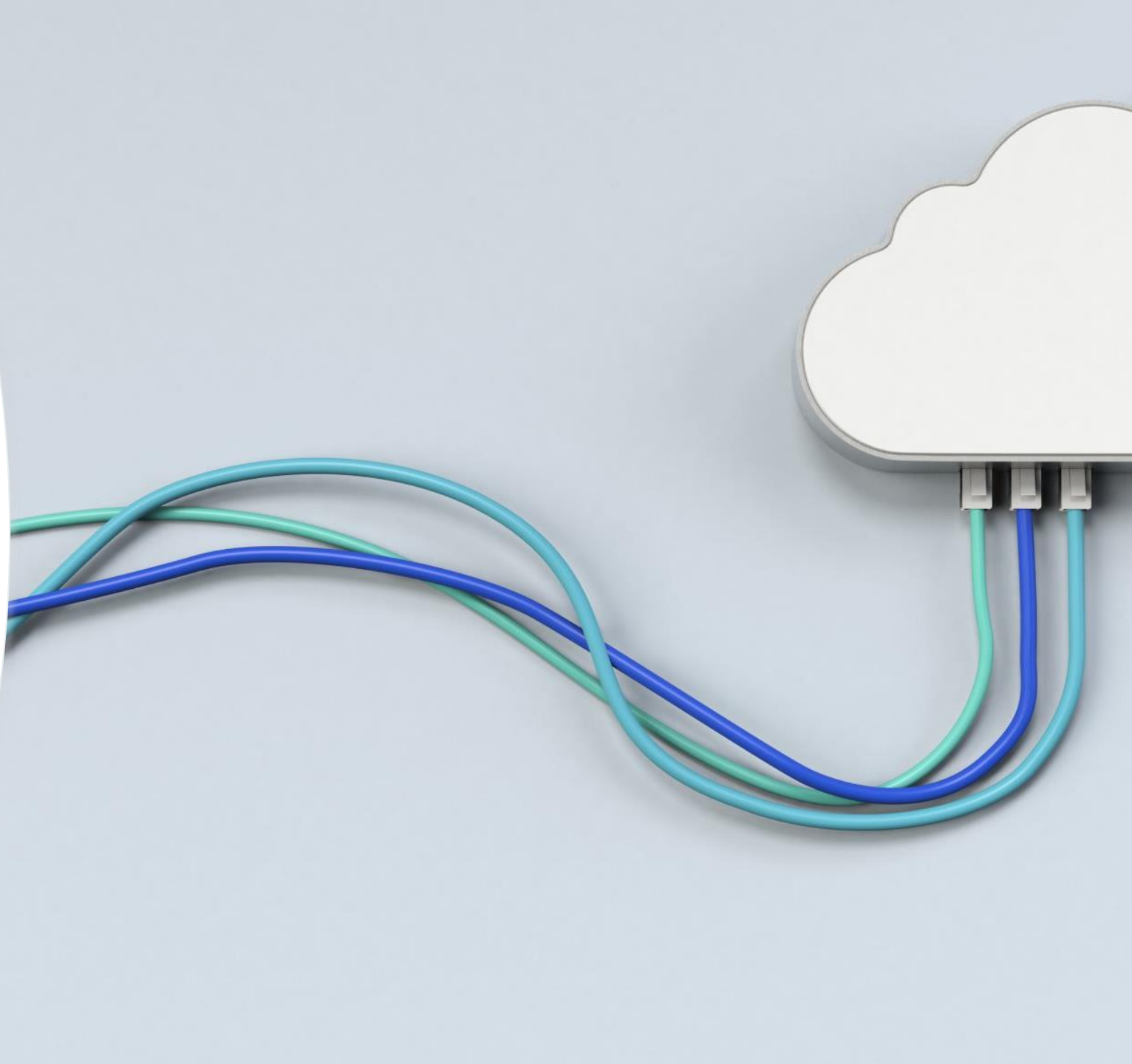
Group 4 Case Study



Group Members

W A Shadman

Sumeet Kaur Saund

Noorpreet Gill

Arshjot Ghuman

Vi Le

Austin Chapdelaine

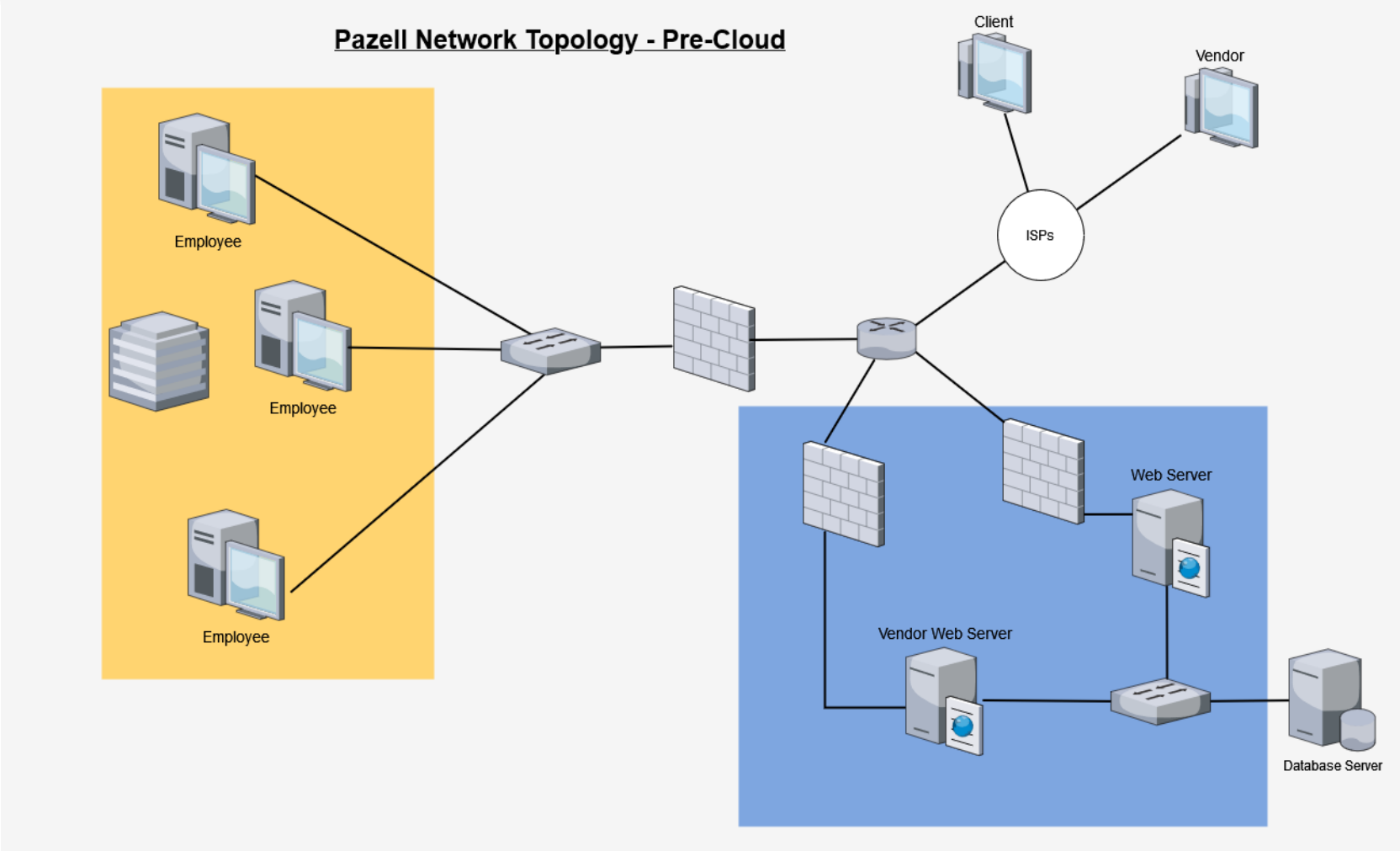
Abstract

Pazell is a major supply chain logistics provider which offers an end-to-end portfolio of solutions that includes warehousing & distribution, transportation logistics, e-commerce fulfilment, last-mile delivery, reverse logistics, and innovative technology.

Pazell wants to migrate all its applications and database servers to the public cloud and use cloud storage to store company intangible assets such as trade secrets, patents, etc.

Our team aims to design and deploy secure cloud infrastructure, including virtual machines, cloud storage, and databases while implementing cloud security best practices, rules and regulatory compliance throughout the infrastructure.

Current Network Topology



Why AWS?

AWS has a large library of products with extensive documentation for all their products which allows users to better understand resources, design and implementation.

It is modular which allows users to choose specific services that will work with their products.

AWS is also scalable which is based on user traffic.

In addition, AWS has good end-user support for implementation and troubleshooting.

Cost Reduction

Asset	Type of Asset	Asset Value	Old System Monthly Cost	AWS Monthly Cost	Cost Reduction
Database servers	Equipment	320,000 USD	9,250 USD	6,235.26 USD	3,014.74 USD
Vendor Servers	Equipment	160,000 USD	3,083 USD	2,078.42 USD	1,004.91 USD
Public Application Server	Equipment	80,000 USD	3,083 USD	2,078.42 USD	1,004.91 USD
Server OS	Software	22,400 USD	41.66 USD	0 USD	41.66 USD
Switches	Equipment	80,000 USD	2,500 USD	0 USD	2,500 USD
Routers	Equipment	13,600 USD	166.66 USD	0 USD	166.66 USD
Firewalls	Software	21,798 USD	416.66 USD	0 USD	416.66 USD
Cloud Firewalls	Software/Hardware	Unknown	0 USD	4,759,50 USD	0 USD
	Total	697,798 USD	18,539.88 USD	15,151,60 USD	3,388.28 USD
				Total Cost Reduction %	18.27%

Cloud Security Best Practices

- Understanding the shared responsibility model.
- Establish And Enforce Cloud Security Policies.
- Implementing identity and access management.
- Protecting user endpoints.
- Encrypting data.
- Implementing intrusion prevention and intrusion detection.
- Conducting Audits And Penetration Testing.
- Maintaining logs and monitoring.

Regulatory Requirements (PCI DSS)

- PCI DSS Firewall Controls.
- Secure Key Management.
- Verifying AWS PCI Compliance with A PCI DSS Audit.

Defense in Depth Strategies

Defense in depth is a security strategy that involves the implementation of multiple layers of security controls to protect against potential security threats and attacks on the system.

The goal of defense in depth is to create a strong and resilient security posture that is capable of withstanding attacks and minimizing the impact of any successful breaches.

MFA, AWS CloudTrail, VPC, AWS WAF, AWS shield, Amazon CloudWatch etc.

Ingress rules

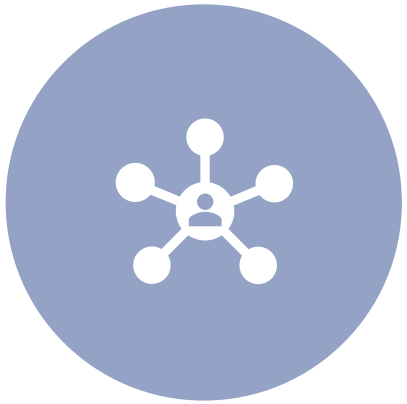
Check IP addresses are within the allowed range.

Only verified IP addresses can connect to the inner layer of cloud.

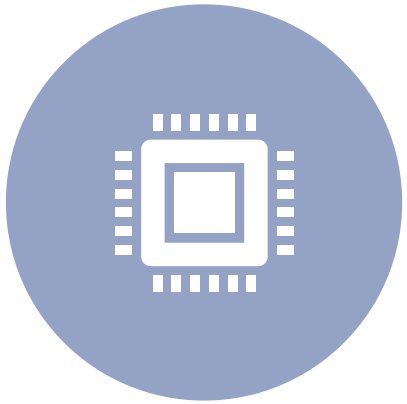
After the third unsuccessful connection to the cloud, that IP address will be blocked by a cloud security system.

All connections and accesses will be logged in the cloud access system.

Egress rules



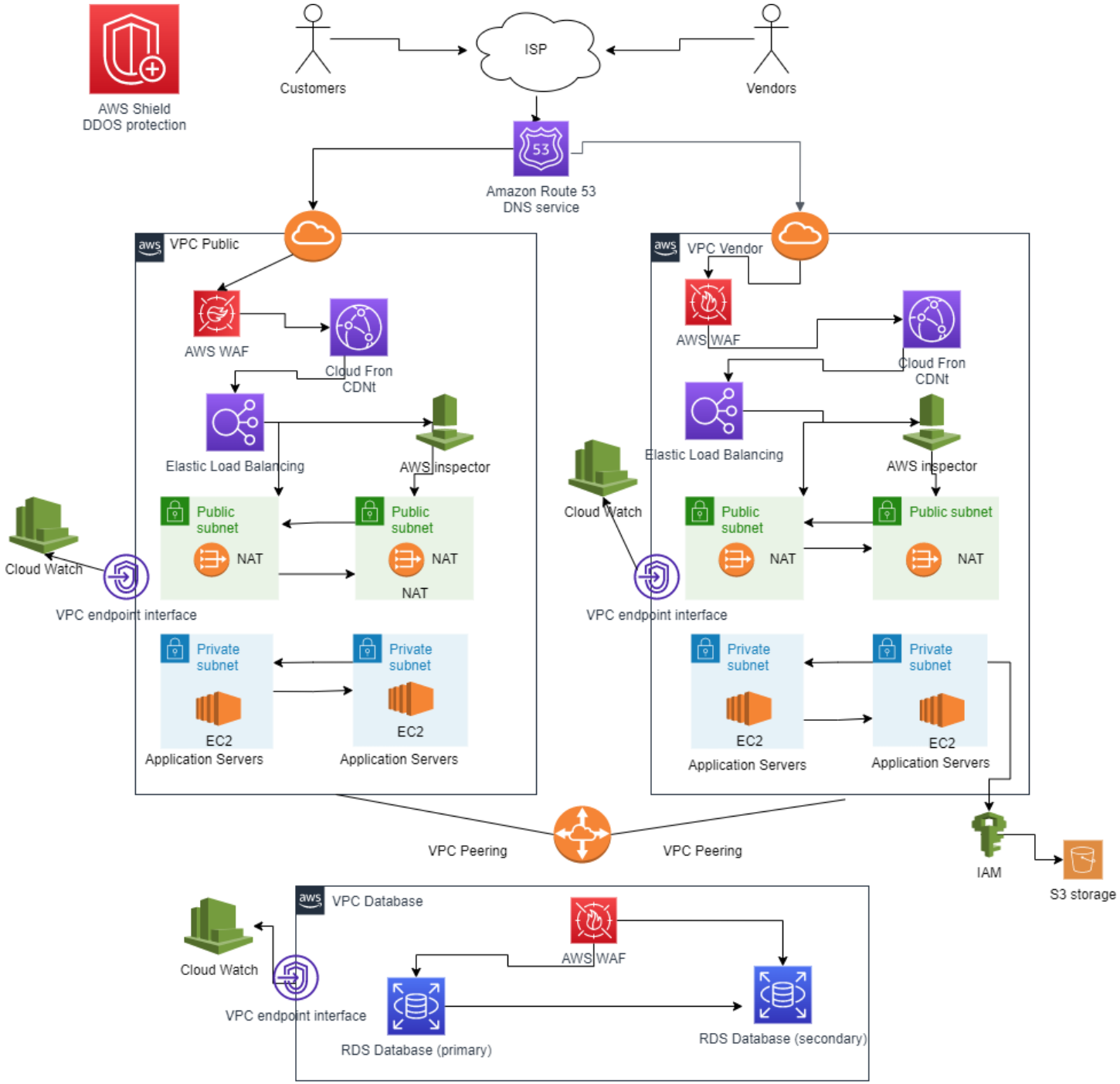
All actions and connections will be logged in the cloud access system.



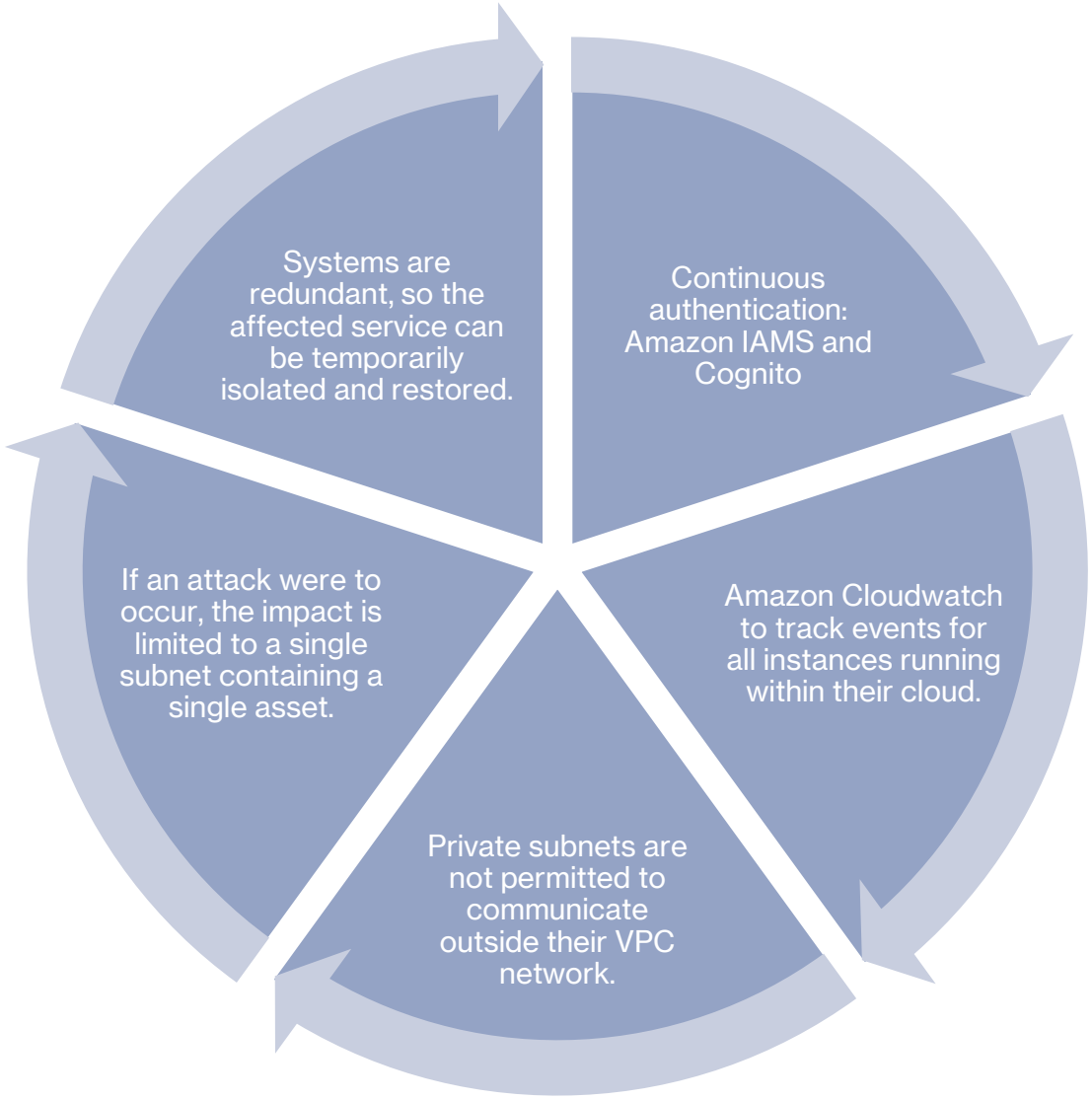
The verified IP address in the cloud perimeter can only connect with other verified IP addresses or verified sources.

Guest IP addresses are not allowed to make any outside connection when it has connected to the cloud.

Network Topology after Cloud Implementation



Zero Trust Security in AWS



Demo

VPC

Your VPCs (4) Info

Actions ▼ | Create VPC

Filter VPCs

1

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set	Main route table
Vendor VPC	vpc-0ceb4bab567582e30	Available	10.1.0.0/16	–	dopt-03633a9ef08894...	rtb-0679ef24b022d0b6a
Database VPC	vpc-0caa1950f42ce62c8	Available	10.2.0.0/16	–	dopt-03633a9ef08894...	rtb-0f53f408823cd4de2
–	vpc-04ec5fc4cd961f2eb	Available	172.31.0.0/16	–	dopt-03633a9ef08894...	rtb-0e4c942923392c82b
Public VPC	vpc-0a9817deaec7e903d	Available	10.0.0.0/16	–	dopt-03633a9ef08894...	rtb-0ea17fdcd4bd5ba0e

Subnets

Subnets (15) Info

Actions ▼ | Create subnet

Filter subnets

1

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses
vendor-vpc-public-...	subnet-09bbead47a56534e1	Available	vpc-0ceb4bab567582e30 | Ve...	10.1.1.0/24	–	251
db-vpc-private-sub...	subnet-076818235b38e1b01	Available	vpc-0caa1950f42ce62c8 | Dat...	10.2.4.0/24	–	251
–	subnet-0715e4965b739a9b8	Available	vpc-04ec5fc4cd961f2eb	172.31.0.0/20	–	4091
vendor-vpc-private...	subnet-0890cd8c1e8a1df8a	Available	vpc-0ceb4bab567582e30 | Ve...	10.1.3.0/24	–	250
–	subnet-0f8c272b1c5832a7f	Available	vpc-04ec5fc4cd961f2eb	172.31.16.0/20	–	4091
public-vpc-private-...	subnet-06ee9e59082db14a2	Available	vpc-0a9817deaec7e903d | Pu...	10.0.4.0/24	–	250
public-vpc-private-...	subnet-0a762ca37bf0631d9	Available	vpc-0a9817deaec7e903d | Pu...	10.0.3.0/24	–	250
db-vpc-public-subn...	subnet-0ba03306be8b0d689	Available	vpc-0caa1950f42ce62c8 | Dat...	10.2.1.0/24	–	250
public-vpc-public-s...	subnet-05eeb797841ab0f76	Available	vpc-0a9817deaec7e903d | Pu...	10.0.1.0/24	–	251
public-vpc-public-s...	subnet-0ce21ba76a1d0fe99	Available	vpc-0a9817deaec7e903d | Pu...	10.0.2.0/24	–	251

Demo

Route Tables

Route tables (4) Info

Actions | Create route table

Filter route tables

1

Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Owner ID
–	rtb-0e4c942923392c82b	–	–	Yes	vpc-04ec5fc4cd961f2eb	989701974721
–	rtb-0ea17fdcd4bd5ba0e	–	–	Yes	vpc-0a9817deaec7e903d | Pu...	989701974721
–	rtb-0679ef24b022d0b6a	–	–	Yes	vpc-0ceb4bab567582e30 | Ve...	989701974721
–	rtb-0f53f408823cd4de2	–	–	Yes	vpc-0caa1950f42ce62c8 | Dat...	989701974721

Internet Gateways

Internet gateways (3) Info

Filter internet gateways

Name	Internet gateway ID	State	VPC ID	Owner
vendor-vpc-ig	igw-0389a729c29fc4630	Attached	vpc-0ceb4bab567582e30 | Vendor VPC	989701974721
public-vpc-ig	igw-0a7f3843e2e822aa5	Attached	vpc-0a9817deaec7e903d | Public VPC	989701974721
–	igw-0aad672efa7a66020	Attached	vpc-04ec5fc4cd961f2eb	989701974721

Demo

Primary DB

primary-database

Modify | Actions

Summary

DB identifier	CPU	Status	Class
primary-database	-	Available	db.t3.micro
Role	**Current activity**	**Engine**	**Region & AZ**
Instance		PostgreSQL	ca-central-1a

Connectivity & security | Monitoring | Logs & events | Configuration | Maintenance & backups | Tags

Connectivity & security

Endpoint & port

Endpoint
primary-database.cvgtag7j3ki6.ca-central-1.rds.amazonaws.com

Port
5432

Networking

Availability Zone
ca-central-1a

VPC
Database VPC (vpc-0caa1950f42ce62c8)

Subnet group
default-vpc-0caa1950f42ce62c8

Subnets
subnet-076818235b38e1b01
subnet-0ba03306be8b0d689
subnet-080fa3e73df874356
subnet-0a77f8c91062d477e

Network type
IPv4

Security

VPC security groups
DeveloperRDSAllowance (sg-048d57bfca1a62abc)
Active

Publicly accessible
No

Certificate authority Info
rds-ca-2019

Certificate authority date
August 22, 2024, 12:08 (UTC-05:00)

DB instance certificate expiration date
August 22, 2024, 12:08 (UTC-05:00)

Demo

Databases

Databases

Group resources | Modify | Actions | Restore from S3 | Create database

Filter by databases

1

DB identifier	Role	Engine	Region & AZ	Size	Status	Actions	CPU	Current activity	Maintenance	VPC	Multi-AZ
primary-database	Instance	PostgreSQL	ca-central-1a	db.t3.micro	Available	2 Actions	-		none	vpc-0caa1950f42ce62c8	No
secondary-database	Instance	PostgreSQL	ca-central-1a	db.t3.micro	Available	2 Actions	-		none	vpc-0caa1950f42ce62c8	No

EC2 Instances

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
public-application-server-1	i-03c5081dc611e38dc	Running	t2.micro	2/2 checks passed	No alarms	ca-central-1a
vendor-application-server-1	i-0166b9e797c3d9bbb	Running	t2.micro	2/2 checks passed	No alarms	ca-central-1a
vendor-application-server-2	i-0bc279e689ead96cf	Running	t2.micro	2/2 checks passed	No alarms	ca-central-1a
public-application-server-2	i-0f9f5e4b28773d7f0	Running	t2.micro	2/2 checks passed	No alarms	ca-central-1b

Demo

EC2 Security Groups

Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count	Outbound rules count
–	sg-01e59639d36b89915	VendorInOut	vpc-04ec5fc4cd961f2eb	Only allow vendors to ...	989701974721	2 Permission entries	3 Permission entries
–	sg-048d57bfca1a62abc	DeveloperRDSAllowance	vpc-0caa1950f42ce62c8	Allows SSH access to d...	989701974721	2 Permission entries	1 Permission entry
–	sg-05809c7543a332374	ApplicationInOut	vpc-0a9817deaec7e903d	Customer-Server relati...	989701974721	2 Permission entries	3 Permission entries
–	sg-06df80a43c151e7ef	default	vpc-0ceb4bab567582e30	default VPC security gr...	989701974721	1 Permission entry	1 Permission entry
–	sg-0892529ed0b2feeb5	application-servers	vpc-0a9817deaec7e903d	SG for all application s...	989701974721	1 Permission entry	1 Permission entry
–	sg-09d44a3d95f4dc112	vendor-applications	vpc-0ceb4bab567582e30	SG for all EC2s in Vend...	989701974721	1 Permission entry	1 Permission entry
–	sg-0d102a3a159329697	default	vpc-0a9817deaec7e903d	default VPC security gr...	989701974721	1 Permission entry	1 Permission entry
–	sg-0d1609ba5c949730a	default	vpc-0caa1950f42ce62c8	default VPC security gr...	989701974721	1 Permission entry	1 Permission entry
–	sg-0ec3031497bb0dd81	default	vpc-04ec5fc4cd961f2eb	default VPC security gr...	989701974721	1 Permission entry	1 Permission entry

IAM User Groups

IAM > User groups

User groups (3) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Filter User groups by property or group name and press enter

Group name	Users	Permissions
pazell-admin	1	Defined
pazell-employee	1	Defined
vendors	1	Defined

Demo

Vendor-In-Out-Ingress

Inbound rules (2)

Manage tags | Edit inbound rules

Filter security group rules

Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
–	sgr-055e7edefa66d786f	IPv4	HTTP	TCP	80	0.0.0.0/32	Only allows specified vendors into vendor server.
–	sgr-0e61f85eefc524ef4	IPv4	HTTPS	TCP	443	0.0.0.0/32	Only allows specified vendors into vendor server.

Vendor-In-Out-Egress

Outbound rules (3)

Manage tags | Edit outbound rules

Filter security group rules

Name	Security group rule...	IP version	Type	Protocol	Port range	Destination	Description
–	sgr-0fac54b37e487f5b7	IPv4	IMAP	TCP	143	0.0.0.0/32	Strict emails to vendors.
–	sgr-0dba7f4019b67e400	IPv4	HTTP	TCP	80	0.0.0.0/32	Request resolved only for specified vendors.
–	sgr-04795e86fe9911b5f	IPv4	HTTPS	TCP	443	0.0.0.0/32	Request resolved only for specified vendors.

Demo

RDS-Allowance-Ingress

Inbound rules (2)

Manage tags | Edit inbound rules

Filter security group rules

1

Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
–	sgr-0e6139cf05a511f93	IPv4	MYSQL/Aurora	TCP	3306	0.0.0.0/16	Internal Devs can send queries
–	sgr-0d4fd1d55e9da9cf1	IPv4	SSH	TCP	22	0.0.0.0/16	Internal devs can SSH

RDS-Allowance-Egress

Outbound rules (1)

Manage tags | Edit outbound rules

Filter security group rules

1

Name	Security group rule...	IP version	Type	Protocol	Port range	Destination	Description
–	sgr-0cfe861ecf40fda3e	IPv4	SSH	TCP	22	0.0.0.0/16	SSH to internal devs only

Demo

Application-In-Out-Ingress

Inbound rules (2)

Manage tags | Edit inbound rules

Filter security group rules

1

Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
–	sgr-0580eae552226c4...	IPv4	HTTP	TCP	80	0.0.0.0/0	Anyone can access the application servers at port 80.
–	sgr-079977f0475fabc1a	IPv4	HTTPS	TCP	443	0.0.0.0/0	Anyone can access the application servers at port 443.

Application-In-Out-Egress

Outbound rules (3)

Manage tags | Edit outbound rules

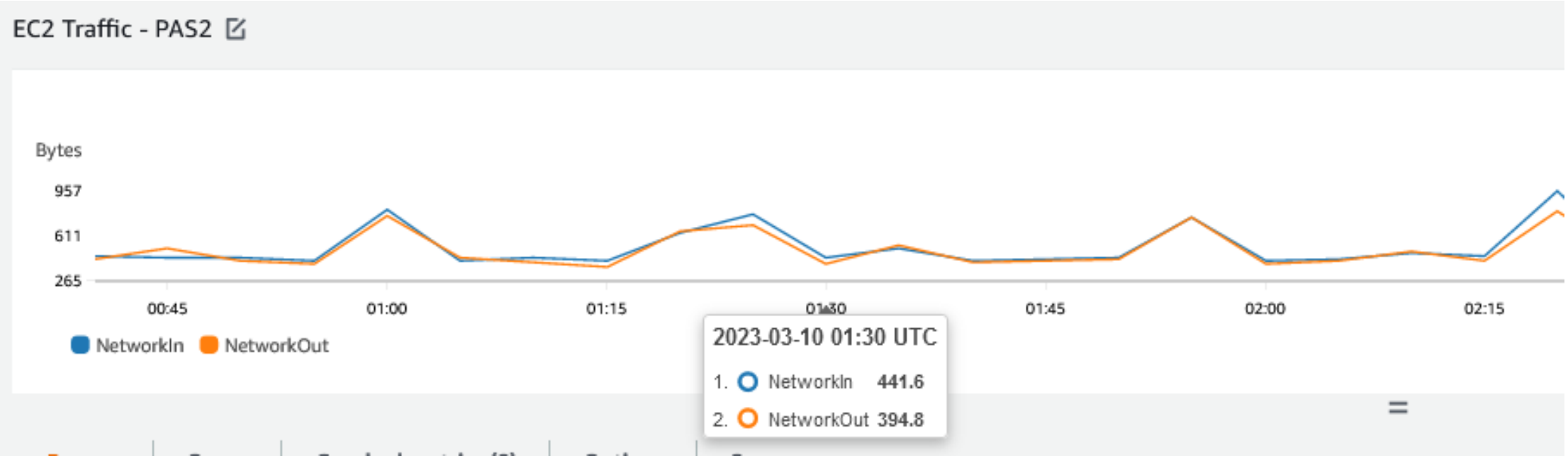
Filter security group rules

1

Name	Security group rule...	IP version	Type	Protocol	Port range	Destination	Description
–	sgr-0945cc95eb5eccf46	IPv4	HTTP	TCP	80	0.0.0.0/0	Client-request resolved
–	sgr-05c42213fdfa1cd4a	IPv4	IMAPS	TCP	993	0.0.0.0/0	For sending emails.
–	sgr-0480389507573d...	IPv4	HTTPS	TCP	443	0.0.0.0/0	Client-request resolved

Demo

CloudWatch Traffic Log



Bibliography

- *AWS::EC2::SecurityGroup Ingress - AWS CloudFormation*. (n.d.). AWS::EC2::SecurityGroup Ingress - AWS CloudFormation. Retrieved March 13, 2023, from https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-ec2-security-group-rule-1.html
- *AWS::EC2::SecurityGroup Egress - AWS CloudFormation*. (n.d.). AWS::EC2::SecurityGroup Egress - AWS CloudFormation. Retrieved March 13, 2023, from https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-ec2-security-group-rule.html
- *Ingress and egress rules | VPC Service Controls | Google Cloud*. (n.d.). Google Cloud. Retrieved March 13, 2023, from https://cloud.google.com/vpc-service-controls/docs/ingress-egress-rules
- *What Is Ingress and Egress In The Cloud? | Aviatrix*. (2020, August 2). Aviatrix. Retrieved March 13, 2023, from https://aviatrix.com/learn-center/cloud-security/egress-and-ingress/
- *AWS Pricing Calculator*. (n.d.). AWS Pricing Calculator. Retrieved March 13, 2023, from https://calculator.aws/#/addService/DMS
- *Cloud Database Migration - AWS Database Migration Service (DMS) - AWS*. (n.d.). Amazon Web Services, Inc. Retrieved March 13, 2023, from https://aws.amazon.com/dms/
- *AWS Pricing Calculator*. (n.d.). AWS Pricing Calculator. Retrieved March 13, 2023, from https://calculator.aws/#/addService/WAF
- *Protect Web Applications – AWS WAF – Amazon Web Services*. (n.d.). Amazon Web Services, Inc. Retrieved March 13, 2023, from https://aws.amazon.com/waf/
- *AWS Pricing Calculator*. (n.d.). AWS Pricing Calculator. Retrieved March 13, 2023, from https://calculator.aws/#/addService/networkfirewall
- *Managed Network Firewall – AWS Network Firewall – Amazon Web Services*. (n.d.). Amazon Web Services, Inc. Retrieved March 13, 2023, from https://aws.amazon.com/network-firewall/
- Vyas, K. (2022, March 18). *Cloud Security Best Practices for 2022 | ITBE*. IT Business Edge. Retrieved March 13, 2023, from https://www.itbusinessedge.com/cloud/cloud-security-best-practices/
- Harvey, C. (2021, September 10). *Top 12 Cloud Security Best Practices | eSecurity Planet*. eSecurityPlanet. Retrieved March 13, 2023, from https://www.esecurityplanet.com/cloud/cloud-security-best-practices/
- *AWS PCI Compliance: 5 Ways to Make Your Cloud Compliant*. (n.d.). Retrieved March 13, 2023, from https://www.tigera.io/learn/guides/pci-compliance/aws-pci-compliance/
- *Achieving PCI Compliance on AWS*. (2022, March 14). KirkpatrickPrice Home. Retrieved March 13, 2023, from https://kirkpatrickprice.com/blog/aws-pci-compliance/
- Even, K., & Tozzi, L. (2014). WAF! Amazon. Retrieved March 9, 2023, from https://docs.aws.amazon.com/waf/latest/developerguide/ddos-overview.html
- Defense-in-depth. CyberArk. (2021, September 28). Retrieved March 9, 2023, from https://www.cyberark.com/what-is/defense-in-depth/#:~:text=A%20defense%2Din%2Ddepth%20strategy,contain%20threats%2C%20and%20mitigate%20risk.
- Engdahl, S. (2008). Blogs. Amazon. Retrieved March 9, 2023, from https://aws.amazon.com/blogs/security/tag/defense-in-depth/
- *An AWS Cloud architecture for web hosting - Web Application Hosting in the AWS Cloud*. (n.d.). An AWS Cloud Architecture for Web Hosting - Web Application Hosting in the AWS Cloud. Retrieved March 13, 2023, from https://docs.aws.amazon.com/whitepapers/latest/web-application-hosting-best-practices/an-aws-cloud-architecture-for-web-hosting.html

Thank you.
Questions?