AWS re:Invent

SEC343-R

Provable access control: Know who can access your AWS resources

Eric Brandwine
Distinguished Engineer/VP
AWS Security
Amazon Web Services

Neha Rungta
Principal Applied Scientist
Automated Reasoning Group
Amazon Web Services

Building a secure system

?

Define “secure”

Bad stuff doesn’t happen

Customers don’t yell at me

My boss keeps paying me

The wrong things don’t happen

The right things *do* happen

Define “secure”

The system has only desired behaviors

In all reachable states

After processing any input

for all given starting states

I do security

Yeah, right!

We can do your job better than you can! All you need is SAT and SMT and three PhDs and did you know that P is basically equal to NP and formal methods can solve any problem, how hard can security be?

byron

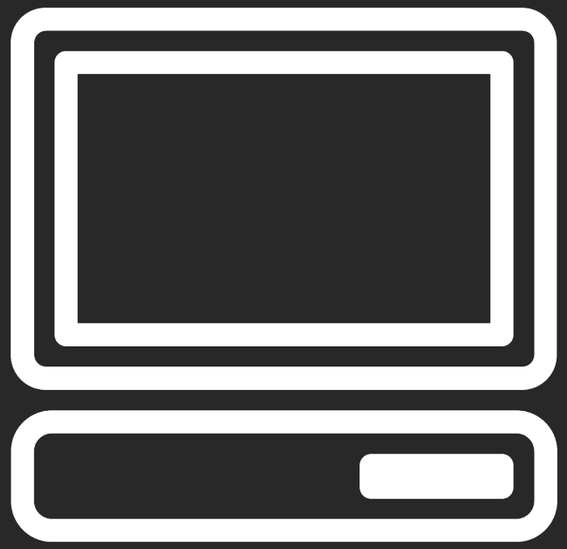
Byron
Cook

rungta

View Badge Photo

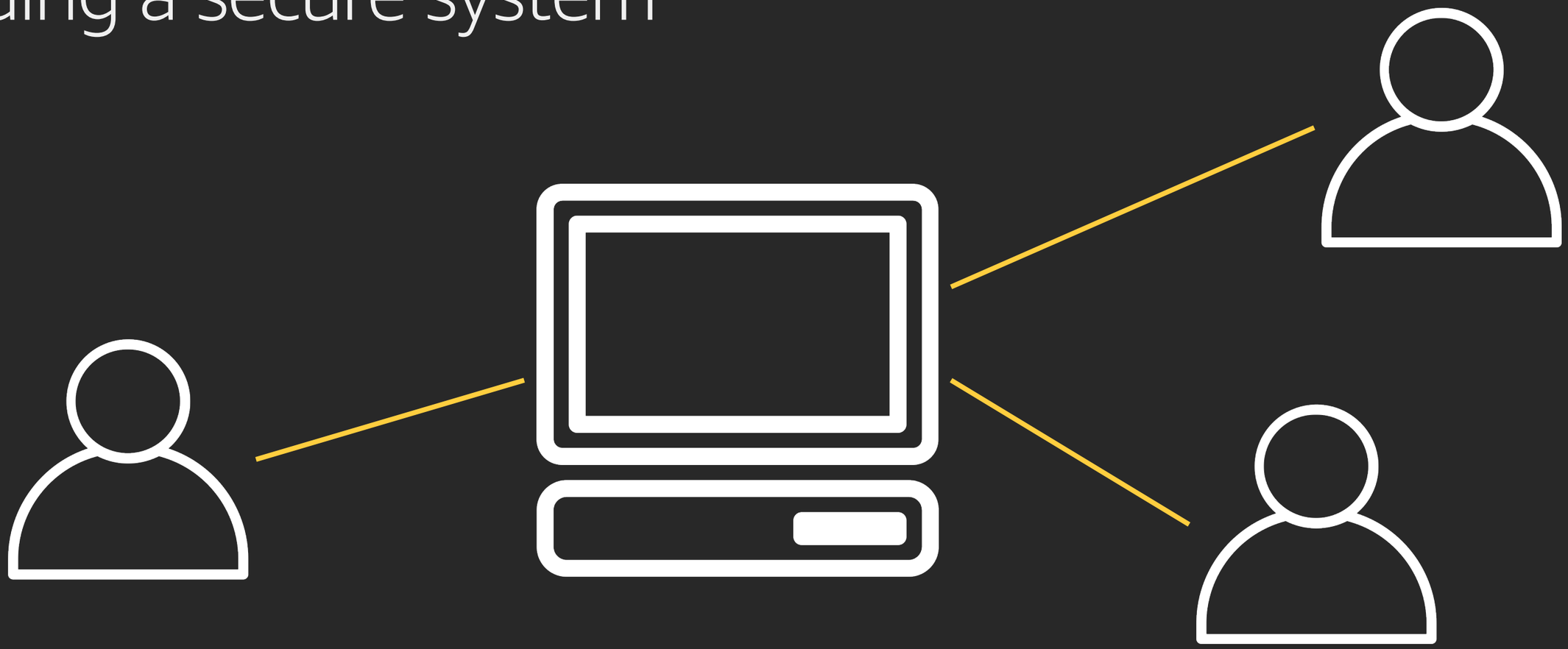
Neha
Rungta

Building a secure system



Does the computer do the right thing?

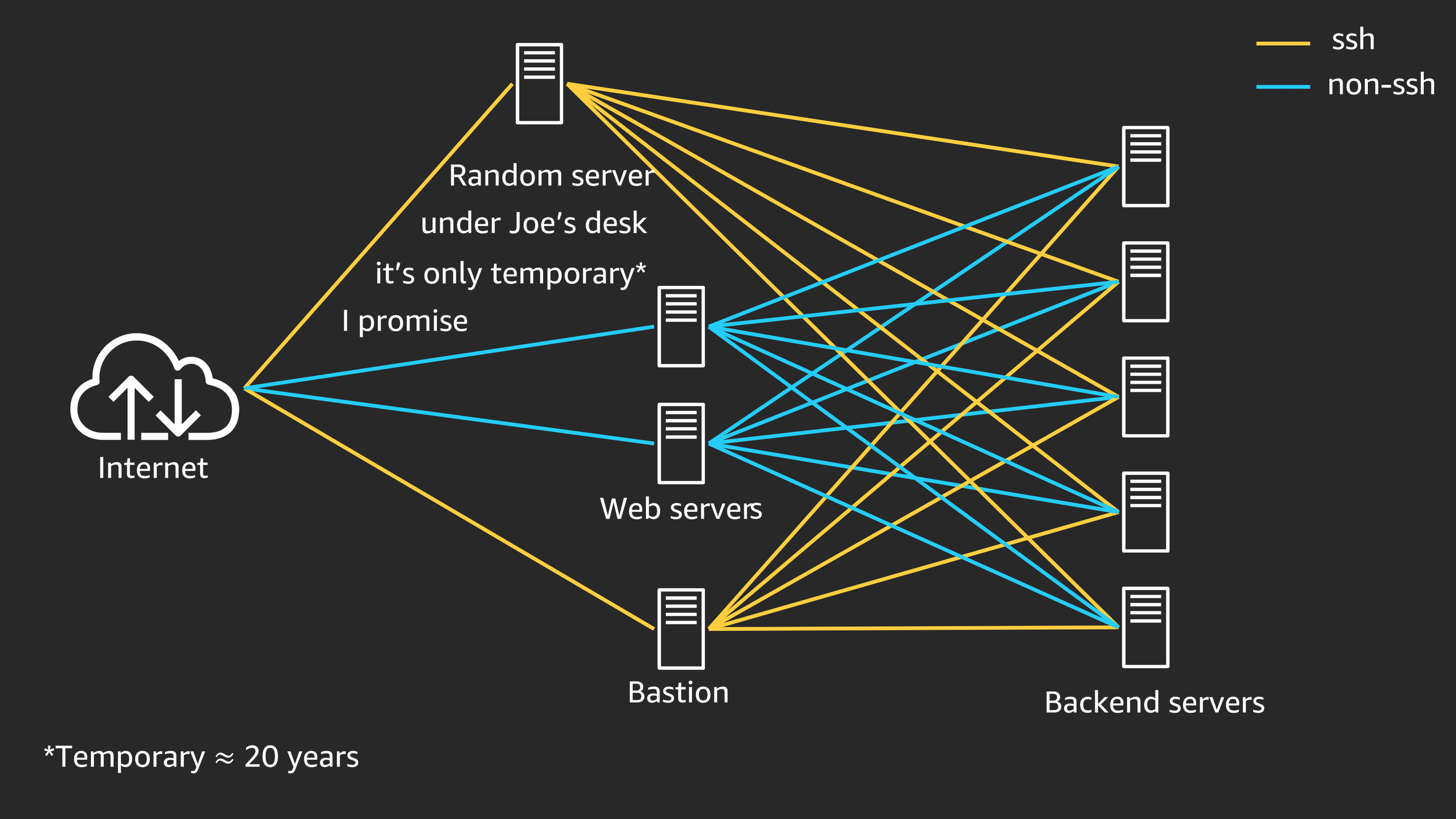
Building a secure system

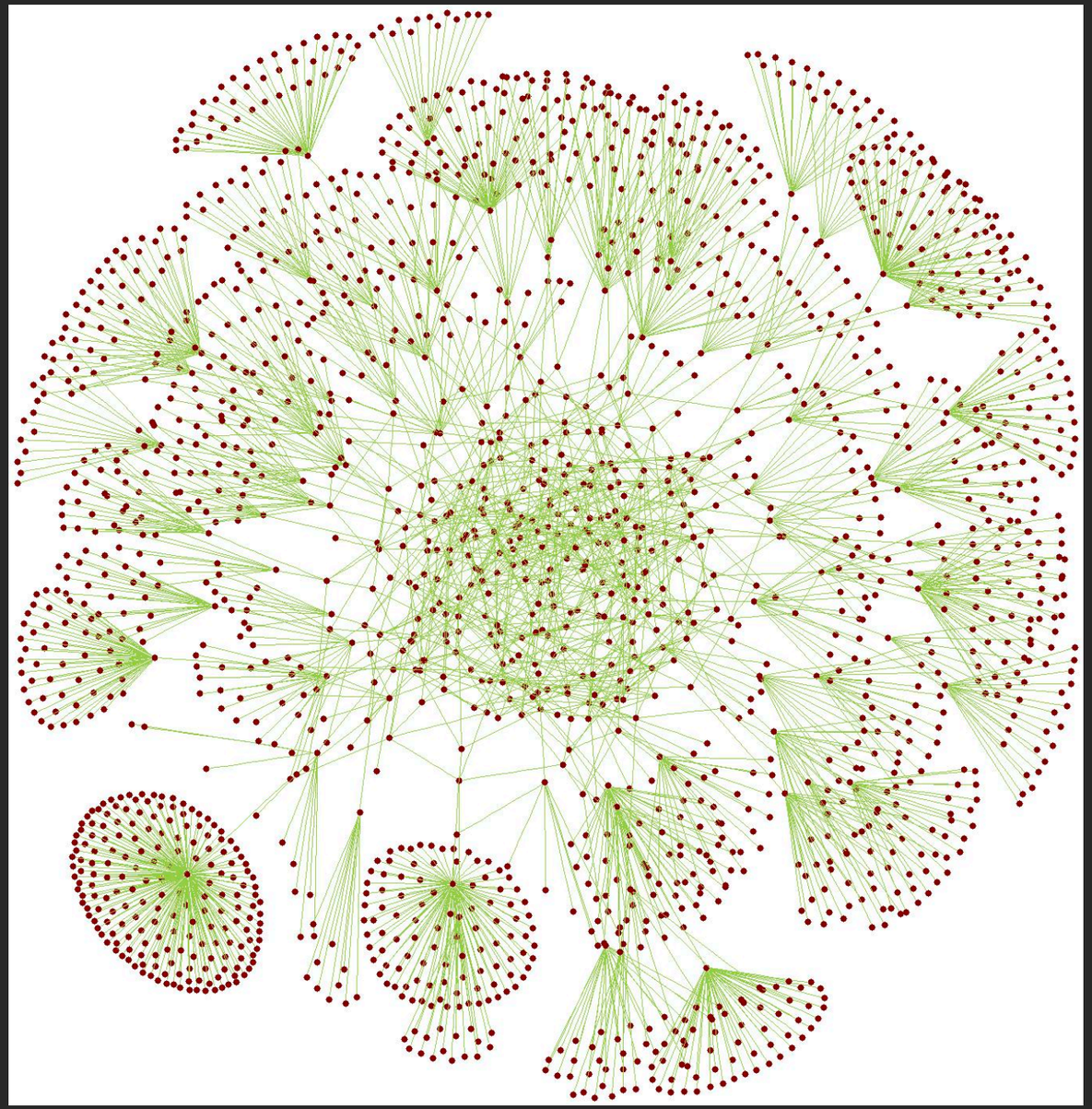


Do the right people have access to the right things?

Building a secure system

Do the right computers have access to the right computers to give the right people the right access to the right things?


ssh
non-ssh
Random server
under Joe's desk
it's only temporary*
I promise
Internet
Web servers
Bastion
Backend servers
*Temporary ≈ 20 years



Networks aren’t special

- Permissions policies
- Interprocess communication
- Code
- Electrical systems
- Vehicles
- Houses

What's a security guy or gal to do?

Security problems are violated assumptions

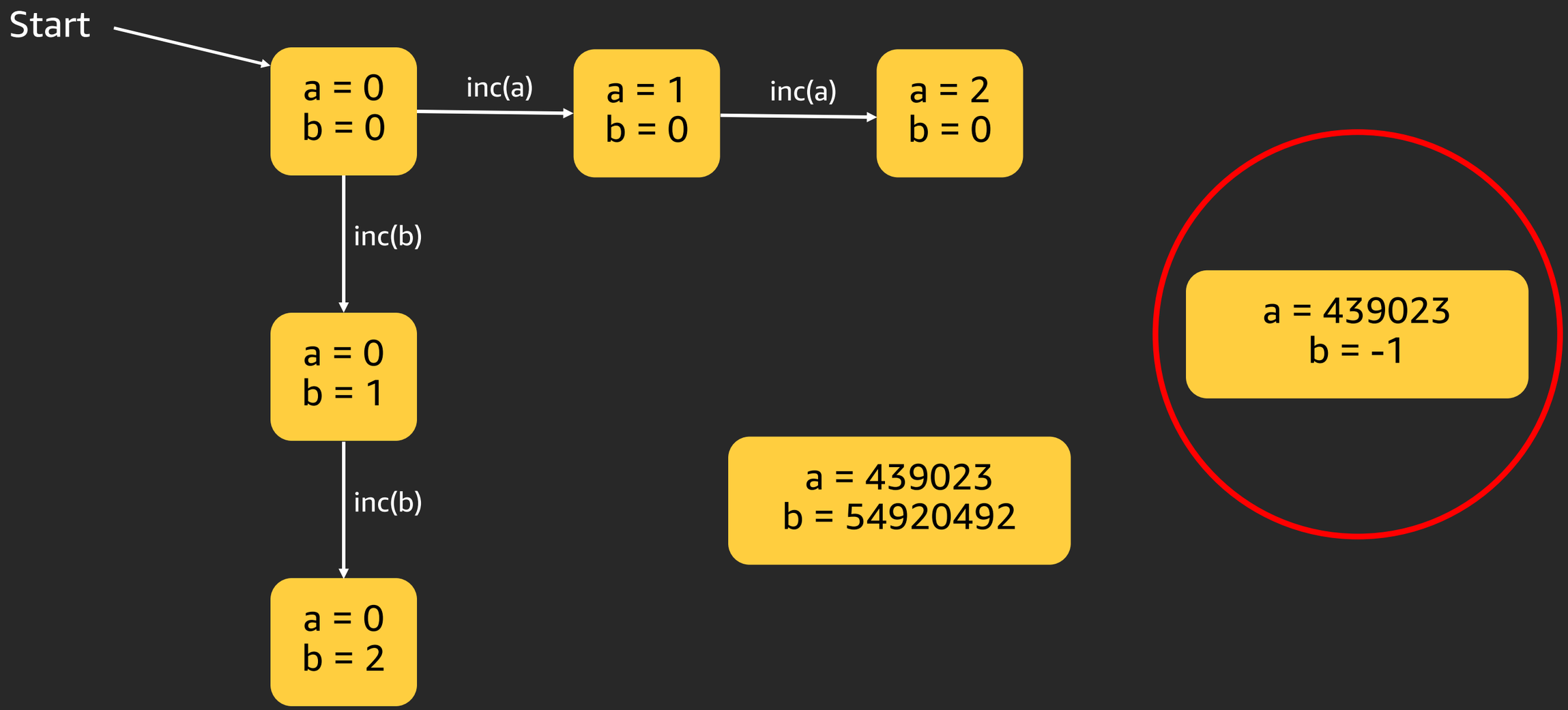
Try to violate some assumptions

Try to spot your assumptions

Penetration testing

Exploring the state space

Exploring the state space



Have you heard this one?

-3 mathematicians walk into a bar….

Why did the <script>alert(“Pwned!”)</script> cross the road?

Just checking the line. Please send me a copy of my message back. My message is 65535 bytes long. Really, it is.

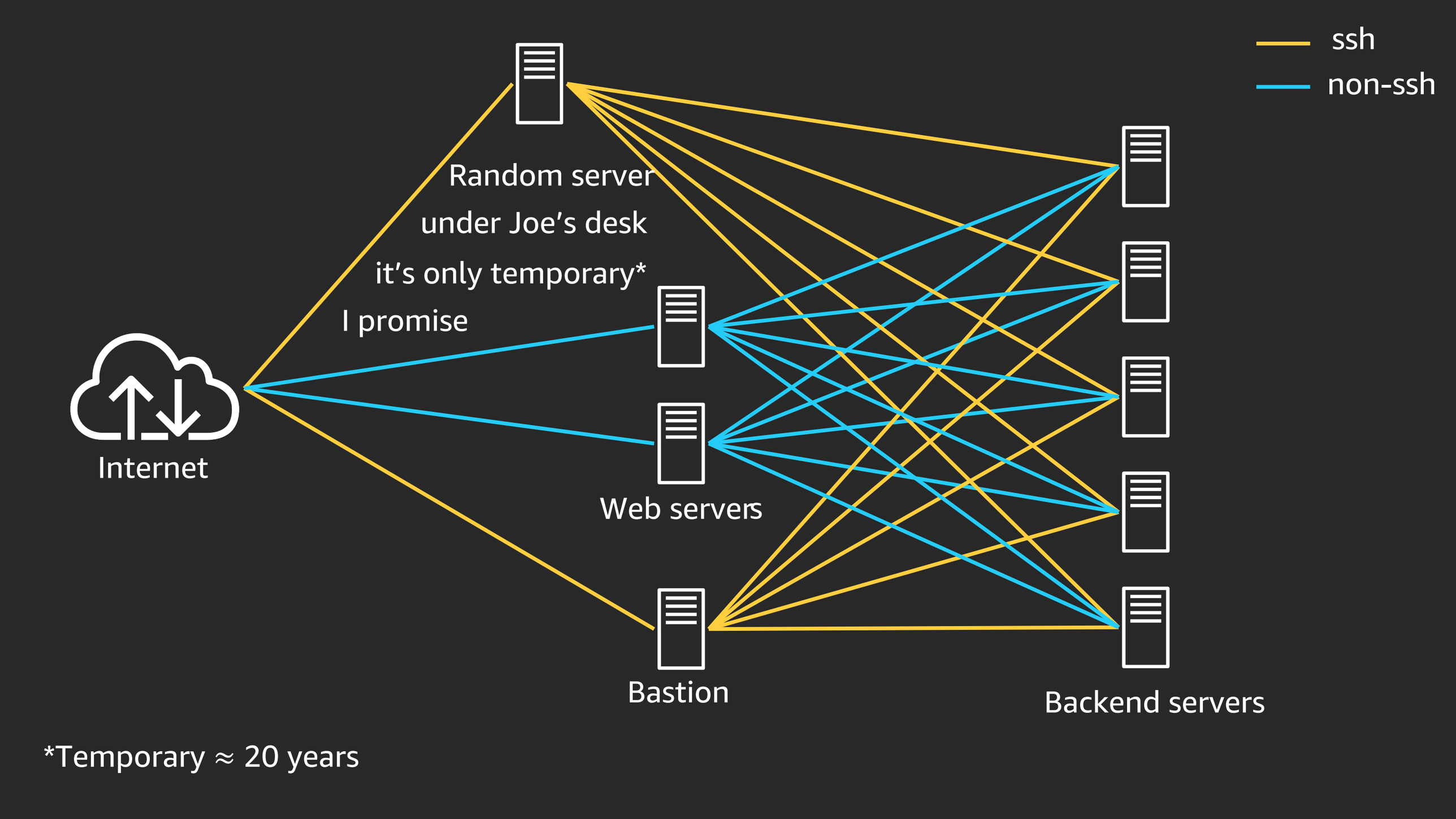
Fuzzing

Most unexpected states lead to invalid execution (crashes)

Unexpected input can lead to unexpected states

Generate random input, wait for crashes

If you’re smart, analyze the code to guide the random inputs


ssh
non-ssh
Random server
under Joe's desk
it's only temporary*
I promise
Internet
Web servers
Bastion
Backend servers
*Temporary ≈ 20 years

No computers under desks in the cloud

ec2:DescribeInstances

ec2:DescribeInternetGateways

ec2:DescribeNatGateways

ec2:DescribeNetworkAcls

ec2:DescribeRouteTables

ec2:DescribeSecurityGroups

ec2:DescribeSubnets

ec2:DescribeVpcEndpoints

ec2:DescribeVpcs

ec2:DescribeVpnGateways

```
for a in accounts:                          5
 for v in VPCs:                             3
  for sub in subnets:                       3
   for a in acls:                           2
    for sg in security_groups:              8
     for r in route_tables:                 2
      for i in instances:                  50
       for p in protos:                     2
        for n in ports:                 65535
         .......
```

9,437,040,000

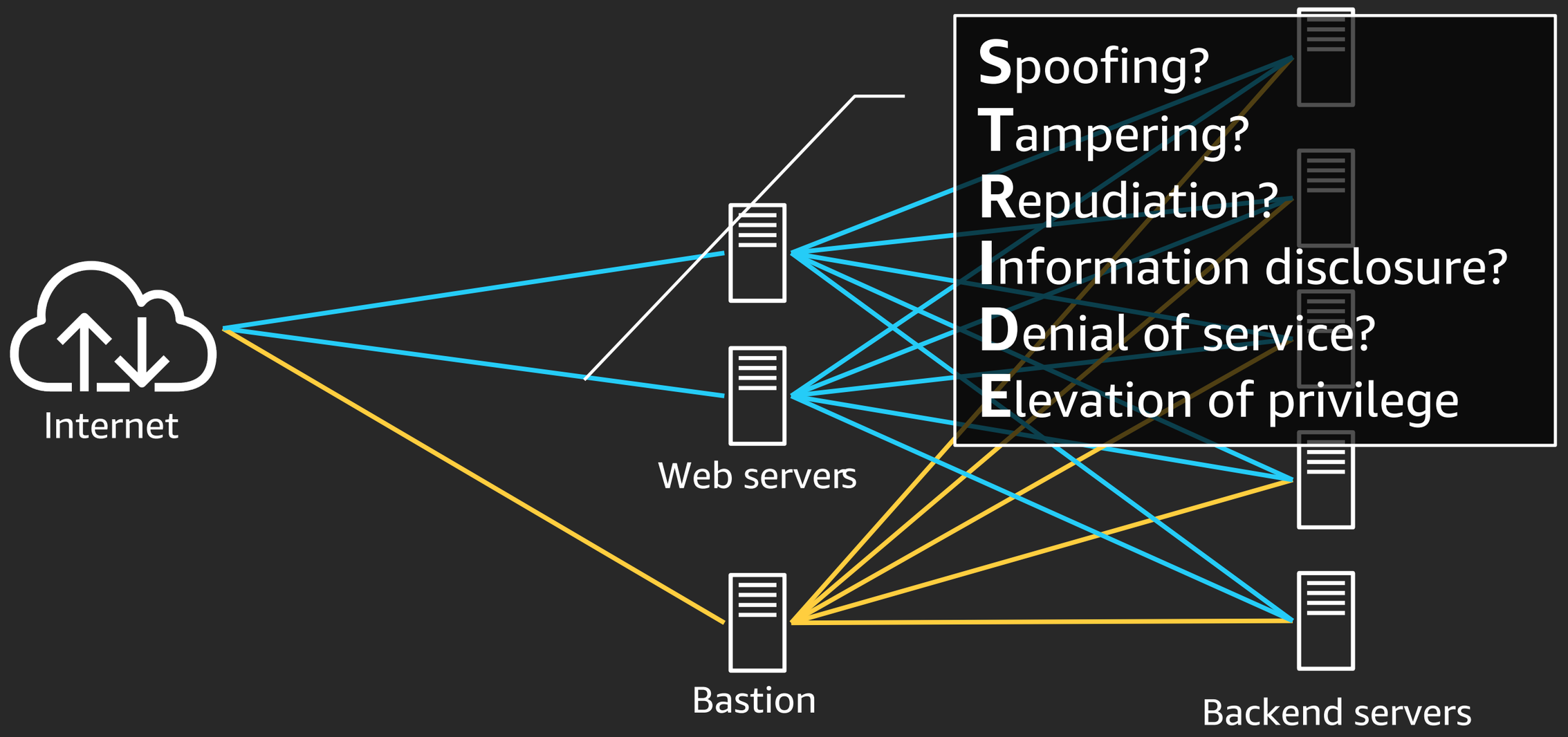
What's a security guy or gal to do?

Security problems are violated assumptions

Try to violate some assumptions

Try to spot your assumptions

Threat modeling



Almost a magic recipe

Humans manually exploring the state space is fun, but slow

Machines randomly exploring the state space is fun, but slow

Modeling your system makes it more tractable

- Too much detail leads to state explosions and headaches
- Too little detail leads to meaningful loss of fidelity

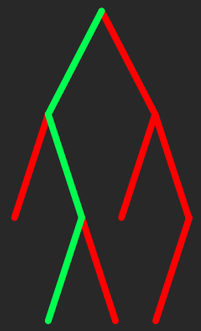
Full state of AWS is captured via APIs

If only….

Automated Reasoning

Infers future behavior of computer systems

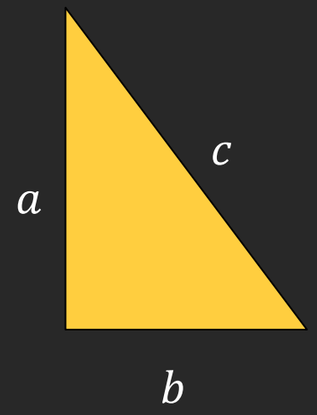
What they might do



What they will do

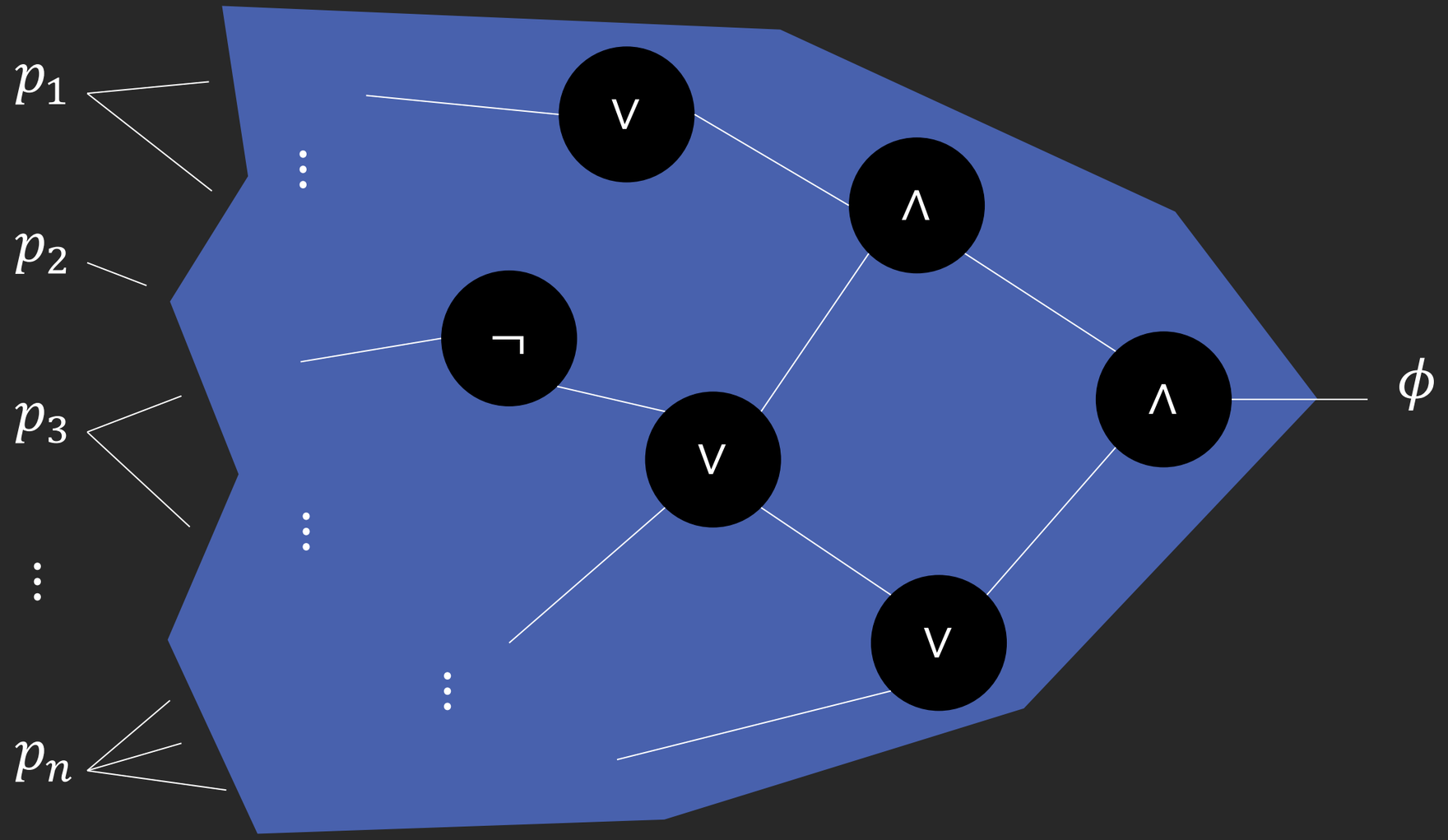
What they never do

Early days of unautomated reasoning



$$a^2 + b^2 = c^2$$

Boolean satisfiability – SAT solving



Theoretical importance

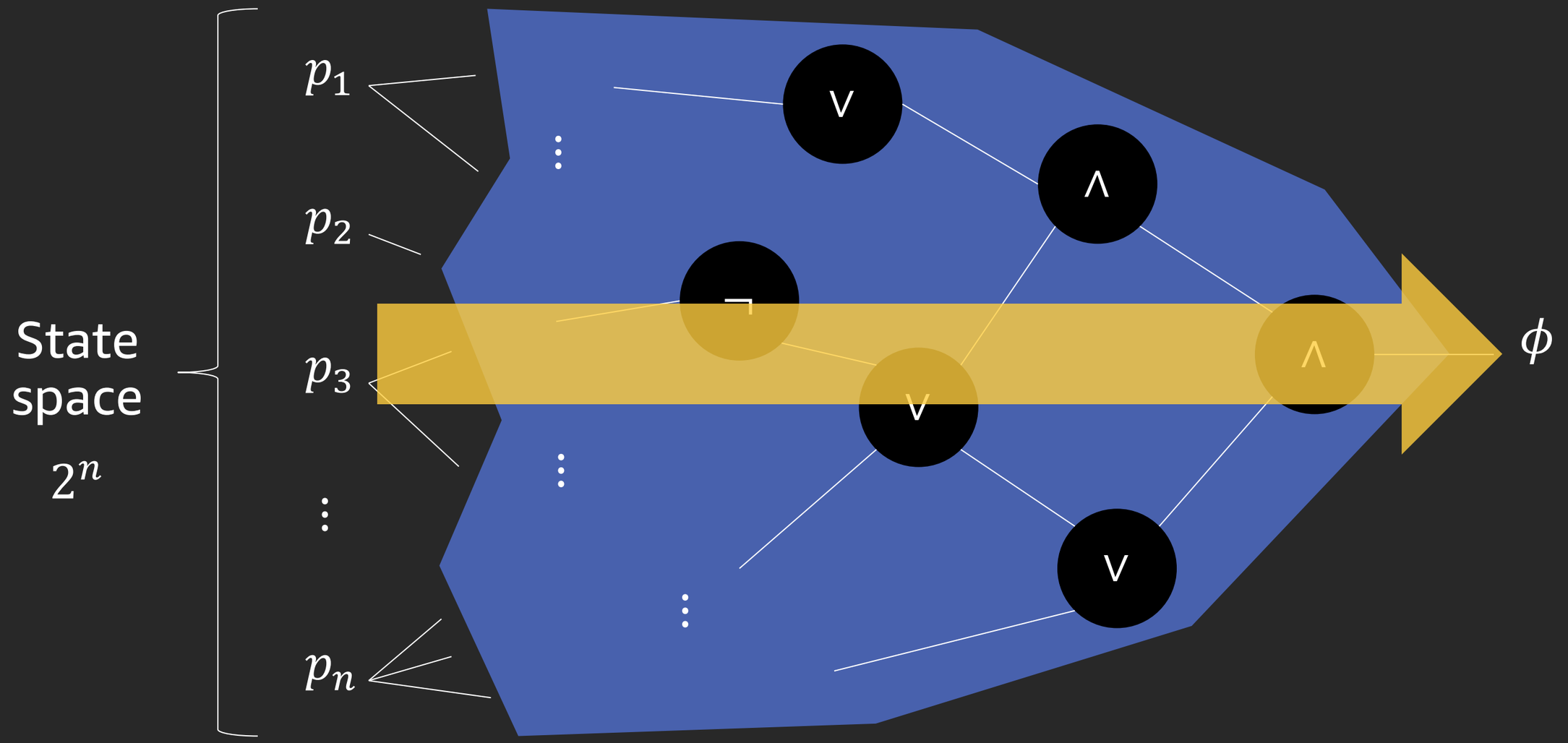
First NP-complete problem

(Cook, 1971)

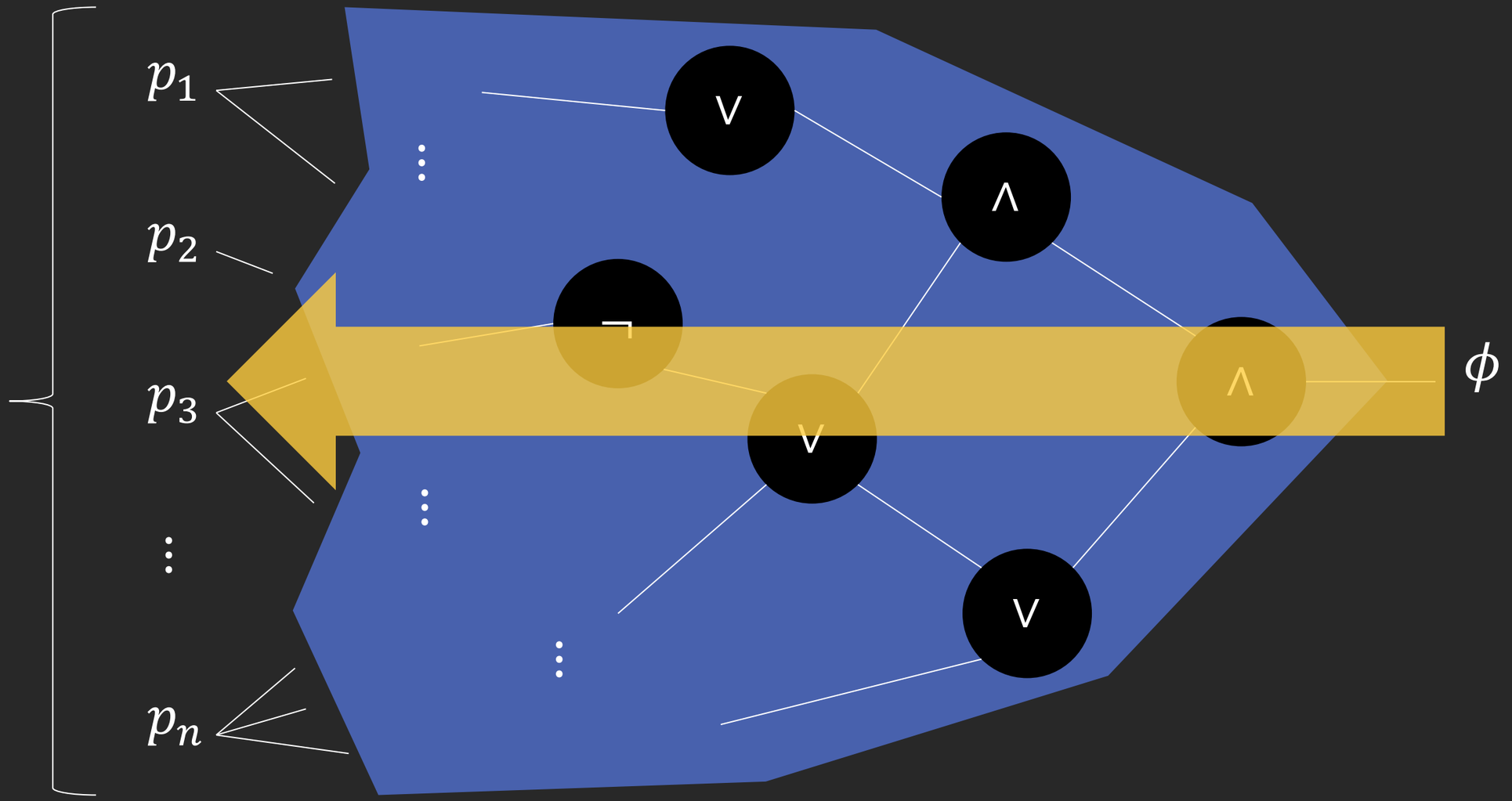
No known algorithm to efficiently determine satisfiability of every possible Boolean formula.

Hard in theory. Efficient in practice.

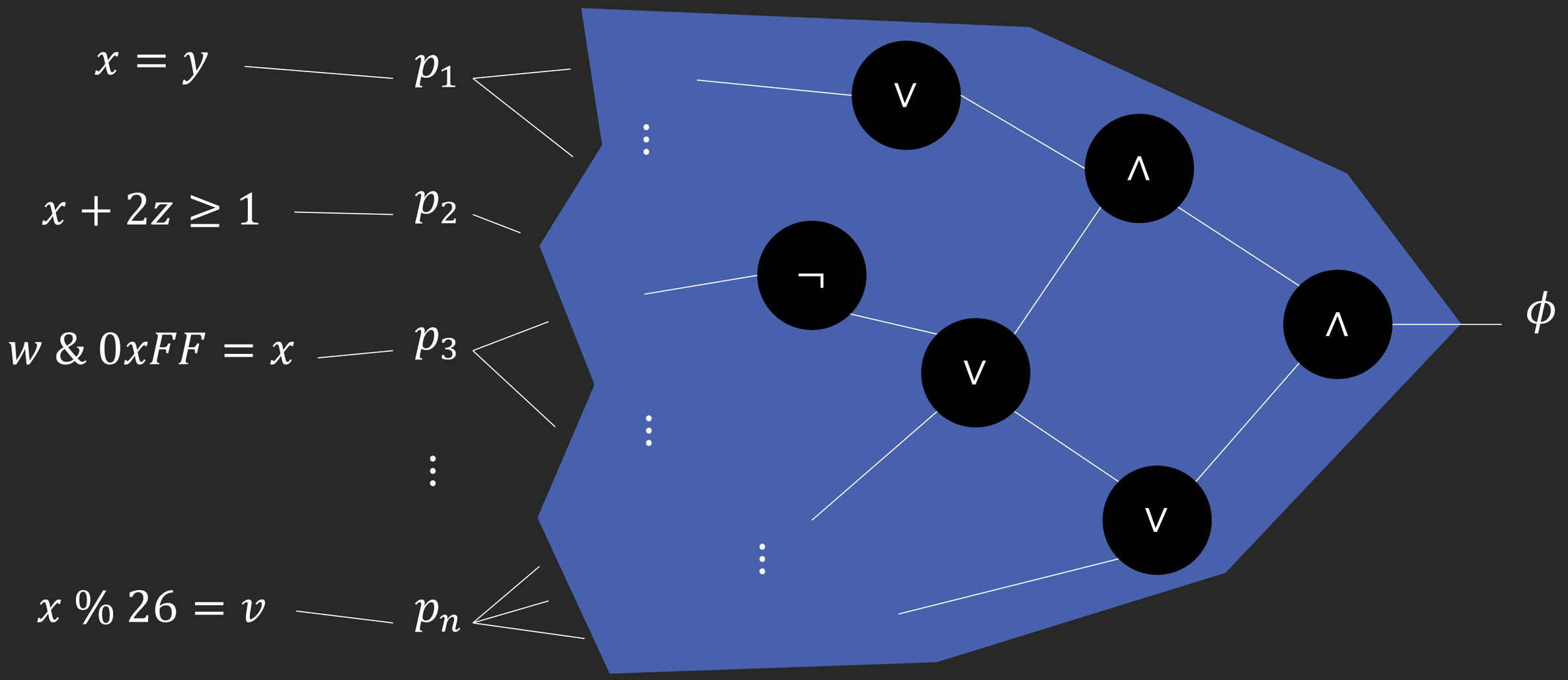
Efficient SAT Solving



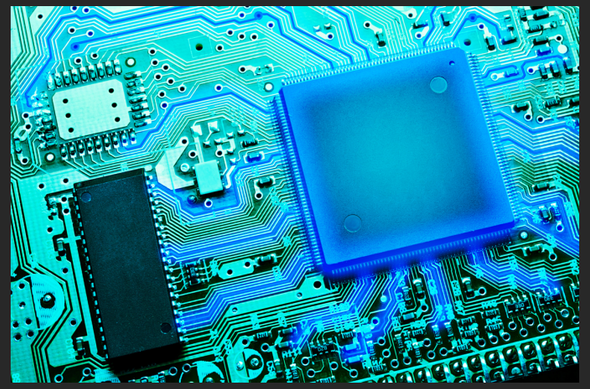
Efficient SAT Solving



Satisfiability modulo theories

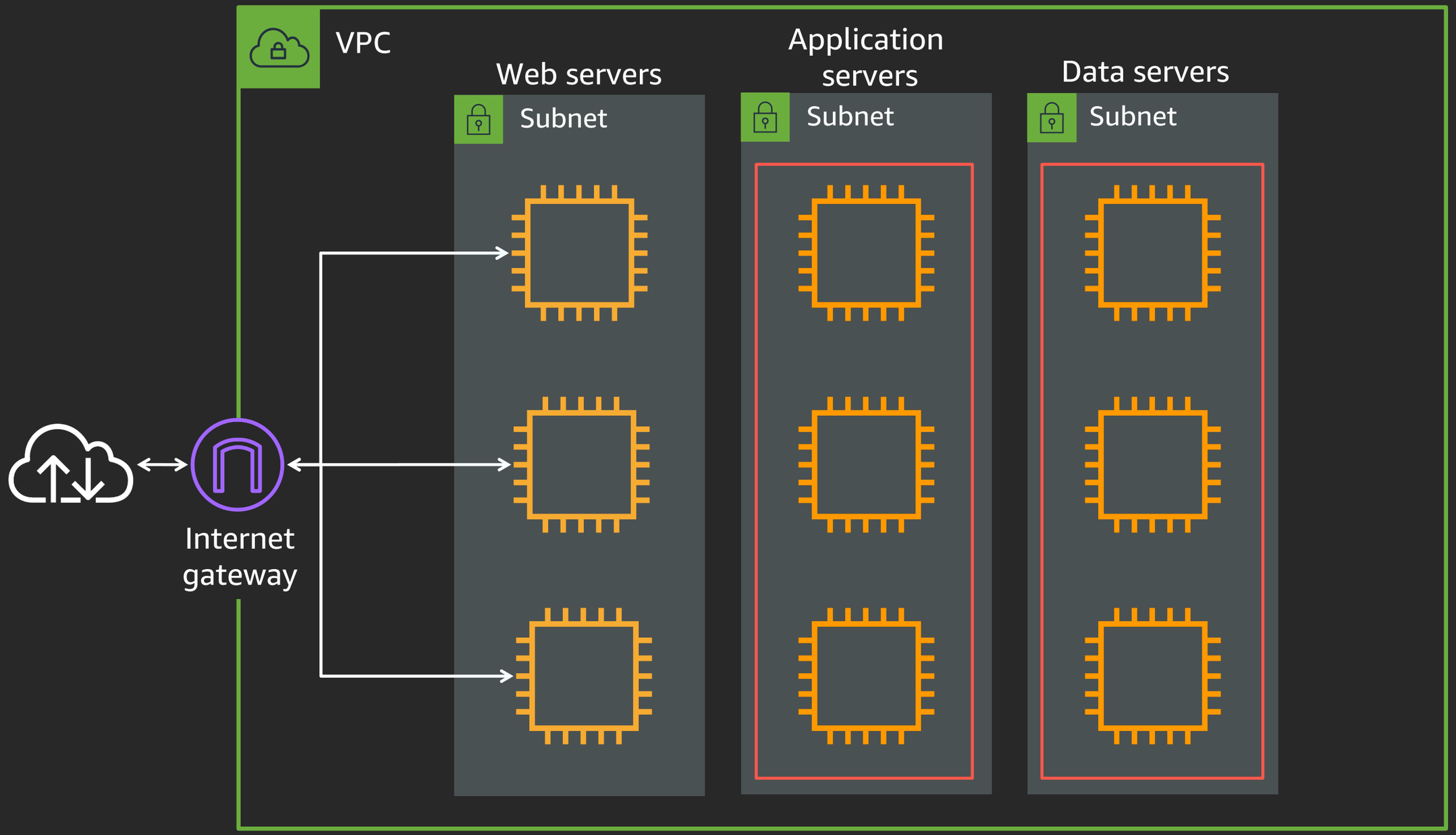


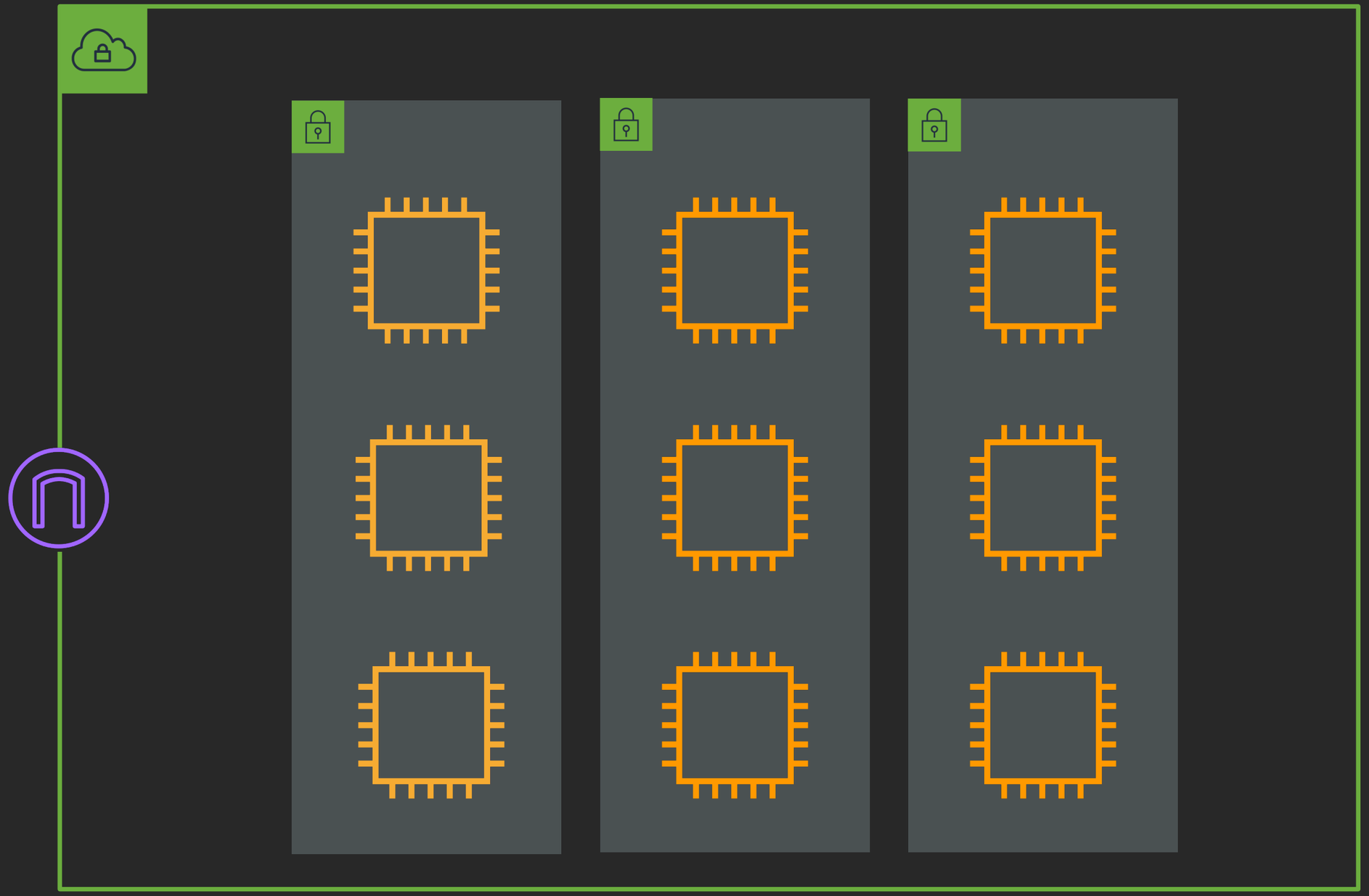
Applications

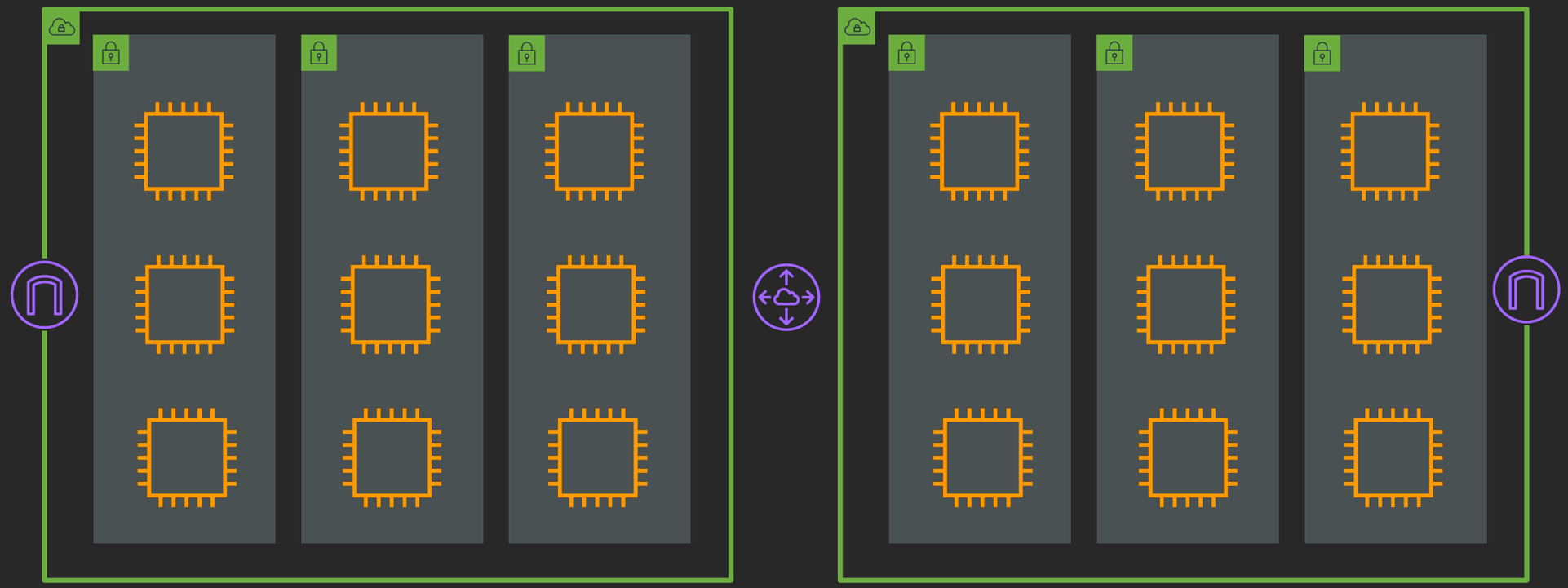


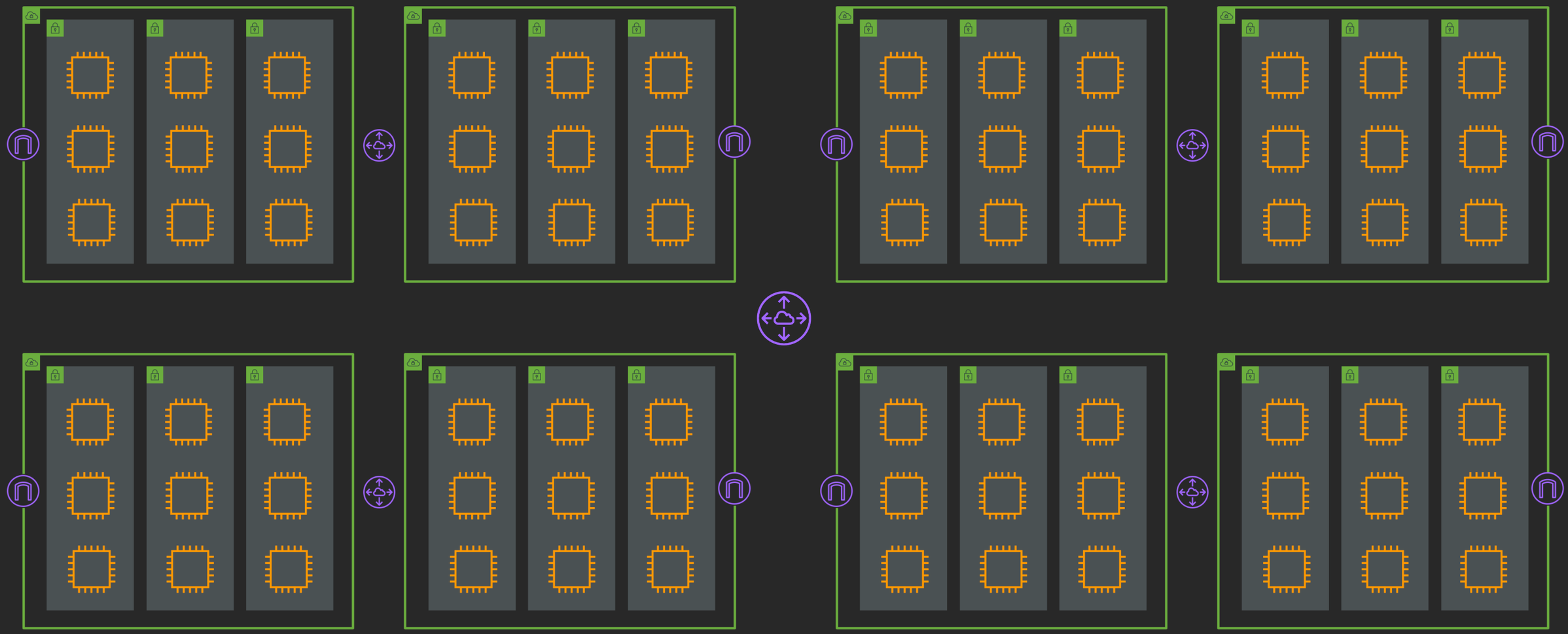
aws

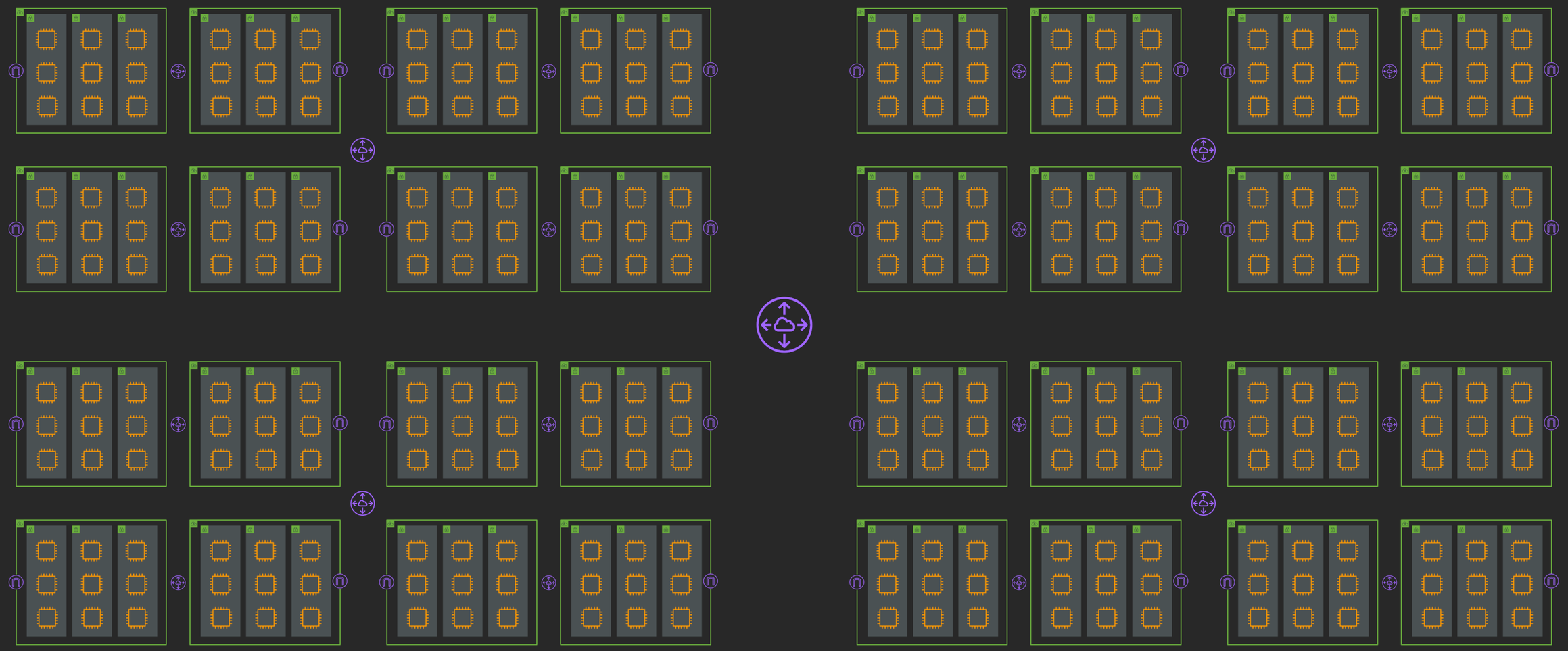
Reasoning about networks

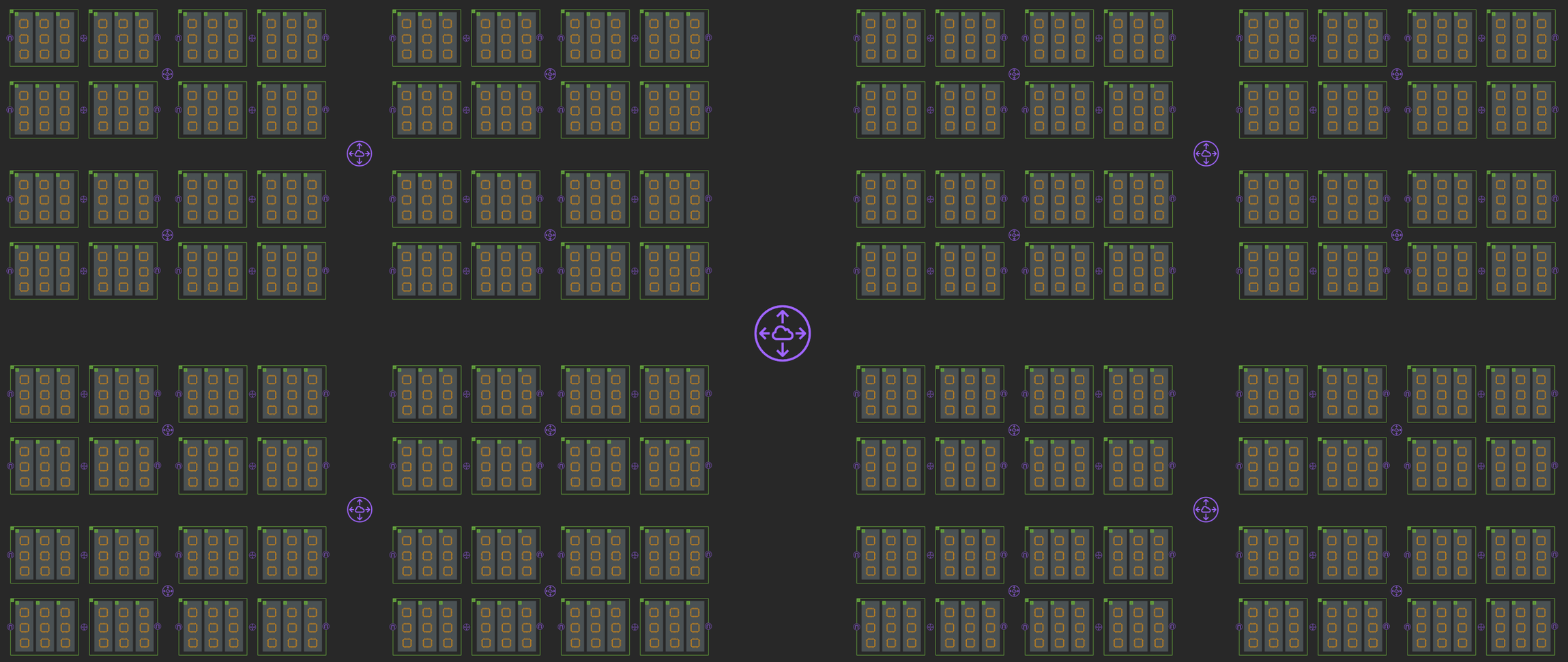

VPC
Web servers
Application servers
Data servers
Subnet
Subnet
Subnet
Internet gateway







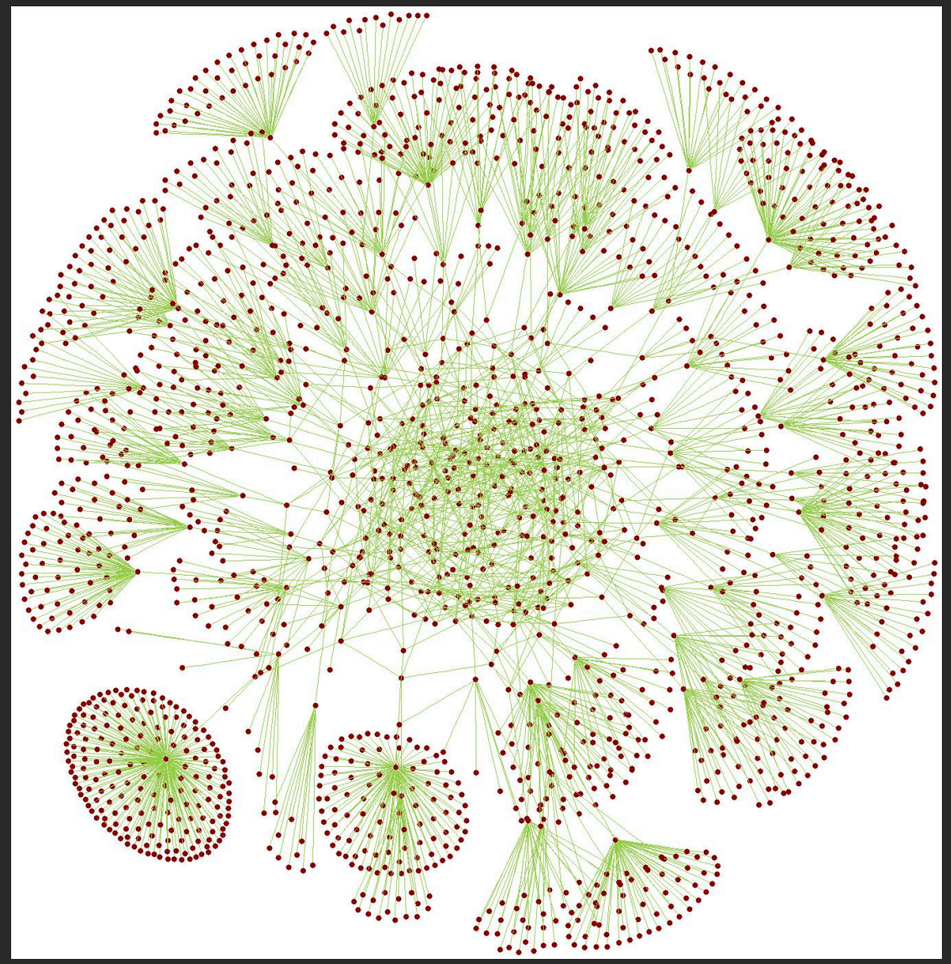




Tiros

Did I build the network I intended?

Did I build what I meant to build?



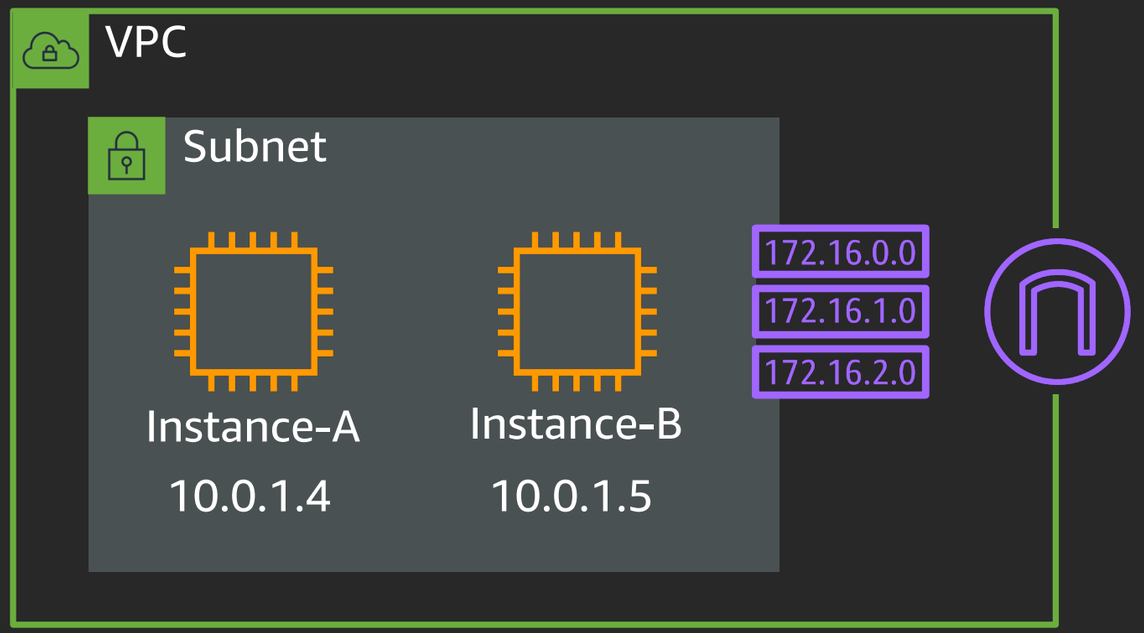
=

1.3: Prohibit direct public access between the internet and any system component in the cardholder data environment

*Partial map of internet – used with permission of University of California San Diego

Network snapshots

ec2:DescribeInstances
ec2:DescribeNetworkInterfaces
ec2:DescribeSubnets
ec2:DescribeRouteTables
ec2:DescribeVpcs
ec2:DescribeInternetGateways



Which instances are reachable from the internet?

What's a route table?

What's an instance?

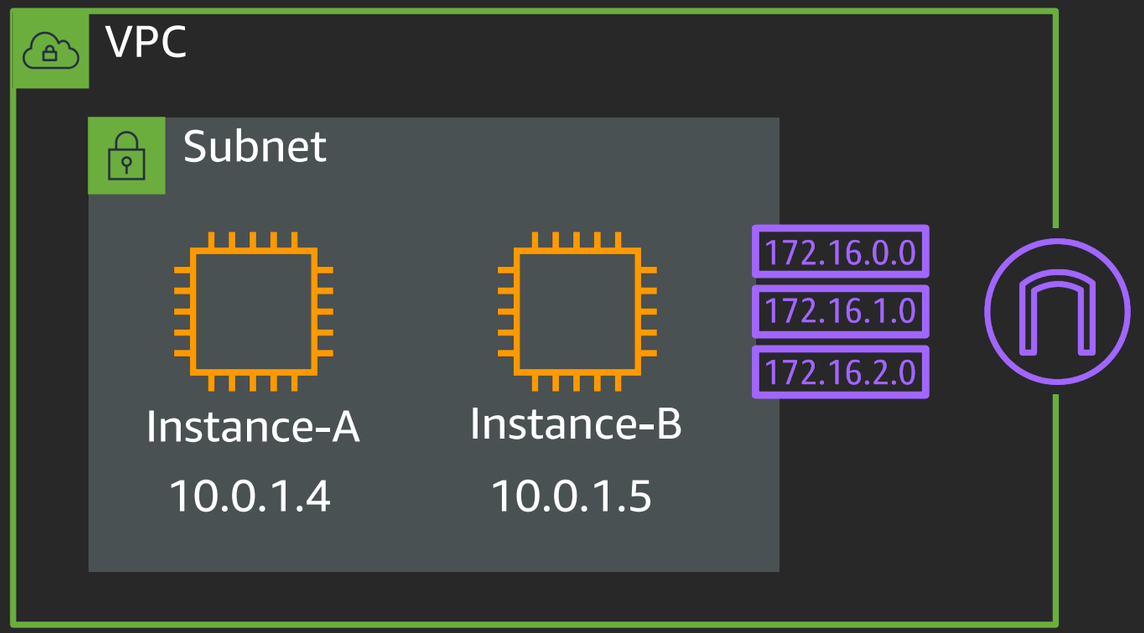
What's an internet gateway?

SMT Solver +

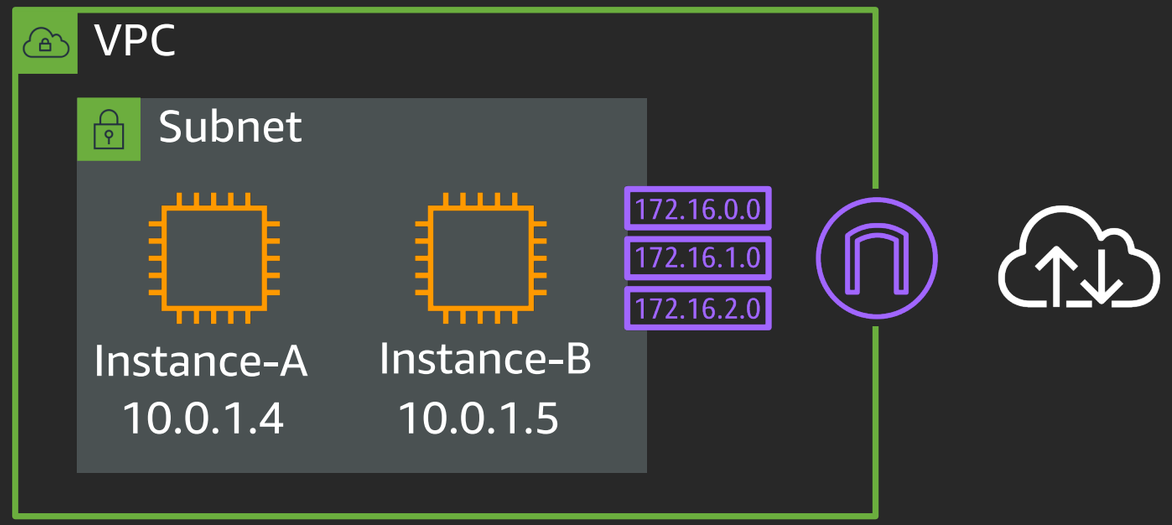
What's the internet?

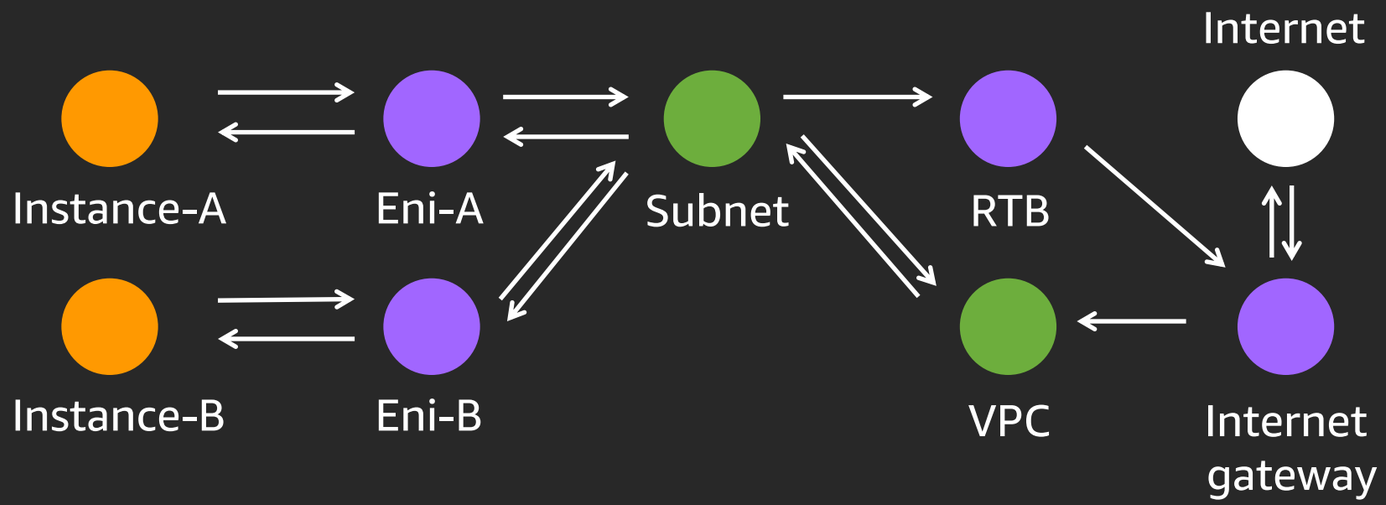
What's a subnet?

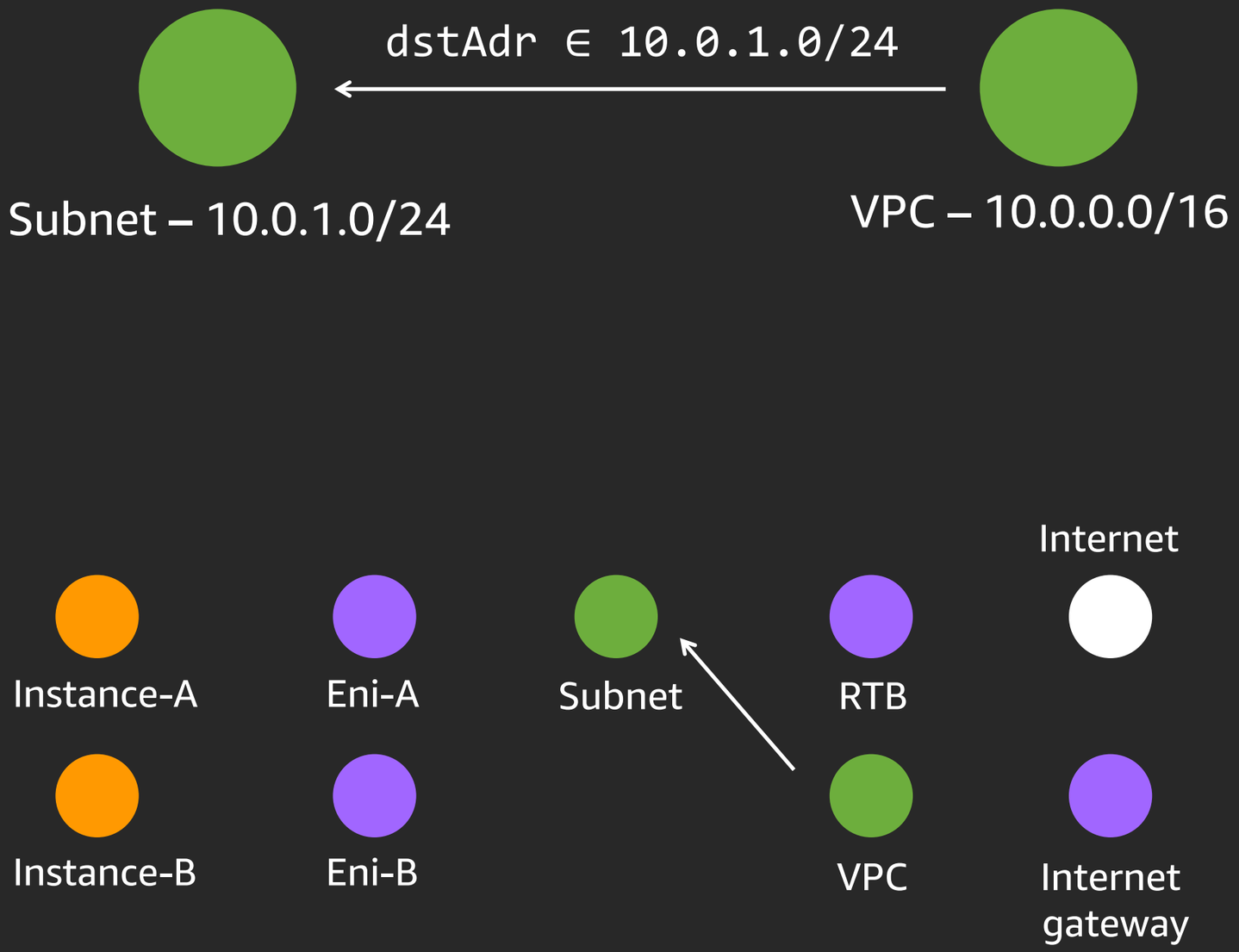
What's a VPC?

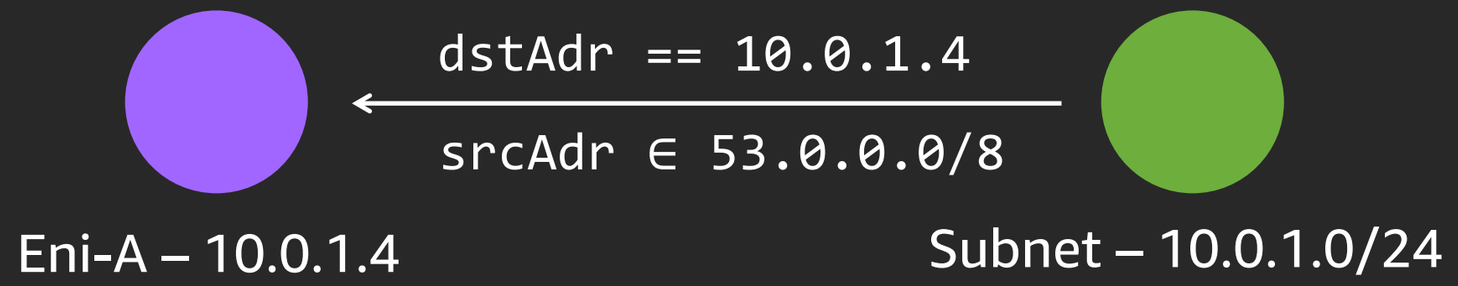


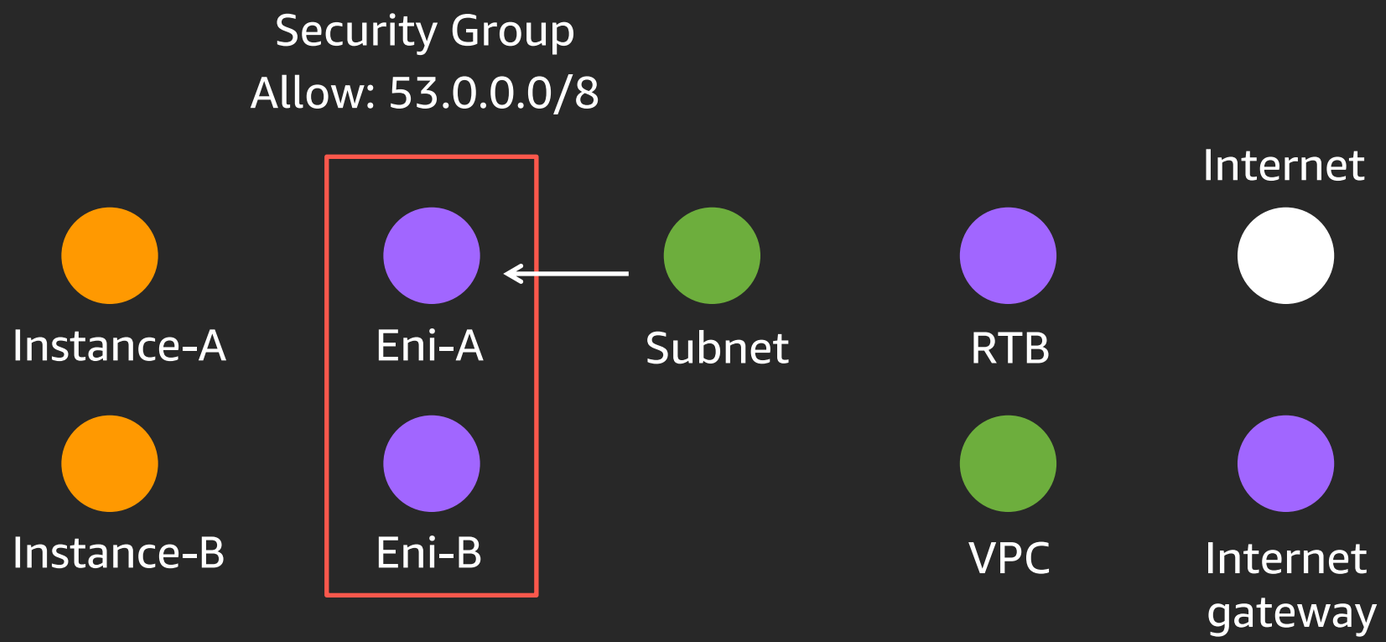
Secret sauce


VPC
Subnet
172.16.0.0
172.16.1.0
172.16.2.0
Instance-A
10.0.1.4
Instance-B
10.0.1.5


Internet
Instance-A
Eni-A
Subnet
RTB
Instance-B
Eni-B
VPC
Internet
gateway


dstAdr ∈ 10.0.1.0/24
Subnet – 10.0.1.0/24
VPC – 10.0.0.0/16
Internet
Instance-A
Eni-A
Subnet
RTB
Instance-B
Eni-B
VPC
Internet gateway


dstAdr == 10.0.1.4
srcAdr ∈ 53.0.0.0/8
Eni-A – 10.0.1.4
Subnet – 10.0.1.0/24

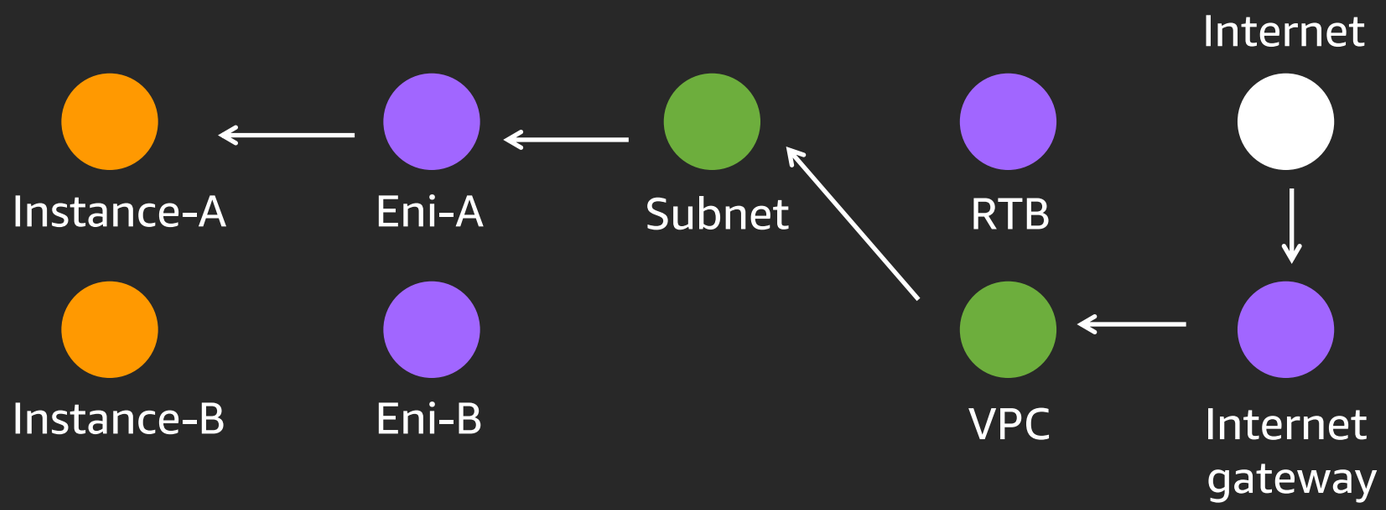

Security Group
Allow: 53.0.0.0/8
Instance-A
Instance-B
Eni-A
Eni-B
Subnet
RTB
VPC
Internet
Internet gateway

Can I SSH into Instance-A from the internet?

```
dstPort == 22 and
srcPort >= 1024 and
protocol == TCP and
reaches(Internet, Instance-A)
```

SMT Solver

```
protocol = TCP
srcAdr = 53.0.0.2,
dstAdr = 10.0.1.4,
dstPrt = 22
```



jbackes

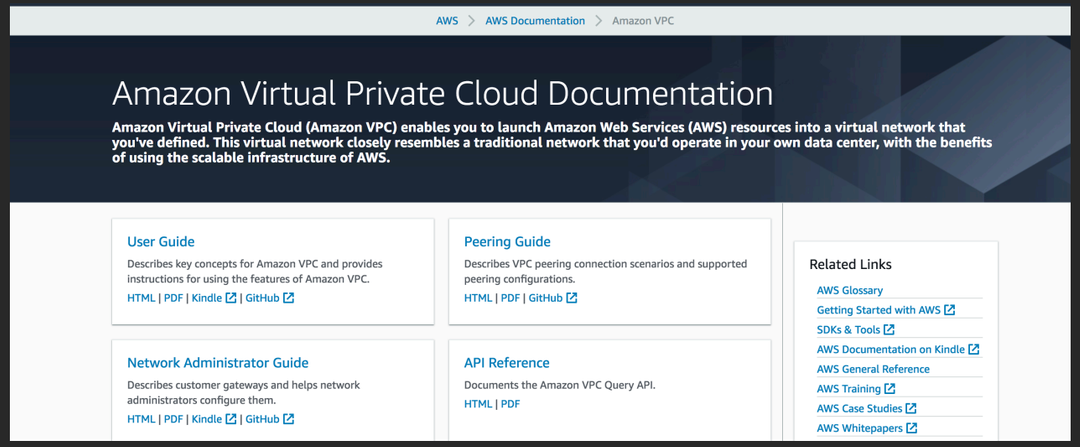
John
Backes

seanmcl

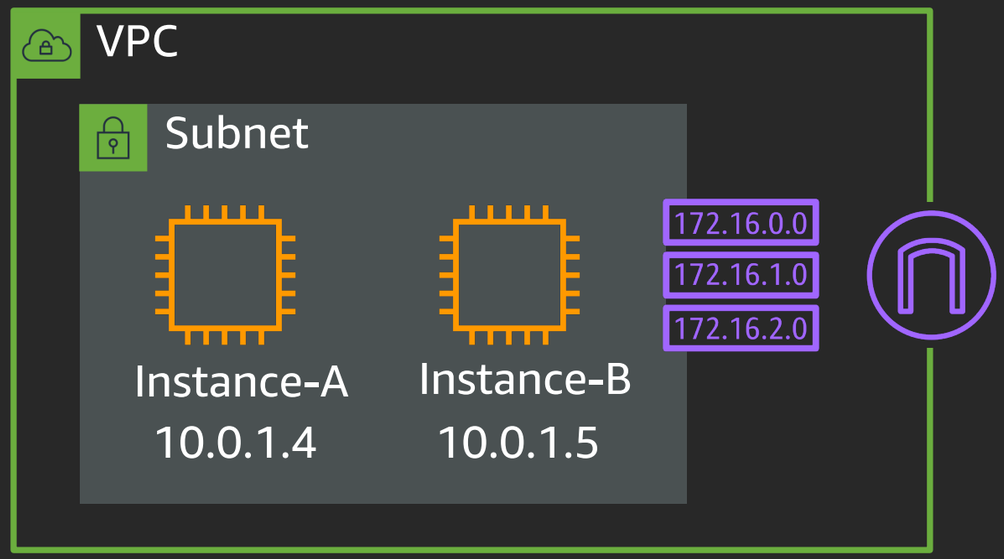
Sean
McLaughlin

=

+



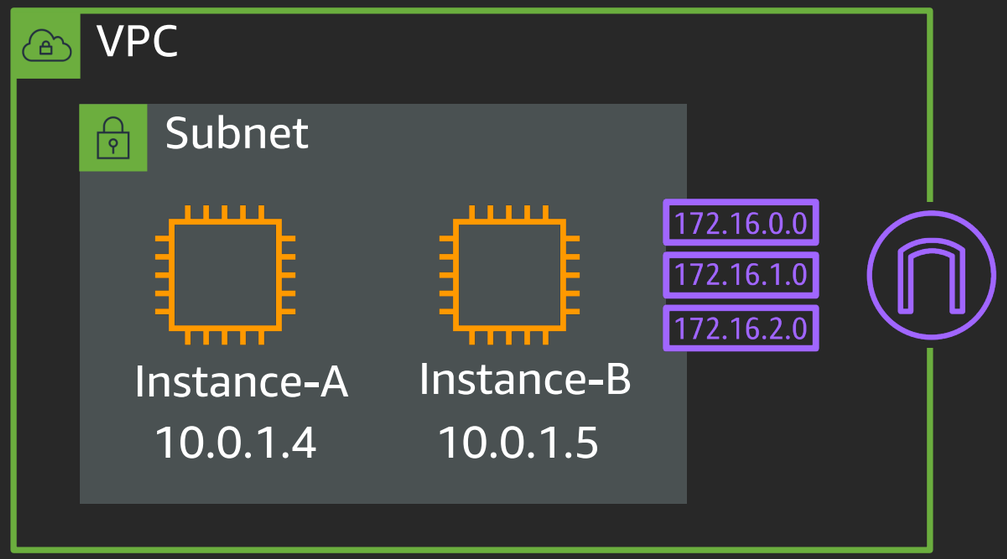
Which instances are reachable from the internet?



+

SMT Solver

Which instances are reachable from the internet?



=

```
i-0dd8ee72393d2dc50,
i-013c20e6045052f1d,
i-0608efa333be2d4f5,
i-04482af06a1546be2
```

Reachability Analysis for AWS-based Networks

J. Backes[1], S. Bayless[14], B. Cook[12], C. Dodge[1], A. Gacek[1], A.J. Hu[4], T. Kahsai[1], B. Kocik[1], E. Kotelnikov[13], J. Kukovec[15], S. McLaughlin[1], J. Reed[6], N. Rungta[1], J. Sizemore[1], M. Stalzer[1], P. Srinivasan[1], P. Subotić[12], C. Varming[1], B. Whaley[1], Y. Wu[1]

[1]Amazon Web Services, [2]University College London, [3]Chalmers University of Technology, [4]University British Columbia, [5]Vienna University of Technology, [6]Semmle Inc

Abstract. Cloud services provide the ability to provision virtual networked infrastructure on demand over the internet. The rapid growth of these virtually provisioned cloud networks has increased the demand for automated reasoning tools capable of identifying misconfigurations or security vulnerabilities. This type of automation gives customers the assurance they need to deploy sensitive workloads. It can also dramatically reduce the cost and time-to-market for regulated customers looking to establish compliance certification for cloud-based applications. In this industrial case-study, we describe a new network reachability reasoning tool, called TIROS, that uses off-the-shelf automated theorem proving tools to fill this need. TIROS is the foundation of a recently introduced network security analysis feature in the *Amazon Inspector* service now available to millions of customers building applications in the cloud. TIROS is also used within Amazon Web Services (AWS) to automate the checking of compliance certification and adherence to security invariants for many AWS services that build on existing AWS networking features.

Do I have to be a Formal Methods SME to use Tiros?

jbackes

John
Backes

seanmcl

Sean
McLaughlin

Amazon Inspector

Amazon Inspector enables you to analyze the behavior of your AWS resources and helps you identify potential security issues.

Get started

Install

Install the AWS agent on your EC2 instances.

Run

Run an assessment for your assessment target.

Analyze

Review your findings and remediate security issues.

Welcome to Amazon Inspector

Amazon Inspector assessments check for security exposures and vulnerabilities in your EC2 instances. Learn more about how Inspector functions.

Inspector uses a Service-linked Role to describe your EC2 instances and network configuration.

Assessment Setup

Check this box for Tiros!

You can use the options below to get the following assessments on all of your EC2 instances in this AWS region. Click **Run weekly** for the assessment to run at this time once a week starting now, **Run once** for a one-time assessment, or **Advanced setup** for custom assessments.

☑ **Network Assessments** (Inspector Agent is not required)

- **Assessments performed:** Network configuration analysis to checks for ports reachable from outside the VPC. Learn more
- **Optional Agent:** If the Inspector Agent is installed on your EC2 instances, the assessment also finds processes reachable on port. Learn more about Inspector Agent
- **Pricing:** Pricing for **network assessments** is based on the monthly volume of instance-assessments, where an instance-assessment denotes a successful assessment of an instance. For example, for 100 instances assessed weekly, the monthly cost would be around $61/month. Learn more

☑ **Host Assessments** (Inspector Agent is required)

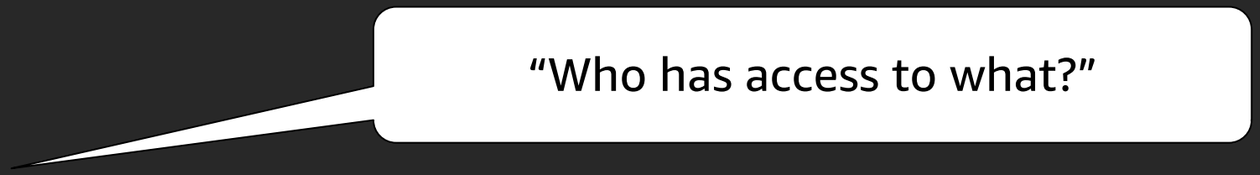
- **Assessments performed:** Vulnerable software (CVE), host hardening (CIS benchmarks), and security best practices. Learn more
- **Agent Deployment:** Inspector assessments require an agent to be installed on your EC2 instances. We will automatically install the agent for instances that allow System Manager Run Command. Learn more about Inspector Agent and how to manually install agent.
- **Pricing:** Pricing for **host assessments** is based on the monthly volume of agent-assessments, where an agent-assessment denotes a successful assessment of an instance. For example, for 100 instances assessed weekly, the monthly cost would be around $120/month. Learn more

Run weekly (recommended) | **Run once** | **Advanced setup** | Cancel

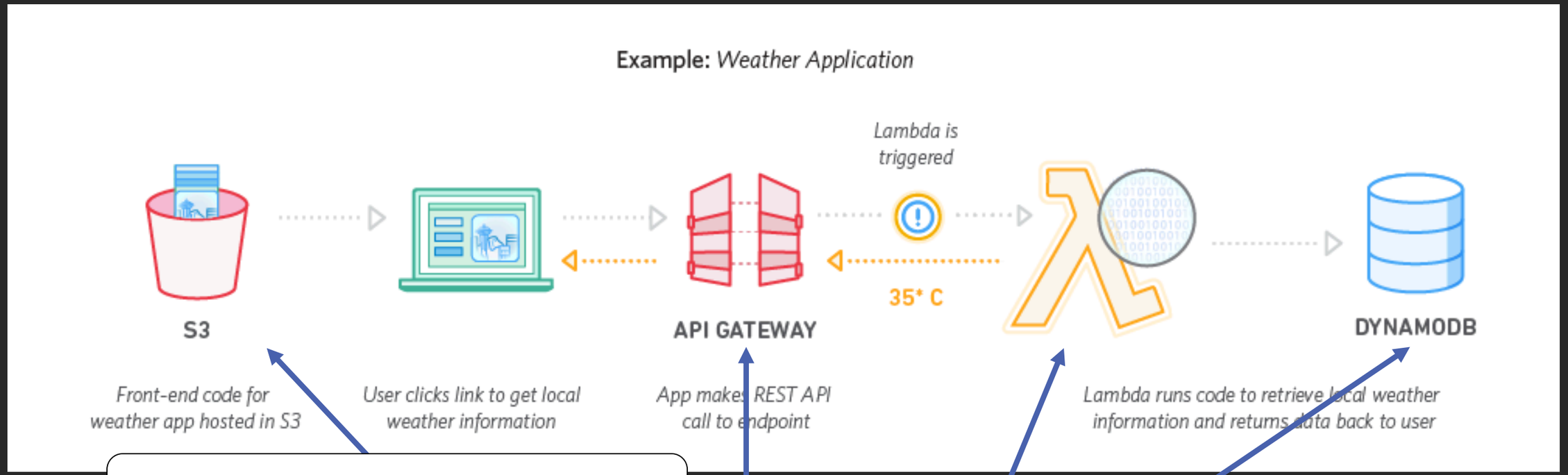
Reasoning about access control

Access control (the traditional model)

Database credentials
SSH keys
File system permissions
Network share drives
…



Access control (the AWS model)



Everything accessible via APIs

All governed by the
AWS Identity and Access Management (IAM)
language

Policy example

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "111122223333"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::my-bucket/*"
    },
    {
      "Effect": ”Deny",
      "Principal": {
        "AWS": "444455556666"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::my-bucket/uploads/*"
    }
  ]
}
```

Who …

… is allowed to do what …

… to what resources?

Policies everywhere

- Organizations have SCPs
- Users and Roles have identity policies
- Amazon S3 buckets have policies
- AWS KMS keys have policies
- Lambda functions have policies
- Amazon SQS queues have policies
- Amazon SNS topics have policies

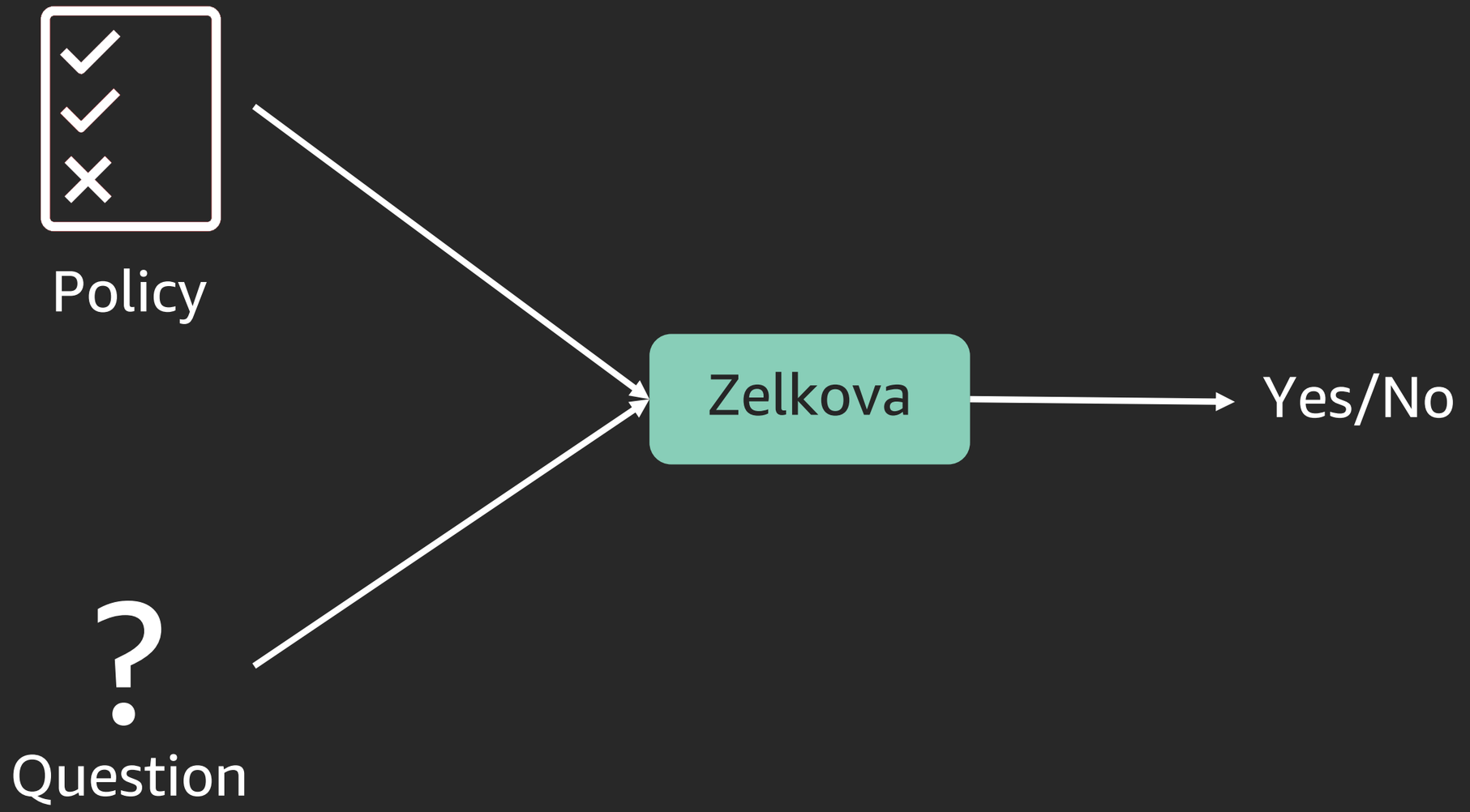
Did I grant permissions that I intended?

```
for acc in accounts:
 for u in users:
  for r in resources:
   for act in actions:
    for srcip in ips:
     for srcvpc in vpcs:
      for ref in referers:
        .......
```

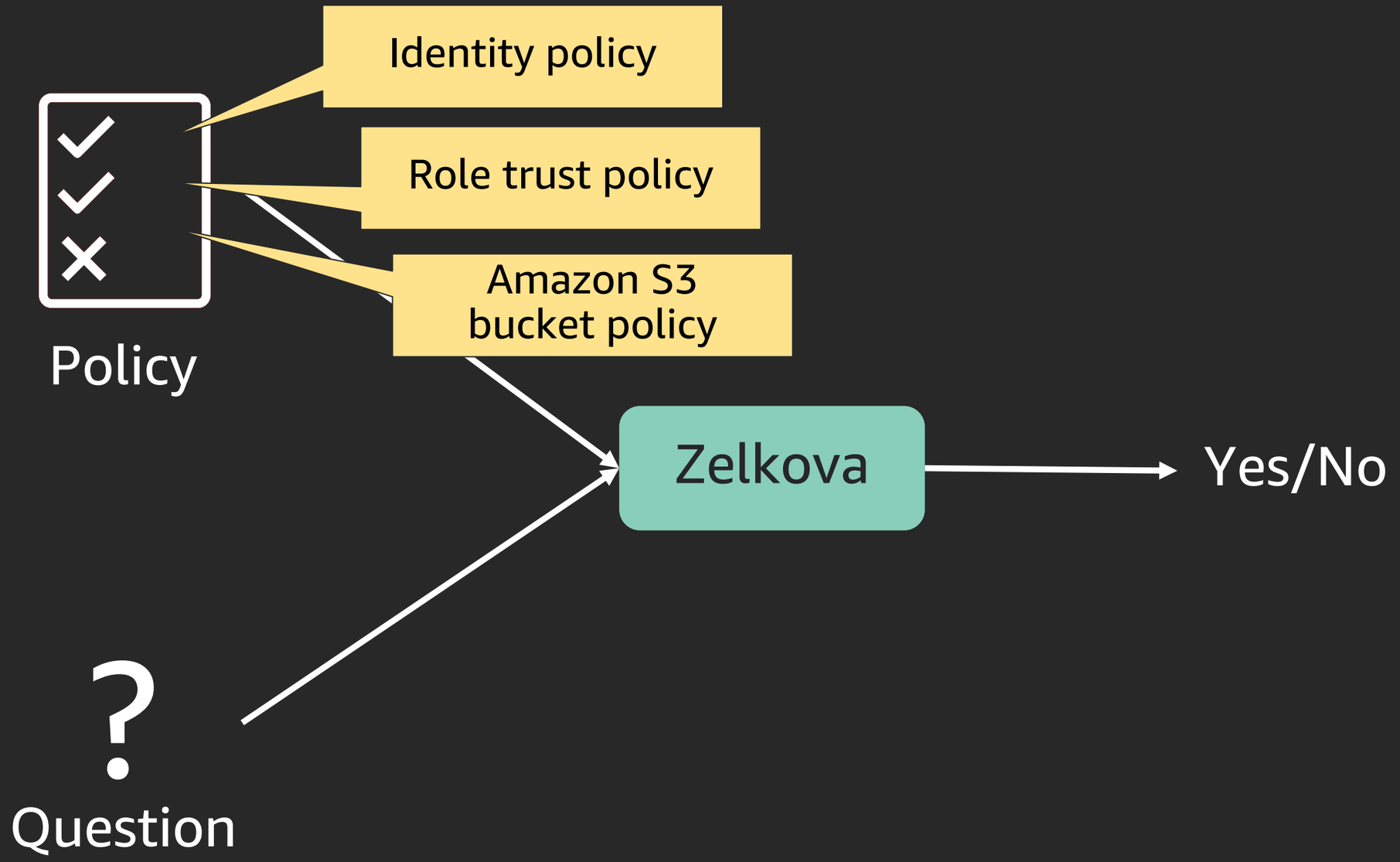
10^{12}
50
1000
2000
2^{32}
36^{8}
∞

∞

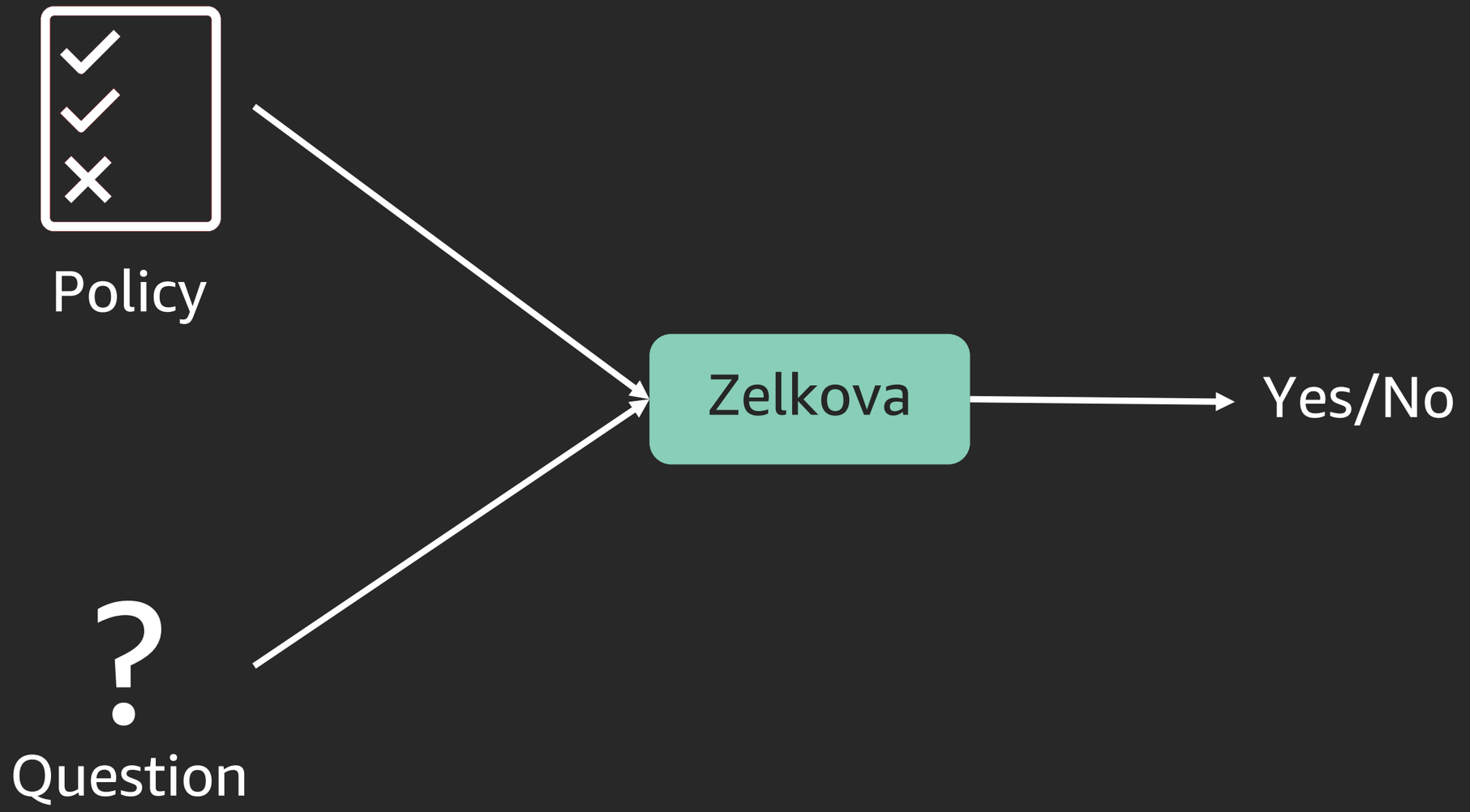
Zelkova



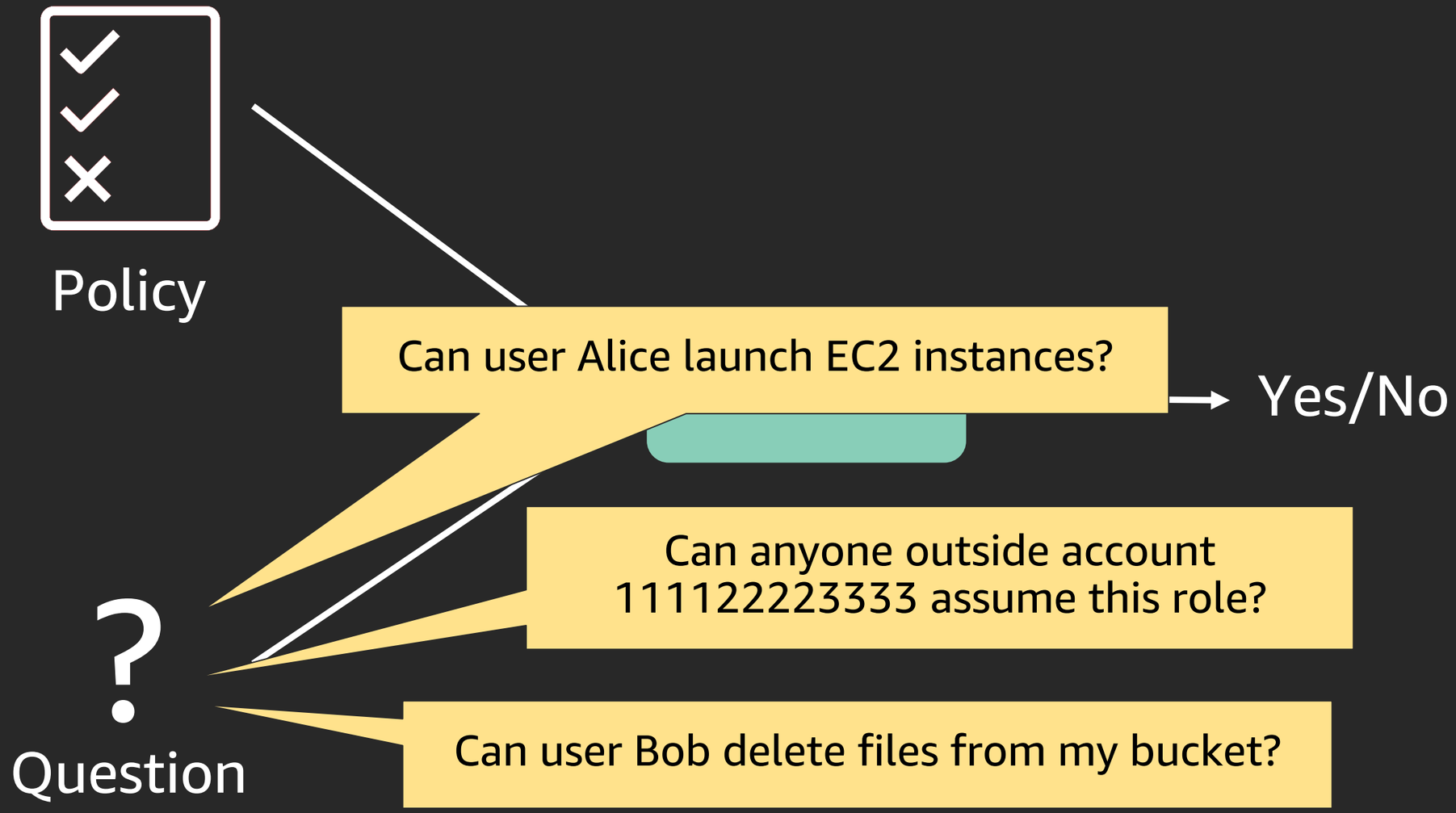
Zelkova


Identity policy
Role trust policy
Amazon S3
bucket policy
Policy
Zelkova
Yes/No
?
Question

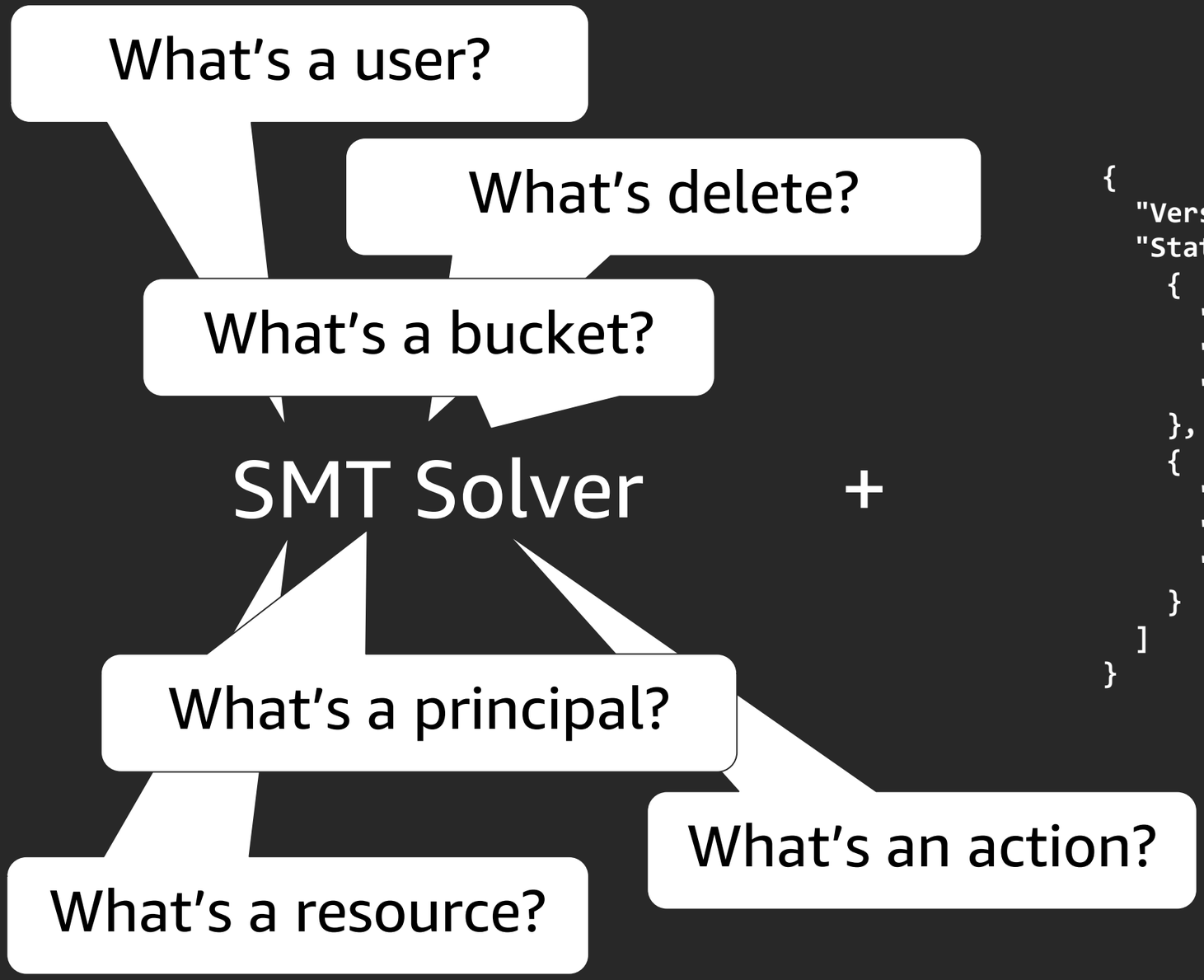
Zelkova



Zelkova


Policy
Can user Alice launch EC2 instances?
Yes/No
Can anyone outside account 111122223333 assume this role?
?
Question
Can user Bob delete files from my bucket?

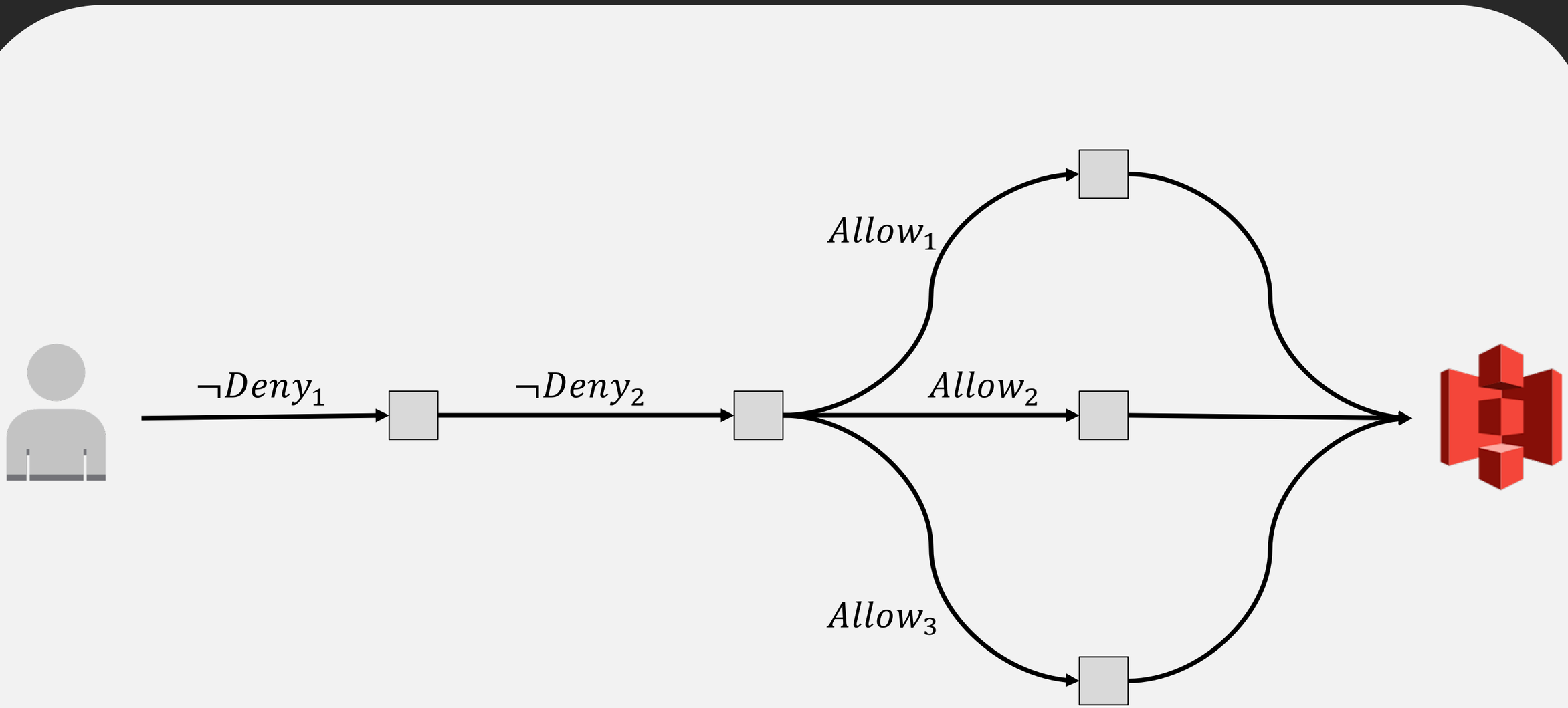
Can user Bob delete files from my bucket?

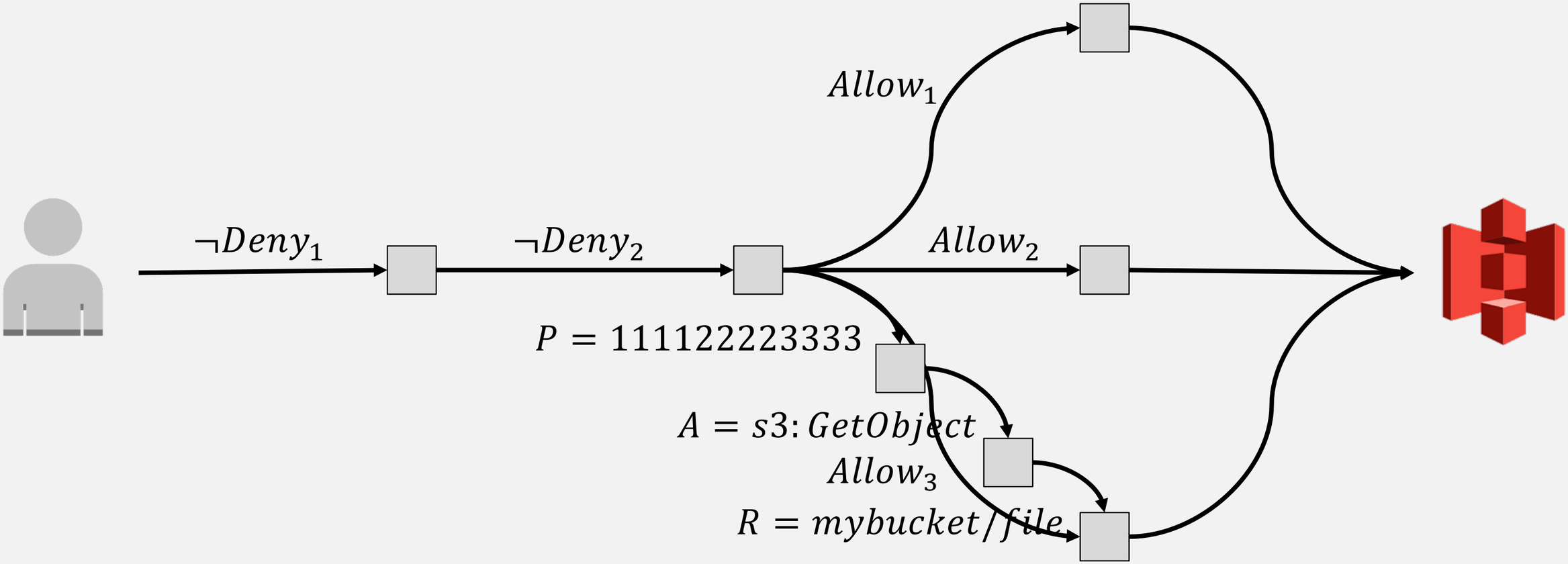


+

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::my-bucket/*"
    },
    {
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::my-bucket/uploads/*"
    }
  ]
}
```

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      ...
    },
    {
      "Effect": "Deny",
      ...
    },
    {
      "Effect": "Allow",
      ...
    },
    {
      "Effect": "Allow",
      ...
    },
    {
      "Effect": "Allow",
      ...
    }
  ]
}
```


$\neg Deny_1$
$\neg Deny_2$
$Allow_1$
$Allow_2$
$Allow_3$


$\neg Deny_1$
$\neg Deny_2$
$Allow_1$
$Allow_2$
$P = 111122223333$
$A = s3{:}GetObject$
$Allow_3$
$R = mybucket/file$

varming

Carsten
Varming

hadarean

Liana
Hadarean

=

+

AWS > AWS Documentation > AWS Identity and Access Management

AWS Identity and Access Management Documentation

AWS Identity and Access Management (IAM) is a web service for securely controlling access to AWS services. With IAM, you can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users and applications can access.

Can user Bob delete files from my bucket?


```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::my-bucket/*"
    },
    {
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::my-bucket/uploads/*"
    }
  ]
}
```

+

SMT Solver

Can user Bob delete files from my bucket?


```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::my-bucket/*"
    },
    {
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::my-bucket/uploads/*"
    }
  ]
}
```

=

No

Semantic-based Automated Reasoning for AWS Access Policies using SMT

John Backes, Pauline Bolignano, Byron Cook, Catherine Dodge, Andrew Gacek,
Kasper Luckow, Neha Rungta, Oksana Tkachuk, Carsten Varming
Amazon Web Services

***Abstract*—Cloud computing provides on-demand access to IT resources via the Internet. Permissions for these resources are defined by expressive access control policies. This paper presents a formalization of the Amazon Web Services (AWS) policy language and a corresponding analysis tool, called ZELKOVA, for verifying policy properties. ZELKOVA encodes the semantics of policies into SMT, compares behaviors, and verifies properties. It provides users a sound mechanism to detect misconfigurations of their policies. ZELKOVA solves a PSPACE-complete problem and is invoked many millions of times daily.**

I. INTRODUCTION

Cloud computing provides on-demand access to IT resources via the Internet. The convenience of accessing resources in the cloud is made secure by user-specified *access control policies*. An access control policy is an expressive specification of what resources can be accessed, by whom, and under what conditions. Properly configured policies are an important part of an organization's security posture. The scale and diversity of cloud-based services is constantly growing (*e.g.*, serverless computing, streaming analytics, edge-computing devices), and each new offering used by an organization may require a different access policy configuration. Moreover, customers are combining these services, which means that the complexity is increasingly moving into policies.

In this paper, we present the development and application of ZELKOVA, a policy analysis tool designed to reason about the semantics of AWS access control policies. ZELKOVA translates policies and properties into Satisfiability Modulo Theories (SMT) formulas and uses SMT solvers to check the validity of the properties. We use off-the-shelf solvers and an in-house extension of Z3 called Z3AUTOMATA.

ZELKOVA reasons about all possible permissions allowed by a policy in order to verify properties. For example, ZELKOVA can answer the questions "Is this resource accessible by a particular user?" and "Can an arbitrary user write to this resource?". The property to be verified is specified in the policy language itself, eliminating the need for a different specification or formalism for properties. In addition, ZELKOVA provides many built-in checks for common properties.

The SMT encoding uses the theory of strings, regular expressions, bit vectors, and integer comparisons. The use of the wildcards $*$ (any number of characters) and ? (exactly one character) in the string constraints makes the decision problem PSPACE-complete. However, our experience with real-world policies is that 99% of policy questions can be answered in less than 160 milliseconds.

ZELKOVA is the underlying policy analysis engine for a growing number of AWS services. Used many millions

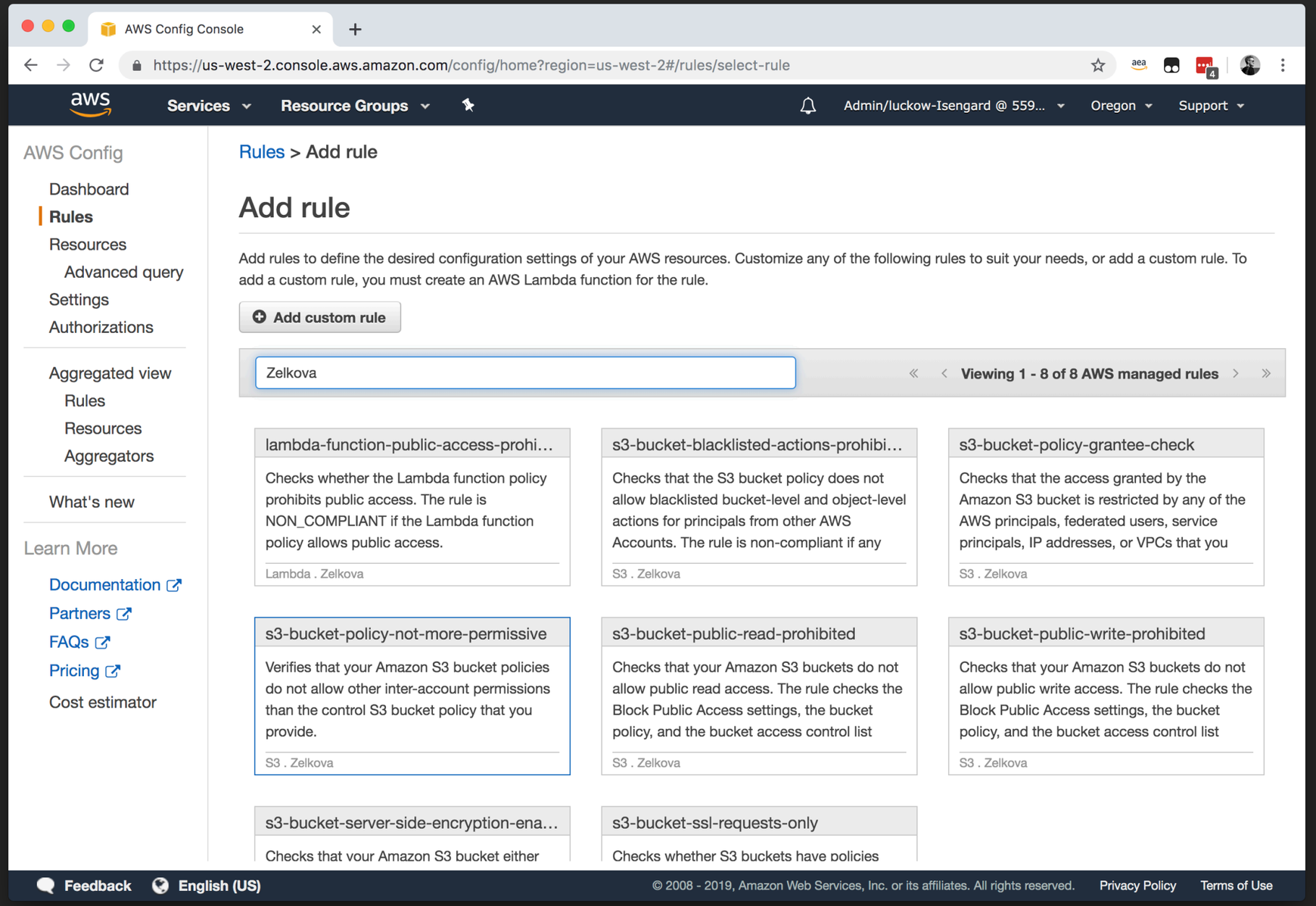
Do I have to be a Formal Methods SME?

varming

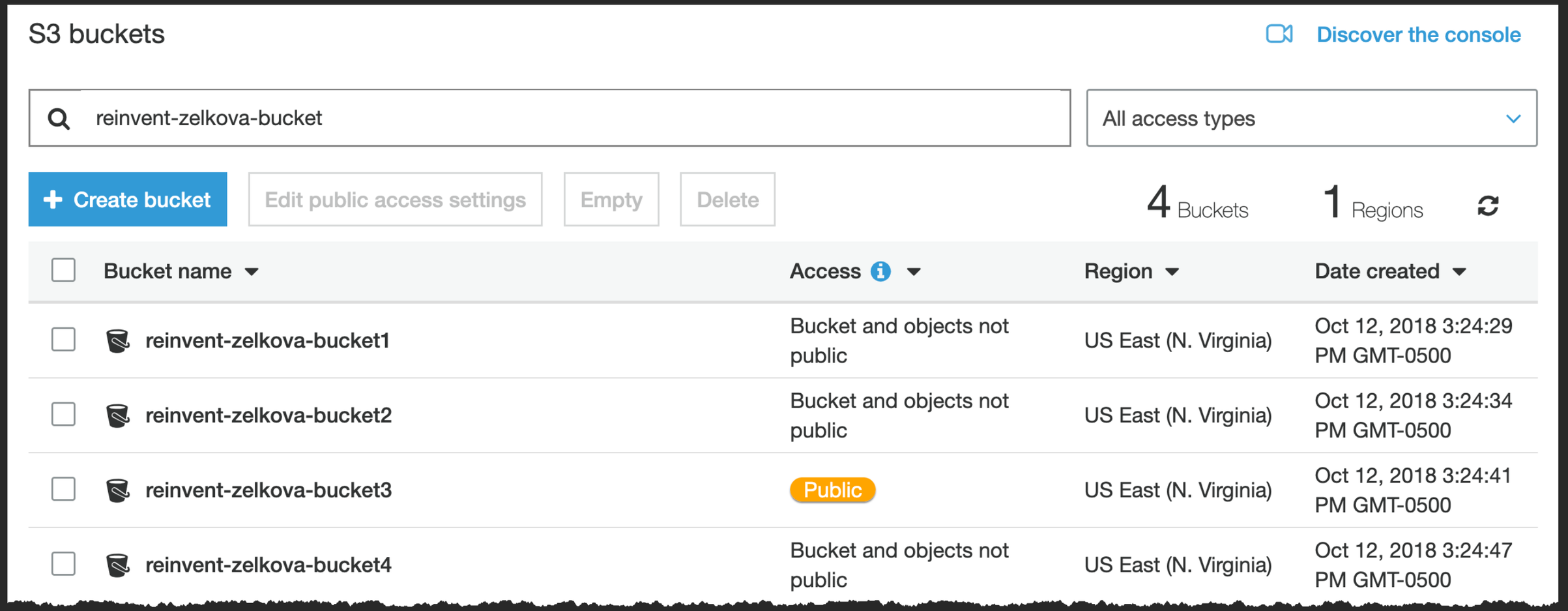
Carsten
Varming

hadarean

Liana
Hadarean


AWS Config Console
https://us-west-2.console.aws.amazon.com/config/home?region=us-west-2#/rules/select-rule
aws
Services
Resource Groups
Admin/luckow-Isengard @ 559...
Oregon
Support
AWS Config
Dashboard
Rules
Resources
Advanced query
Settings
Authorizations
Aggregated view
Rules
Resources
Aggregators
What's new
Learn More
Documentation
Partners
FAQs
Pricing
Cost estimator
Rules > Add rule
Add rule
Add rules to define the desired configuration settings of your AWS resources. Customize any of the following rules to suit your needs, or add a custom rule. To add a custom rule, you must create an AWS Lambda function for the rule.
Add custom rule
Zelkova
Viewing 1 - 8 of 8 AWS managed rules
lambda-function-public-access-prohi...
Checks whether the Lambda function policy prohibits public access. The rule is NON_COMPLIANT if the Lambda function policy allows public access.
Lambda . Zelkova
s3-bucket-blacklisted-actions-prohibi...
Checks that the S3 bucket policy does not allow blacklisted bucket-level and object-level actions for principals from other AWS Accounts. The rule is non-compliant if any
S3 . Zelkova
s3-bucket-policy-grantee-check
Checks that the access granted by the Amazon S3 bucket is restricted by any of the AWS principals, federated users, service principals, IP addresses, or VPCs that you
S3 . Zelkova
s3-bucket-policy-not-more-permissive
Verifies that your Amazon S3 bucket policies do not allow other inter-account permissions than the control S3 bucket policy that you provide.
S3 . Zelkova
s3-bucket-public-read-prohibited
Checks that your Amazon S3 buckets do not allow public read access. The rule checks the Block Public Access settings, the bucket policy, and the bucket access control list
S3 . Zelkova
s3-bucket-public-write-prohibited
Checks that your Amazon S3 buckets do not allow public write access. The rule checks the Block Public Access settings, the bucket policy, and the bucket access control list
S3 . Zelkova
s3-bucket-server-side-encryption-ena...
Checks that your Amazon S3 bucket either
s3-bucket-ssl-requests-only
Checks whether S3 buckets have policies
Feedback
English (US)
© 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

Amazon S3 console “Public” badge



Create bucket

Name and region | Configure options | 3 **Set permissions** | 4 Review

Note: You can grant access to specific users after you create the bucket.

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, or both. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block *all* public access. These settings apply only to this bucket. AWS recommends that you turn on Block *all* public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

- [x] **Block *all* public access**

  Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

  - [ ] **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
    S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
  - [ ] **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
    S3 will ignore all ACLs that grant public access to buckets and objects.
  - [ ] **Block public access to buckets and objects granted through *new* public bucket policies**
    S3 will block new bucket policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

Previous | Next

But…. Who has access to what?

“Who has access to what?”

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "11112222333"
  },
  "Action": "s3:GetObject",
  "Resource": "arn:aws:s3:::my-bucket/*"
},
{
  "Effect": "Deny",
  "Principal": "*",
  "Action": "*",
  "Resource": "arn:aws:s3:::my-bucket/*",
  "Condition": {
    "StringNotEquals": {
      "aws:SourceVpc": "vpc-abc"
    }
  }
}
```

```
Principal: 111122223333
Principal: *
aws:SourceVpc: vpc-abc
```

has

```
Action: s3:GetObject
Action: *
```

access to

```
Resource: my-bucket
```

“Who has access to what?”

Does 111122223333 have * access to my-bucket?

Does * have GetObject access to my-bucket?

Does * have * access to my-bucket?

Does 111122223333 with vpc-abc have GetObject access to my-bucket?

```
Principal: 111122223333
Principal: *
aws:SourceVpc: vpc-abc
```

has

```
Action: s3:GetObject
Action: *
```

access to

```
Resource: my-bucket
```

“Who has access to what?”

Does 111122223333 have * access to my-bucket?

Does * have GetObject access to my-bucket?

Does * have * access to my-bucket?

Does 111122223333 with vpc-abc have GetObject access to my-bucket?

```
Principal: 111122223333
Principal: *
aws:SourceVpc: vpc-abc
```

has

```
Action: s3:GetObject
Action: *
```

access to

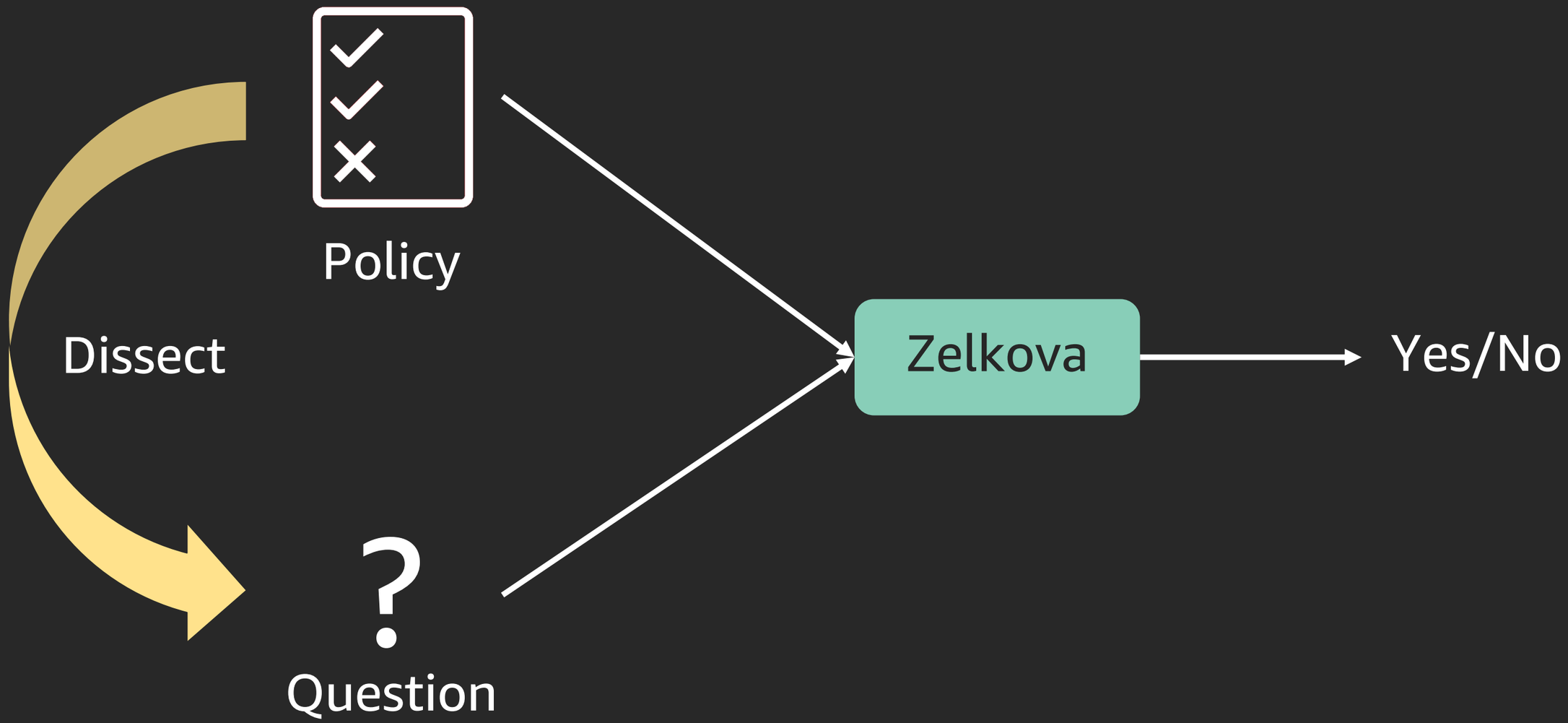
```
Resource: my-bucket
```

“Who has access to what?”

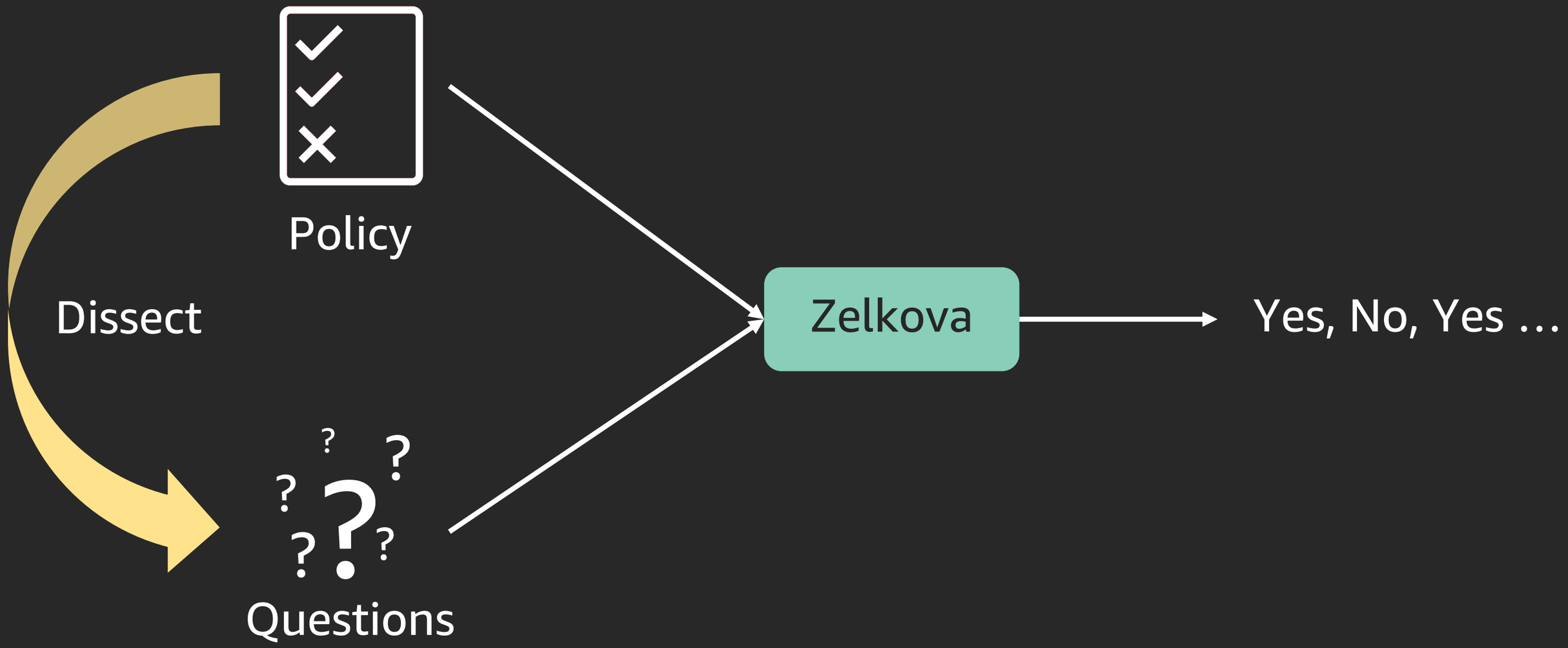
```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "11112222333"
  },
  "Action": "s3:GetObject",
  "Resource": "arn:aws:s3:::my-bucket/*"
},
{
  "Effect": "Deny",
  "Principal": "*",
  "Action": "*",
  "Resource": "arn:aws:s3:::my-bucket/*",
  "Condition": {
    "StringNotEquals": {
      "aws:SourceVpc": "vpc-abc"
    }
  }
}
```

Finding
Principal: 111122223333
Action: s3:GetObject
Resource: my-bucket
Condition:
  aws:SourceVpc: vpc-abc

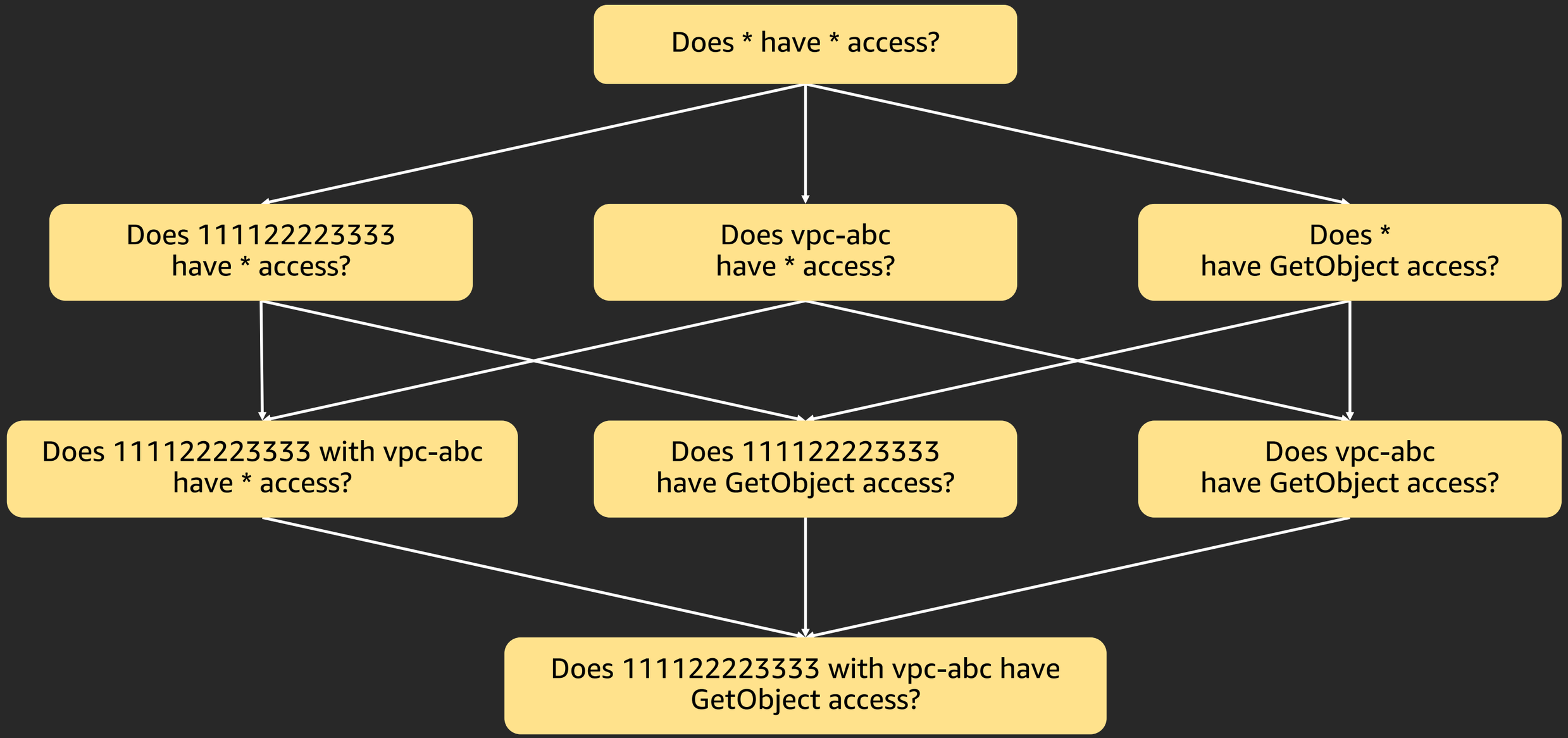
Access Analyzer



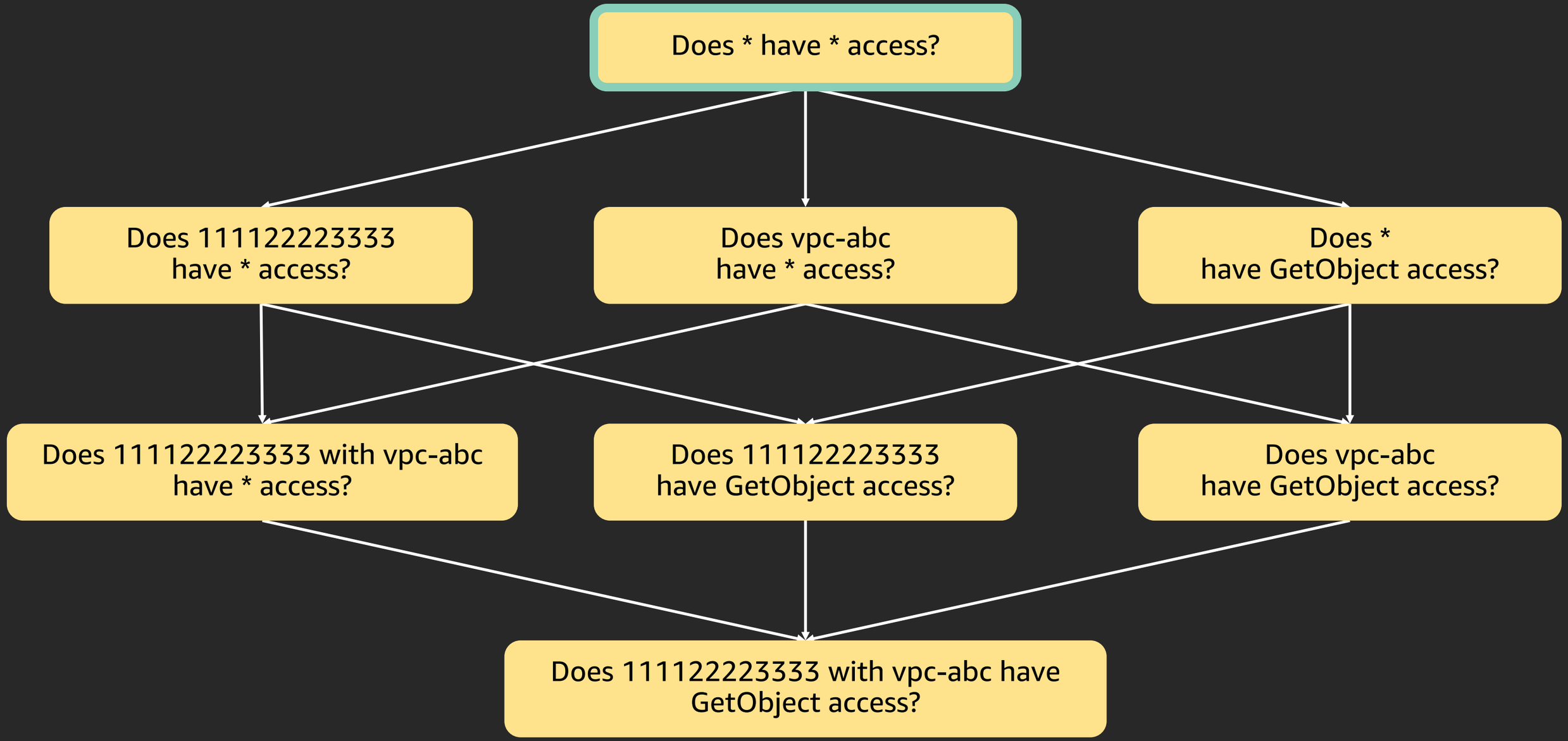
Access Analyzer



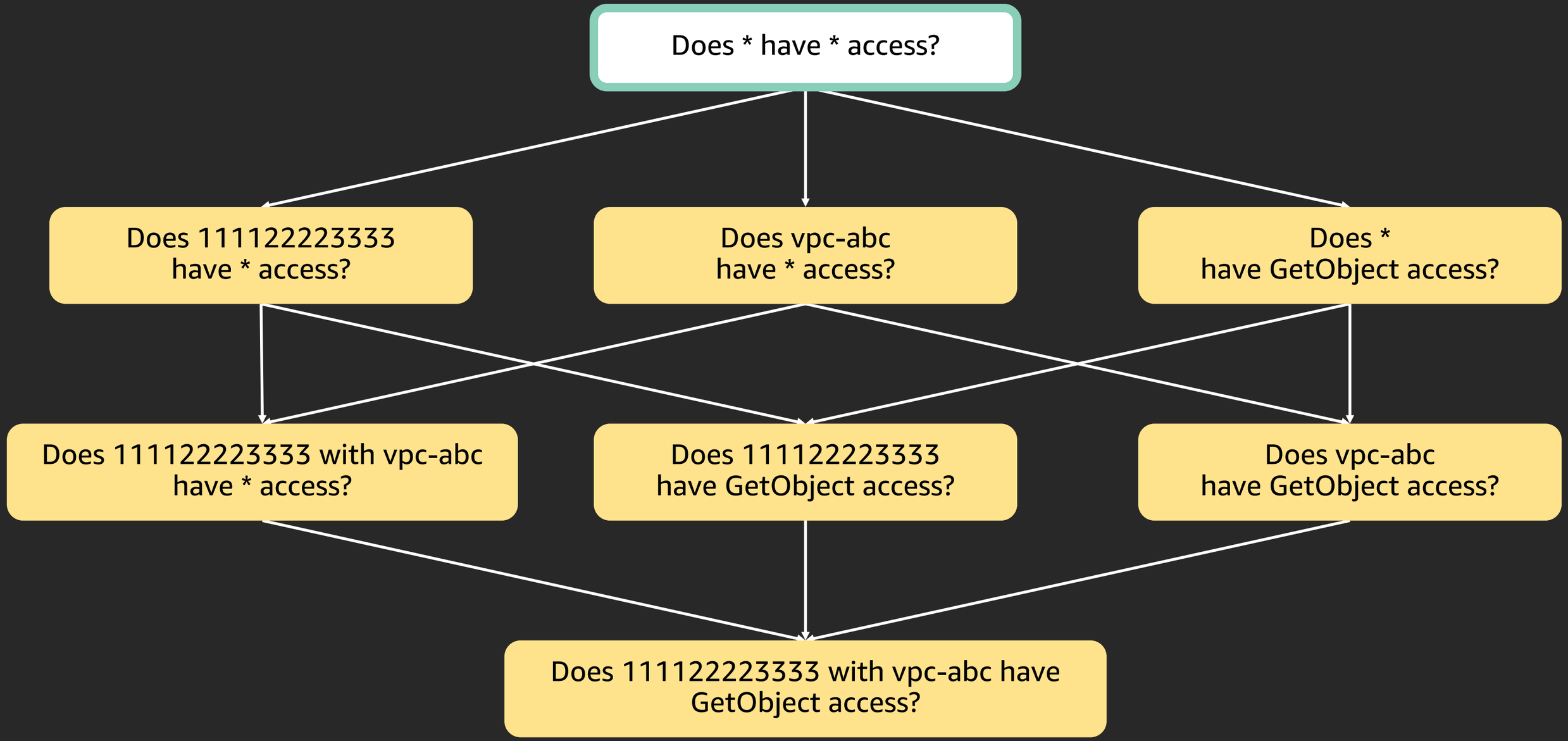
Twenty questions



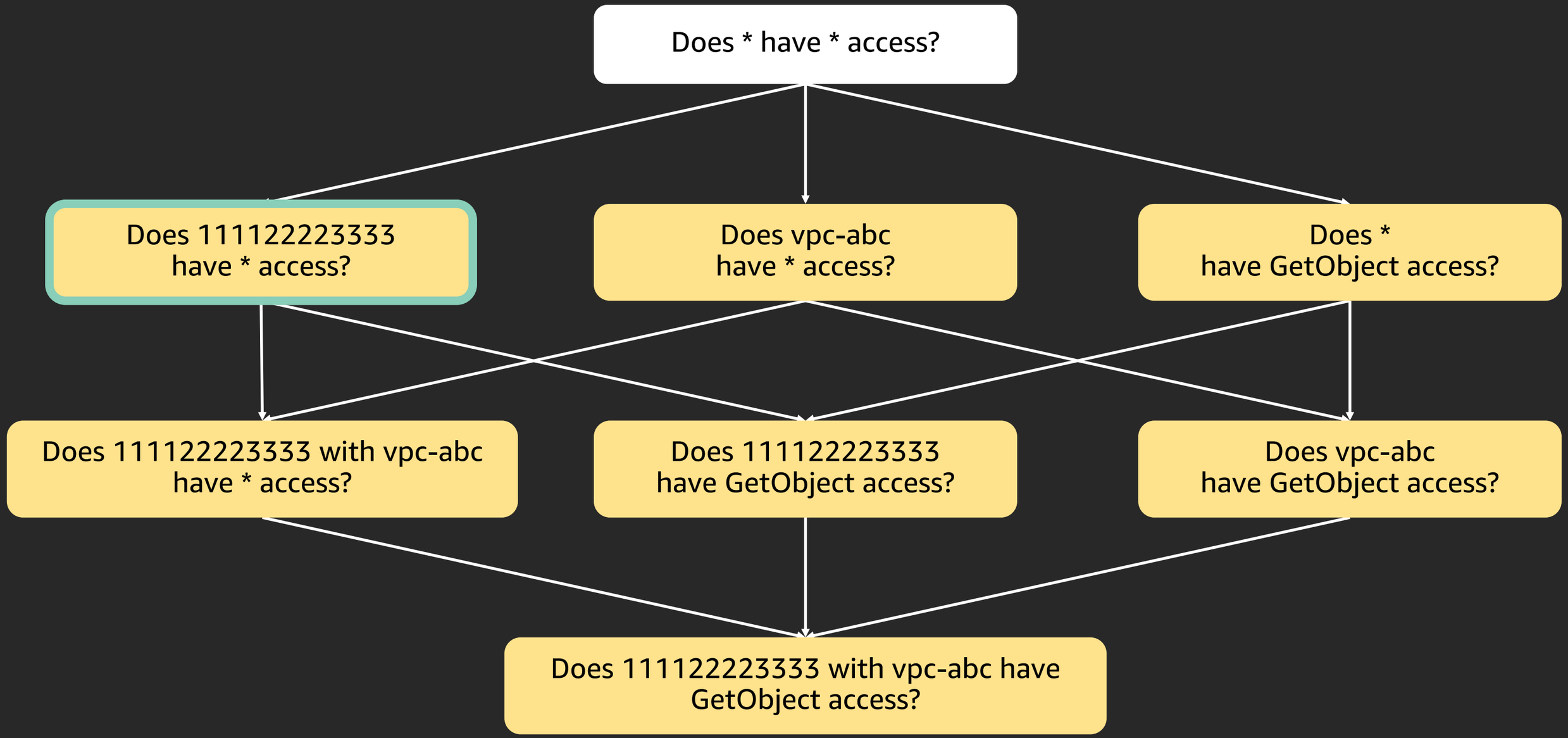
Twenty questions



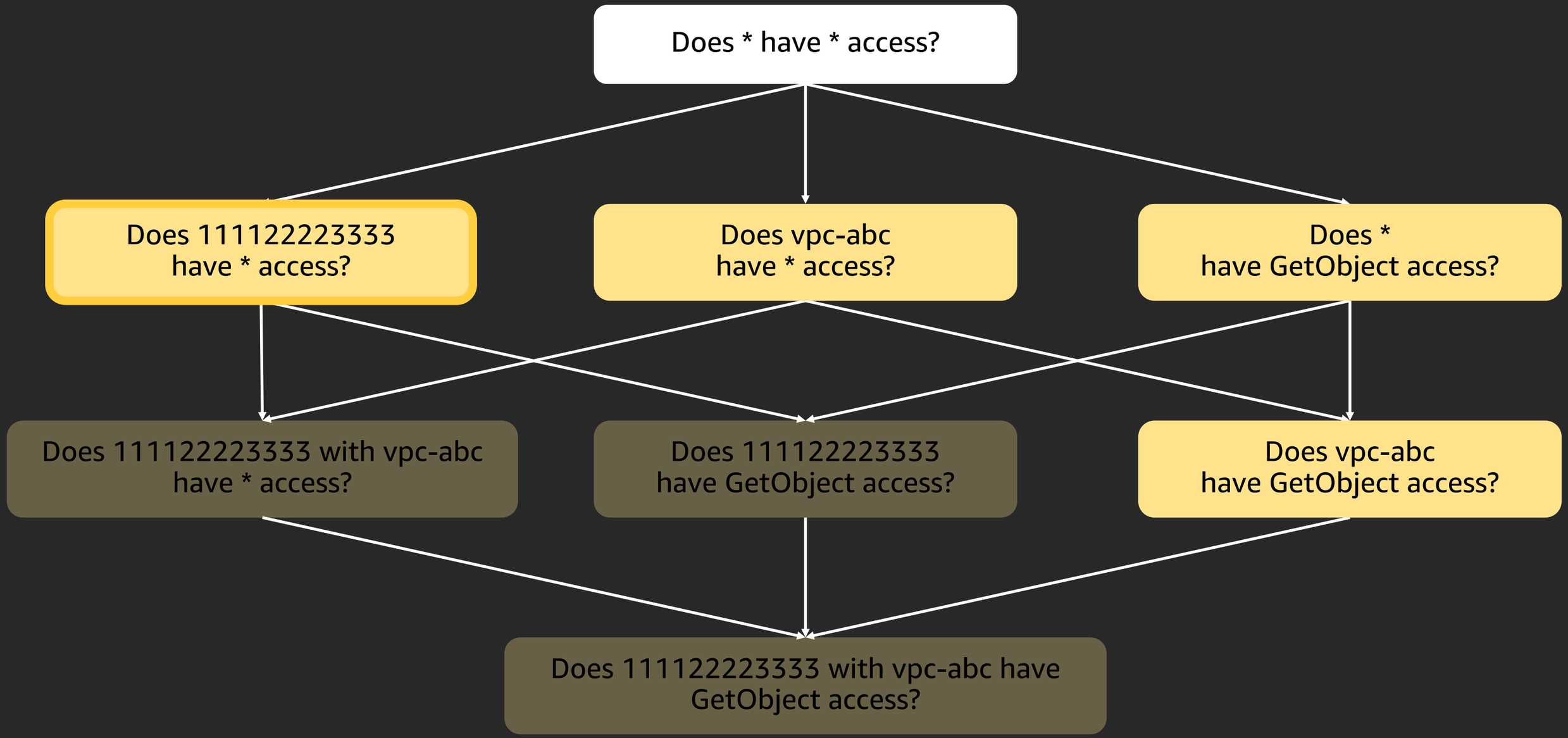
Twenty questions



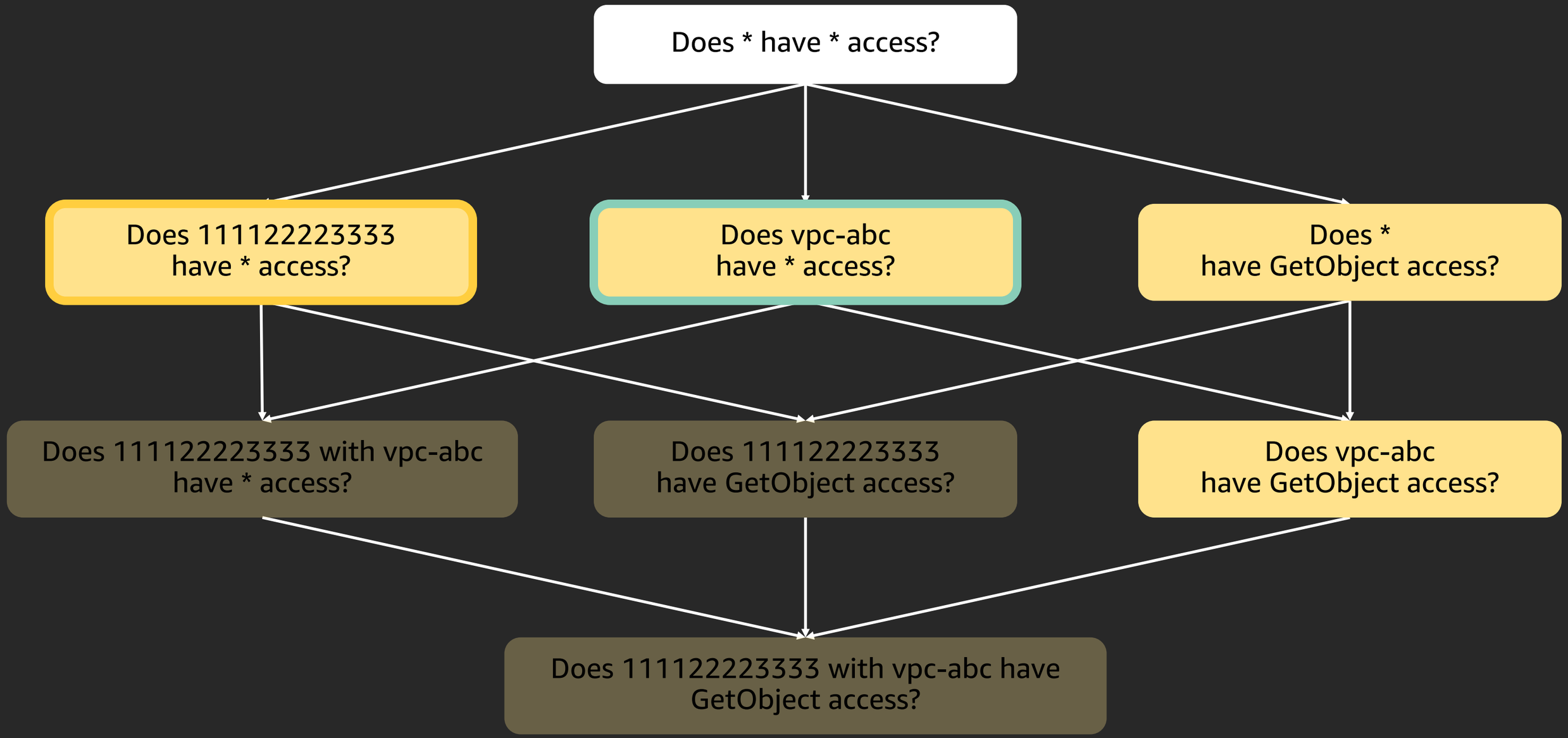
Twenty questions



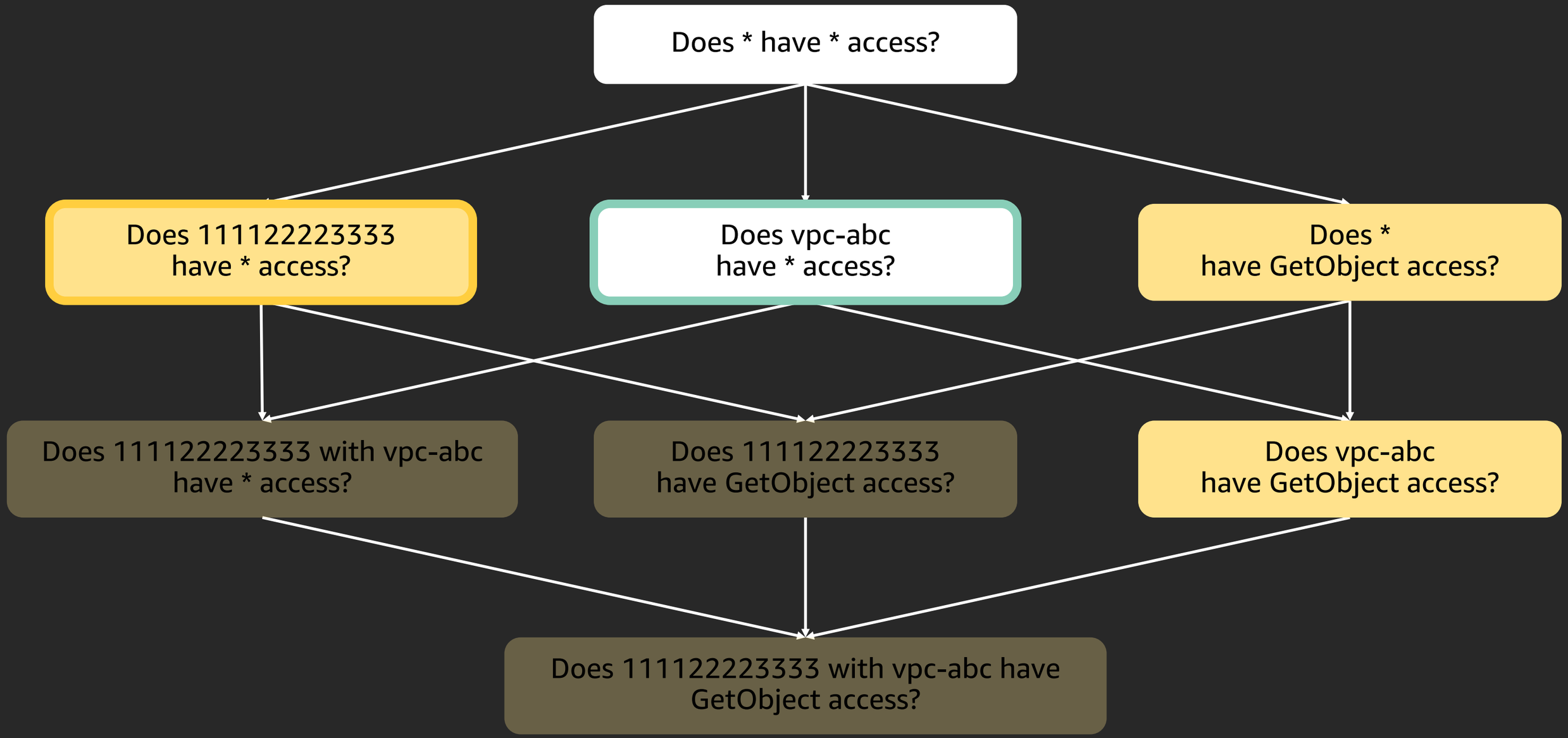
Twenty questions



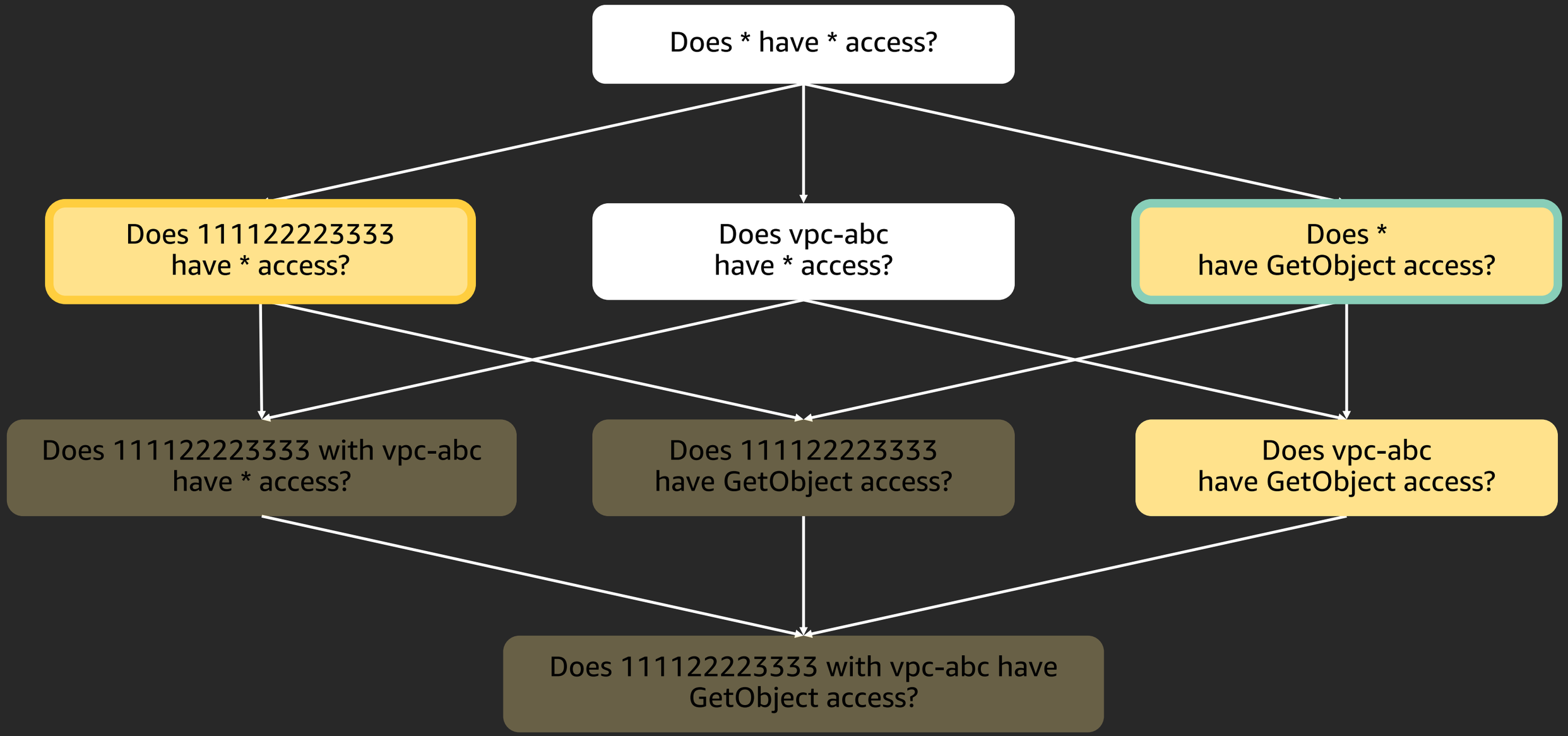
Twenty questions



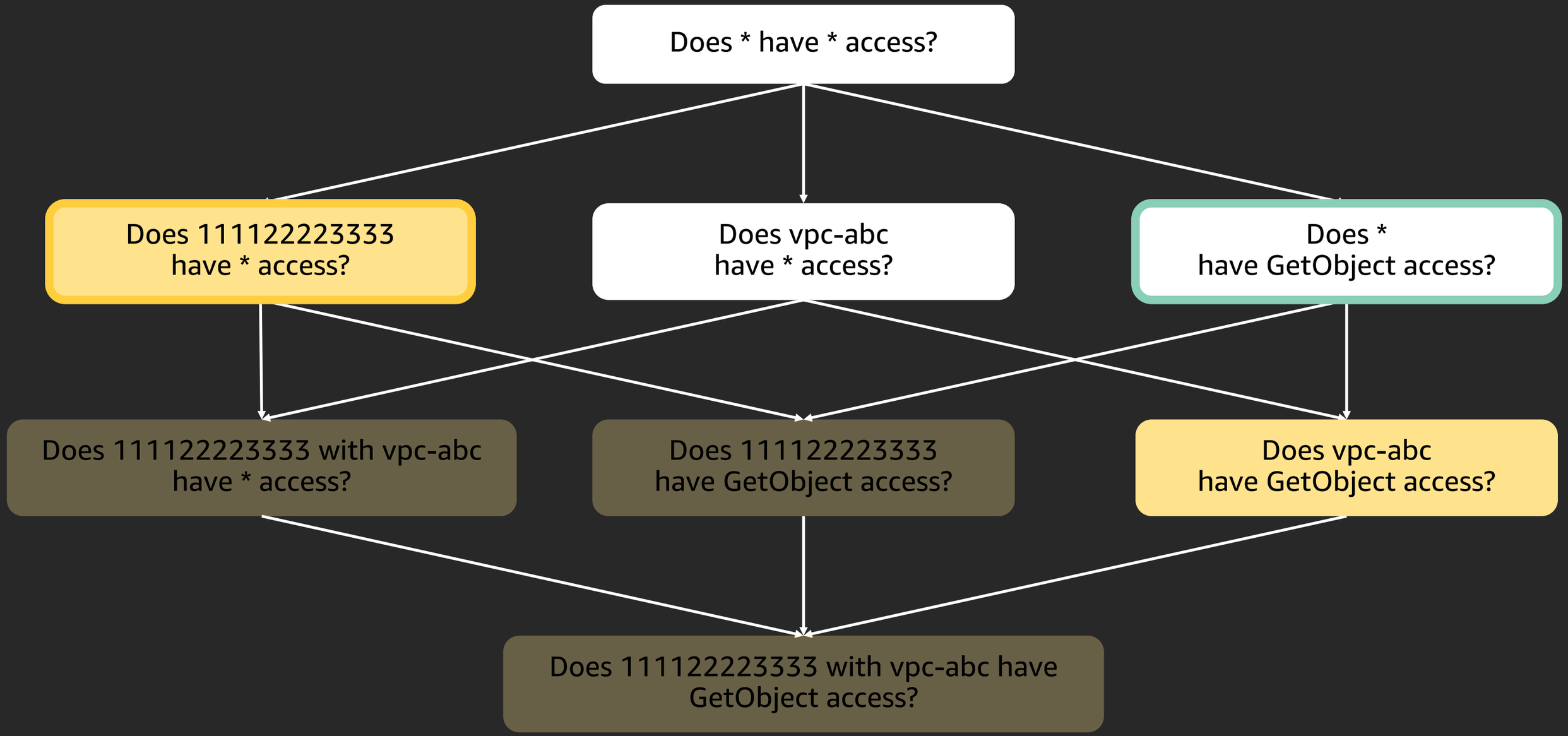
Twenty questions



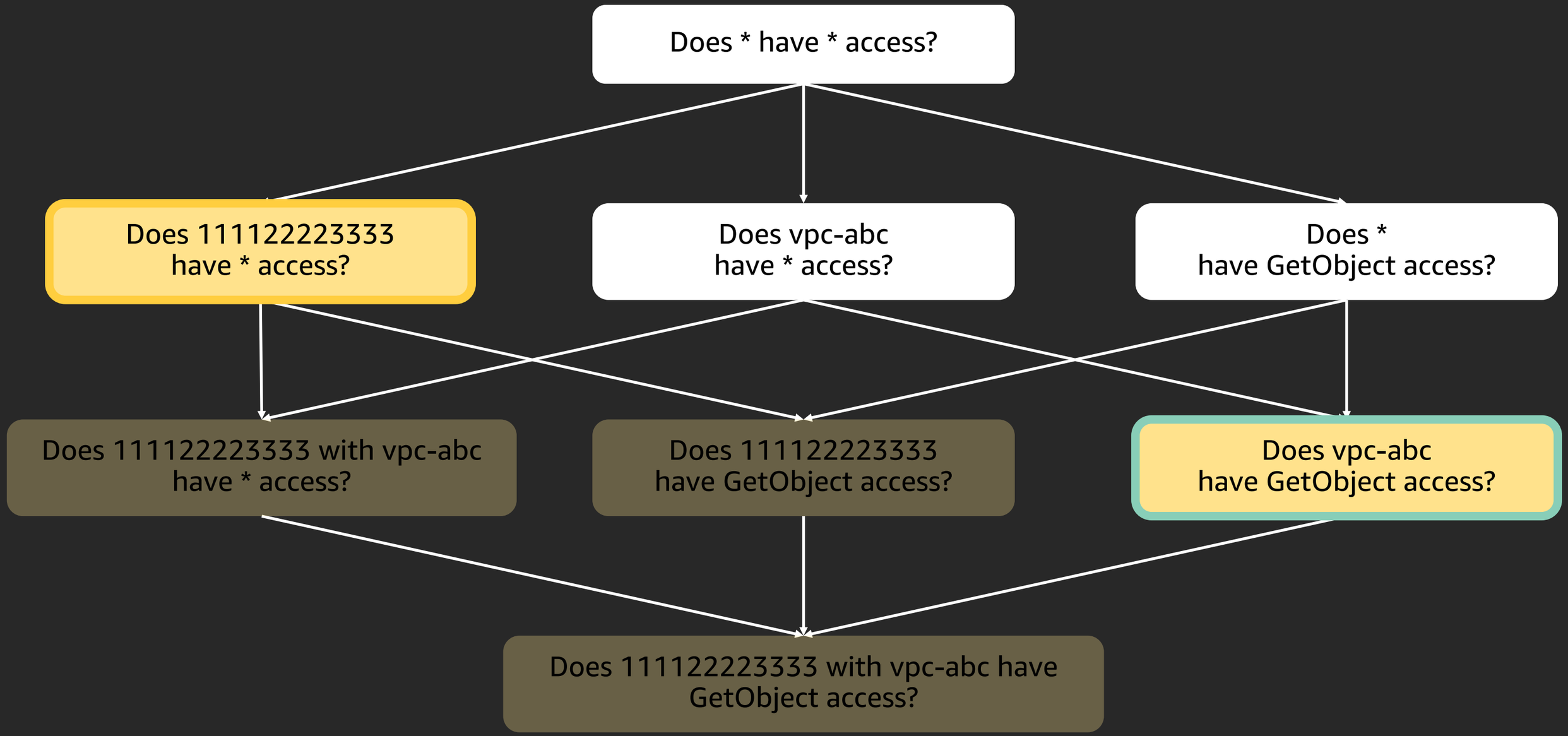
Twenty questions



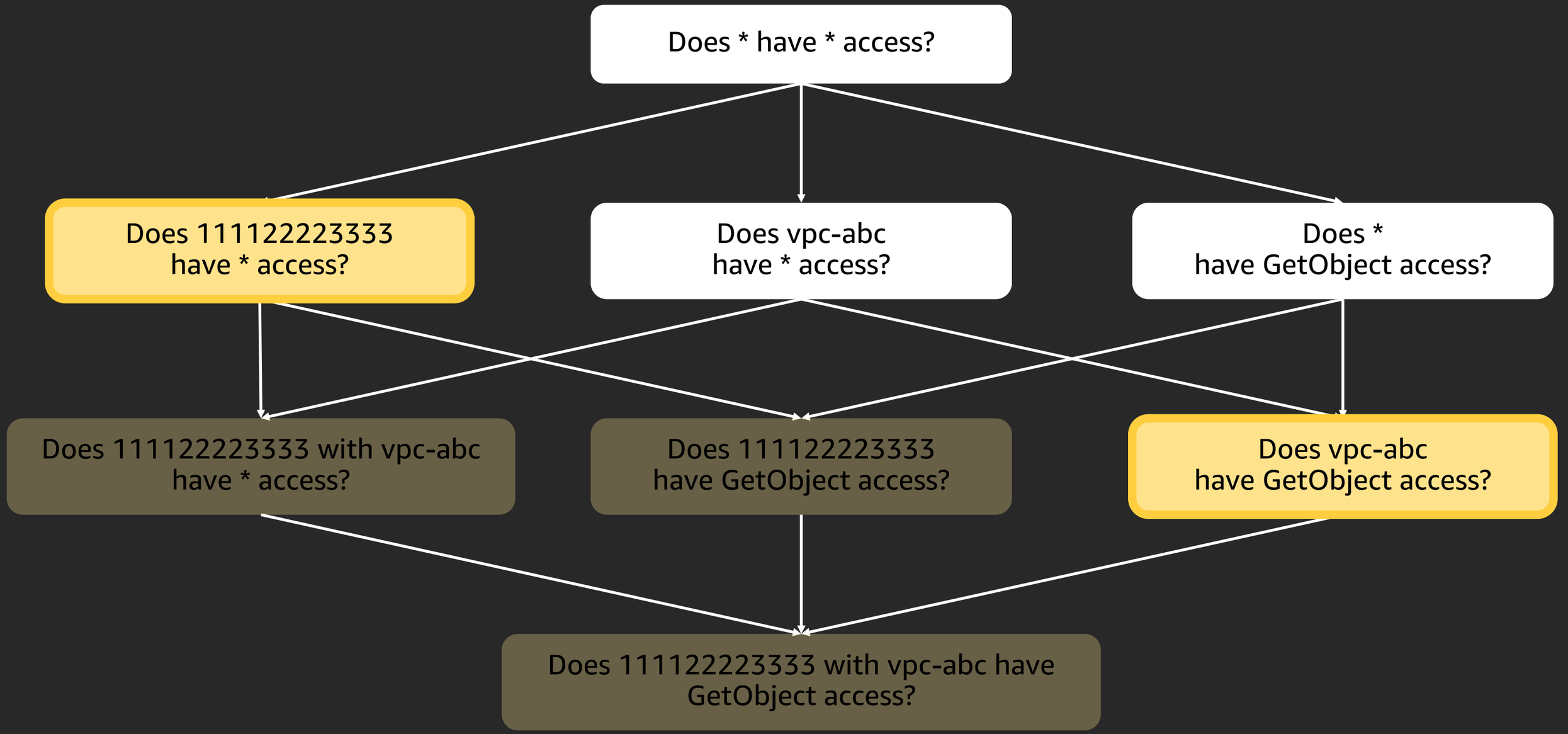
Twenty questions



Twenty questions



Twenty questions



Dashboard

Access management

Groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analyzer details

Credential report

Organization activity

Service control policies (SCP)

AWS account ID:
271132323480

Access Analyzer

Monitor access to resources

Create analyzer

How it works

1 Create an analyzer

The scope for the analyzer is your AWS account, which is your zone of trust. The analyzer scans all of the supported resources within your zone of trust.

2 Review active findings

When Access Analyzer finds a policy that allows access to a resource from outside of your zone of trust, it generates an active finding. Findings include details about the access so that you can take action.

3 Take action

If the access is intended, you can archive the finding so that you can focus on reviewing active findings. If the access is not intended, you can resolve the finding by modifying the policy to remove access to the resource.

Learn about the permissions you need to enable Access Analyzer. Learn more

Getting started

- What is Access Analyzer?
- Access Analyzer User Guide

Access Analyzer Info

Last scan: 2 hours ago

Active | Archived | Resolved | All

Active findings

Actions

Filter active findings

1

Finding ID	Resource	External principal	Condition	Access level	Updated
b2145731-2544-…	SQS Queue A2TestResource…	AWS Account 024774767089	-	Write	7 days ago
3a984fb4-88fc-4…	Lambda Function A2TestResource…	AWS Account 024774767089	-	Write	7 days ago
c580894d-9106-…	S3 Bucket citadel-test01	All Principals	Source VPCE vpce-abc	Write, Tagging, Read…	7 days ago
35336416-57bc-…	S3 Bucket a2testresources…	All Principals	Principal OrgID o-12345 Source VPC vpc-47ea5	Read	7 days ago
57010b45-608c-…	S3 Bucket checkconfigstate	AWS Account 711213078704	-	List	7 days ago
d7644690-6dae-…	S3 Bucket a2testresources…	All Principals	Source VPC vpc-47ea5	Read	7 days ago
b7e1ad85-be8b-…	S3 Bucket a2testresources…	All Principals	Source IP 72.21.196.66	Read	7 days ago
687b8fa3-0fba-4…	S3 Bucket a2testresources…	AWS Account 024774767089	-	Write	7 days ago

7674f39a-771e-471a-ba7c-b48d878d9e51 Info

Rescan

Details

Finding ID	Updated	Status
7674f39a-771e-471a-ba7c-b48d878d9e51	7 days ago	Active

Resource	External principal (AWS Account)	Condition	Access level
arn:aws:s3:::a2testresources-mb2-1dwfmvorjxgno	024774767089	-	Read • s3:GetObject

Next steps

Intended access

If the access is intended, such as access necessary for business processes, you can archive the finding. This lets you focus on findings that are related to potential security risks. When you archive a finding, it's removed from Active findings and the status changes to Archived.

Archive

Not intended

If the access isn't intended, it indicates a potential security risk. Use the console for the service associated with the resource to modify or remove the policy that grants the unintended access. To confirm that your change removed the access, choose **Rescan**. If the access is removed, the status changes to Resolved.

Go to S3 console

arn:aws:s3:::a2testresources-mb2-1dwfmvorjxgno

IAM > Access Analyzer > Archive rules

Archive rules Info

Archive rules

Delete | Edit | Create archive rule

< 1 >

Name	Rule
ArchiveRule-3f471750-303b-48f1-9e06-36b1487ebb86	Source Account equals 111122223333

Wired

"What we're hoping to achieve is to get a kind of provable security out of our systems. By provable security I don't mean that what we get out is infallible security. Instead what we're trying to get is a formal analysis, and a methodical way that we have gone about verifying that the security controls we put into place are working the way we think they're working."

- Greg Frascadore, Security Architect at Bridgewater Associates

If automated reasoning is so awesome, why are you still employed?

Automated Reasoning is expensive

Automated Reasoning has no business judgment

“All models are wrong but some are useful.” – George Box

Right on!

byron

Byron
Cook

some of
We can do your job better than you can! All you need is SAT and SMT and three PhDs and did you know that P is basically equal to NP and formal methods can solve any problem, how hard can security be?

rungta

View Badge Photo

Neha
Rungta

Thank you!

Eric Brandwine & Neha Rungta

ericbran@amazon.com
rungta@amazon.com

AWS re:Invent

aws

Please complete the session survey in the mobile app.