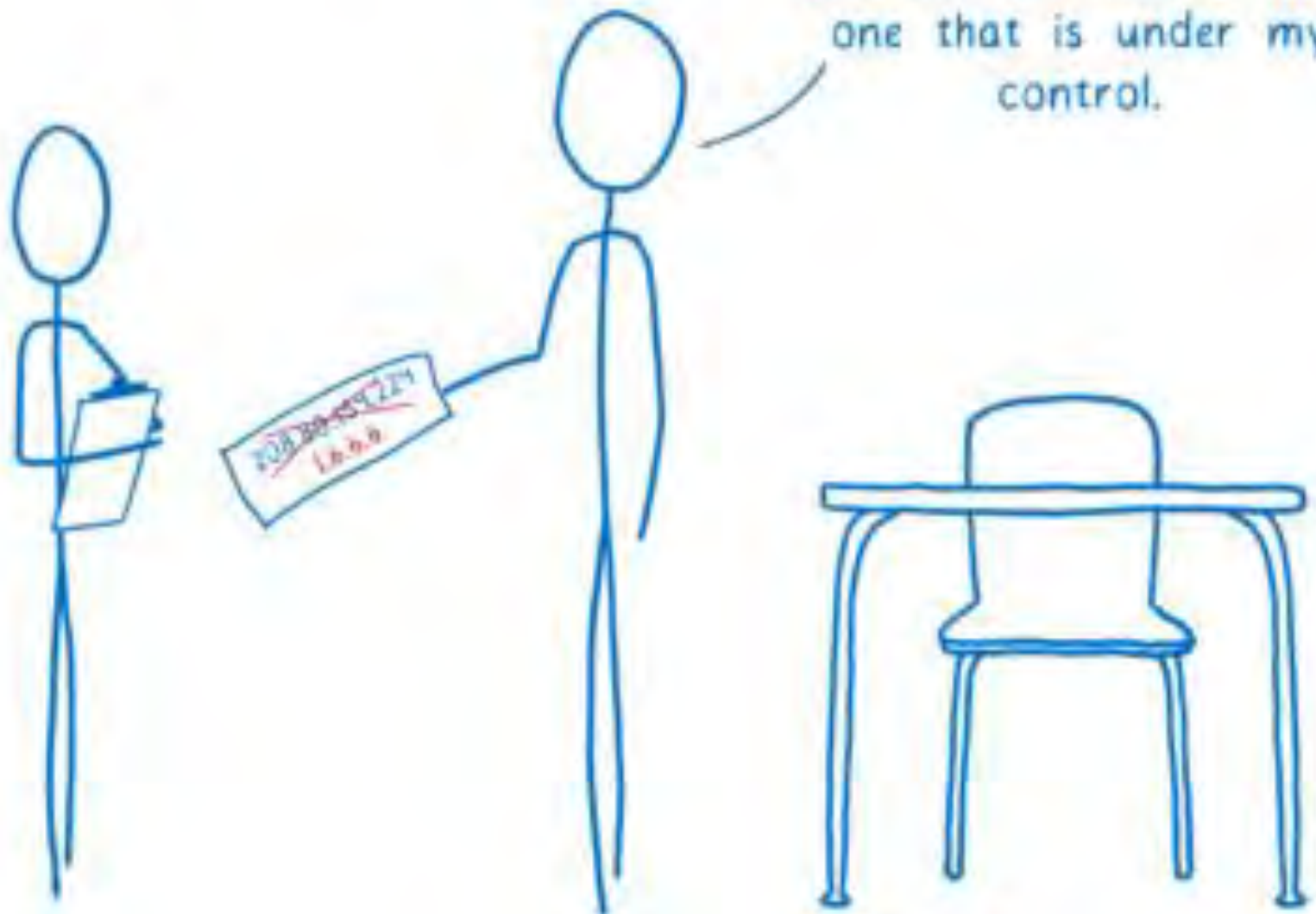


CONQUERING HYBRID DNS WITH ROUTE 53 RESOLVER

Atif Siddiqui



Send it to 1.6.6.6...
that's totally the right
address and not a fake
one that is under my
control.



AGENDA

- Life without Route 53 Resolver
- Route 53 Resolver Overview
- Hybrid DNS design
- Security Tooling
- New Capability: Route 53 Profiles

LIFE WITHOUT ROUTE 53 RESOLVER

- Custom solution required for VPC resources to be aware of on-prem network
 - Set up DNS server on EC2(s) to forward corporate domains to on-prem network
 - Onus on customer to build resiliency and scalability into the custom solution

ROUTE 53 RESOLVER OVERVIEW

- Known by another name +2 or .2 resolver
- Available by default in VPCs
- Capability achieved via Resolver endpoints
- Allows AWS resources to recursively resolve DNS queries
 - Intra VPC resource e.g. EC2 name
 - Private hosted zone records
 - Public domains

ROUTE 53 RESOLVER ENDPOINTS

- Endpoints manifest as ENIs
- Inbound endpoints
 - Enables on-prem network to resolve VPC resources in AWS private hosted zone
- Outbound endpoints
 - Enables VPC resources to resolve on-prem network



Recursive queries

PROVISIONING RESOLVER ENDPOINTS

Route 53 > Resolver > Configure endpoints

Step 1
[Configure endpoints](#)

Step 2
Configure inbound endpoint

Step 3
[Configure outbound endpoint](#)

Step 4
[Create rule](#)

Step 5
Review and create

Configure inbound endpoint [info](#)

An inbound endpoint contains the information that Resolver needs to route DNS queries from your network to your VPCs.

General settings for inbound endpoint

Endpoint name
A friendly name lets you easily find your endpoint on the dashboard.

The endpoint names can range up to 64 characters. Valid characters are: A-Z, 0-9, space, _ (underscore), and - (hyphen).

VPC in the Region: us-east-1 (N. Virginia) [info](#)
All inbound DNS queries will flow through this VPC on the way to Resolver. You can't change this value after you create an endpoint.

Security group for this endpoint [info](#)
A security group controls access to this VPC. The security group that you choose must include low or medium-risk rules. You can't change this value after you create an endpoint.
Choose security group:

Endpoint Type
Route 53 Resolver endpoints support IPv4, IPv6, and dual-stack IP addresses. For a dual-stack connection, endpoints can use both IPv4 and IPv6 addresses to connect to a VPC.

Protocols for this endpoint [info](#)
The protocols for this endpoint determine how data is transmitted to this endpoint. Choose the data transmission protocol with the level of security required for your inbound endpoint.
Choose protocol:

IP addresses [info](#)

To improve resiliency, Resolver requires that you specify two IP addresses for DNS queries. We recommend that you specify IP addresses in two different Availability Zones. After you add the first two IP addresses, you can optionally add more in the same or different Availability Zones.

IP address #1

Availability Zone [info](#)
The Availability Zone that you choose for inbound DNS queries must be configured with a subnet.

You must choose an Availability Zone.

Subnet [info](#)
The subnets that you choose must have an available IP address.

IPv4 address [info](#)
For inbound DNS queries, you can either let the service choose an IP address for you from the available IP addresses in the subnet, or you can specify the IP address yourself.
 Use an IPv4 address that is selected automatically
 Use an IPv4 address that you specify

IP address #2

Availability Zone [info](#)
The Availability Zone that you choose for inbound DNS queries must be configured with a subnet.

You must choose an Availability Zone.

Subnet [info](#)
The subnets that you choose must have an available IP address.

IPv4 address [info](#)
For inbound DNS queries, you can either let the service choose an IP address for you from the available IP addresses in the subnet, or you can specify the IP address yourself.
 Use an IPv4 address that is selected automatically
 Use an IPv4 address that you specify

FORWARDING RULES

Step 1

[Configure endpoints](#)

Step 2

[Configure inbound endpoint](#)

Step 3

[Configure outbound endpoint](#)

Step 4

Create rule

Step 5

Review and create

Create rule [Info](#)

Rule for outbound traffic

For queries that originate in your VPC, you can define how to forward DNS queries out of the VPC.

Name

A friendly name helps you find your rule on the dashboard.

The rule name can have up to 64 characters. Valid characters: a-z, A-Z, 0-9, space, _ (underscore), and - (hyphen)

Rule type [Info](#)

Choose **Forward** to forward DNS queries to the IP addresses that you specify in **Target IP addresses** section near the bottom of this page. Choose **System** to have Resolver handle queries for a specified subdomain. You can't change this value after you create a rule.

Domain name [Info](#)

DNS queries for this domain name are forwarded to the IP address that you specify in the **Target IP addresses** section near the bottom of the page. If a query matches multiple rules (example.com and www.example.com), outbound DNS queries are routed using the rule that contains the most specific domain name (www.example.com). You can't change this value after you create a rule.

VPCs that use this rule - optional [Info](#)

You can associate this rule with as many VPCs as you want. To remove a VPC, choose the X for that VPC.

Outbound endpoint [Info](#)

Resolver uses the outbound endpoint to route DNS queries to the IP addresses that you specify in the **Target IP addresses** section near the bottom of this page.

IP Address Type

An outbound endpoint type can have an IP address of IPv4, IPv6, or a dual stack that includes both. The Resolver rule you create must have the same IP address type as the outbound endpoint. If the outbound endpoint has a dual stack IP address, you can choose either IPv4 or IPv6, but you can't choose both.

Target IP addresses


DNS queries are forwarded to the following IP addresses:






IPv4 address

Port

Transmission Protocol

ENIs FOR RESOLVER

Network interfaces (4) [Info](#) Last updated 1 minute ago  [Actions](#) [Create netw](#)

<input type="checkbox"/>	Name 	Network interface ID	Subnet ID	VPC ID	Availability Zone	Security group n...	Interface Type	Description	Status	Primary private IPv4 address
<input type="checkbox"/>		eni-06b1cddced1aa5f97	subnet-0fe15c2c9188ceb28	vpc-028ba3cbd10c64b79	us-east-1b	route53-resolver-en...	Elastic network interface	Route 53 Resolver: rslvr-out-f2ea33396...	 In-use	10.0.0.155
<input type="checkbox"/>		eni-02ce3e9adcef8af9e	subnet-0fe15c2c9188ceb28	vpc-028ba3cbd10c64b79	us-east-1b	route53-resolver-en...	Elastic network interface	Route 53 Resolver: rslvr-in-df391ae60f2...	 In-use	10.0.0.152
<input type="checkbox"/>		eni-05e71c9410bf88afc	subnet-09c1adb16e10133d7	vpc-028ba3cbd10c64b79	us-east-1a	route53-resolver-en...	Elastic network interface	Route 53 Resolver: rslvr-in-df391ae60f2...	 In-use	10.0.0.138
<input type="checkbox"/>		eni-08da5321ac3da0ef5	subnet-09c1adb16e10133d7	vpc-028ba3cbd10c64b79	us-east-1a	route53-resolver-en...	Elastic network interface	Route 53 Resolver: rslvr-out-f2ea33396...	 In-use	10.0.0.142

SECURITY GROUP FOR ENDPOINTS

EC2 > Security Groups > sg-0d8b13814a6e29617 - route53-resolver-endpoint

sg-0d8b13814a6e29617 - route53-resolver-endpoint

Actions ▾

Details

Security group name
route53-resolver-endpoint

Security group ID
sg-0d8b13814a6e29617

Description
SG for Route 53 resolver endpoints

VPC ID
[vpc-028ba3cbd10c64b79](#)

Owner
767398026346

Inbound rules count
2 Permission entries

Outbound rules count
1 Permission entry

Inbound rules

Outbound rules

Tags

Inbound rules (2)



Manage tags

Edit inbound rules

Search

< 1 > ⚙

<input type="checkbox"/>	Name ▾	Security group rule... ▾	IP version ▾	Type ▾	Protocol ▾	Port range ▾	Source ▾	Description ▾
<input type="checkbox"/>	-	sgr-0c826fb2f1f86bc4c	IPv4	DNS (TCP)	TCP	53	10.0.0.0/8	-
<input type="checkbox"/>	-	sgr-02dd7e1b2640f13...	IPv4	DNS (UDP)	UDP	53	10.0.0.0/8	-

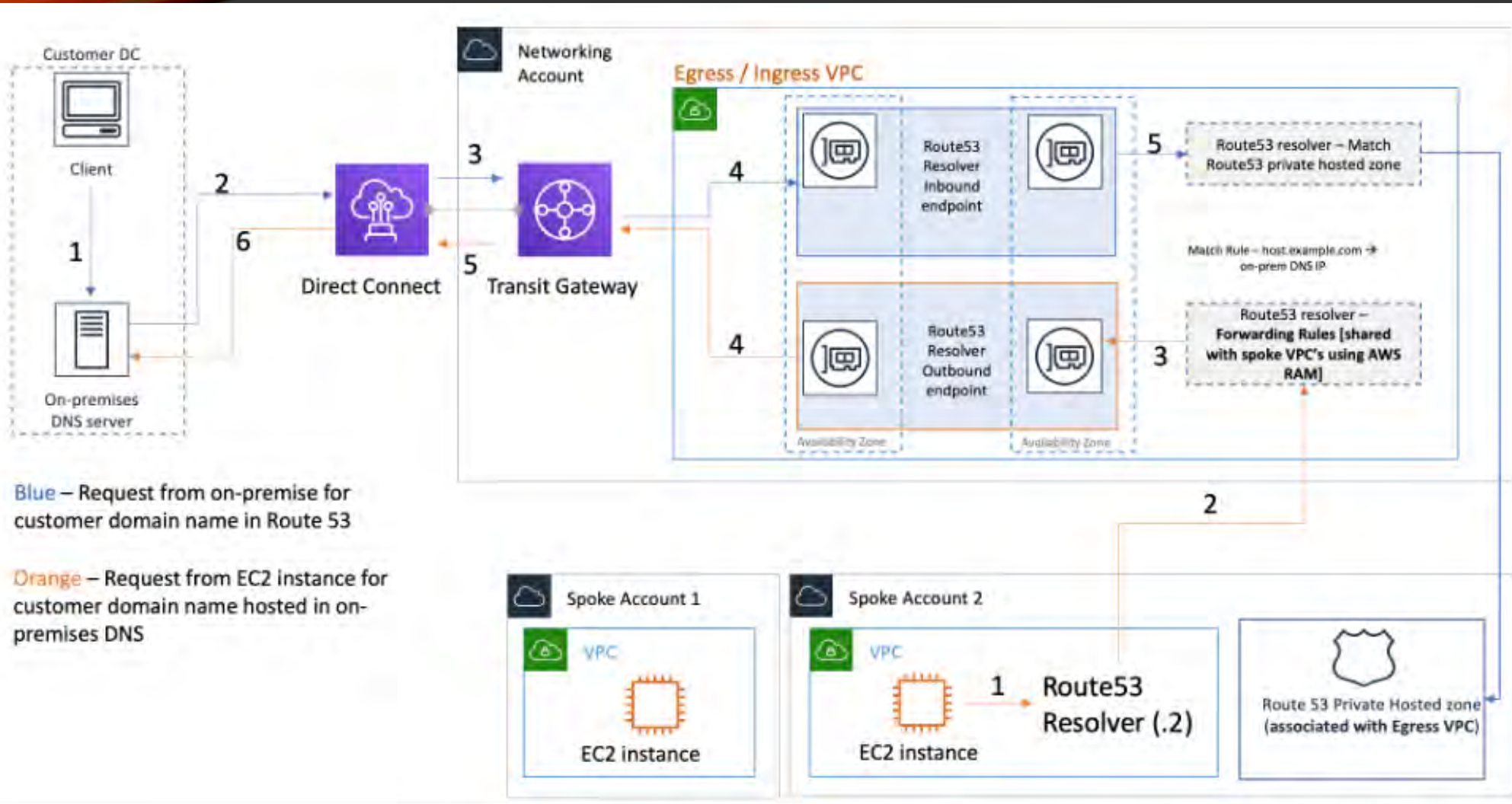
RESOURCE ACCESS MANAGER (RAM)

- Scaling hybrid DNS setup
- Re-using resolver rules across AWS accounts
- Supported list of shareable resources
 - Route 53 Resolver
 - Transit Gateway
 - Subnet
 - License Manager

ASSOCIATING PHZ WITH VPC

- Private Hosted Zones (PHZ) in Spoke accounts have to be associated with VPC(s) of Core Network account where Route 53 Resolver endpoints are provisioned
- Route 53 Profiles is a new capability that simplifies this implementation

HYBRID DNS DESIGN

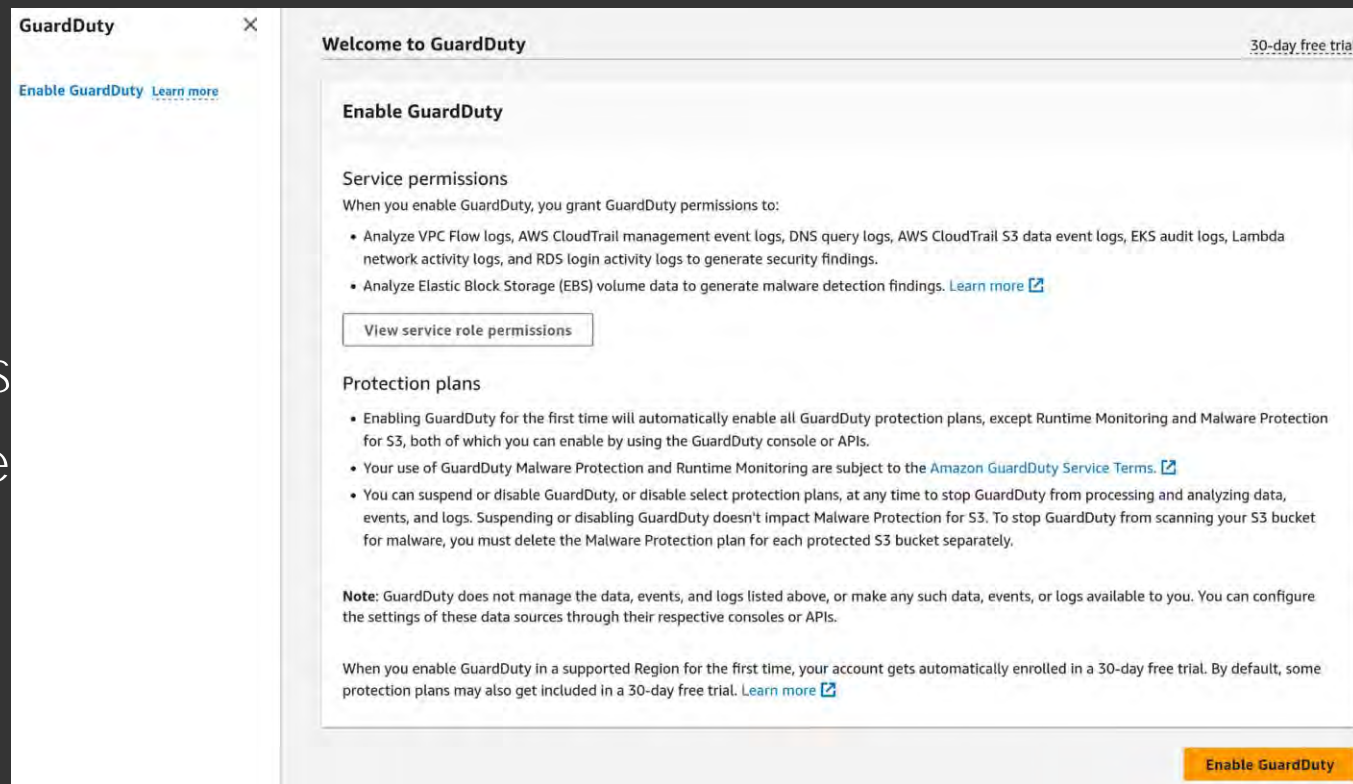


Blue – Request from on-premise for customer domain name in Route 53

Orange – Request from EC2 instance for customer domain name hosted in on-premises DNS

SECURITY TOOL: GUARDDUTY

- Threat Detection system that continuously monitors AWS accounts
- Analyzes three types of logs
 - VPC flow logs
 - CloudTrail logs
 - DNS logs
- One click enablement
- GuardDuty has added capabilities over time



The screenshot shows the AWS GuardDuty console interface. The main heading is "Welcome to GuardDuty" with a "30-day free trial" badge in the top right. Below the heading, there is a section titled "Enable GuardDuty". Under this section, there is a "Service permissions" section that explains that enabling GuardDuty grants permissions to analyze VPC Flow logs, AWS CloudTrail management event logs, DNS query logs, AWS CloudTrail S3 data event logs, EKS audit logs, Lambda network activity logs, and RDS login activity logs to generate security findings. It also mentions analyzing Elastic Block Storage (EBS) volume data for malware detection. A button labeled "View service role permissions" is provided. Below this is a "Protection plans" section, which states that enabling GuardDuty for the first time will automatically enable all protection plans except Runtime Monitoring and Malware Protection for S3. It also notes that users can suspend or disable GuardDuty or select protection plans at any time. A "Note" section clarifies that GuardDuty does not manage the data, events, and logs listed above, or make any such data, events, or logs available to the user. At the bottom, there is a note about the 30-day free trial and a large orange "Enable GuardDuty" button.

GuardDuty ×

[Enable GuardDuty](#) [Learn more](#)

Welcome to GuardDuty 30-day free trial

Enable GuardDuty

Service permissions
When you enable GuardDuty, you grant GuardDuty permissions to:

- Analyze VPC Flow logs, AWS CloudTrail management event logs, DNS query logs, AWS CloudTrail S3 data event logs, EKS audit logs, Lambda network activity logs, and RDS login activity logs to generate security findings.
- Analyze Elastic Block Storage (EBS) volume data to generate malware detection findings. [Learn more](#)

[View service role permissions](#)

Protection plans

- Enabling GuardDuty for the first time will automatically enable all GuardDuty protection plans, except Runtime Monitoring and Malware Protection for S3, both of which you can enable by using the GuardDuty console or APIs.
- Your use of GuardDuty Malware Protection and Runtime Monitoring are subject to the [Amazon GuardDuty Service Terms](#).
- You can suspend or disable GuardDuty, or disable select protection plans, at any time to stop GuardDuty from processing and analyzing data, events, and logs. Suspending or disabling GuardDuty doesn't impact Malware Protection for S3. To stop GuardDuty from scanning your S3 bucket for malware, you must delete the Malware Protection plan for each protected S3 bucket separately.

Note: GuardDuty does not manage the data, events, and logs listed above, or make any such data, events, or logs available to you. You can configure the settings of these data sources through their respective consoles or APIs.

When you enable GuardDuty in a supported Region for the first time, your account gets automatically enrolled in a 30-day free trial. By default, some protection plans may also get included in a 30-day free trial. [Learn more](#)

[Enable GuardDuty](#)

SECURITY TOOL: DNS FIREWALL

- Service offered for Route 53 Resolver
- Regulates outbound DNS traffic for VPCs
- Supports both custom and AWS managed domain lists
- Specific query type can be filtered
- Best practice is to use AWS Firewall Manager to enable DNS firewall across AWS Org

Add rule Info

Rule details

Name

The name must have 1-128 characters. Valid characters: A-Z, a-c, 0-9, -(hyphen), and _(underscore).

Configurations

Domain list
You can choose your own domain list or an AWS managed domain list. See [Amazon Route 53 DNS Firewall pricing for AWS managed domain lists](#). [You can't change the domain list of a rule after you create the rule.](#)

Add my own domain list
Use this option to create or migrate your own domain list.

Add AWS managed domain list
These are subscribed domain lists provided by Amazon.

Choose a domain list

Domain redirection setting
You can choose to inspect all the domains or only the first domain in the DNS redirection chain, such as CNAME, DNAME, and ALIAS. See [Amazon Route 53 DNS Firewall rule settings for valid domain redirection setting types](#).

Inspect all (Default)
Inspects all the domains in the DNS redirection chain. You need to add individual domains in the redirection chain to the domain list.

Trust redirection domains
Inspects only the first domain in the DNS redirection chain. You don't need to add the individual domains in the redirection chain to the domain list.

Query type - optional
The DNS query type you want the rule to filter. If you don't make a selection, the rule applies to all query types. See [Amazon Route 53 DNS Firewall rule settings for valid query types](#). [You can't change the query type of a rule after you create it.](#)

Action

Choose an action to take when a DNS query fits the matches

Cancel Add rule

ROUTE 53 PROFILES

- New capabilities released last April (2024)
- Bundle configuration: private hosted zone associations, resolver forwarding rules and DNS Firewall rule groups
- Profiles can be shared via Resource Access Manager

THANK YOU

- References

- [AWS History and Timeline regarding Amazon Route 53](#)
- [Introducing AWS Resource Access Manager \(amazon.com\)](#)
- [DNS - Building a Scalable and Secure Multi-VPC AWS Network Infrastructure \(amazon.com\)](#)
- [Set up DNS resolution for hybrid networks in a multi-account AWS environment - AWS Prescriptive Guidance \(amazon.com\)](#)
- [Simplify DNS management in a multi-account environment with Route 53 Resolver | AWS Security Blog \(amazon.com\)](#)
- [Announcing Amazon GuardDuty – Intelligent Threat Detection](#)
- [Route 53 Resolver DNS Firewall Announcement](#)