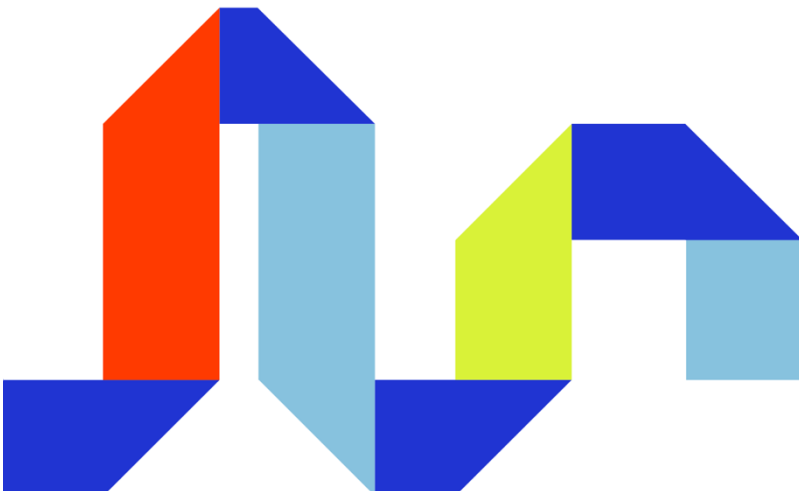


# INTRUSION SHIELD STRATUS

LAUNCHING FOR AWS



November 2025  
[SUPPORT@INTRUSION.COM](mailto:SUPPORT@INTRUSION.COM)

## Contents

What is Shield Stratus for AWS?	2
Key Features	2
How Does Shield Stratus Work?	2
Architecture Overview	3
Installation of Intrusion Shield Stratus for AWS	5
Requirements/Prerequisites	5
Purchasing a Shield Stratus Subscription	7
Deploying Shield Stratus via CloudFormation	8
CloudFormation Scenario #1 – Single Instance Only	9
CloudFormation Scenario #2 – Filtering VPC Only	9
CloudFormation Scenario #3 – Full Environment	11
CloudFormation Scenario #4 – Filtering Subnets Only	12
Example: Launching Shield Stratus via CloudFormation Template #3 – Full Environment	13
Example: Launching Shield Stratus via CloudFormation Template #4 – Filtering Subnets Only	20
Activating Shield Stratus	31
Creating an Intrusion Command Hub Account	31
Intrusion Command Hub	34
Configuring DNS Clients	36
Testing	36
Command Hub Management of Shield Stratus	37
Viewing Traffic	38
Adding Custom Permits	40
Frequently Asked Questions	42
General	42
Provisioning	42
Command Hub	43
High Availability	43
Logging	43
Data Collection Policy	44

## What is Shield Stratus for AWS?

Modern cloud environments make it difficult for security teams to see and control every network flow. AWS provides strong building blocks, but they focus on known threats or perimeter activity, leaving gaps in visibility and correlation across workloads and VPCs. Shield Stratus closes that gap.

Built on AWS Gateway Load Balancer (GWLB) and the GENEVE protocol, Shield Stratus acts as a transparent packet-filtering layer that monitors and enforces policy on all inbound and outbound traffic from cloud workloads. It applies Intrusion's Applied Threat Intelligence to evaluate reputation, behavioral risk, and historical context, not just known malicious indicators, to flag or block risky connections before they become incidents. The result is complete flow-level visibility and intelligent enforcement that strengthens both cloud-native and hybrid defenses.

## Key Features

- Intelligence-Driven Protection: Enforces Intrusion's continuously updated global threat database to stop C2 communications, DNS tunnels, and exfiltration attempts
- Centralized reporting from a fleet of devices within Intrusion Command Hub for aiding investigations and threat hunting
- Centralized management of policies from Intrusion Command Hub
- Filtering of inbound and outbound DNS and IP traffic from all resources in a VPC

## How Does Shield Stratus Work?

Intrusion Shield Stratus is implemented as a filter for an AWS Gateway Load Balancer (GWLB). As traffic traverses the Gateway Load Balancer inbound or outbound from a VPC, it is sent to the Geneve filter instance to make a verdict on whether to allow or block the traffic.

Shield Stratus protects in two ways:

- DNS requests traversing the GWLB are checked against Intrusion's ATI reputation database. Hosts of poor reputation or hosts resolving to IPs of poor reputation are redirected to a sinkhole.
- IP/TCP/UDP flows are compared against Intrusion's ATI reputation database and can be blocked in real-time.

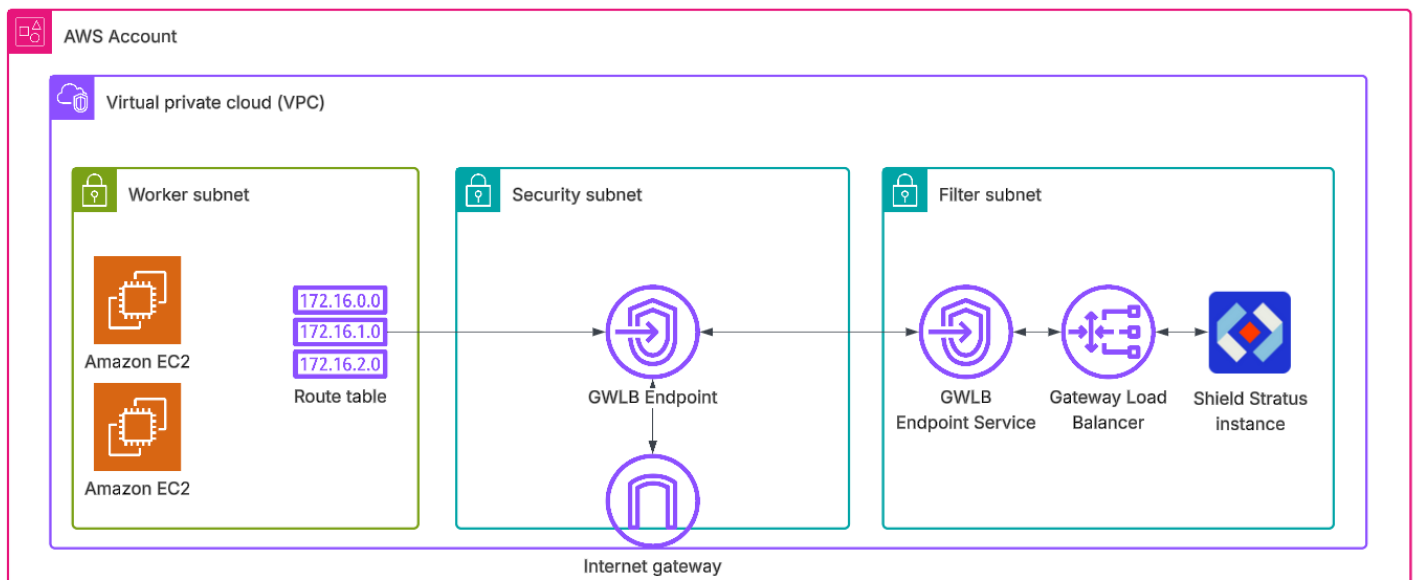
## Architecture Overview

Shield Stratus is deployed as a GENEVE filter for an AWS [Gateway Load Balancer](#). At a high level:

- A Gateway Load Balancer is created, with the target group pointing to one or more Shield Stratus instances
- A Gateway Load Balancer Endpoint Service is created to provide a means a routing traffic to the Gateway Load Balancer
- A Gateway Load Balancer Endpoint is created within a subnet that forwards traffic to the Gateway Load Balancer endpoint service.
- A route table is configured in other subnets of the VPC to send outbound traffic through the Gateway Load Balancer Endpoint
- An optional Edge Route Table is created to pass inbound traffic through the Gateway Load Balancer Endpoint

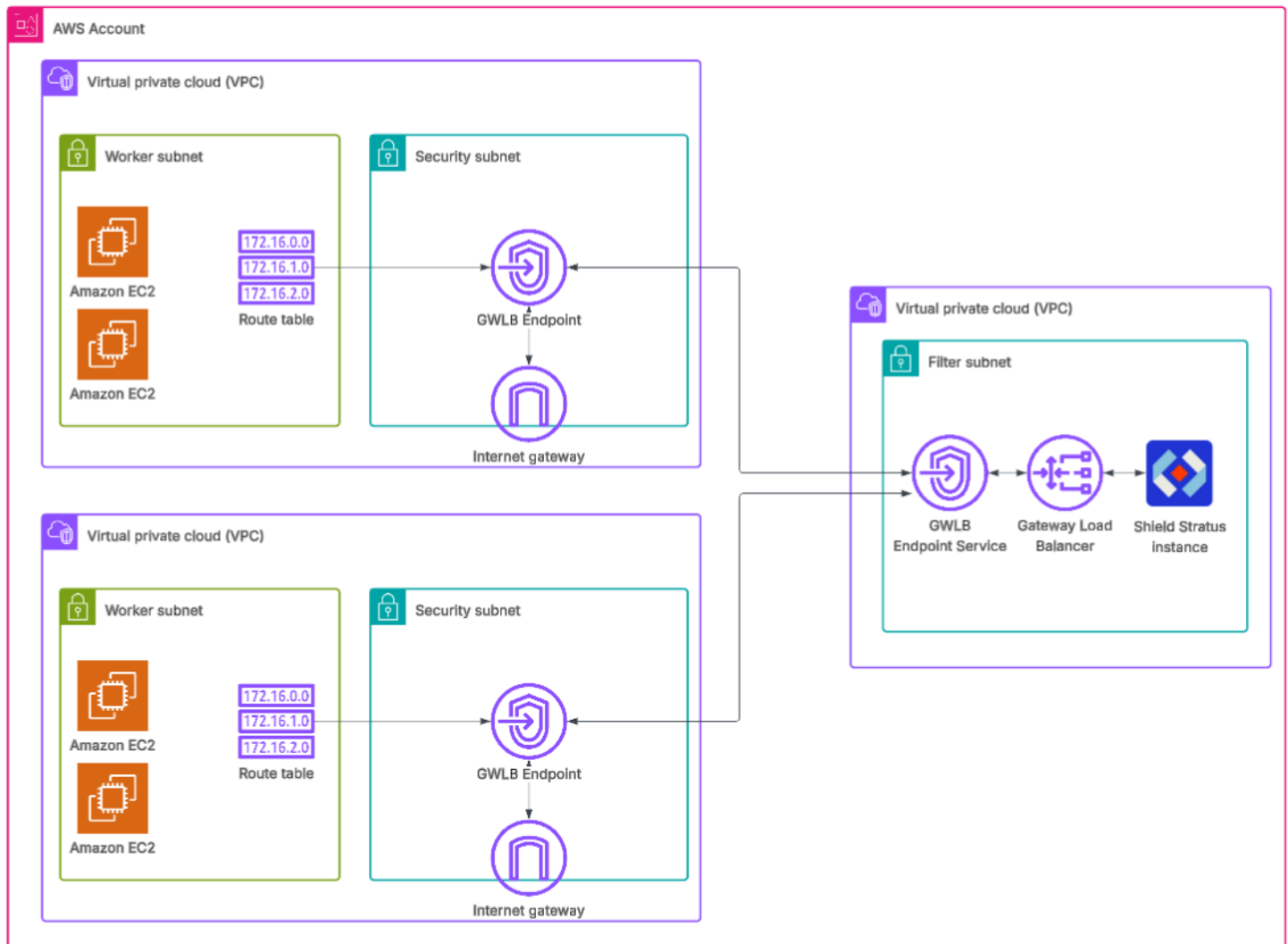
In the following example, this infrastructure is deployed in one VPC with multiple subnets.

- Worker subnet – where customer workloads are hosted (i.e. EC2 instances, Lambda Functions, etc.)
- Security subnet – routing subnet that houses the GWLB endpoint
- Filter subnet – houses the Gateway Load Balancer and Shield Stratus instances.



In the next example, the Gateway Load Balancer is deployed in a separate VPC. This allows one GWLB and Shield Stratus group to filter traffic for multiple VPCs in the customer account.

Note that this may incur costs for intra-VPC bandwidth.



# Installation of Intrusion Shield Stratus for AWS

This section describes the steps needed to setup a Shield Stratus filter in your AWS environment. At a high level, the steps are:

1. Purchase a subscription to Intrusion Shield Stratus from the AWS Marketplace
2. Use the CloudFormation Template through AWS Marketplace to provision an instance of Shield Stratus attached to a Gateway Load Balancer in a given VPC.
3. Register your account with Intrusion Command Hub, thereby registering the Shield Stratus instance
4. Use Command Hub to activate and configure the Shield Stratus instance

## Requirements/Prerequisites

Verify you have the following before proceeding:

- An active AWS Account
- An AWS IAM user with permission to:
  - Purchase from AWS marketplace
  - AWS Console access
  - Ability to create AWS resources (see below)
- Email address for creating a Command Hub user account

Specifically, the IAM user needs at least the following permissions

### CloudFormation

- cloudformation:CreateStack
- cloudformation:DescribeStacks
- cloudformation:DescribeStackEvents
- cloudformation:GetTemplateSummary
- cloudformation:UpdateStack
- cloudformation>DeleteStack

### IAM

- iam:CreateRole
- iam:PutRolePolicy
- iam:CreateInstanceProfile
- iam:AddRoleToInstanceProfile
- iam:PassRole (iam:PassedToService: ec2.amazonaws.com)
- iam:RemoveRoleFromInstanceProfile
- iam:DeleteInstanceProfile
- iam>DeleteRole
- iam>DeleteRolePolicy

### EC2

- ec2:CreateSecurityGroup
- ec2:AuthorizeSecurityGroupEgress
- ec2:RevokeSecurityGroupEgress
- ec2:CreateNetworkInterface
- ec2:ModifyNetworkInterfaceAttribute

- ec2:RunInstances
- ec2:CreateTags
- ec2>DeleteTags
- ec2:TerminateInstances
- ec2>DeleteNetworkInterface
- ec2>DeleteSecurityGroup
- ec2:DescribeVpcs
- ec2:DescribeSubnets
- ec2:DescribeSecurityGroups
- ec2:DescribeImages
- ec2:DescribeNetworkInterfaces

# Purchasing a Shield Stratus Subscription

Shield Stratus can be purchased through the AWS Marketplace

<https://aws.amazon.com/marketplace/pp/prodview-4pobngnssr5ug>

aws marketplace

Search

AboutCategoriesDelivery MethodsSolutionsResourcesYour Saved List

Become a Channel PartnerSell in AWS Marketplace

[AWS Marketplace](#) > [IT Support](#) > [Amazon Machine Image \(AMI\)](#) > [Shield Stratus](#)

Intrusion

Shield Stratus

Info

Sold by: [Intrusion](#)

Deployed on AWS

Free Trial

View purchase options

Try for free

Shield Stratus is a cloud security product built for protecting AWS VPC traffic using reputation-based filtering. Functioning as a bump-in-the-wire, Shield Stratus is able to inspect inbound and outbound flows in public or...

Show more

☆☆☆☆☆ (0) 0 AWS reviews

Overview

Pricing

Legal

Usage

Support

Similar products

Reviews

Overview

Shield Stratus simplifies compliance and operational overhead with automated firmware updates, detailed audit trails, and built in network flow metadata collection. Whether you are protecting IaaS, PaaS, SaaS, or FaaS resources, Shield Stratus delivers enterprise grade VPC security, freeing your team to focus on innovation while we handle network defense.

Shield Stratus offers two modes. When placed in Protect, Shield Stratus will block all incoming and outgoing malicious traffic to keep your cloud protected. In Observe mode, Shield Stratus will allow traffic to proceed as normal while still sending all observed traffic to Intrusion's Command Hub.

Highlights

- Transparently filters network traffic based on Intrusion's global threat engine, with threat intelligence spanning over 30 years.
- Autonomous Network Enforcement for the cloud. Can deploy as a standalone security product, or work in concert with existing firewalls and security solutions.
- Deploys as a GWLB Geneve filter



## Deploying Shield Stratus via CloudFormation

Intrusion provides multiple AWS CloudFormation templates to aid in deploying Shield Stratus in different scenarios.

Return to the AWS marketplace listing for Shield Stratus and select “Launch Instance”

- Service: **AWS CloudFormation**
- Then select one of the **CloudFormation template** options corresponding to the type of environment you want to setup. See the following sections for descriptions and examples of each option.

The screenshot shows the AWS Marketplace interface for launching Shield Stratus. The left sidebar contains navigation links: AWS Marketplace, Manage subscriptions, Shield Stratus, and Launch. The main content area is titled 'Launch Shield Stratus' and includes an 'Info' link. The 'Setup' section contains the following options:

- Service:** ☒ AWS CloudFormation (Automated, one-step deployment.) and ☐ Amazon EC2 (Custom deployment using Amazon Machine Image (AMI)).
- Launch method:** ☒ AWS CloudFormation template.
- Version:** A dropdown menu showing 'Shield Stratus 0.17 (Nov 12, 2025) - latest, stable'.
- CloudFormation template:** A section with three radio button options: ☐ option2-portable-vpc, ☐ option3-single-vpc-blank, and ☐ option4-single-vpc-existing. This section is highlighted with a red box.

The 'Launch' section at the bottom contains the text: 'Complete setup to see launch instructions'.

- Then click **Launch With CloudFormation**

## CloudFormation Scenario #1 - Single Instance Only

**Use Case:** I only want CloudFormation to provision the Shield Stratus instance and I will build infrastructure around it.

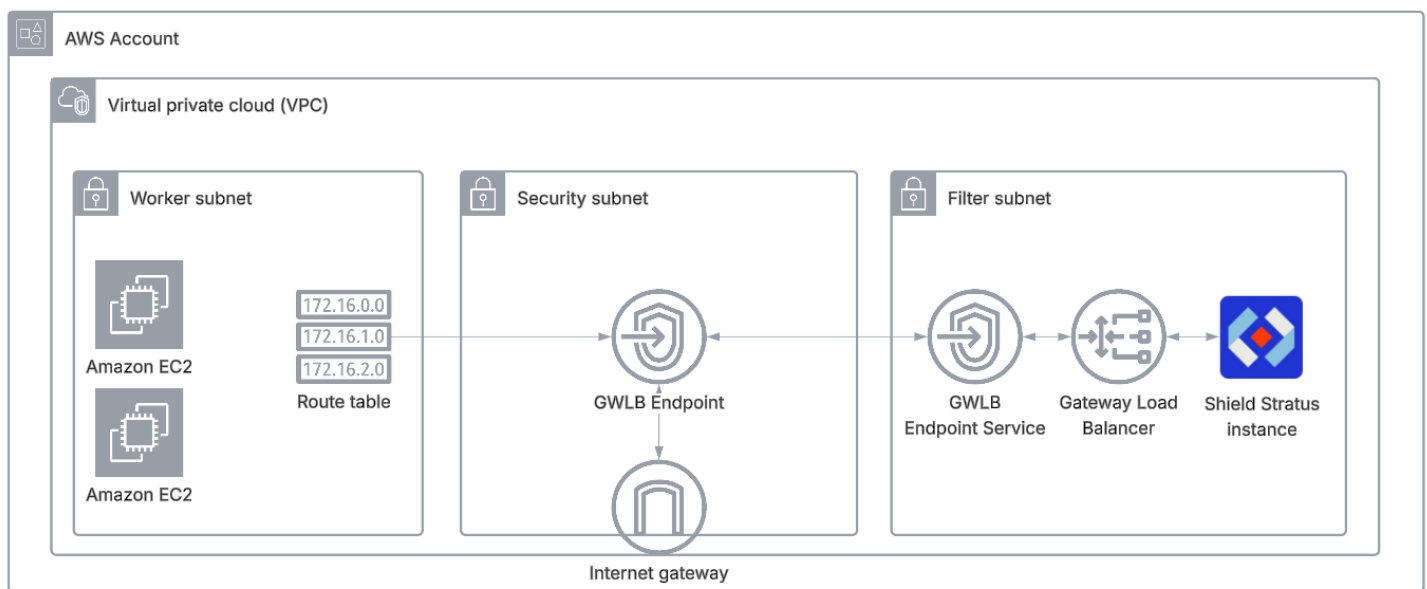
This minimalist CloudFormation template only deploys the Shield Stratus instance. The user must create the GWLB and associate it with the Shield Stratus instance target. This provides the most flexibility in integrating in existing environments, but puts most of the effort on the user to create the plumbing.

Prerequisites:

- Customer must have an existing VPC and filter subnet setup

Creates:

- Shield Stratus EC2 instance



Note, due to AWS Marketplace limitations, only three CloudFormation templates can be associated with a listing. This scenario is not listed in the Marketplace in lieu of the other scenarios, but it can be manually specified with the S3 url:

<https://poc-shield-cloud-us-east-2-markeplace-template-main.s3.us-east-2.amazonaws.com/ShieldFlow/v0.5/option1-standalone.yaml>

## CloudFormation Scenario #2 – Filtering VPC Only

**Use Case:** I only want CloudFormation to provision the Shield Stratus instance and GWLB service in its own VPC and I will attach other VPCs to it.

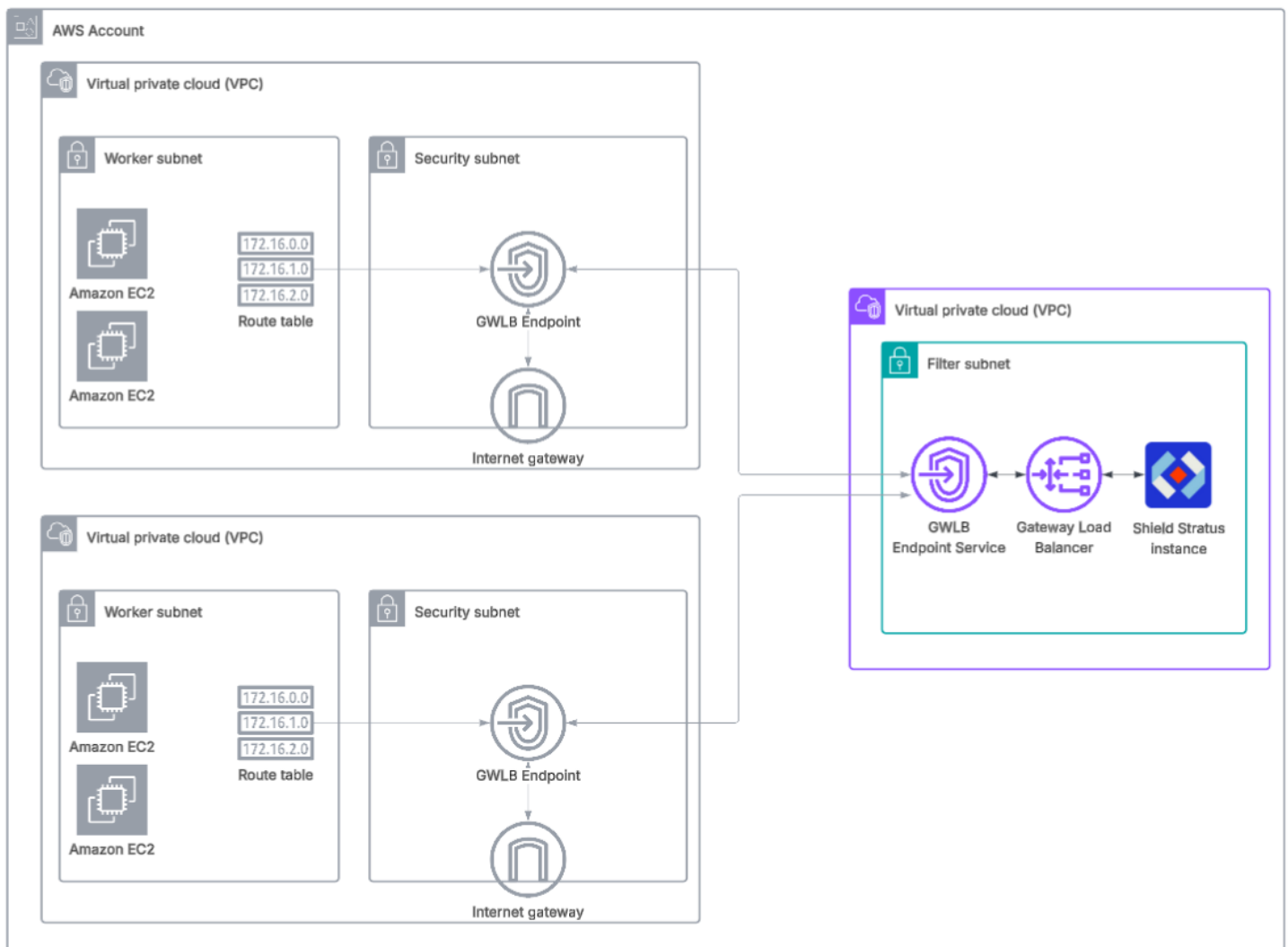
This CloudFormation template deploys a new VPC with GWLB and Shield Stratus instance. This allows the user to then create their own worker infrastructure in other VPCs to connect to the filter via GWLB Endpoints. This provides everything you need to get started with Shield Stratus, but requires the customer to provision the rest of the infrastructure.

Prerequisites:

- None

Creates:

- VPC, GWLB, GWLB Endpoint Service, Shield Stratus EC2 instance



## CloudFormation Scenario #3 – Full Environment

**Use Case:** I want CloudFormation to setup a fully functional environment protected by Shield Stratus ready for me to deploy workloads.

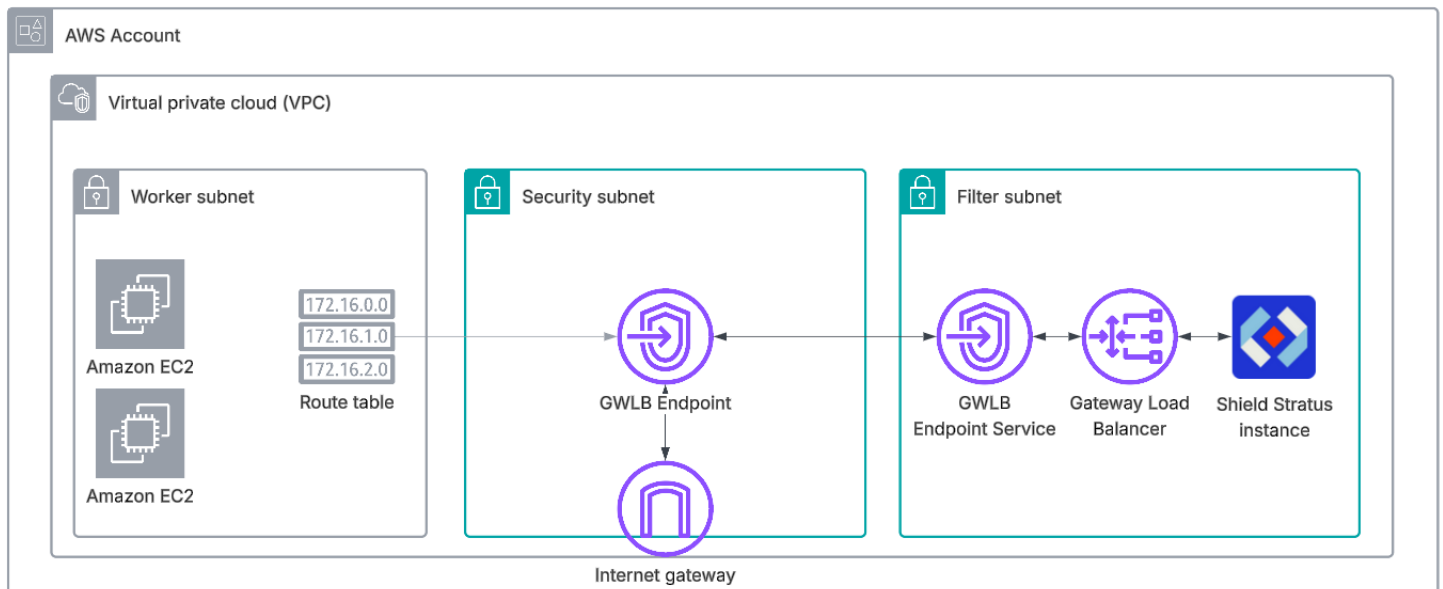
This CloudFormation template deploys everything you need to get started with Shield Stratus, including example subnets within a VPC. All you need to do is deploy instances within the Worker Subnet and they will be filtered by Shield Stratus. This is the easiest way to get started, but may not be flexible if you have existing infrastructure.

Prerequisites:

- An existing VPC

Creates:

- Subnets, Internet Gateway, GWLB, GWLB Endpoint Service, Routing tables, Shield Stratus EC2 instance



## CloudFormation Scenario #4 – Filtering Subnets Only

**Use Case:** I have an existing simple VPC and subnet and I want to enable Shield Stratus filtering

In this CloudFormation template, we compliment an existing VPC by adding a GWLB with Shield Stratus. Ideally this should allow a user to add filtering without disturbing their existing infrastructure.

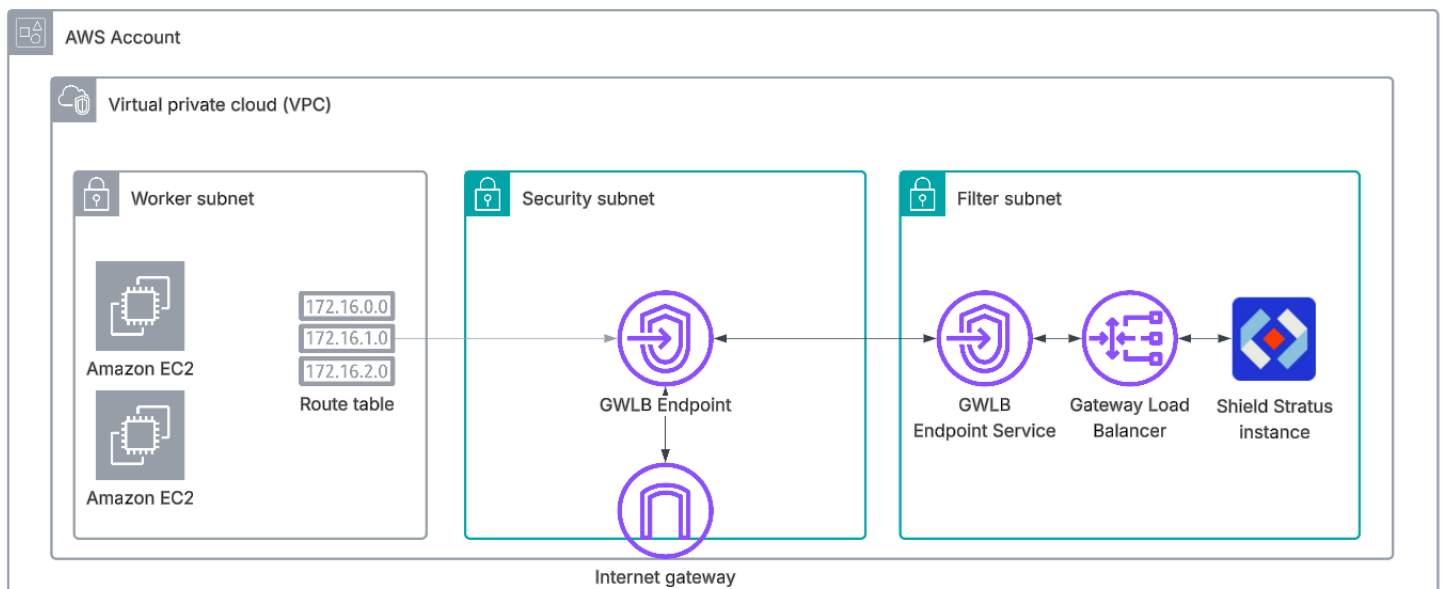
- In one subnet (filter subnet), the filtering EC2 instance, a GWLB, and a GWLB endpoint service. Connect the filtering EC2 instance to the GWLB, and the GWLB to the GWLB endpoint service. Also deploy any necessary networking, security, identity stuff that is needed.
- In another subnet (security subnet), deploys an IGW (for all other VPC communication), and a GWLB endpoint that connects to the GWLB endpoint service in the first subnet. For this subnet's route table, 0.0.0.0/0 should point to the IGW. Also creates a route table with no subnet association, but a edge association to the IGW that points all local VPC traffic to the GWLB endpoint (to handle inbound traffic processing).

Prerequisites:

- An existing VPC and optionally an existing Internet Gateway

Creates:

- Filter and Security subnets, Internet Gateway (optional), GWLB, GWLB Endpoint Service, Routing tables, Shield Stratus EC2 instance



## Example: Launching Shield Stratus via CloudFormation Template #3 – Full Environment

We will walk through the deployment of CloudFormation Template Scenario #3, since it contains the best representation of a sample deployment.

Select the CloudFormation template **option3-single-vpc-blank**.

The screenshot shows the AWS Marketplace console for the Shield Stratus service. The breadcrumb navigation at the top reads: AWS Marketplace > Manage subscriptions > Shield Stratus > Launch. On the left, the 'AWS Marketplace' sidebar is visible with links to Discover products, Procurement insights, Manage subscriptions (highlighted), Private offers, Vendor Insights, Private Marketplace, Your Private Marketplace, Legacy version, and Settings. The main content area is divided into two sections: 'Service' and 'Launch'. In the 'Service' section, the 'Launch method' is set to 'AWS CloudFormation template'. The 'Version' dropdown is set to 'Shield Stratus 0.17 (Nov 12, 2025) - latest, stable'. Under 'CloudFormation template', 'option3-single-vpc-blank' is selected. The 'Region' is set to 'US East (Ohio)'. In the 'Launch' section, there is a 'Launch with CloudFormation' button and a link to 'View template in CloudFormation Designer'. Below that, there is a 'Vendor's launch and connection instructions' section with a link to a PDF document.

**Service** | Info

☒ AWS CloudFormation  
Automated, one-step deployment.

☐ Amazon EC2  
Custom deployment using Amazon Machine Image (AMI).

**Launch method** | Info  
AWS CloudFormation template

**Version** | Info  
Shield Stratus 0.17 (Nov 12, 2025) - latest, stable

▶ Release notes

**CloudFormation template**

☐ option2-portable-vpc

☒ option3-single-vpc-blank

☐ option4-single-vpc-existing

**Region**  
US East (Ohio)

**Launch**

**Launch with CloudFormation**  
AWS CloudFormation automates consistent and reliable deployment. Its reusable templates mean less errors and security risks.  
[View template in CloudFormation Designer](#)

[Launch with CloudFormation](#)

**Vendor's launch and connection instructions**  
<https://poc-shield-cloud-us-east-2-markeplace-template-main.s3.us-east-2.amazonaws.com/ShieldFlow/Shield+Stratus+AWS.pdf>

You will be redirected to the CloudFormation Create Stack screen.

On the **Create Stack** screen, leave at the defaults to use the Intrusion-provided CloudFormation template.

CloudFormation > Stacks > Create > Template

Step 1  
● **Create stack**

Step 2  
○ Specify stack details

Step 3  
○ Configure stack options

Step 4  
○ Review and create

### Create stack

**Prerequisite - Prepare template**

You can also create a template by scanning your existing resources in the [IaC generator](#).

**Prepare template**

Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

☒ **Choose an existing template**  
Upload or choose an existing template.

☐ **Build from Infrastructure Composer**  
Create a template using a visual builder.

**Specify template** Info

This [GitHub repository](#) contains sample CloudFormation templates that can help you get started on new infrastructure projects. [Learn more](#)

**Template source**

Selecting a template generates an Amazon S3 URL where it will be stored. A template is a JSON or YAML file that describes your stack's resources and properties.

☒ **Amazon S3 URL**  
Provide an Amazon S3 URL to your template.

☐ **Upload a template file**  
Upload your template directly to the console.

☐ **Sync from Git**  
Sync a template from your Git repository.

**Amazon S3 URL**

Amazon S3 template URL

S3 URL: <https://awsmp-cft-211125678794-1707910187780.s3.us-east-1.amazonaws.com/ab514ae9-fa1b-4fb4-a9c4-c78c76286c89/ab514ae9-fa1b-4fb4-a9c4-c78c76286c89/prod-ovxirbeyzsnoc/921a38b5-fe9d-4bf6-bf5e-60bd711508f0/option3-single-vpc-blank.yaml>

[View in Infrastructure Composer](#)

[Cancel](#) [Next](#)

In the **Specify stack details** screen, provide the following inputs:

- **Stack name** – a name for your deployment
- **Tech contact email** – the email which will receive the registration activation link.
- **Display Name for Intrusion Command Hub** – a friendly name that will tag the instance in Intrusion Command Hub.
- **Instance type** – select the EC2 instance type
- **VPC Name** – the name of the new VPC that will be created
- **VPC CIDR** – CIDR Range of the new VPC (to include all subnets)
- **Single Availability Zone** – the name of the AWS AZ (i.e. us-east-1a, us-west-2b) to deploy. This must be within the region in which you are launching the CloudFormation template
- **Filter Subnet Name** – the name of the subnet created where the Shield Stratus AMI will exist
- **Filter Subnet CIDR** – the CIDR range for the filter subnet (must exist within VPC CIDR)
- **Security Subnet Name** – the name of the subnet created where the GWLB endpoint will exist
- **Security Subnet CIDR** – the CIDR range for the security subnet (must exist within VPC CIDR)
- **Worker Subnet Name** – the name of the public subnet created where your workloads will exist
- **Worker Subnet CIDR** – the CIDR range for the worker subnet (must exist within VPC CIDR)

- Step 1  
Create stack
- Step 2  
Specify stack details
- Step 3  
Configure stack options
- Step 4  
Review and create

## Specify stack details

### Provide a stack name

Stack name

ShieldStratusFullEnvironment

Stack name must contain only letters (a-z, A-Z), numbers (0-9), and hyphens (-) and start with a letter. Max 128 characters. Character count: 28/128.

### Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

#### Contact & AMI

##### Technical contact email

Customer email to receive activation link

shieldcloudtest@intrusion.com

##### AMI ID (Shield Stratus filter)

This is the alias of the Marketplace AMI that will be deployed as part of this stack. Ensure this parameter is set to the following value: /aws/service/marketplace/prod-ovxirbeyznoc/shield-stratus-0.17.

/aws/service/marketplace/prod-ovxirbeyznoc/shield-stratus-0.17

##### Existing Intrusion API key (optional)

Optional: existing intrusion API key to enroll without email. Leave blank to enroll via TechContact.

Enter String

##### Display name for device in Intrusion Command Hub (optional)

Optional: display name for device in Intrusion Command Hub. Leave blank for default display name

shield-stratus-3

### Compute

#### Instance type (x86\_64 only)

EC2 instance type for the sensor

t3.small

### VPC & Subnets (New)

#### VPC name

Name tag for the new VPC (for identification only)

shield-stratus-vpc3

#### VPC CIDR (e.g., 10.1.0.0/16)

CIDR block for the new VPC (must not overlap with connected networks)

10.0.0.0/16

#### Single Availability Zone (e.g., us-east-2a)

Availability Zone for Filter, Security, and Worker subnets (must exist in this region).

us-east-2a

#### Filter subnet name

Name tag for the filter subnet

filter-subnet

#### Filter subnet CIDR

CIDR block for the filter subnet (must be within the VPC CIDR)

10.0.2.0/24

#### Security subnet name

Name tag for the security subnet (hosts the GWLB endpoint)

security-subnet

#### Security subnet CIDR

CIDR block for the security subnet (must be within the VPC CIDR)

10.0.1.0/24

#### Worker subnet name

Name tag for the worker/application subnet

worker-subnet

#### Worker subnet CIDR

CIDR block for the worker/application subnet (must be within the VPC CIDR)

10.0.3.0/24



In the **Configure Stack Options** screen, you may leave these at the default values.

CloudFormation > Stacks > Create > Template

① | ②

Step 1  
Create stack

Step 2  
Specify stack details

Step 3  
Configure stack options

Step 4  
Review and create

**Configure stack options**

**Tags - optional**

Tags (key-value pairs) are used to apply metadata to AWS resources, which can help in organizing, identifying, and categorizing those resources. You can add up to 50 unique tags for each stack.

No tags associated with the stack.

Add new tag

You can add 50 more tag(s)

**Permissions - optional**

Specify an existing AWS Identity and Access Management (IAM) service role that CloudFormation can assume.

**IAM role - optional**

Choose the IAM role for CloudFormation to use for all operations performed on the stack.

IAM role name

Sample-role-name

Remove

**Stack failure options**

**Behavior on provisioning failure**

Specify the roll back behavior for a stack failure. [Learn more](#)

☒ Roll back all stack resources

Roll back the stack to the last known stable state.

☐ Preserve successfully provisioned resources

Preserves the state of successfully provisioned resources, while rolling back failed resources to the last known stable state. Resources without a last known stable state will be deleted upon the next stack operation.

**Delete newly created resources during a rollback**

Specify whether resources that were created during a failed operation should be deleted regardless of their deletion policy. [Learn more](#)

☒ Use deletion policy

Retains or deletes created resources according to their attached deletion policy.

☐ Delete all newly created resources

Deletes created resources during a rollback regardless of their attached deletion policy.

16

In the **Review and Create** screen, you must acknowledge that the CloudFormation may create IAM resources.

### Additional settings

You can set additional options for your stack, like notification options and a stack policy. [Learn more](#) 

► **Stack policy - *optional***

Defines the resources that you want to protect from unintentional updates during a stack update.

► **Rollback configuration - *optional***

Specify alarms for CloudFormation to monitor when creating and updating the stack. If the operation breaches an alarm threshold, CloudFormation rolls it back.

► **Notification options - *optional***


Specify a new or existing Amazon Simple Notification Service topic where notifications about stack events are sent.

► **Stack creation options - *optional***

Specify the timeout and termination protection options for stack creation.

### Capabilities

① **The following resource(s) require capabilities: [AWS::IAM::Role]**

This template contains Identity and Access Management (IAM) resources that might provide entities access to make changes to your AWS account. Check that you want to create each of these resources and that they have the minimum required permissions. [Learn more](#) 

☒ I acknowledge that AWS CloudFormation might create IAM resources.

[Cancel](#)

[Previous](#)

[Next](#)

Once launched, you will be redirected to the AWS Console showing the status of the CloudFormation stacks deployment. This typically takes 4-5 minutes to deploy.

CloudFormation > Stacks > ShieldStratusFullEnvironment

**Stacks (1)**

stratus

Filter status: Active View nested

Stacks

ShieldStratusFullEnvironment  
2025-11-14 06:06:24 UTC-0600  
CREATE\_COMPLETE

**ShieldStratusFullEnvironment**

Delete Update stack Stack actions Create stack

Stack info Events Resources Outputs Parameters Template Change sets Git sync

Table view Timeline view

**Events (93)**

Search events

Timestamp	Logical ID	Status	Detailed status	Status reason
2025-11-14 06:11:07 UTC-0600	<a href="#">ShieldStratusFullEnvironment</a>	CREATE_COMPLETE	-	-
2025-11-14 06:11:05 UTC-0600	WorkerDefaultToVPCE	CREATE_COMPLETE	-	-
2025-11-14 06:11:05 UTC-0600	EdgeRouteWorkerToGwlbe	CREATE_COMPLETE	-	-
2025-11-14 06:11:05 UTC-0600	WorkerDefaultToVPCE	CREATE_IN_PROGRESS	-	Resource creation Initiated
2025-11-14 06:11:05 UTC-0600	EdgeRouteWorkerToGwlbe	CREATE_IN_PROGRESS	-	Resource creation Initiated
2025-11-14 06:11:04 UTC-0600	EdgeRouteWorkerToGwlbe	CREATE_IN_PROGRESS	-	-
2025-11-14 06:11:04 UTC-0600	WorkerDefaultToVPCE	CREATE_IN_PROGRESS	-	-
2025-11-14 06:11:03 UTC-0600	<a href="#">VPCESecurity</a>	CREATE_COMPLETE	-	-
2025-11-14 06:08:58 UTC-0600	EndpointServicePermissionsSelf	CREATE_COMPLETE	-	-

When the stack is fully deployed, the CloudFormation stack will transition from **CREATE\_IN\_PROGRESS** TO **CREATE\_COMPLETE**. Click on the **Resources** tab to view the created resources.

CloudFormation > Stacks > ShieldStratusFullEnvironment

Stacks (1)

stratus

Filter status

Active

View nested

Stacks

ShieldStratusFullEnvironment

2025-11-14 06:06:24 UTC-0600

CREATE\_COMPLETE

ShieldStratusFullEnvironment

Delete Update stack Stack actions Create stack

Stack info Events Resources Outputs Parameters Template Change sets Git sync

Resources (28)

Search resources

Logical ID	Physical ID	Type	Status	Module
EdgeRouteWorkerToGwlbe	rtb-0c94cb88f9f965b91 10.0.3.0/24	AWS::EC2::Route	CREATE_COMPLETE	-
EdgeRT	rtb-0c94cb88f9f965b91	AWS::EC2::RouteTable	CREATE_COMPLETE	-
EdgeRTA	igw-048501a8df3543a7c	AWS::EC2::GatewayRouteTableAssociation	CREATE_COMPLETE	-
EndpointService	vpce-svc-03fa96b6e2c1f2df6	AWS::EC2::VPCEndpointService	CREATE_COMPLETE	-
EndpointServicePermissionSelf	vpce-svc-03fa96b6e2c1f2df6	AWS::EC2::VPCEndpointServicePermissions	CREATE_COMPLETE	-
FilterDefaultRoute	rtb-06e3162573804383e 0.0.0.0/0	AWS::EC2::Route	CREATE_COMPLETE	-
FilterRT	rtb-06e3162573804383e	AWS::EC2::RouteTable	CREATE_COMPLETE	-
FilterRTA	rtbassoc-0ed488267a2265644	AWS::EC2::SubnetRouteTableAssociation	CREATE_COMPLETE	-
FilterSubnet	subnet-0fec4f874a3d62e26	AWS::EC2::Subnet	CREATE_COMPLETE	-

VPC > Your VPCs > vpc-0497b66c61c0f5141

VPC dashboard < Filter by VPC

Virtual private cloud

Subnets

Route tables

Internet gateways

Egress-only internet gateways

DHCP option sets

Elastic IPs

Managed prefix lists

NAT gateways

Peering connections

Route servers

Security

Network ACLs

Security groups

PrivateLink and Lattice

Getting started

Endpoints

Endpoint services

Service networks

Lattice services

vpc-0497b66c61c0f5141 / shield-stratus-vpc3

Details

VPC ID

vpc-0497b66c61c0f5141

State

Available

Tenancy

default

Default VPC

No

Network Address Usage metrics

Disabled

Block Public Access

Off

DHCP option set

dopt-0230d569963ebe225

IPv4 CIDR

10.0.0.0/16

Route 53 Resolver DNS Firewall rule groups

-

DNS hostnames

Enabled

Main route table

rtb-0e67c83a42d0f6701

IPv6 pool

-

Owner ID

225989362918

Resource map

CIDRs

Flow logs

Tags

Integrations

Resource map

VPC

Your AWS virtual network

shield-stratus-vpc3

Subnets (3)

Subnets within this VPC

us-east-2a

security-subnet

filter-subnet

worker-subnet

Route tables (5)

Route network traffic to resources

shield-stratus-vpc3-edge-rt

rtb-0e67c83a42d0f6701

security-subnet-rt

filter-subnet-rt

worker-subnet-rt

Network Connections (1)

Connections to other networks

shield-stratus-vpc3-igw

## Example: Launching Shield Stratus via CloudFormation Template #4 – Filtering Subnets Only

We will walk through the deployment of CloudFormation Template Scenario #4. In this scenario, the user already has a VPC and may already have existing subnets in the VPC they want to protect with Shield Stratus. Therefore, Shield Stratus will only provision the security and filtering subnets and you will need to connect your own subnets to filter.

Select the CloudFormation template **option4-single-vpc-existing**.

**AWS Marketplace** > **Manage subscriptions** > **Shield Stratus** > **Launch**

**Service** | **Info**

☒ **AWS CloudFormation**  
Automated, one-step deployment.

☐ **Amazon EC2**  
Custom deployment using Amazon Machine Image (AMI).

**Launch method** | **Info**  
AWS CloudFormation template

**Version** | **Info**  
Shield Stratus 0.17 (Nov 12, 2025) - latest, stable

► Release notes

**CloudFormation template**

☐ option2-portable-vpc

☐ option3-single-vpc-blank

☒ **option4-single-vpc-existing**

**Region**  
US East (Ohio)

**Launch**

**Launch with CloudFormation**  
AWS CloudFormation automates consistent and reliable deployment. Its reusable templates mean less errors and security risks.  
[View template in CloudFormation Designer](#)

**Launch with CloudFormation**

**Vendor's launch and connection instructions**  
<https://poc-shield-cloud-us-east-2-markeplace-template-main.s3.us-east-2.amazonaws.com/ShieldFlow/Shield+Stratus+AWS.pdf>

On the **Create Stack** screen, leave at the defaults to use the Intrusion-provided CloudFormation template.

CloudFormation > Stacks > Create > Template

Step 1  
● **Create stack**

Step 2  
○ Specify stack details

Step 3  
○ Configure stack options

Step 4  
○ Review and create

### Create stack

**Prerequisite - Prepare template**

You can also create a template by scanning your existing resources in the [IaC generator](#).

**Prepare template**

Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

☒ **Choose an existing template**  
Upload or choose an existing template.

☐ **Build from Infrastructure Composer**  
Create a template using a visual builder.

**Specify template** [Info](#)

This [GitHub repository](#) contains sample CloudFormation templates that can help you get started on new infrastructure projects. [Learn more](#)

**Template source**

Selecting a template generates an Amazon S3 URL where it will be stored. A template is a JSON or YAML file that describes your stack's resources and properties.

☒ **Amazon S3 URL**  
Provide an Amazon S3 URL to your template.

☐ **Upload a template file**  
Upload your template directly to the console.

☐ **Sync from Git**  
Sync a template from your Git repository.

**Amazon S3 URL**

`https://awsmp-cft-211125678794-1707910187780.s3.us-east-1.amazonaws.com/ab514ae9-fa1b-4fb4-a9c4-c78c76286c89/ab514ae9-fa1b-4fb4-a9c4-c78c76286c89`

Amazon S3 template URL

S3 URL: `https://awsmp-cft-211125678794-1707910187780.s3.us-east-1.amazonaws.com/ab514ae9-fa1b-4fb4-a9c4-c78c76286c89/ab514ae9-fa1b-4fb4-a9c4-c78c76286c89/prod-ovxirbeyzsnoc/921a38b5-fe9d-4bf6-bf5e-60bd711508f0/option3-single-vpc-blank.yaml`

[View in Infrastructure Composer](#)

[Cancel](#) [Next](#)

In the **Specify stack details** screen, provide the following inputs:

- **Stack name** – a name for your deployment
- **Tech contact email** – the email which will receive the registration activation link.
- **Display Name for Intrusion Command Hub** – a friendly name that will tag the instance in Intrusion Command Hub.
- **Instance type** – select the EC2 instance type
- **VPC Name** – the name of the existing VPC in which to create resources
- **VPC CIDR** – CIDR Range of the new VPC (to include all subnets). This must match the existing IP range of the specified VPC.
- **Single Availability Zone** – the name of the AWS AZ (i.e. us-east-1a, us-west-2b) to deploy. This must be within the region in which you are launching the CloudFormation template.
- **Filter Subnet Name** – the name of the subnet created where the Shield Stratus AMI will exist
- **Filter Subnet CIDR** – the CIDR range for the filter subnet (must exist within VPC CIDR)
- **Security Subnet Name** – the name of the subnet created where the GWLB endpoint will exist
- **Security Subnet CIDR** – the CIDR range for the security subnet (must exist within VPC CIDR)
- **Reuse Existing IGW** – whether to reuse an existing VPC Internet Gateway (IGW) or to create a new one. If this is set to True, you must give the AWS ARN of the existing internet gateway.

- Step 1  
Create stack
- Step 2  
**Specify stack details**
- Step 3  
Configure stack options
- Step 4  
Review and create

## Specify stack details

### Provide a stack name

#### Stack name

ShieldStratusExistingVPC

Stack name must contain only letters (a-z, A-Z), numbers (0-9), and hyphens (-) and start with a letter. Max 128 characters. Character count: 24/128.

### Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

#### Contact & AMI

##### Technical contact email

Customer email to receive activation link

shieldcloudtest@intrusion.com

##### AMI ID (Shield Stratus filter)

This is the alias of the Marketplace AMI that will be deployed as part of this stack. Ensure this parameter is set to the following value: `/aws/service/marketplace/prod-ovxirbeyznoc/shield-stratus-0.17`.

/aws/service/marketplace/prod-ovxirbeyznoc/shield-stratus-0.17

##### Existing Intrusion API key (optional)

Optional: existing intrusion API key to enroll without email. Leave blank to enroll via TechContact.

Enter String

##### Display name for device in Intrusion Command Hub (optional)

Optional: display name for device in Intrusion Command Hub. Leave blank for default display name

shield-stratus-4

#### Compute

##### Instance type (x86\_64 only)

EC2 instance type for the sensor

t3.small

### Existing VPC & New Subnets

#### Existing VPC ID

Existing VPC where new subnets, GWLB, and endpoints will be created

vpc-0a88e3d8cc0ce7a79

#### Existing VPC CIDR

CIDR of the existing VPC (used for SG scoping and edge route).

10.0.0.0/16

#### Single Availability Zone (e.g., us-east-2a)

Availability Zone for Filter and Security subnets (must exist in this region).

us-east-2a

#### Filter subnet name

Name tag for the filter subnet (hosts the sensor and GWLB)

filter-subnet-a

#### Filter subnet CIDR

CIDR block for the filter subnet (must be within the VPC CIDR)

10.0.17.0/24

#### Security subnet name

Name tag for the security subnet (hosts the GWLB endpoint)

security-subnet

#### Security subnet CIDR

CIDR block for the security subnet (must be within the VPC CIDR)

10.0.16.0/24

### Internet Gateway

#### Reuse existing IGW?

Set to 'true' to reuse an existing IGW attached to this VPC; 'false' to create and attach a new IGW.

true

#### Existing IGW ID (igw-...)

Required when UseExistingIgws='true'. Must be an IGW already attached to the VPC.

igw-0132c013b2b82d8f2

In the **Configure Stack Options** screen, you may leave these at the default values.

CloudFormation > Stacks > Create > Template

① | ②

Step 1  
Create stack

Step 2  
Specify stack details

Step 3  
Configure stack options

Step 4  
Review and create

### Configure stack options

**Tags - optional**

Tags (key-value pairs) are used to apply metadata to AWS resources, which can help in organizing, identifying, and categorizing those resources. You can add up to 50 unique tags for each stack.

No tags associated with the stack.

Add new tag

You can add 50 more tag(s)

**Permissions - optional**

Specify an existing AWS Identity and Access Management (IAM) service role that CloudFormation can assume.

**IAM role - optional**

Choose the IAM role for CloudFormation to use for all operations performed on the stack.

IAM role name ▼

Sample-role-name ▼

Remove ↻

**Stack failure options**

**Behavior on provisioning failure**

Specify the roll back behavior for a stack failure. [Learn more](#)

☒ Roll back all stack resources

Roll back the stack to the last known stable state.

☐ Preserve successfully provisioned resources

Preserves the state of successfully provisioned resources, while rolling back failed resources to the last known stable state. Resources without a last known stable state will be deleted upon the next stack operation.

**Delete newly created resources during a rollback**

Specify whether resources that were created during a failed operation should be deleted regardless of their deletion policy. [Learn more](#)

☒ Use deletion policy

Retains or deletes created resources according to their attached deletion policy.

☐ Delete all newly created resources

Deletes created resources during a rollback regardless of their attached deletion policy.

23



In the **Review and Create** screen, you must acknowledge that the CloudFormation may create IAM resources.

### Additional settings

You can set additional options for your stack, like notification options and a stack policy. [Learn more](#)

#### ► Stack policy - *optional*

Defines the resources that you want to protect from unintentional updates during a stack update.

#### ► Rollback configuration - *optional*

Specify alarms for CloudFormation to monitor when creating and updating the stack. If the operation breaches an alarm threshold, CloudFormation rolls it back.

#### ► Notification options - *optional*

Specify a new or existing Amazon Simple Notification Service topic where notifications about stack events are sent.

#### ► Stack creation options - *optional*

Specify the timeout and termination protection options for stack creation.

### Capabilities

#### ① The following resource(s) require capabilities: [AWS::IAM::Role]

This template contains Identity and Access Management (IAM) resources that might provide entities access to make changes to your AWS account. Check that you want to create each of these resources and that they have the minimum required permissions. [Learn more](#)

☒ I acknowledge that AWS CloudFormation might create IAM resources.

[Cancel](#)

[Previous](#)

[Next](#)

Once launched, you will be redirected to the AWS Console showing the status of the CloudFormation stacks deployment. This typically takes 4-5 minutes to deploy.

CloudFormation > Stacks > ShieldStratusExistingVPC

Stacks (1)

Q existing

Filter status

Active View nested

Stacks

ShieldStratusExistingVPC

2025-11-14 06:26:09 UTC-0600

CREATE\_IN\_PROGRESS

### ShieldStratusExistingVPC

Delete Update stack Stack actions Create stack

Stack info Events Resources Outputs Parameters Template Change sets Git sync

Table view Timeline view

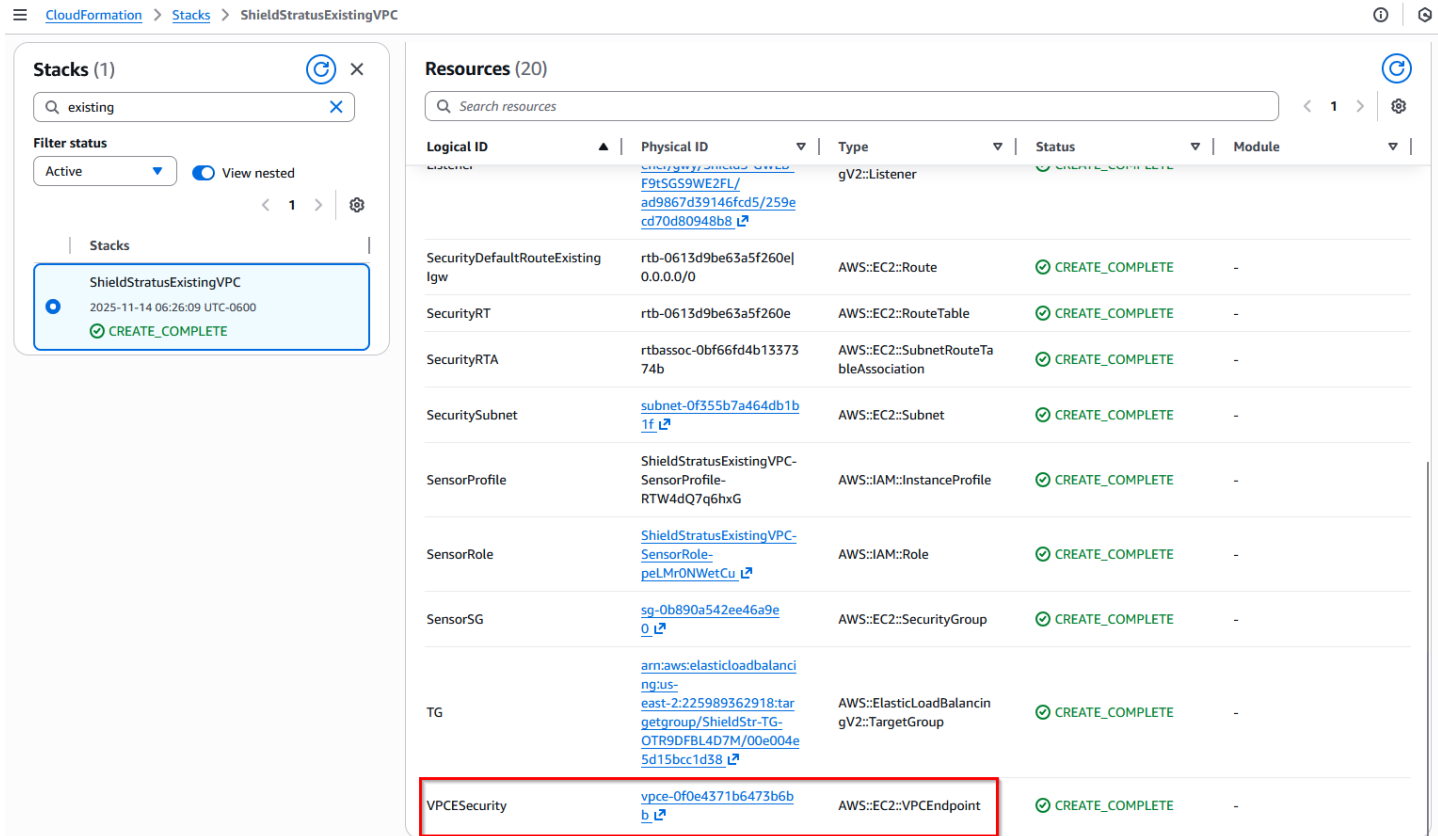
#### Events (47)

View root cause

Search events

Timestamp	Logical ID	Status	Detailed status	Status reason
2025-11-14 06:26:31 UTC-0600	Instance	CREATE_IN_PROGRESS	-	-
2025-11-14 06:26:31 UTC-0600	SensorProfile	CREATE_IN_PROGRESS	CONFIGURATION_COMPLETE	Eventual consistency check initiated
2025-11-14 06:26:30 UTC-0600	SensorProfile	CREATE_IN_PROGRESS	-	Resource creation Initiated
2025-11-14 06:26:30 UTC-0600	SensorProfile	CREATE_IN_PROGRESS	-	-
2025-11-14 06:26:29 UTC-0600	<a href="#">SensorRole</a>	CREATE_COMPLETE	-	-
2025-11-14 06:26:26 UTC-0600	SecurityDefaultRouteExistingIgw	CREATE_COMPLETE	-	-
2025-11-14 06:26:26 UTC-0600	FilterDefaultRouteExistingIgw	CREATE_COMPLETE	-	-
2025-11-14 06:26:25 UTC-0600	SecurityDefaultRouteExistingIgw	CREATE_IN_PROGRESS	-	Resource creation Initiated

When the stack is fully deployed, the CloudFormation stack will transition from **CREATE\_IN\_PROGRESS** TO **CREATE\_COMPLETE**. Click on the **Resources** tab to view the created resources.



The screenshot shows the AWS CloudFormation console for the stack **ShieldStratusExistingVPC**. The stack is in the **CREATE\_COMPLETE** state. The **Resources** tab is selected, displaying a list of 20 resources. The **VPCESecurity** resource is highlighted with a red box. The resource details are as follows:

Logical ID	Physical ID	Type	Status	Module
gV2Listener	<a href="#">arn:aws:elasticloadbalancing:us-east-2:225989362918:targetgroup/ShieldStr-TG-OTR9DFBL4D7M/00e004e5d15bcc1d38</a>	gV2::Listener	CREATE_COMPLETE	-
SecurityDefaultRouteExistingIgw	rtb-0613d9be63a5f260e	AWS::EC2::Route	CREATE_COMPLETE	-
SecurityRT	rtb-0613d9be63a5f260e	AWS::EC2::RouteTable	CREATE_COMPLETE	-
SecurityRTA	rtbassoc-0bf66fd4b1337374b	AWS::EC2::SubnetRouteTableAssociation	CREATE_COMPLETE	-
SecuritySubnet	<a href="#">subnet-0f355b7a464db1b1f</a>	AWS::EC2::Subnet	CREATE_COMPLETE	-
SensorProfile	ShieldStratusExistingVPC-SensorProfile-RTW4dQ7q6hXG	AWS::IAM::InstanceProfile	CREATE_COMPLETE	-
SensorRole	<a href="#">ShieldStratusExistingVPC-SensorRole-peLMr0NWetCu</a>	AWS::IAM::Role	CREATE_COMPLETE	-
SensorSG	<a href="#">sg-0b890a542ee46a9e0</a>	AWS::EC2::SecurityGroup	CREATE_COMPLETE	-
TG	<a href="#">arn:aws:elasticloadbalancing:us-east-2:225989362918:targetgroup/ShieldStr-TG-OTR9DFBL4D7M/00e004e5d15bcc1d38</a>	AWS::ElasticLoadBalancingV2::TargetGroup	CREATE_COMPLETE	-
VPCESecurity	<a href="#">vpce-0f0e4371b6473b6bb</a>	AWS::EC2::VPCEndpoint	CREATE_COMPLETE	-

Make note of the **VPCESecurity endpoint** URN as it will be needed in the next step.

## Routing Subnets

Now that the GWLB and GWLB endpoint have been created, you will need to provisioning the routing on your worker subnets to use the GWLB endpoint in order to inspect with Shield Stratus.

This will involve two steps:

1. Setting an outbound route on your worker subnets to point to the GWLB endpoint
2. (If public) Setting an inbound edge route on the VPC to direct incoming traffic to the subnet

At this point, it assumes that the worker subnets already exist (either before Shield Stratus was deployed or they were created after).

Navigate to the **VPC dashboard** of the AWS console and select the VPC that houses your Shield Stratus and worker subnets. Click on the **Resource map** tab.

The screenshot displays the AWS VPC console interface. On the left, the navigation pane shows the 'VPC dashboard' and various VPC-related resources. The main content area shows the 'Your VPCs (1/1)' list with a table containing details for 'shield-status-vpc-4'. Below this, the 'Resource map' tab is selected, showing a visual representation of the VPC's resources. The map includes a VPC box, a Subnets box (containing 'public-worker-subnet', 'filter-subnet-a', and 'security-subnet'), a Route tables box (containing 'rtb-08497bd35c5e225d1', 'rtb-public', 'security-subnet-rt', 'filter-subnet-a-rt', and 'edge-rt'), and a Network Connections box (containing 'igw'). Orange lines connect the 'public-worker-subnet' to the 'rtb-public' route table, and the 'igw' to the 'rtb-public' route table. A hand cursor is pointing at the 'rtb-public' box.

Name	VPC ID	State	Block Public...	IPv4 CIDR	IPv6 CIDR	DHCP option set	Main route table
shield-status-vpc-4	vpc-0a88e3d8cc0ce7a79	Available	Off	10.0.0.0/16	-	dopt-0230d569963ebe...	rtb-08497bd35c5e...

Click on the existing subnet associated with your workload (in this example we called it “public-worker subnet”), then open the route table associated with that subnet.

VPC > Route tables > rtb-08b4c0540b1084d2d

**rtb-08b4c0540b1084d2d / rtb-public**

**Details**

Route table ID: rtb-08b4c0540b1084d2d

VPC: vpc-0a88e3d8cc0ce7a79 | shield-status-vpc-4

Main: No

Owner ID: 225989362918

Explicit subnet associations: subnet-071e087bb2b9ba9c5 / public-worker-subnet

Edge associations: -

**Routes (2)**

Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	igw-0132c013b2b82d8f2	Active	No	Create Route
10.0.0.0/16	local	Active	No	Create Route Table

[Edit routes](#)

Then click **Edit Routes**. Add a new route for the default gateway.

Destination: 0.0.0.0/0

Target: **Gateway Load Balancer Endpoint**

Then select the Gateway Load Balancer Endpoint name created by CloudFormation in the previous section. Then select Save changes.

VPC > Route tables > rtb-08b4c0540b1084d2d > Edit routes

**Edit routes**

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	CreateRouteTable
0.0.0.0/0	Gateway Load Balancer Endpoint	Active	No	CreateRoute

[Add route](#)

[Cancel](#) [Preview](#) [Save changes](#)

If your worker subnet requires inbound access, you will also need to create an Edge Route to instruct the GWLB how to route incoming traffic back to your worker subnet after inspection.

Return to the **VPC dashboard**, select your VPC and visit **Resource map** again. This time select the edge route from the **Route Tables** column. It should be named ending in **\*-edge-rt**.

The screenshot shows the AWS VPC dashboard. On the left is a navigation menu with sections: VPC dashboard, Virtual private cloud, Security, and PrivateLink and Lattice. The main content area is titled 'Your VPCs (1/1) Info' and shows a table with one VPC: shield-stratus-vpc-4. Below this, the 'Resource map' is displayed for vpc-0a88e3d8cc0ce7a79. The map shows four categories: VPC (shield-stratus-vpc-4), Subnets (3: public-worker-subnet, filter-subnet-a, security-subnet), Route tables (5: rtb-08497bd35c5e225d1, rtb-public, security-subnet-rt, filter-subnet-a-rt, and edge-rt), and Network Connections (1: igw). The 'edge-rt' route table is highlighted in orange.

Open the link to this page and select **Edit route**.

The screenshot shows the details of a specific route table: rtb-04937c72789542305 / edge-rt. The 'Details' section shows the route table ID, VPC, Main status (No), Owner ID, Explicit subnet associations (none), and Edge associations (igw-0132c013b2b82d8f2 / igw). Below this, the 'Routes' section shows a single route with destination 10.0.0.0/16, target local, status Active, propagated No, and route origin Create Route Table. The 'Edit routes' button is highlighted with a red box.

Similarly, create a new route.

Destination: <CIDR Range of your worker subnet>

Target: **Gateway Load Balancer Endpoint**

Then select the same Gateway Load Balancer Endpoint name created by CloudFormation in the previous section. Then select Save changes.

VPC > Route tables > rtb-04937c72789542305 > Edit routes

### Edit routes

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	CreateRouteTable
10.0.0.0/20	Gateway Load Balancer Endpoint		No	CreateRoute

[Add route](#) [Cancel](#) [Preview](#) [Save changes](#)

At this point you should be able to successfully route traffic inbound and outbound to your worker subnet and have Shield Stratus inspect and filter the traffic.

## Activating Shield Stratus

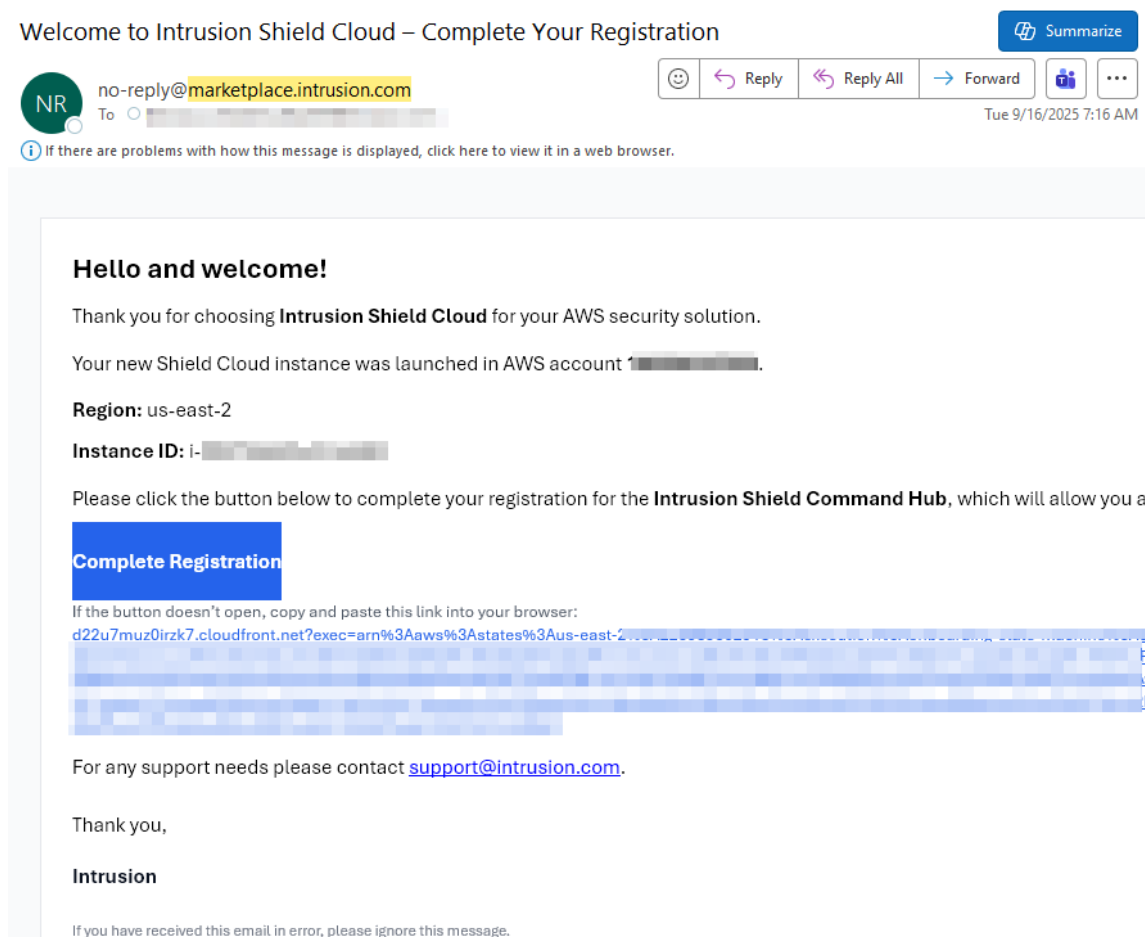
Although Shield Stratus is instantiated and will route traffic, it will not filter traffic, log traffic, or activate port forwarding until it has been activated.

Intrusion will send an email to the email address provided in the CloudFormation template upon activation of a Shield Stratus instance.

## Creating an Intrusion Command Hub Account

Shield Stratus detects whether an Intrusion Command Hub account has been registered for your AWS account. If a previous activation is associated with your AWS account, you may continue to use your previously setup credentials to login to the Command Hub.

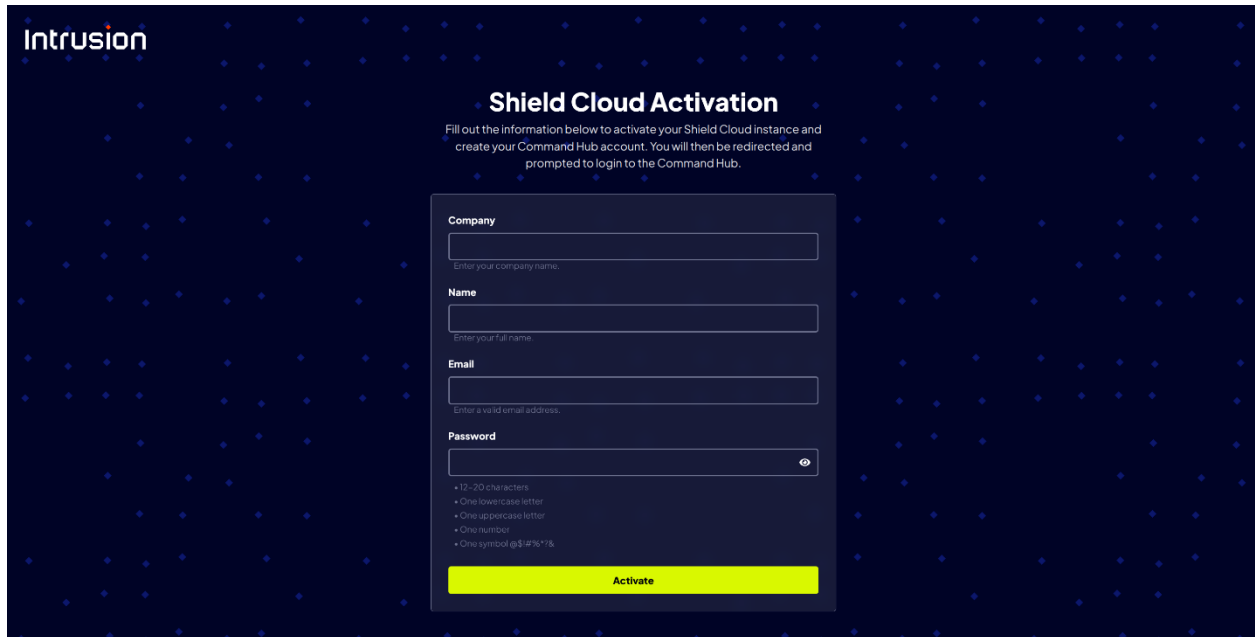
If your AWS account is not tied to an existing Command Hub account, it will send an activation link in an email.





Clicking the link will direct you to an account creation page. On this page, you will create an account for the Intrusion Command Hub.

The email and password provided will serve as a login to Shield Command Hub.

The image shows a 'Shield Cloud Activation' form on a dark blue background with a pattern of small white dots. The form is centered and has a dark gray background. It includes fields for 'Company', 'Name', 'Email', and 'Password'. The 'Password' field has a toggle icon (an eye) to the right. Below the password field, there are four bullet points listing password requirements: 12-20 characters, one lowercase letter, one uppercase letter, one number, and one symbol from the set @\$!%\*'^&. At the bottom of the form is a bright yellow 'Activate' button. The 'Intrusion' logo is in the top left corner of the page.

**Intrusion**

### Shield Cloud Activation

Fill out the information below to activate your Shield Cloud instance and create your Command Hub account. You will then be redirected and prompted to login to the Command Hub.

**Company**  
  
Enter your company name.

**Name**  
  
Enter your full name.

**Email**  
  
Enter a valid email address.

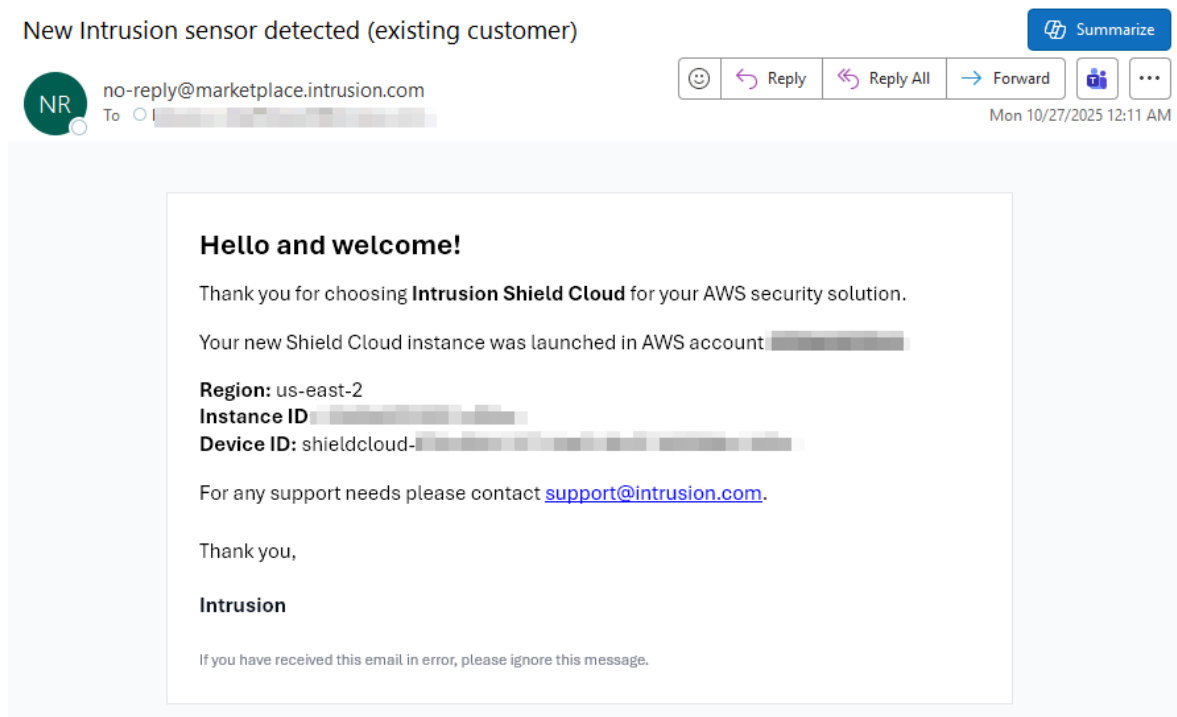
**Password**  
  
• 12-20 characters  
• One lowercase letter  
• One uppercase letter  
• One number  
• One symbol @\$!%\*'^&

**Activate**

Once the form is successfully completed, it will present a link to the Intrusion Command Hub.

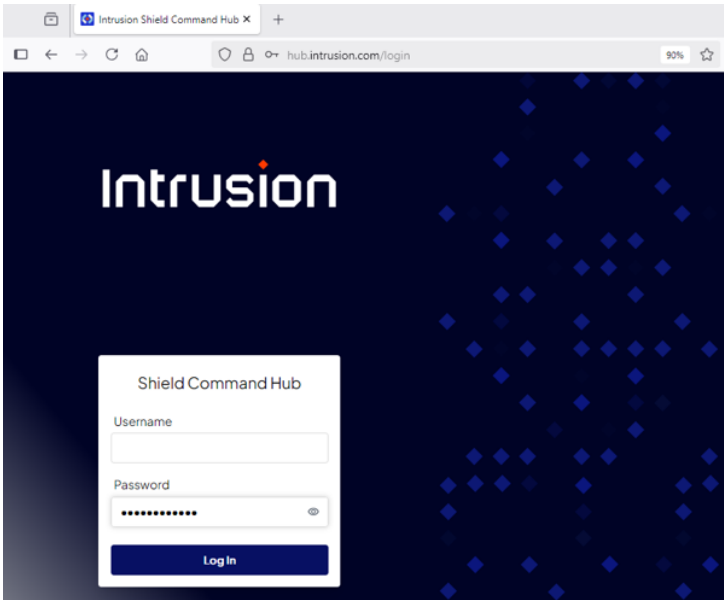
Additionally, this will trigger your Shield Stratus instance to register with this account within a few minutes.

If you have already registered previously with your AWS account, then Shield Stratus will use the previously created Command Hub account to associate with the new Shield Stratus instance. You will receive an email similar to the following.



# Intrusion Command Hub

The Intrusion Command Hub (<https://hub.intrusion.com>) can be accessed with the newly created credentials. For more information, see [Command Hub Management of](#) .



Once logged in, click on the Devices tab.

Overview

Time Interval: Last 72hr to 3:41pm

Devices: Shieldcloud-674e58cf-3f71-4e03-9b47-082888e1430c

Generate Report

Network Health

7,834 Kills

last 24hr

5577% 138 Kills (previous 24hr)

7,813 Outbound Kills

last 24hr

5603% 137 Outbound Kills (previous 24hr)

21 Inbound Kills

last 24hr

2000% 1 Inbound Kills (previous 24hr)

Countries Visited

Country	Connections	Volume (KB)
China	51	3,570
Singapore	30	1,440
Greece	10	322
Hong Kong	4	152
Russia	3	106
Romania	2	66
Brazil	2	36
Kazakhstan	1	36
Angola	1	36
Bahrain	1	84

Top High Risk Categories

AI Insights Summary - Beta

Unable to Load Any Summary for Currently Selected Devices

AI Recommendations - Beta

No Actionable Insights Found for Current Device

Top Requested Domains

Domain	Killed Requests	Total Requests	Maximum Risk Level
amazonaws.com	0	202	
ubuntu.com	0	104	
snapcraft.io	0	40	
canonical.com	0	16	

At Risk Devices

Client IP	Client Hostname	Connections	Volume (KB)	Risk	Shield Dev...
10.0.2.145		7,972	846	5	shieldclou...

34

Then select **Shield Stratus** under the Device Type dropdown. This will show your registered Shield Stratus instances.

Intrusion Shield Command Hub

OverviewAI InsightsTrafficPermits**Devices**Advanced Reports

Device TypeShield Stratus▼Devices: Shieldflow-077ee1d3-3a02-4207-97eb-18dd46c5ab2a▼

Search

ColumnsFiltersSort

Device ID	Display Name	Device Type	Sync Status	Last Sync Time	Mode	Version
shieldflow-077ee1d3-3a02-4...	shield-stratus-3	Shield Stratus	Sync Successful	2025-11-14 6:30:02 AM CST	Protect	1.0.5

For more information, see [Command Hub Management of](#) .

## Configuring DNS Clients

By default, AWS VPCs will enable DNS resolution from AWS resolvers from inside the VPC without traversing the VPC. In this case, Shield Stratus will have no visibility to protect DNS requests as the DNS traffic does not flow through the GWLB.

In order for Shield Stratus to inspect and filter outbound DNS requests, the clients must point to DNS resolvers outside of the VPC.

## Testing

To verify that the Intrusion ATl is working, try resolving various domains.

For example, run the following test domains from a Linux client.

```
dig @8.8.8.8 google.com
dig @8.8.8.8 imnottxhacker.com
```

**google.com** should resolve to a public IP

**imnottxhacker.com** should fail to resolve, meaning it has been blocked by Shield

## Command Hub Management of Shield Stratus

Once Shield Stratus is registered with the Command Hub, the Command Hub can be used to view traffic reports and to administer Shield Stratus instances.

Reporting can be accessed via the Intrusion Shield Hub dashboard at <https://hub.intrusion.com>.

### Managed Features

Feature	Direction	Description
Device Mode	Inbound and Outbound	Enables and disables the traffic monitoring and filtering services
IP Permits	Inbound and Outbound	IP addresses to explicitly allow
DNS Permits	Outbound	FQDNs to explicitly allow

# Viewing Traffic

The Command Hub **Traffic** table shows a summary of network traffic observed by Shield Stratus, both inbound and outbound of your VPC. It shows a summary of DNS requests, TCP connections, UDP sessions and ICMP packets over a 72 hour period.

IntrusionShield Command Hub

OverviewAI InsightsTrafficPermitsDevicesAdvanced Reports

TrafficFilters: Direction = Outbound,Time Interval: 72 HoursFrom: 11/11/2025, 8:37:02 AM to 11/14/2025, 8:37:02 AMDevices: Fc404927-E3ff-4e00-9305-37618123c520

Show Custom Cards

Search

ColumnsFiltersSelect filter...Save FilterManage Saved FiltersClear FiltersReset to DefaultExport

	Status	Device Name	Type	Product	VLAN	Risk	Client IP	Server IP	Domain	Port	Direction	Count	First Seen	Last Seen
	Killed	www...	TCP	Shield Stratus	0	0	136.112.99.7	10.0.134.62		443	Outbound	1	2025-11-12 9:46:46 AM CST	2025-11-12 10:20:07 AM CST
	Killed	www...	TCP	Shield Stratus	0	0	89.97.218.142	10.0.192.191		22	Outbound	1	2025-11-12 10:17:38 AM CST	2025-11-12 10:17:54 AM CST
	Killed	www...	TCP	Shield Stratus	0	0	78.128.112.74	10.0.134.62		22	Outbound	1	2025-11-12 10:13:28 AM CST	2025-11-12 10:14:00 AM CST
	Killed	www...	TCP	Shield Stratus	0	0	103.133.214.209	10.0.134.62		443	Outbound	1	2025-11-12 10:13:29 AM CST	2025-11-12 10:14:00 AM CST
	Killed	www...	TCP	Shield Stratus	0	0	45.156.131.7	10.0.134.62		443	Outbound	1	2025-11-12 10:02:41 AM CST	2025-11-12 10:03:13 AM CST
	Killed	www...	TCP	Shield Stratus	0	0	156.245.248.226	10.0.134.62		22	Outbound	1	2025-11-12 9:56:31 AM CST	2025-11-12 9:57:02 AM CST
	Killed	www...	TCP	Shield Stratus	0	0	2.189.5.222	10.0.134.62		443	Outbound	1	2025-11-12 9:50:11 AM CST	2025-11-12 9:55:28 AM CST
	Killed	www...	TCP	Shield Stratus	0	0	2.189.5.218	10.0.134.62		443	Outbound	1	2025-11-12 9:49:05 AM CST	2025-11-12 9:49:37 AM CST
	Killed	www...	TCP	Shield Stratus	0	0	209.42.16.160	10.0.192.191		80	Outbound	1	2025-11-12 9:42:07 AM CST	2025-11-12 9:42:22 AM CST
	Killed	www...	TCP	Shield Stratus	0	0	14.103.107.26	10.0.192.191		22	Outbound	1	2025-11-12 9:38:54 AM CST	2025-11-12 9:39:26 AM CST
	Passed	www...	TCP	Shield Stratus	0	0	10.0.134.62	52.38.250.151		443	Outbound	92	2025-11-13 2:21:01 PM CST	2025-11-14 8:27:06 AM CST
	Passed	www...	TCP	Shield Stratus	0	0	160.19.240.30	10.0.192.191		443	Outbound	20	2025-11-13 9:09:29 PM CST	2025-11-14 8:27:06 AM CST
	Passed	www...	TCP	Shield Stratus	0	0	160.19.243.127	10.0.134.62		443	Outbound	19	2025-11-13 9:10:50 PM CST	2025-11-14 8:27:06 AM CST
	Passed	www...	TCP	Shield Stratus	0	0	160.19.240.207	10.0.192.191		443	Outbound	18	2025-11-13 9:12:52 PM CST	2025-11-14 8:27:06 AM CST
	Passed	www...	TCP	Shield Stratus	0	0	160.19.240.137	10.0.192.191		443	Outbound	18	2025-11-13 9:38:12 PM CST	2025-11-14 8:27:06 AM CST
	Passed	www...	TCP	Shield Stratus	0	0	160.19.243.95	10.0.134.62		443	Outbound	21	2025-11-13 9:01:26 PM CST	2025-11-14 8:27:05 AM CST
	Passed	www...	TCP	Shield Stratus	0	0	160.19.243.55	10.0.134.62		443	Outbound	20	2025-11-13 10:06:26 PM CST	2025-11-14 8:27:05 AM CST
	Passed	www...	TCP	Shield Stratus	0	0	160.19.240.73	10.0.192.191		443	Outbound	18	2025-11-13 9:07:26 PM CST	2025-11-14 8:27:05 AM CST
	Passed	www...	TCP	Shield Stratus	0	0	160.19.240.24	10.0.134.62		443	Outbound	15	2025-11-13 9:11:59 PM CST	2025-11-14 8:27:05 AM CST
	Passed	www...	TCP	Shield Stratus	0	0	160.19.240.172	10.0.192.191		443	Outbound	14	2025-11-13 9:23:08 PM CST	2025-11-14 8:27:05 AM CST
	Passed	www...	TCP	Shield Stratus	0	0	160.19.243.101	10.0.192.191		443	Outbound	13	2025-11-13 9:02:24 PM CST	2025-11-14 8:27:05 AM CST
	Passed	www...	TCP	Shield Stratus	0	0	160.19.241.75	10.0.134.62		443	Outbound	12	2025-11-13 11:05:15 PM CST	2025-11-14 8:27:05 AM CST

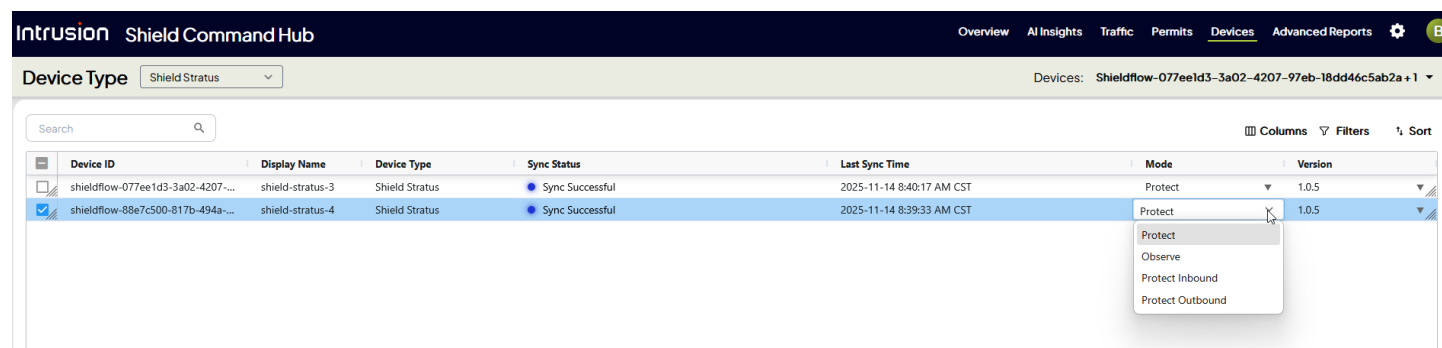
100Items per pageShowing 1 to 100 of 87927 entries

Traffic summaries are updated from Shield Stratus approximately every 15 minutes.

For more detailed information about the meaning of the data and the filtering capabilities, see the Intrusion Command Hub User Guide.

## Managing Devices

Shield Stratus devices appear in the **Devices** tab. From the **Device Type** dropdown, select **Shield Stratus** to see a list of devices registered to your account. The Devices tab allows users to select Device type and choose to modify a device if necessary.



By default, Shield Stratus starts in **On** mode, meaning that inspects and filters traffic. If you want to disable global filtering, the **Mode** toggle to deactivate it.

The Shield Stratus devices have the following properties.

Parameter	Type	Description
Device ID	Read-only	The unique identifier of the Shield Stratus instance, generated on first boot
Device Name	Read-only	Name of the device, based on the local reported hostname
Sync Status	Read-only	The status of the Command Hub sync <ul style="list-style-type: none"><li>Pending – device has been registered but has not synchronized state</li><li>Sync Successful – device has synchronized status at least once</li></ul>
Last Sync	Read-only	The last synchronization time
Mode	Read-write	The provisioned mode of the <ul style="list-style-type: none"><li><b>Protect</b> – DNS and IP filtering are enabled for both inbound and outbound traffic. Traffic logging is enabled.</li><li><b>Observe</b> – DNS and IP filtering are disabled but Traffic logging is still active</li><li><b>Protect Inbound</b> – DNS and IP filtering are only enabled for inbound traffic (originating from outside the VPC). Traffic logging for both inbound and outbound is enabled.</li><li><b>Protect Outbound</b> – DNS and IP filtering are only enabled for outbound traffic (originating from inside the VPC). Traffic logging for both inbound and outbound is enabled.</li></ul>
Version	Read-only	Shield Stratus software version

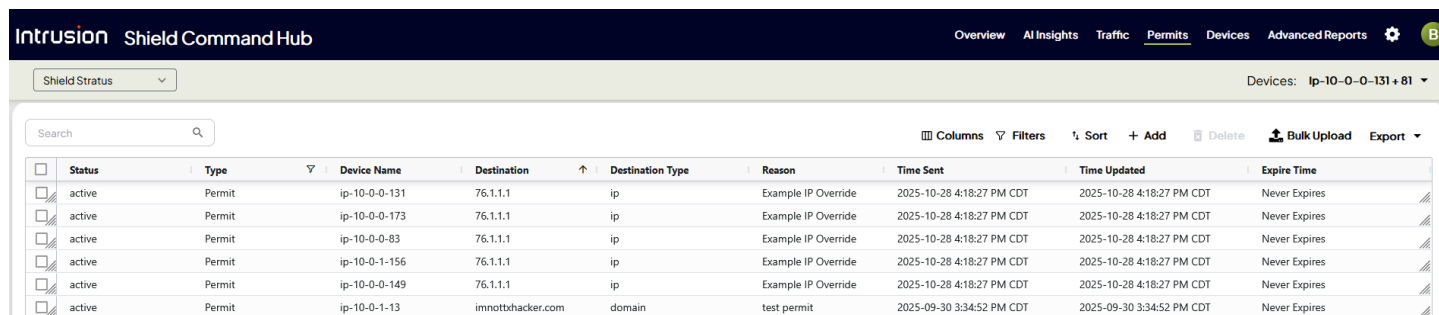


## Adding Custom Permits

When the Shield Stratus device is on **On** mode, Intrusion's Applied Threat Intelligence monitors all inbound and outbound IP connections and outbound DNS requests and selectively blocking high risk communications.

In the case that Shield Stratus reputation blocking decisions inadvertently block a DNS resolution or IP address that should be allowed, the user has the ability to override the logic by creating explicit permits for Domains/Hostnames and IPs.

From the **Permits** tab, select the **Device Type** of **Shield Stratus**. This will list all active user-specified permits. An admin user can add and remote custom permitted IPs and hostnames.



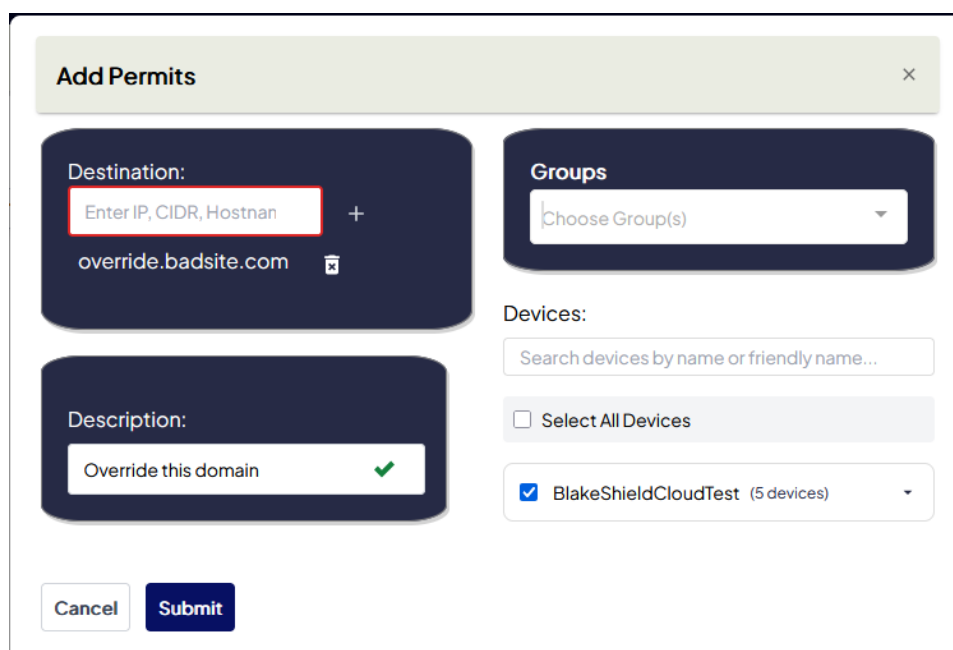
The screenshot shows the 'Intrusion Shield Command Hub' interface. The 'Permits' tab is selected, displaying a table of active permits. The table has columns for Status, Type, Device Name, Destination, Destination Type, Reason, Time Sent, Time Updated, and Expire Time. There are six rows of permits, all with a status of 'active' and a type of 'Permit'. The destinations include IP addresses and a domain name.

Status	Type	Device Name	Destination	Destination Type	Reason	Time Sent	Time Updated	Expire Time
active	Permit	ip-10-0-0-131	76.1.1.1	ip	Example IP Override	2025-10-28 4:18:27 PM CDT	2025-10-28 4:18:27 PM CDT	Never Expires
active	Permit	ip-10-0-0-173	76.1.1.1	ip	Example IP Override	2025-10-28 4:18:27 PM CDT	2025-10-28 4:18:27 PM CDT	Never Expires
active	Permit	ip-10-0-0-83	76.1.1.1	ip	Example IP Override	2025-10-28 4:18:27 PM CDT	2025-10-28 4:18:27 PM CDT	Never Expires
active	Permit	ip-10-0-1-156	76.1.1.1	ip	Example IP Override	2025-10-28 4:18:27 PM CDT	2025-10-28 4:18:27 PM CDT	Never Expires
active	Permit	ip-10-0-0-149	76.1.1.1	ip	Example IP Override	2025-10-28 4:18:27 PM CDT	2025-10-28 4:18:27 PM CDT	Never Expires
active	Permit	ip-10-0-1-13	imnotthacker.com	domain	test permit	2025-09-30 3:34:52 PM CDT	2025-09-30 3:34:52 PM CDT	Never Expires

To add a new permit, click the **+ Add** button. The **Destination** can be an IP, CIDR range, or hostname. An individual Shield Stratus device can be selected, or a group can be selected.

Populate with

- **Destination** – a FQDN or IP address. Make sure to click the plus sign (+) after each one.
- **Description** – a required note for why you are unblocking
- **Devices** – one or more current Shield Stratus devices to which you want to apply the permit



The 'Add Permits' dialog box is shown. It has a title bar with 'Add Permits' and a close button. The dialog is divided into several sections: 'Destination' with a text input field containing 'Enter IP, CIDR, Hostname' and a plus sign button, and a list of destinations including 'override.badsite.com'; 'Groups' with a dropdown menu showing 'Choose Group(s)'; 'Description' with a text input field containing 'Override this domain' and a green checkmark icon; and 'Devices' with a search bar, a 'Select All Devices' checkbox, and a dropdown menu showing 'BlakeShieldCloudTest (5 devices)' with a checkmark. At the bottom are 'Cancel' and 'Submit' buttons.

Then click **Submit**. The sync of the permit to the Shield Stratus instance may take 1-2 minutes before it reflects in live traffic decisions.

Admins can also upload a CSV of permits to load to a device or group, as well as export the current list of permits via a CSV or Excel file.

The image shows two parts of a web interface. On the left is a modal window titled 'Add Permits' with a close button (X). It contains a 'Destination' field with a placeholder 'Enter IP, CIDR, Hostname' and a plus icon, a 'Groups' dropdown menu with 'Choose Group(s)' selected, a 'Description' text area, and 'Cancel' and 'Submit' buttons at the bottom. To the right of the modal is a list of devices under the heading 'Devices:'. The first device is 'bddtest' with an unchecked checkbox. Below it are several other device names, some partially obscured, each with an unchecked checkbox. To the right of the device list is a dropdown menu with 'Upload CSV' and 'Export' options. The 'Export' dropdown is open, showing 'CSV Export' and 'Excel Export' buttons.

Note that changes only apply to selected existing instances and not to new instances.

# Frequently Asked Questions

## General

How does Intrusion Shield Stratus for AWS differ from Intrusion Shield Gateway for AWS?

Both Shield Stratus and Shield Gateway implement Intrusion's reputation-based filtering for protecting and monitoring DNS and IP flows. The difference is the network architecture in which they are deployed.

Shield Gateway is implemented as a [NAT instance](#). It is meant to act as a router between a Public subnet and a Private subnet. Shield Gateway also acts as a firewall, restricting all inbound traffic by default unless explicitly allowed. Thus it requires your workload to exist in a Private subnet.

Shield Stratus is a more flexible option that does not require NATing and works with existing public and private subnets. It is implemented as a transparent bump-in-the-wire [GENEVE filter](#) meant to be used in concert with an AWS Gateway Load Balancer. Though it requires a slightly more advanced network architecture setup, it is more transparent to your existing workflows and network addressing.

## Provisioning

### 1. What instance type is recommended?

The size depends on your network traffic profile. This varies from case to case, as it is not just a function of bandwidth but also number of concurrent sessions, number of hosts, and number of destinations.

We recommend starting with the **t3.small** instance, which can handle over 600Mbps of throughput, and switch to larger instances if needed.

### 2. Does Shield Stratus support Auto Scaling Groups?

At a technical level, Shield Stratus is built to operate as a GWLB filter target, and this exists in a target group which can be an autoscaling group. While it is possible, currently in Shield Stratus Beta release, Intrusion does not offer support for this scenario, and it is left to the architect to implement. Also, Intrusion Command Hub does not currently offer the concept of grouping or syncing configurations of Shield Stratus instances in parallel.

### 3. How do I find the Device ID of a Shield Stratus instance?

The Device ID is sent in the registration email when a new Shield Stratus device comes online.

### 4. Can I instantiate Shield Stratus without a CloudFormation template?

Currently, Shield Stratus requires certain metadata passed to the instance via CloudFormation for it to activate and register with the Intrusion Command Hub. Please contact support for assistance with custom integrations.

## Command Hub

### 5. How do I obtain an Intrusion Command Hub login?

Upon the deployment of a Shield Stratus instance for the first time in your AWS account, you will receive an activation email that guides you through the process of creating a Command Hub customer account and user login. Subsequent Shield Stratus deployments will be associated with that same customer account, and instantiation of subsequent Shield Stratus deployments will trigger an alert email to that user.

### 6. I no longer maintain the email that was used to register with Command Hub. How do I associate my AWS account with a different user?

Please contact Intrusion support.

### 7. How frequently does Shield Stratus sync with Command Hub?

Shield Stratus synchronizes provisioning information with Command Hub once per minute. Changes made in the Command Hub may take up to 1 minute to apply.

Shield Stratus uploads traffic metadata approximately every 15 minutes.

## High Availability

### 8. Can Shield Stratus be deployed in High Availability mode in AWS?

Yes, multiple Shield Stratus can be associated with a Gateway Load Balancer target group, effectively supporting parallel processing of network flows.

## Logging

### 9. Does Shield Stratus support CloudWatch Logs?

Currently ShieldFlow does not support CloudWatch Logs.

## Data Collection Policy

In general, Shield decodes and records machine-to-machine network flow metadata used to make security decisions about observed traffic endpoints. In general, it does not look at the inner payload of the connections, except for relevant protocols like DNS that contain attributes related to flows. No traffic decryption is performed.

The following types of data are captured on the Shield Appliance:

- Shield Stratus records network flow metadata, including source and destination IP addresses, MAC addresses, ports, byte counts and timestamps of Layer 1-4 network flow headers.
- Shield Stratus decodes DNS requests and responses containing IP to hostname resolutions and selectively modifies the responses for the purpose of filtering.
- Shield Stratus records log files related to the appliance's health (such as uptime information, packet counts, memory and CPU information, crash dumps)
- Shield Command Hub logs user activity on the dashboard which may include username and local IP address (such as logins, administrative changes, permits)

Intrusion uses the data to (A) provide customer-accessible dashboards and control to report and manage fleets of their devices, (B) incorporate such Customer Shield Data into Intrusion's proprietary database, (C) to modify, expand, and to improve the performance of the Shield Service.