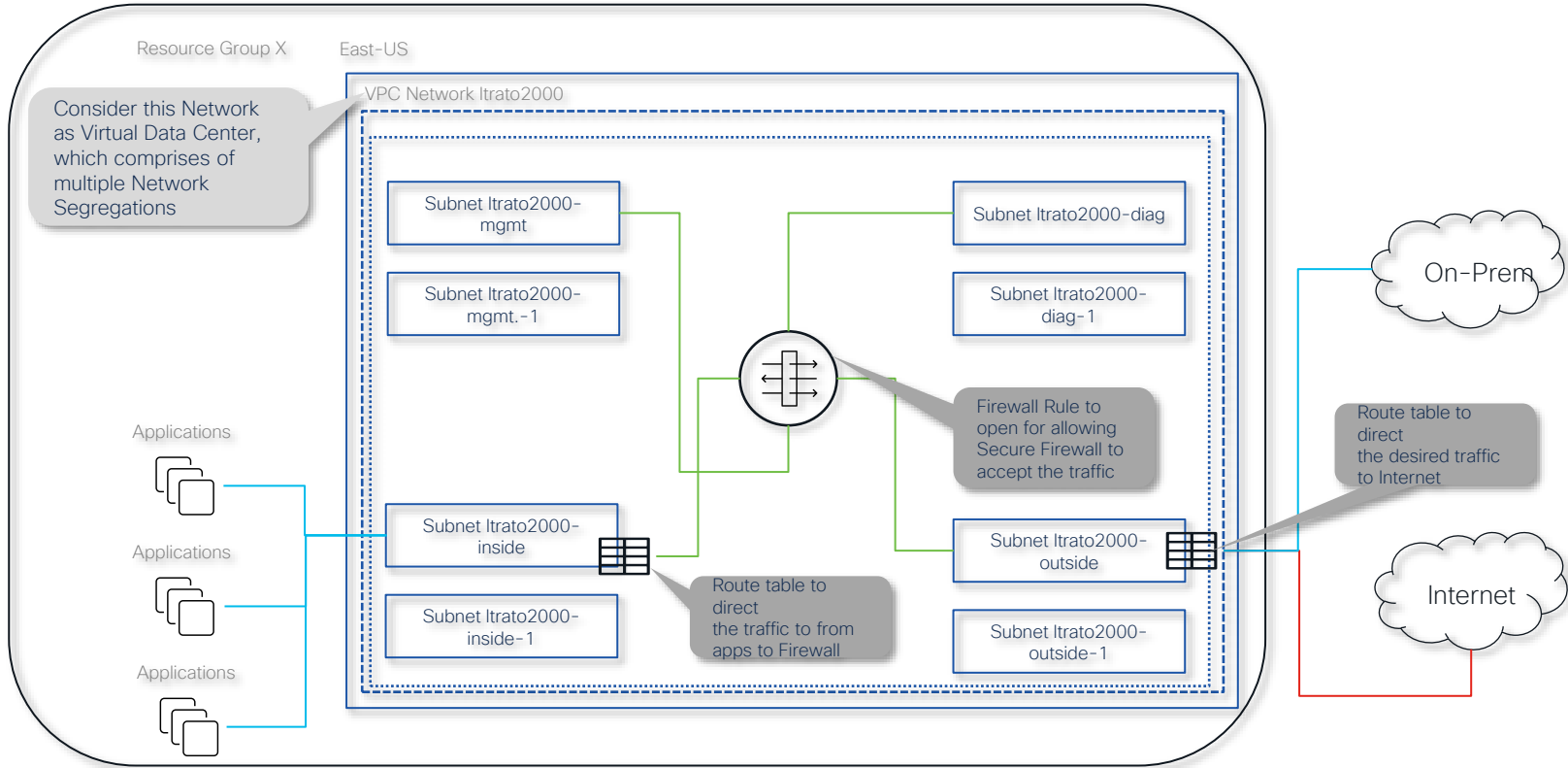
- Time Saving
- Cost Reduction
- Re-Use of asset
- Enforce Review and Audit



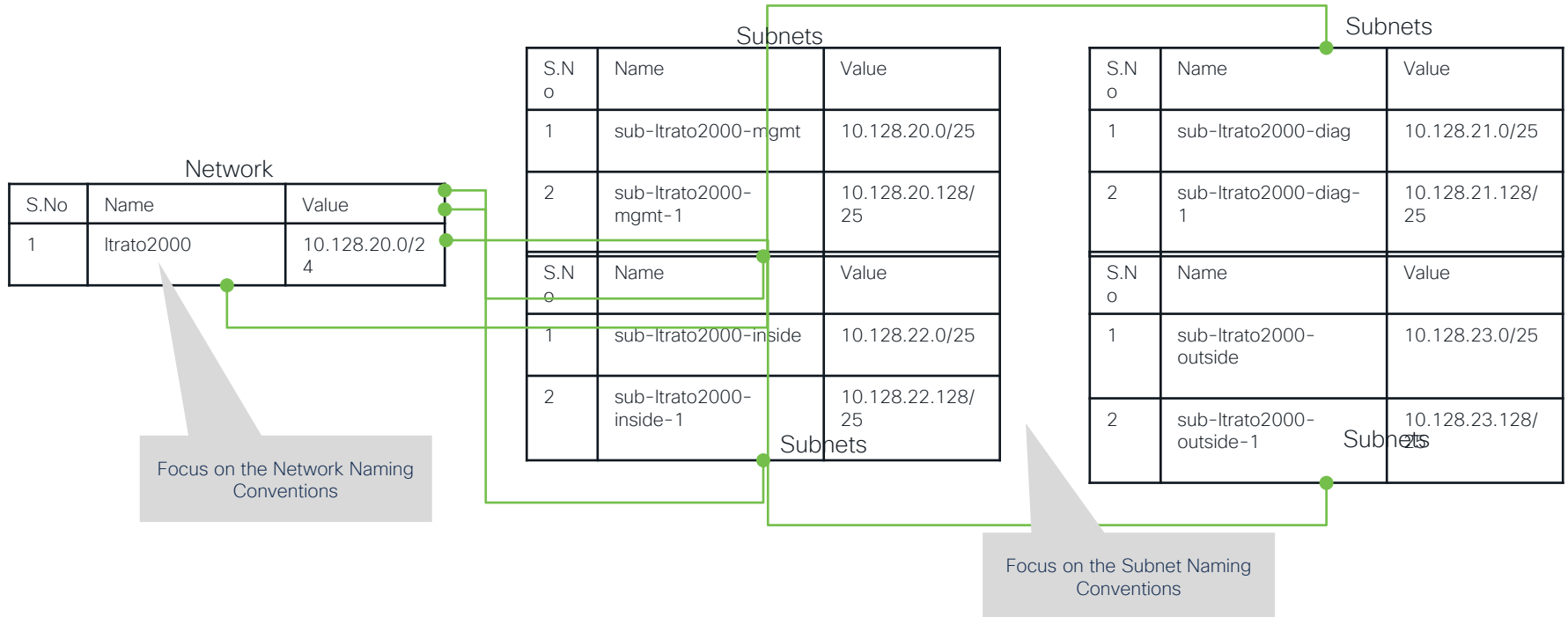
Let's Build Secure Firewall in Azure



Step -1 Planning

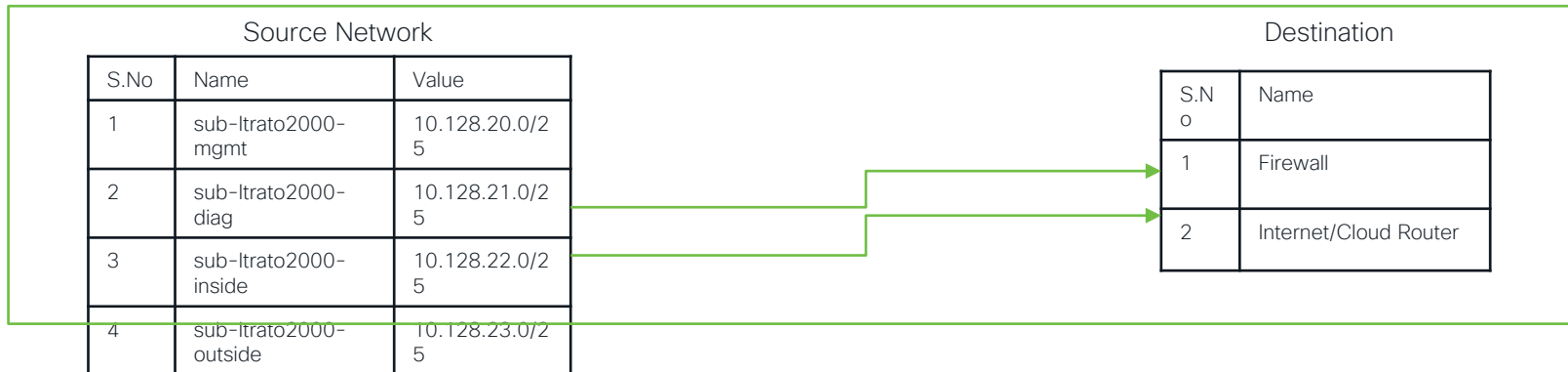


Step -2a Detailing- Networks



Step -2b Detailing- Firewall Rules and Routes

Routes



Firewall Rules

S.No	Resource	Traffic	Network
1	Firewall	All traffic	ltrato2000-inside
2	Firewall	All traffic	ltrato2000-outside
3	Firewall	tcp 8305, tcp 22, tcp 443, tcp 80	ltrato2000-mgmt

What we need from Terraform Template?

A Template should:

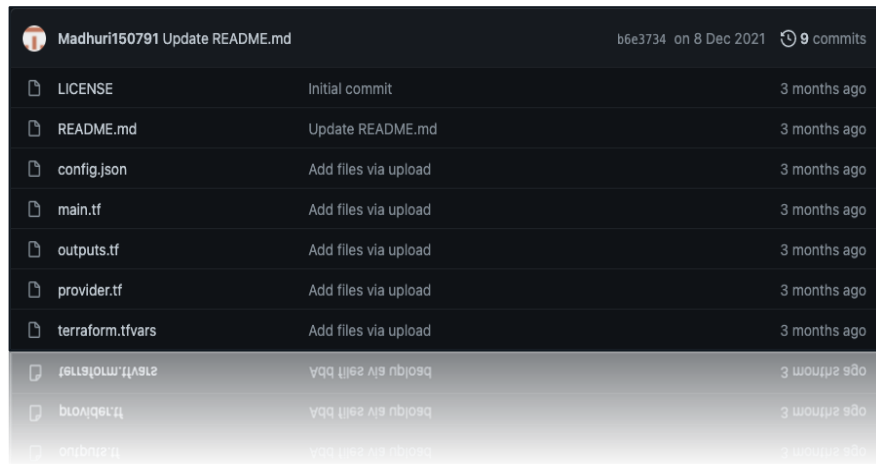
- Create the required Network
- Create the required Subnets
- Create Routes for Traffic flow
- Allow Firewall Rules
- Read through Image IDs of Cisco Secure Firewall
- Deploy the Firewall as per topology



Step -3a Create Terraform Templates

Structure configuration files:

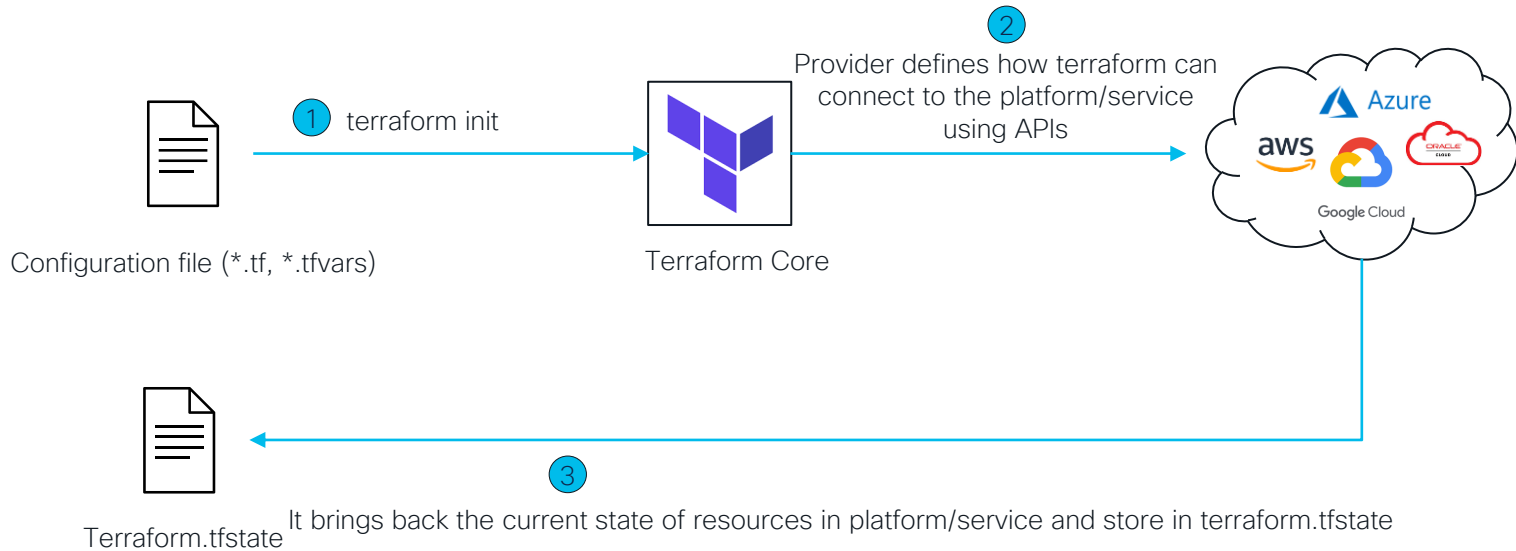
- Keep all variables in `terraform.tfvars`
- Move the provider out of main file in `provider.tf`
- Move each resource in separate file as `network.tf`, `route.tf`, `ftd.tf`, `fmc.tf` and store the resource id



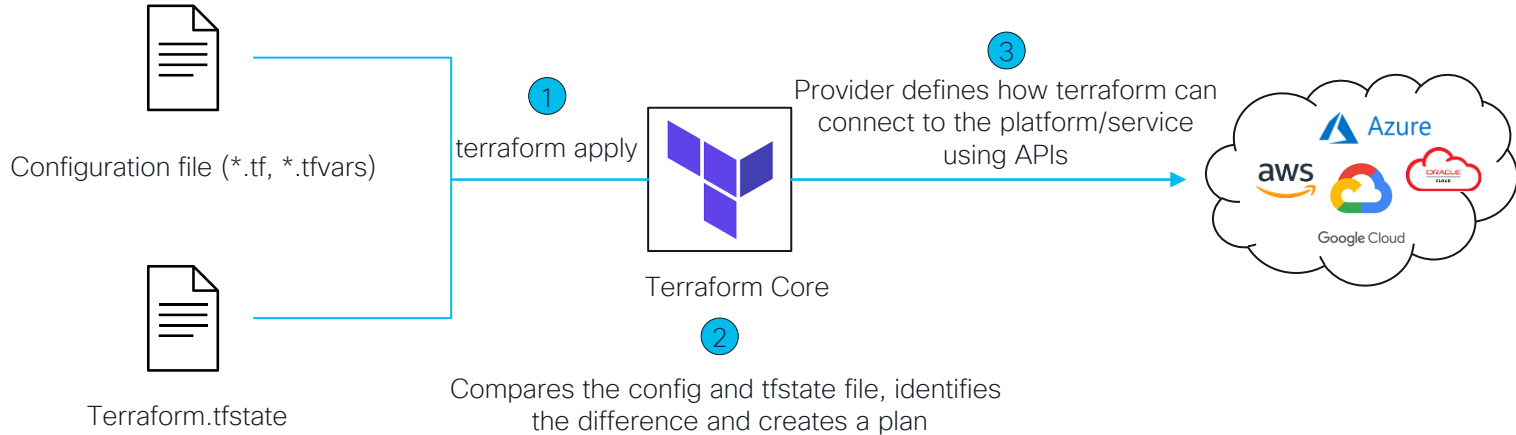
Madhuri150791 Update README.md		
b6e3734 on 8 Dec 2021 9 commits		
LICENSE	Initial commit	3 months ago
README.md	Update README.md	3 months ago
config.json	Add files via upload	3 months ago
main.tf	Add files via upload	3 months ago
outputs.tf	Add files via upload	3 months ago
provider.tf	Add files via upload	3 months ago
terraform.tfvars	Add files via upload	3 months ago
terraform.tfvars	Add files via upload	3 months ago
provider.tf	Add files via upload	3 months ago
outputs.tf	Add files via upload	3 months ago

Working of Terraform Template

(No tfstate is present)



Working of Terraform Template(tfstate is present)



Summary of Part 1

Summary

Market Trends of Public Cloud

Market Trends of Multi Cloud

Basics of Public Cloud

Need for Automation

Terraform Basics & Workflow

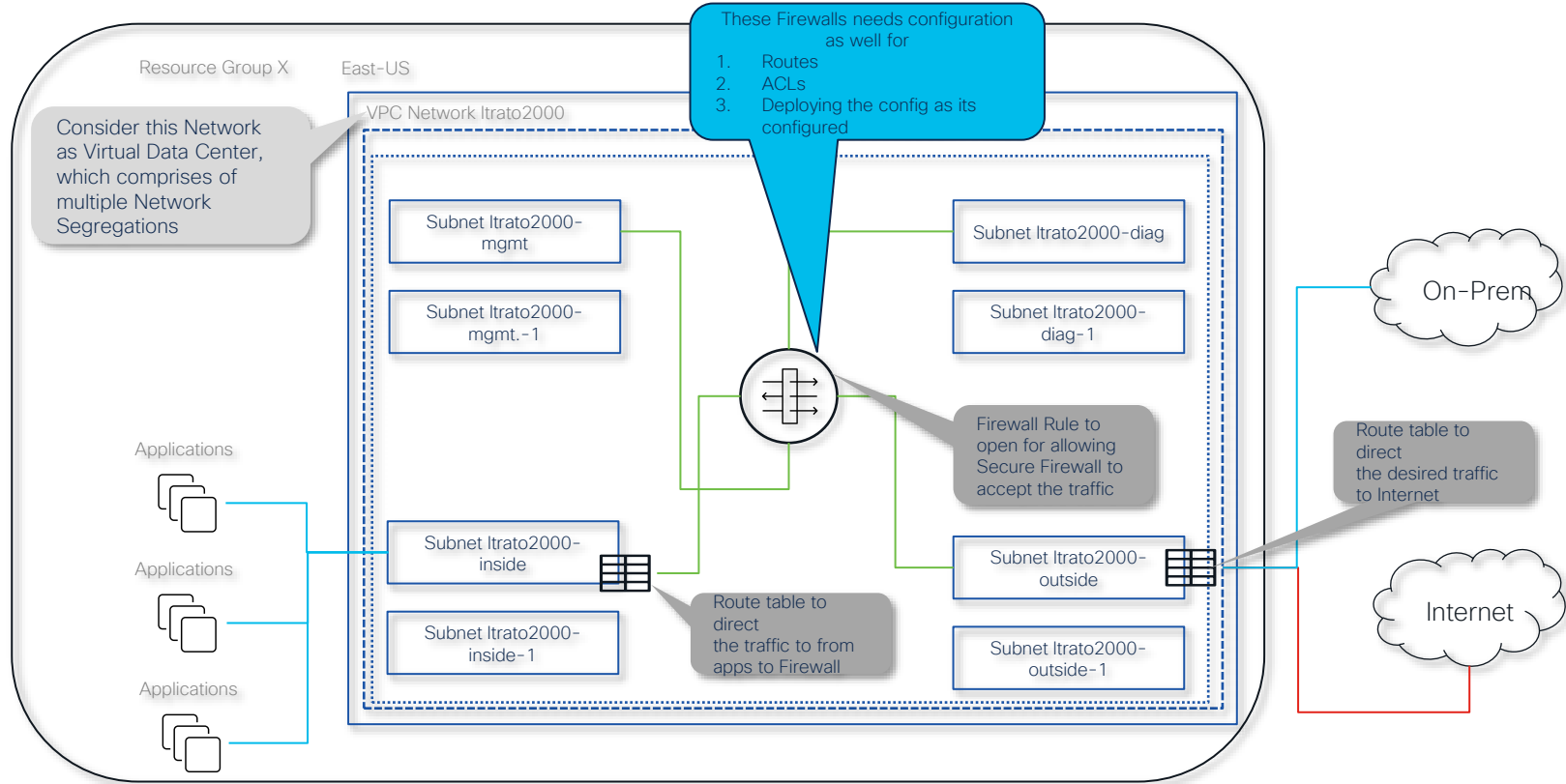
Cisco Secure Firewall Build



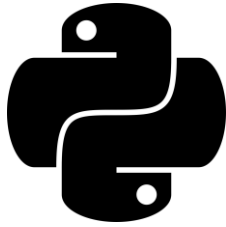
Automated Configuration Management of Cisco Secure Firewall



Configuration Required?



Different ways to Automate Configuration



Python

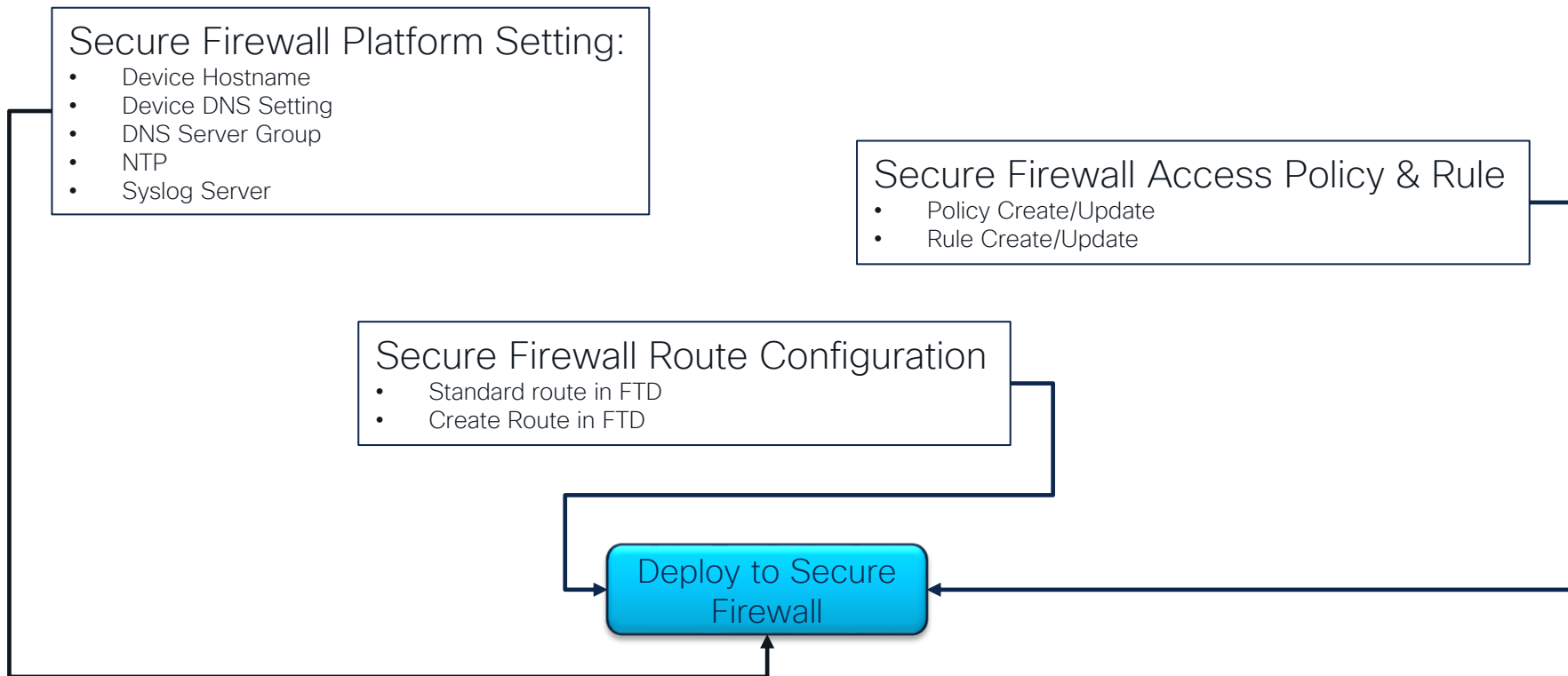


Ansible

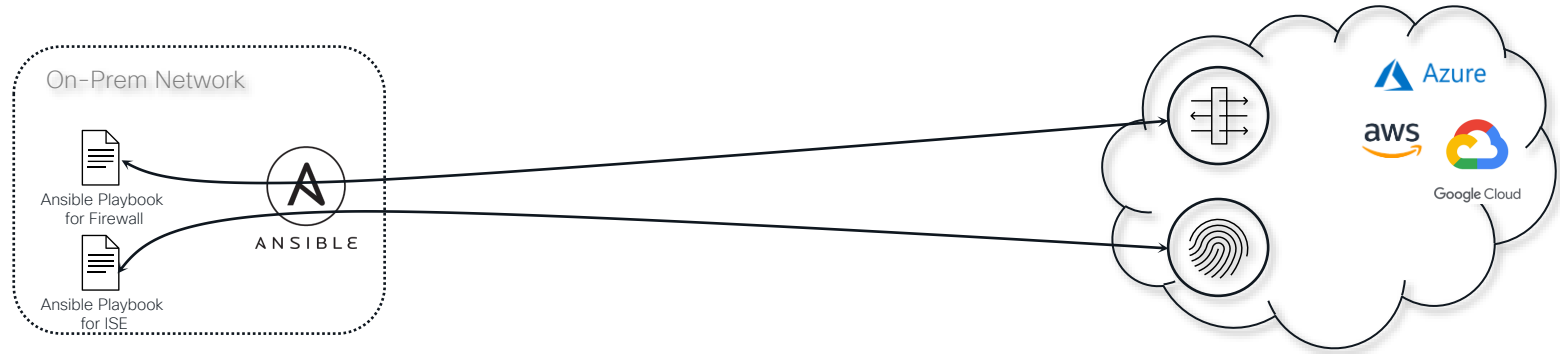


Terraform

Configuration Management Use cases

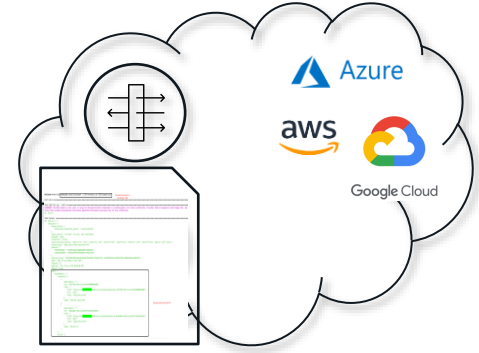
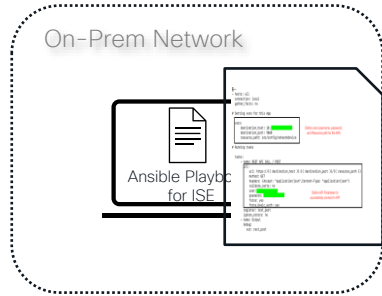


Configuration Management Using Ansible



- Ansible is geared towards configuration management.
- With Ansible, basic necessity of what changes made, is provided by default.

How it works?



- Ansible is geared towards configuration management.
- With Ansible, basic necessity of what changes made, is provided by default.

Demo

Summary of Part 2

Summary

Need for Configuration
Management

Ways of Configuration
Management

Ansible Workflow

Demo





The bridge to possible

Thank you

CISCO *Live!*

Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at <https://www.ciscolive.com/emea/learn/sessions/session-catalog.html>



Continue Your Education



Visit the Cisco Showcase for related demos.



Book your one-on-one Meet the Engineer meeting.



Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.



Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.

CISCO *Live!*

ALL IN