INTRUSION SHIELD STRATUS

Launching for Azure

March 2026

SUPPORT@INTRUSION.COM

Contents

What is Shield Stratus for Azure?

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

Built on Azure Load Balancer, 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 VNet

How Does Shield Stratus Work?

Intrusion Shield Stratus is implemented as a filter for an Azure Gateway Load Balancer (GWLB). As traffic traverses the Gateway Load Balancer inbound or outbound from a VNet, it is sent to the 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

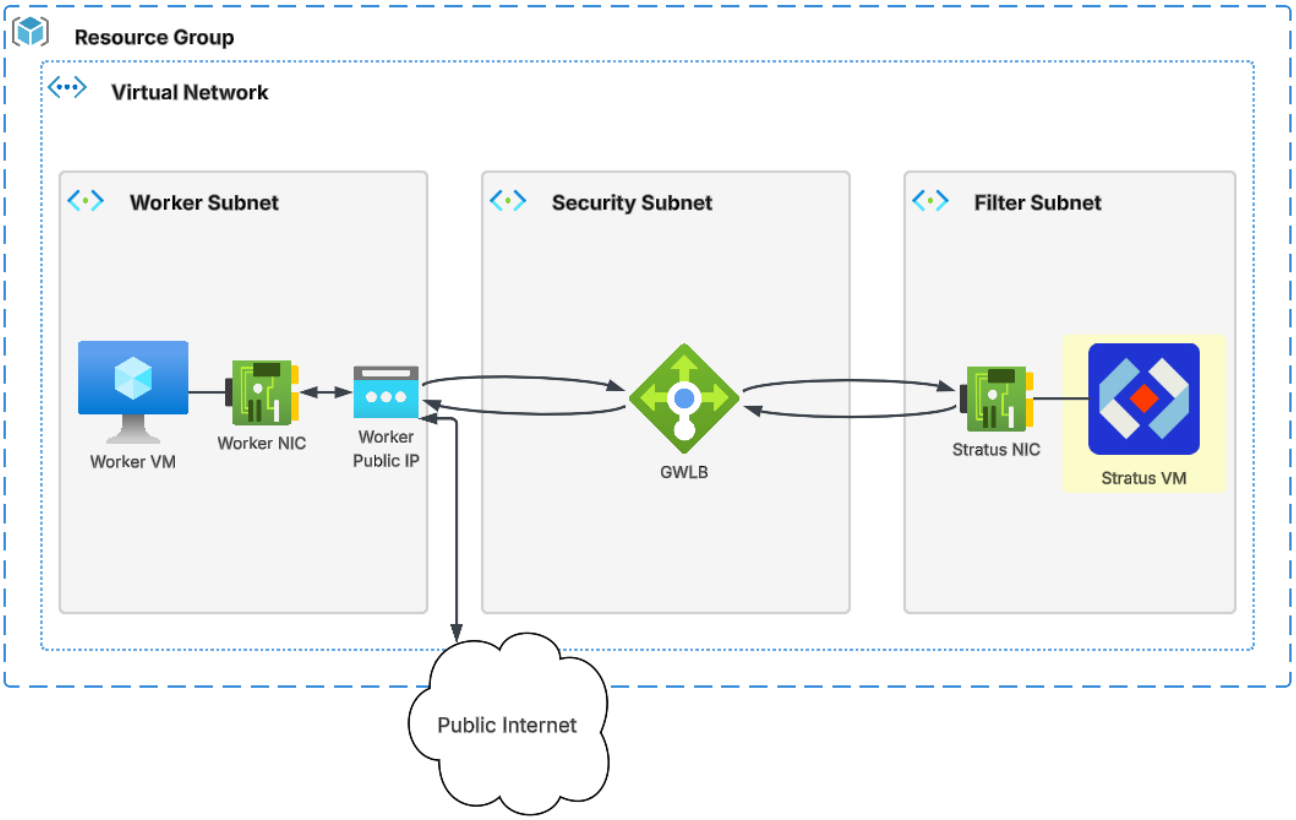
Shield Stratus is deployed as a filter for an Azure Gateway Load Balancer. At a high level:

- A Gateway Load Balancer is created, with the target group pointing to one or more Shield Stratus instances
- Optionally, Outbound and/or Edge Load Balancers can be created

Public vs Private Endpoints

There are different blueprints for protecting resources with Public IPs versus Private IPs.

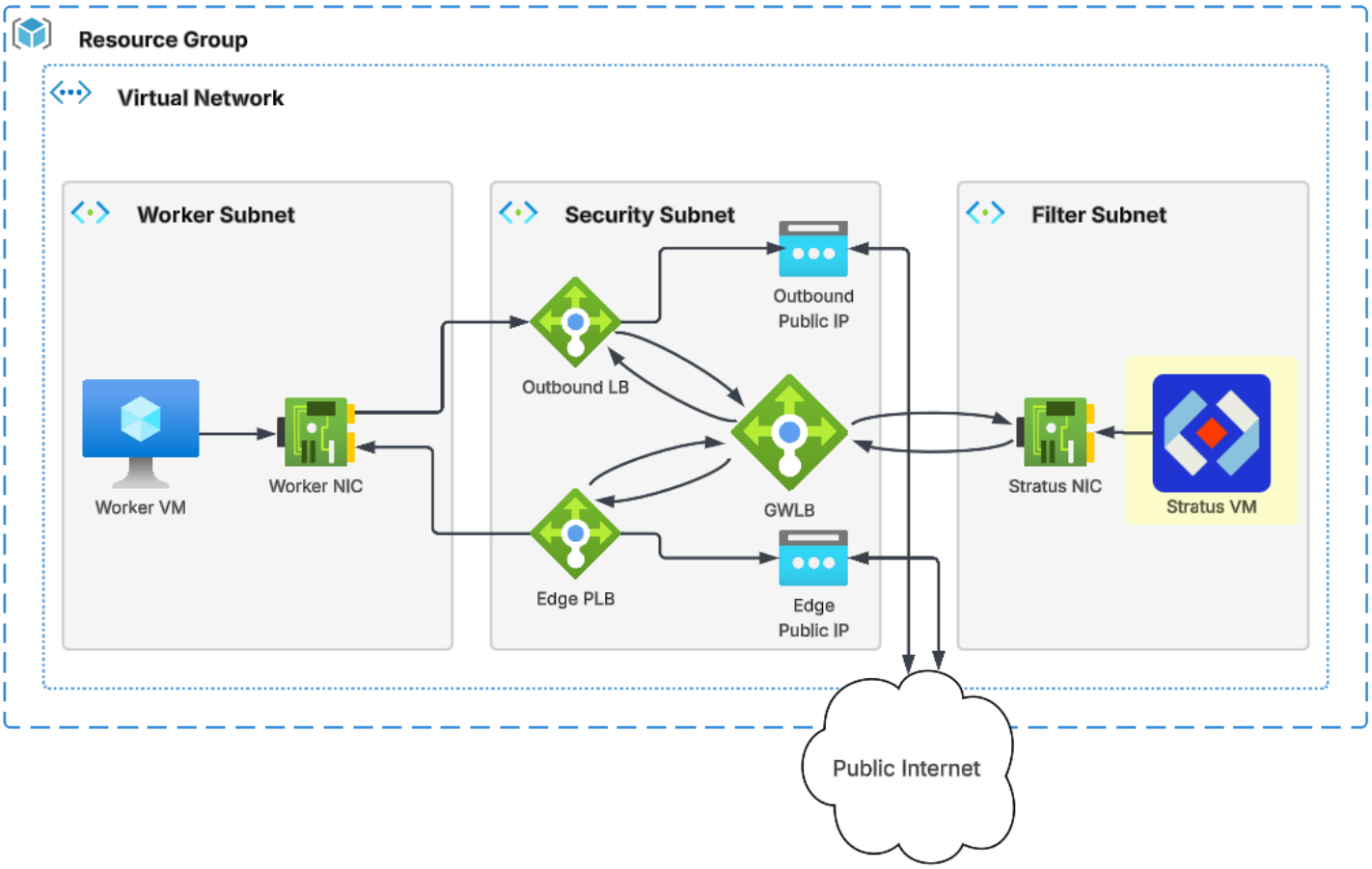
Consider a basic example of a worker VM with a public IP. To protect both inbound and outbound flows from this Public IP, a GWLB instance is deployed. This GWLB has a target of a Shield Stratus instance. All inbound and outbound flows pass through the GWLB which forwards to the Stratus VM for inspection and filtering.



In the Private IP case using a private subnet, the flow is more complex, as there are three load balancers involved:

- the Gateway Load Balancer to perform filtering
- an Edge public load balancer to handle incoming traffic
- an outbound load balancer to handle outbound traffic initiated from the private subnet

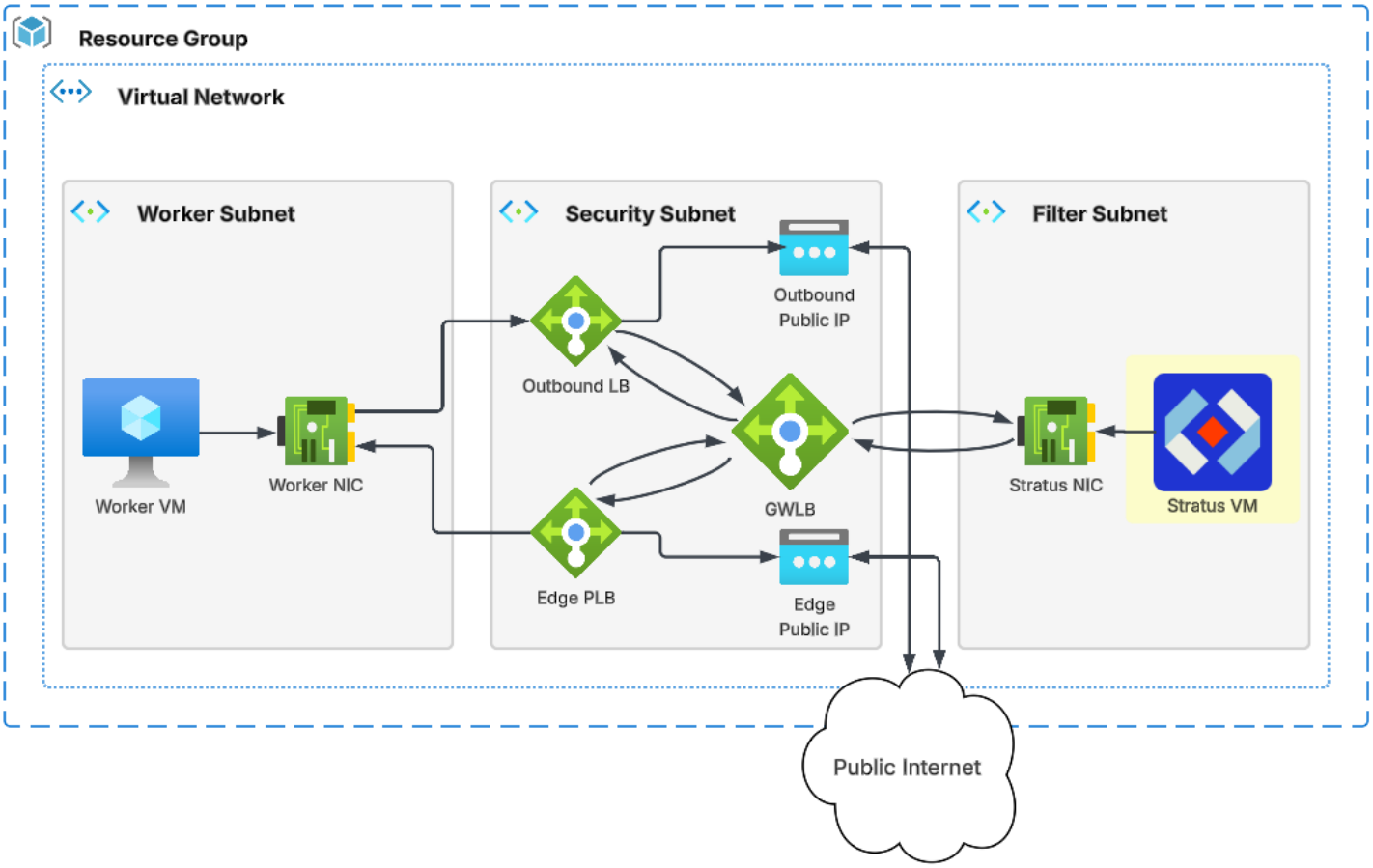
The Shield Stratus VM operates the same, but the plumbing of the load balancers are more complex.



VNet Deployments

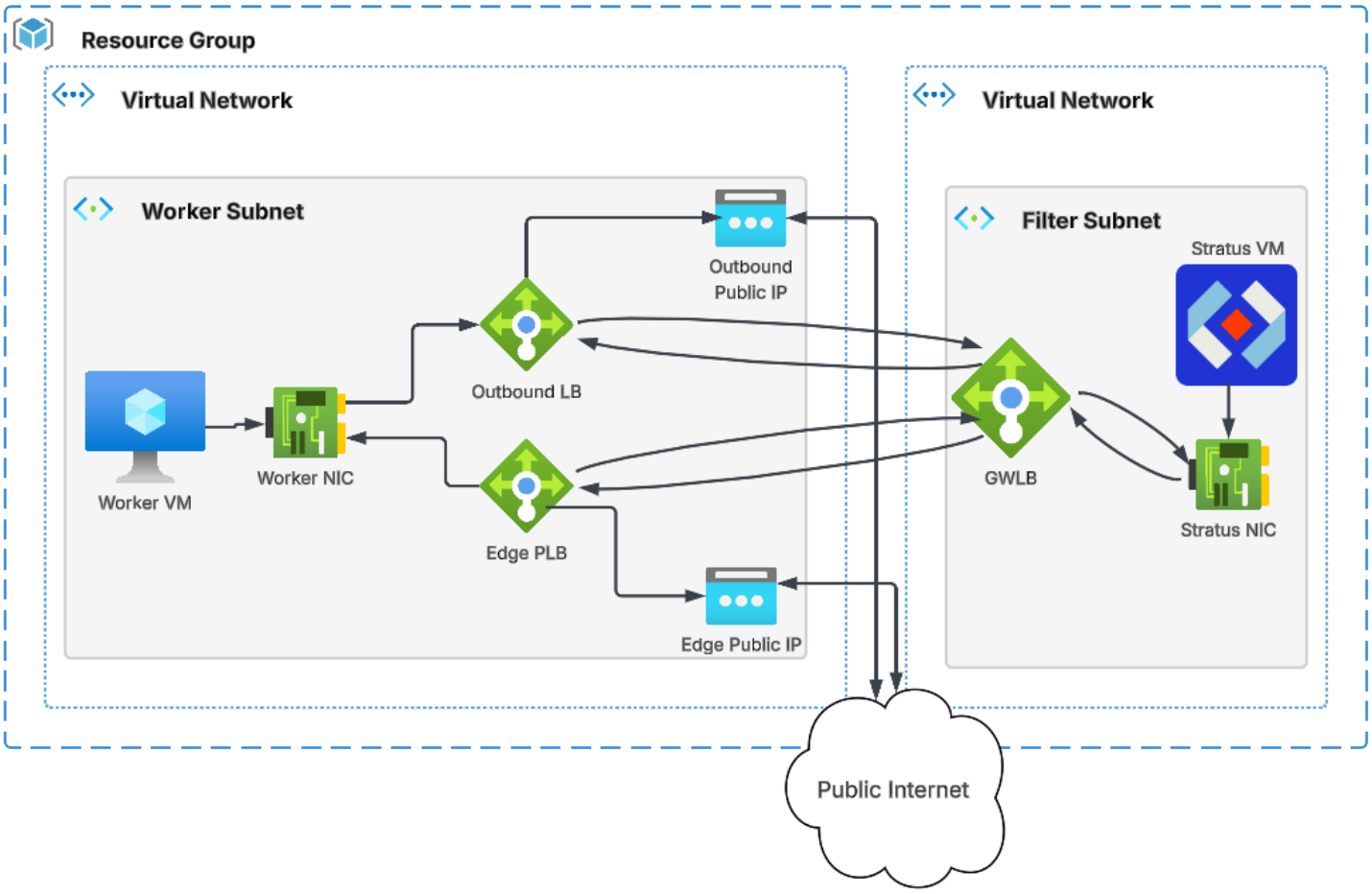
In the following example, this infrastructure is deployed in one VNet with multiple subnets.

- Worker subnet – where customer workloads are hosted (i.e. VM instances, Azure Functions, etc.)
- Security subnet – routing subnet that houses the GWLB endpoint
- Filter subnet – houses the Shield Stratus instance.



In the next example, the Gateway Load Balancer is deployed in a separate VNet. This allows one GWLB and Shield Stratus group to filter traffic for multiple VNets that are peered.

Note that this may incur costs for VNet peering bandwidth.



Installation of Intrusion Shield Stratus for Azure

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

1. Subscribe to **Intrusion Shield Stratus (ARM Templates)** from the Azure Marketplace. There are no charges for these templates directly.
2. Select a deployment plan from one of the template options. These are covered later in this document.
3. The Azure Marketplace will prompt you to subscribe to the **Intrusion Shield Stratus (VM Only)** offer. Use of this image will be charged per hour.
4. Complete the ARM Template to deploy Shield Stratus to an Azure Resource Group.
5. You will receive a welcome email to the email specified with a link to sign up to the Intrusion Command Hub.
6. Register your account with Intrusion Command Hub, thereby registering the Shield Stratus instance.
7. Use Command Hub to activate and configure the Shield Stratus instance.

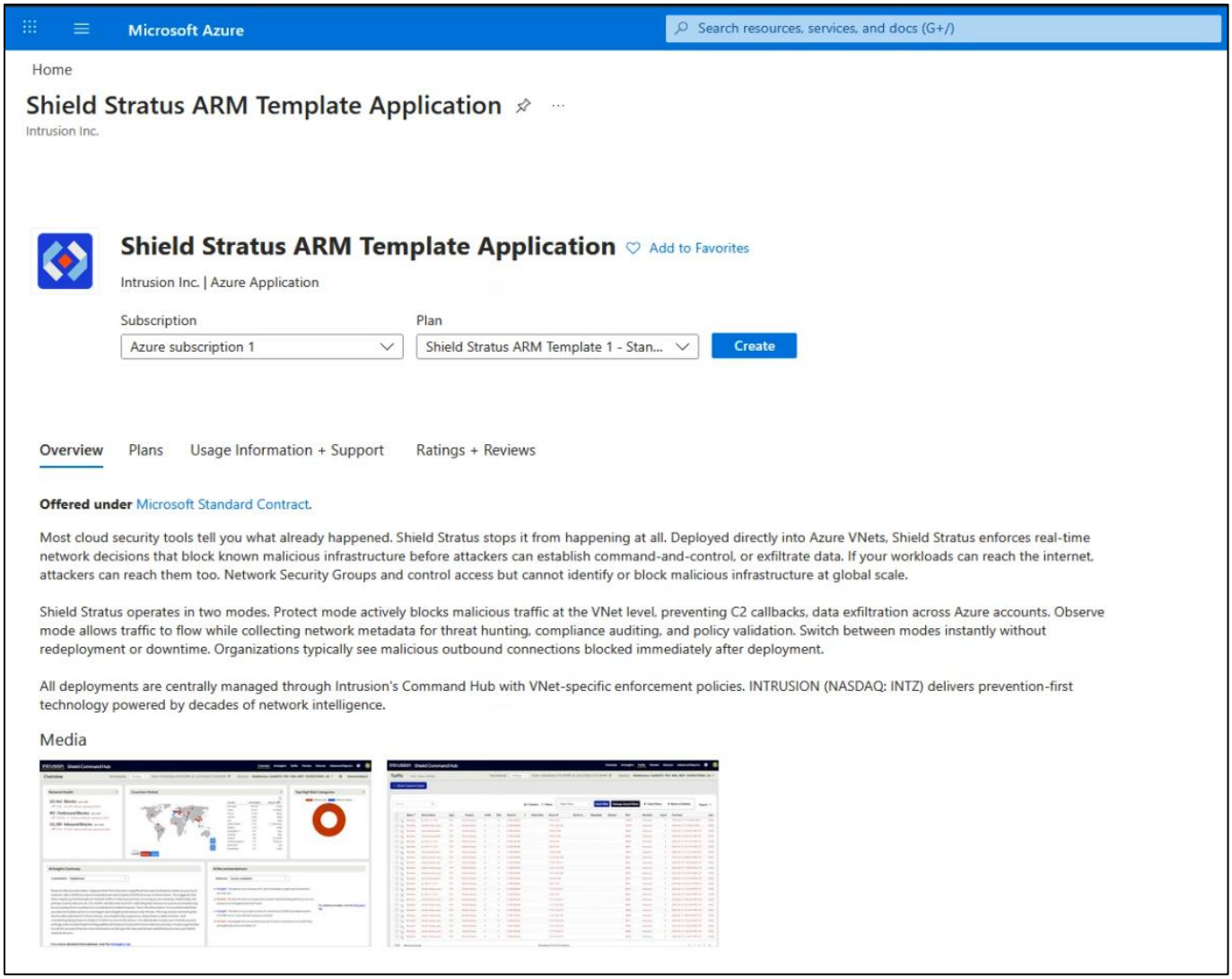
Requirements/Prerequisites

Verify you have the following before proceeding:

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

Purchasing a Shield Stratus Subscription

Shield Stratus can be purchased through the Azure Marketplace
https://portal.azure.com/#create/intrusioninc1769014305150.shield_stratus_arm_application-previewstratus_arm_template1a



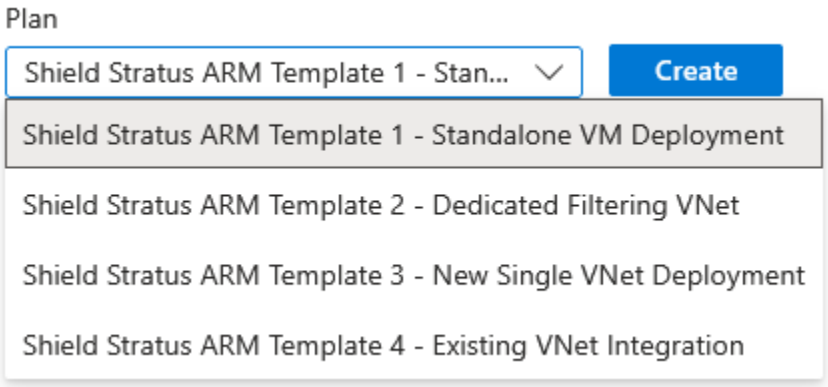
Deploying Shield Stratus via ARM Template

Azure Resource Manager (ARM) templates provide an easy way to deploy Shield Stratus by handling some of the prerequisites such as VNet creation, subnet creation, and load balancer creation.

Intrusion provides multiple Azure ARM templates to aid in deploying Shield Stratus in different scenarios depending on your architecture and use case.

Within the Azure marketplace page, there are four ARM template plans from which one can choose. Select one of the options corresponding to the type of environment you want to set up. See the following sections for descriptions and examples of each option.

It is recommended to start with **Stratus ARM Template 3** for a greenfield deployment.



Then click **Create**.

Shield Stratus ARM Template 1 - Standalone VM Deployment

This deployment option installs **only the Shield Stratus filtering virtual machine** into an existing Azure network environment. It is intended for advanced users who want full control over the surrounding infrastructure.

The template deploys:

- A **Shield Stratus VM**
- A network interface attached to a user-specified subnet
- Optional public IP
- Required security groups and VM configuration
- Key Vault resources for configuration secrets

This template **does not deploy any load balancers, Gateway Load Balancers, VNets, or routing infrastructure.**

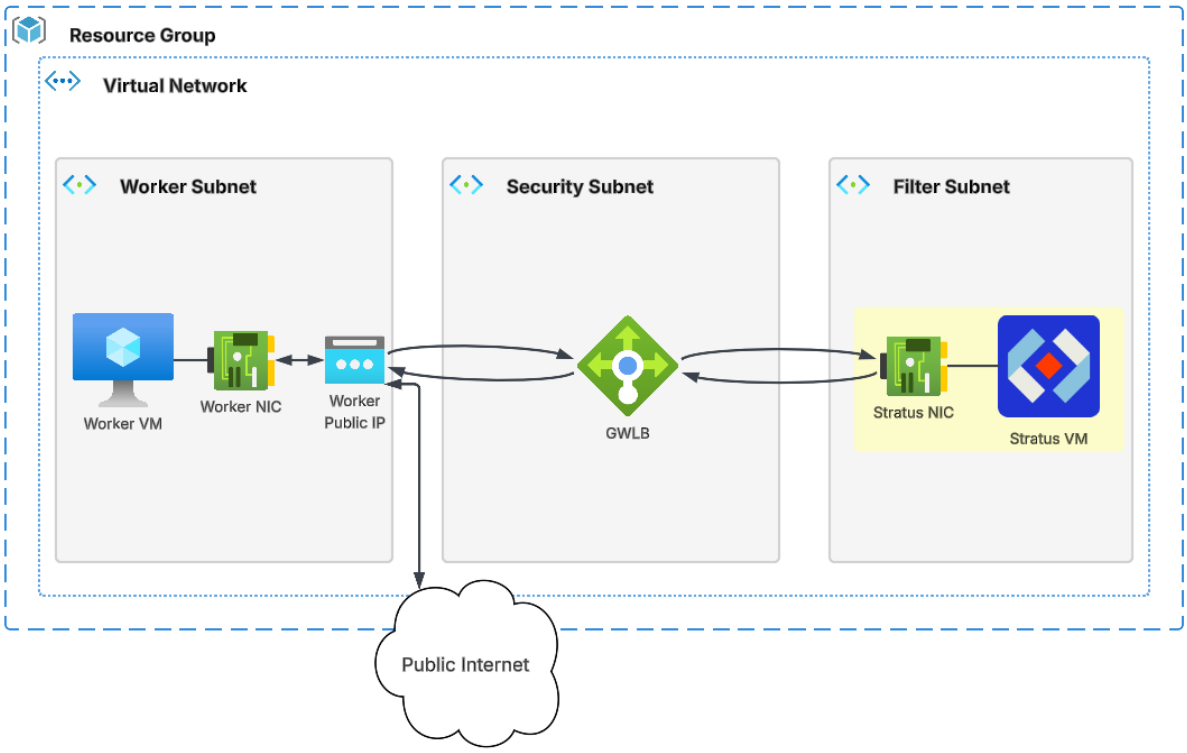
After deployment, the customer must configure the surrounding architecture manually, such as:

- Azure Gateway Load Balancer
- service chaining
- routing and security policies
- public endpoints or NAT

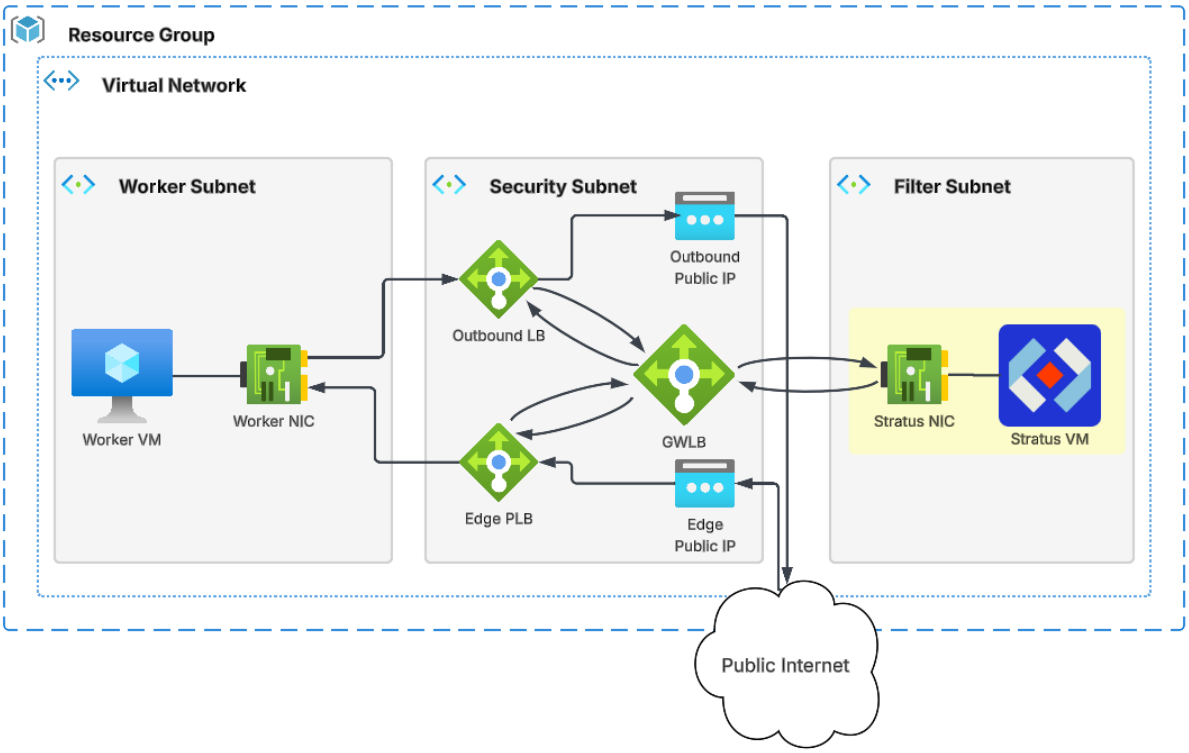
This deployment is best suited for custom architectures or advanced integrations where infrastructure is already in place.

The following is an illustration of the architecture of the ARM Template 1 deployment. This template will only deploy the Stratus VM and NIC, as highlighted in yellow. All other resources, such as the filter subnet and GWLB are left to the user to deploy separately.

Template 1 example reference public worker deployment.



Template 1 example reference private worker deployment.



The following table lists the fields for ARM Template 1.

Template Variable	Label	Description
Shield Stratus VM Name	Name of the Intrusion Shield Stratus VM.	Shield Stratus VM Name
Shield Stratus VM Size	Choose the VM size for the Stratus VM.	Shield Stratus VM Size
adminUsername	Admin username	Linux admin username to be created on the VM.
sshPublicKey	SSH public key (optional)	Optional SSH public key to place in authorized_keys for the admin user (recommended). Leave blank only if your image supports another access path.
subnetResourceId	Existing subnet resource ID	Resource ID of an EXISTING subnet where the VM NIC will be attached (e.g., /subscriptions/<sub>/resourceGroups/<rg>/providers/Microsoft.Network/ virtualNetworks/<vnet>/subnets/<subnet>).
sensorPrivateIP	Sensor private IP (optional static)	Optional static private IP within the selected subnet. Leave blank to use Dynamic allocation.
createPublicIP	Create a Public IP for the VM NIC	If enabled, the VM NIC gets a Public IP. If disabled, the VM is private-only.
TechContact	Customer email to receive activation link (or existing customer API key)	Customer email to receive activation link (or existing customer API key)
DisplayName	Command Hub display name (optional)	Optional display name for the Shield Stratus instance in Intrusion Command Hub. Leave blank to use the default.
keyVaultName	Key Vault name (optional override)	Leave blank to use <vmName>-kv. If you set this, it must be globally unique and follow Key Vault naming rules.
existingConfigSecretUri	Existing config secret URI (optional)	Optional: existing Key Vault Secret URI for Shield Stratus config. If set the template will not create the config secret.
enableKeyVaultPurgeProtection	Enable Key Vault purge protection	If enabled, purge protection is turned on for the Key Vault.
healthPort	Health port (TCP)	TCP health probe port exposed by the service.
enableEncryptionAtHost	Enable Encryption at Host	If enabled, turns on Encryption at Host for the VM (end-to-end encryption including temp/resource disk).

Shield Stratus ARM Template 2 - Dedicated Filtering VNet

This deployment creates a **dedicated inspection VNET** that hosts Shield Stratus together with an Azure Gateway Load Balancer (GWLB). The resulting environment acts as a **shared traffic inspection hub** that other VNets or load balancers can chain through.

The template automatically deploys:

- A new Virtual Network
- Inspection subnet
- Security/GWLB subnet
- filtering **Shield Stratus VM**
- Azure Gateway Load Balancer
- required network security configuration
- Key Vault resources
- optional NAT gateway
- optional flow logs

The template **does not deploy any application workloads or protected services.**

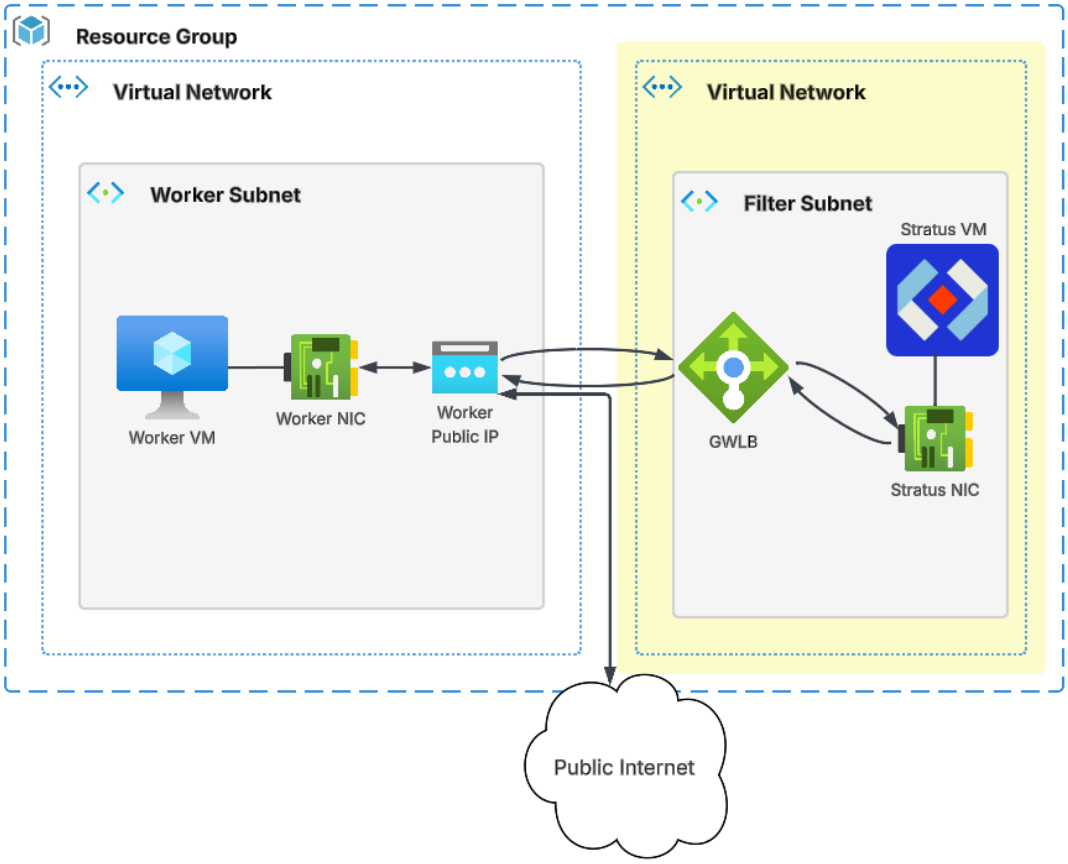
After deployment, customers can connect workloads by:

- chaining Standard Load Balancers to the GWLB
- connecting additional VNets using service chaining

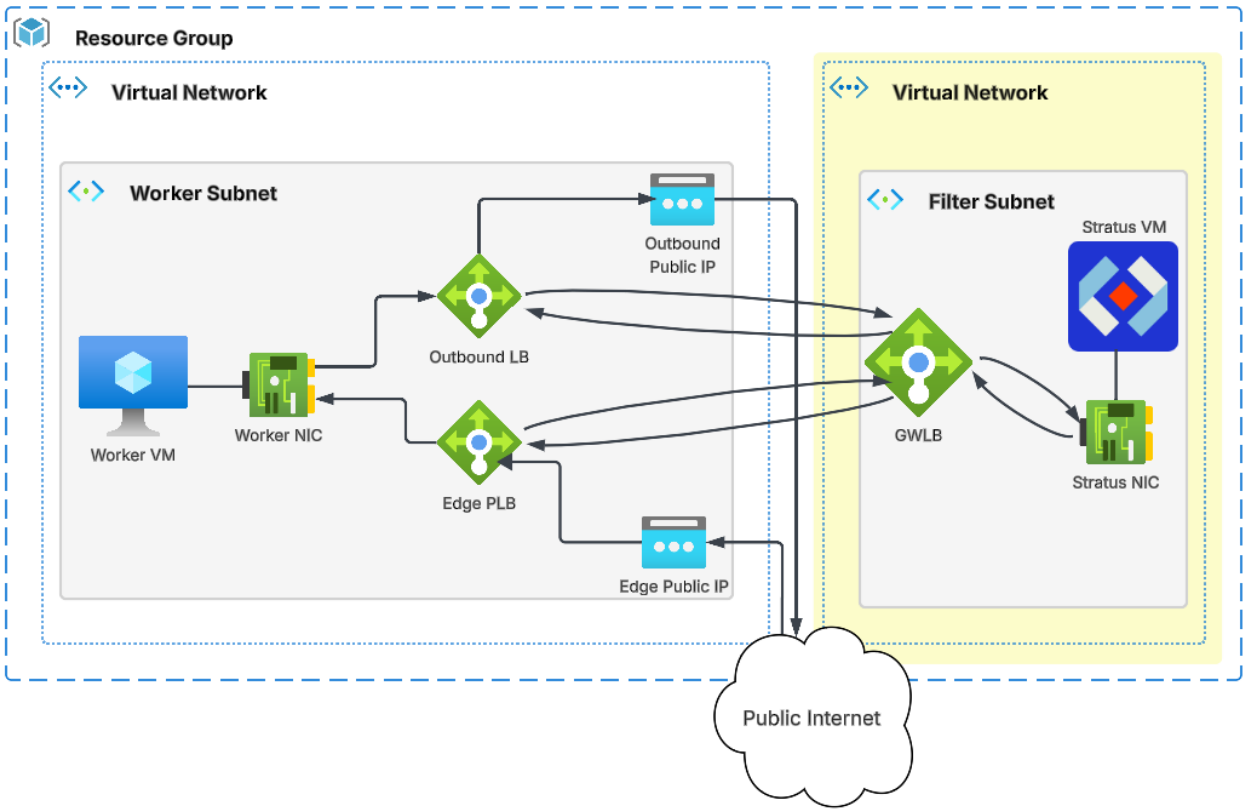
This architecture works well for **centralized security inspection across multiple VNets or applications.**

The following is an illustration of the architecture of the ARM Template 2 deployment. This template will deploy the entire filtering VNet containing the GWLB and Shield Stratus VM, as highlighted in yellow. All other resources, such as the worker network to protect, are left to the user to deploy separately.

Template 2 example reference public worker deployment.



Template 2 example reference private worker deployment.



The following table lists the fields for ARM Template 2.

Template Variable	Label	Description
vmName	Shield Stratus VM Name	Name of the Intrusion Shield Stratus VM.
vmSize	Shield Stratus VM Size	Choose the VM size for the Stratus VM.
adminUsername	Admin username	Linux admin username to be created on the VM.
sshPublicKey	SSH public key	SSH public key to place in authorized_keys for the admin user.
vnetName	Virtual network name	Name for the new VNet (parity with VpcName).
vnetCidr	VNet address space (CIDR)	CIDR for the VNet. Example: 10.20.0.0/16
subnetName	Subnet name	Subnet name.
subnetCidr	Subnet CIDR	CIDR for the subnet. Example: 10.20.1.0/24
sensorPrivateIP	Sensor private IP (optional static)	Optional static private IP inside the subnet CIDR. Leave blank to use Dynamic allocation.
useNatGateway	Use NAT Gateway for sensor outbound internet	If enabled: the sensor NIC will NOT get a Public IP. A NAT Gateway (with a static Public IP) will be attached to the subnet for outbound internet.
TechContact	Customer email to receive activation link (or existing customer API key)	Customer email to receive activation link (or existing customer API key)
DisplayName	Command Hub display name (optional)	Optional display name for the Shield Stratus instance in Intrusion Command Hub. Leave blank to use the default.
enableEncryptionAtHost	Enable Encryption at Host	If enabled, turns on Encryption at Host for the sensor VM (end-to-end encryption including temp/resource disk).
enableKeyVaultPurgeProtection	Enable Key Vault purge protection	If enabled, the Key Vault will have purge protection enabled.
existingConfigSecretUri	Existing config secret URI (optional)	Optional: existing Key Vault Secret URI for Shield Stratus config. If set the template will not create the config secret.
enableVnetFlowLogs	Enable VNet flow logs	If enabled, the deployment will configure VNet Flow Logs.
vnetFlowLogsRetentionDays	Flow logs retention (days)	Retention in days (1–365).
vnetFlowLogsStorageAccountName	Existing Storage Account name (optional)	Optional: existing storage account name for flow logs. Leave blank to auto-create one.
existingNetworkWatcherId	Existing Network Watcher resource ID (optional)	Optional: full resourceId of an existing Network Watcher. Leave blank to auto-create one (if supported for your scenario).
healthPort	Health port (TCP)	TCP health probe port (1–65535).
vxlanPortInternal	VXLAN port (internal, UDP)	UDP port for the internal tunnel interface (1–65535).
vxlanVniInternal	VXLAN VNI (internal)	VNI for the internal tunnel interface.
vxlanPortExternal	VXLAN port (external, UDP)	UDP port for the external tunnel interface (1–65535).
vxlanVniExternal	VXLAN VNI (external)	VNI for the external tunnel interface.
adminUsername	Admin username	Linux admin username to be created on the VM.

Shield Stratus ARM Template 3 - New Single VNet Deployment

This option deploys a **complete secure virtual network environment** with built-in traffic inspection. It is designed for new environments where customers want a **ready-to-use secure architecture**.

The template automatically deploys:

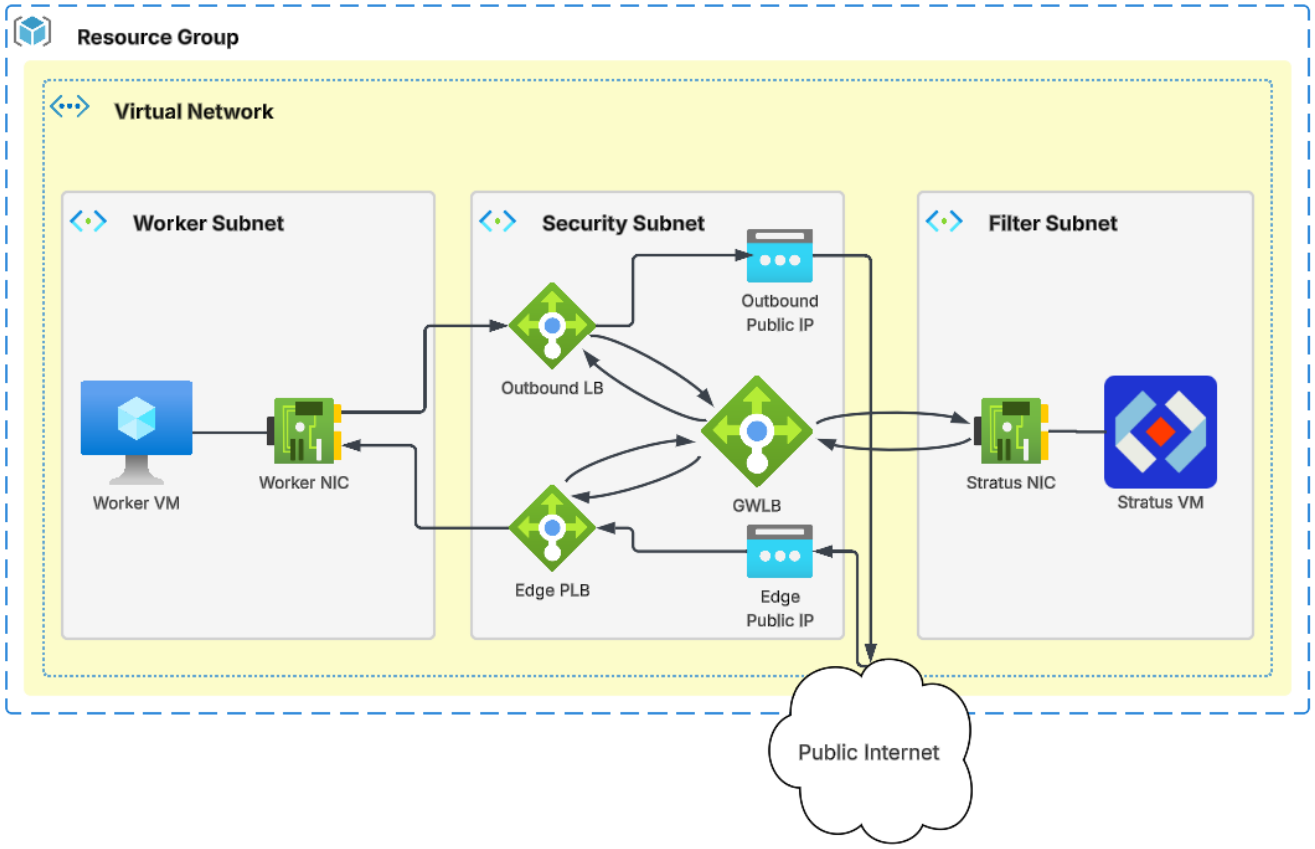
- A new Virtual Network
- Inspection subnet
- Security subnet
- Worker/application subnet
- filtering **Shield Stratus VM**
- Gateway Load Balancer
- Internal Standard Load Balancer
- optional example worker VMs

Traffic entering the internal load balancer is automatically routed through the Gateway Load Balancer and inspected by Shield Stratus before reaching application workloads.

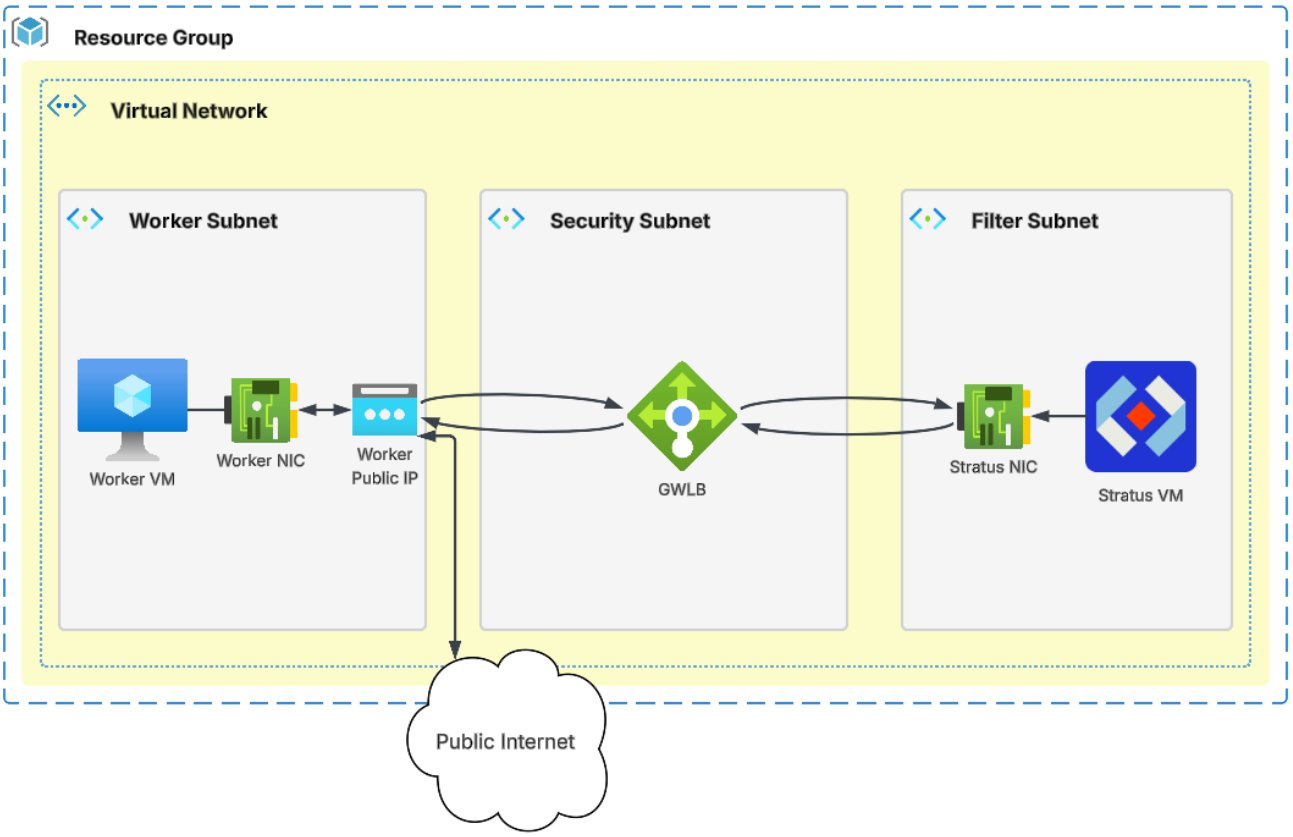
This template is ideal for **fresh deployments or proof-of-concept environments.**

The following is an illustration of the architecture of the ARM Template 3 deployment. This template will deploy an entire functioning test network as highlighted in yellow.

Template 3 example reference public worker deployment.



Template 3 example reference private worker deployment.



The following table lists the fields for ARM Template 3.

Template Variable	Label	Description
vmName	Shield Stratus VM Name	Name of the Intrusion Shield Stratus VM.
vmSize	Shield Stratus VM Size	Choose the VM size for the Stratus VM.
adminUsername	Admin username	Linux admin username to be created on the VMs.
sshPublicKey	SSH public key	SSH public key to place in authorized_keys for the admin user (recommended).
vnetName	Virtual network name	Name of the virtual network to create.
vnetCidr	VNet address space (CIDR)	Example: 10.30.0.0/16
filterSubnetName	Filter subnet name	Name of the filter subnet (2–64 chars; letters/numbers and - _ .).
filterSubnetCidr	Filter subnet CIDR	CIDR for this subnet (example: 10.30.1.0/24).
securitySubnetName	Security subnet name	Name of the security subnet (2–64 chars; letters/numbers and - _ .).
securitySubnetCidr	Security subnet CIDR	CIDR for this subnet (example: 10.30.2.0/24).
workerSubnetName	Worker subnet name	Name of the worker subnet (2–64 chars; letters/numbers and - _ .).
workerSubnetCidr	Worker subnet CIDR	CIDR for this subnet (example: 10.30.3.0/24).
sensorPrivateIP	Sensor private IP (static)	Must be within the Filter subnet CIDR and unused.
useNatGateway	Use NAT Gateway for sensor outbound internet	If enabled: the sensor NIC will NOT get a Public IP. A NAT Gateway (with a static Public IP) will be attached to the filter subnet for outbound internet.
deployPrivateWorker	Deploy private worker VM	Deploy the private worker VM and NIC (used for traffic generation / egress).
privateWorkerVmSize	Private worker VM size	Choose the VM size for the private worker VM.
deployPublicWorker	Deploy public worker VM	Deploy the public worker VM + NIC + public IP + NSG.
publicWorkerVmSize	Public worker VM size	Choose the VM size for the public worker VM.
allowedAdminCidr	Allowed admin CIDR for PublicWorker SSH (22/tcp)	Restrict SSH access to a trusted IP range in production (example: your office/home public IP /32).
TechContact	Customer email to receive activation link (or existing customer API key)	Customer email to receive activation link (or existing customer API key)
DisplayName	Command Hub display name (optional)	Optional display name for the Shield Stratus instance in Intrusion Command Hub. Leave blank to use the default.
healthPort	Health port (TCP)	Port used for health checks (1–65535).
vxlanPortInternal	VXLAN port (internal, UDP)	UDP port used for internal VXLAN encapsulation (1–65535).
vxlanVniInternal	VXLAN VNI (internal)	Internal VXLAN VNI (numeric).
vxlanPortExternal	VXLAN port (external, UDP)	UDP port used for external VXLAN encapsulation (1–65535).
vxlanVniExternal	VXLAN VNI (external)	External VXLAN VNI (numeric).
enableEncryptionAtHost	Enable Encryption at Host (sensor VM)	Enables Encryption at Host on the sensor VM (end-to-end encryption including temp/resource disk).
enableKeyVaultPurgeProtection	Enable Key Vault purge protection	Recommended for production. Helps prevent permanent deletion of Key Vault.
keyVaultName	Key Vault name (optional)	Leave blank to auto-generate from VNet name (vnetName-kv).
existingConfigSecretUri	Existing config secret URI (optional)	Optional: existing Key Vault Secret URI for Shield Stratus config. If set the template will not create the config secret.
enableVnetFlowLogs	Enable VNet Flow Logs	If enabled, VNet Flow Logs will be configured to write to a Storage Account.
vnetFlowLogsRetentionDays	Flow logs retention (days)	Retention in days (1–365).

vnetFlowLogsStorageAccountName	Existing Storage Account name for flow logs (optional)	If blank, the template creates one. If provided, must be an existing Storage Account in this resource group.
existingNetworkWatcherId	Existing Network Watcher resource ID (optional)	Optional. Full resourceId of an existing Network Watcher (can be in another resource group). Leave blank to create one.

Shield Stratus ARM Template 4 - Existing VNet Integration

This deployment integrates Shield Stratus traffic inspection into an **existing Azure virtual network**.

The template deploys:

- Inspection subnet
- Security subnet
- filtering **Shield Stratus VM**
- Gateway Load Balancer
- Internal Standard Load Balancer
- optional edge and outbound load balancers

The template **does not modify or redeploy existing workloads.**

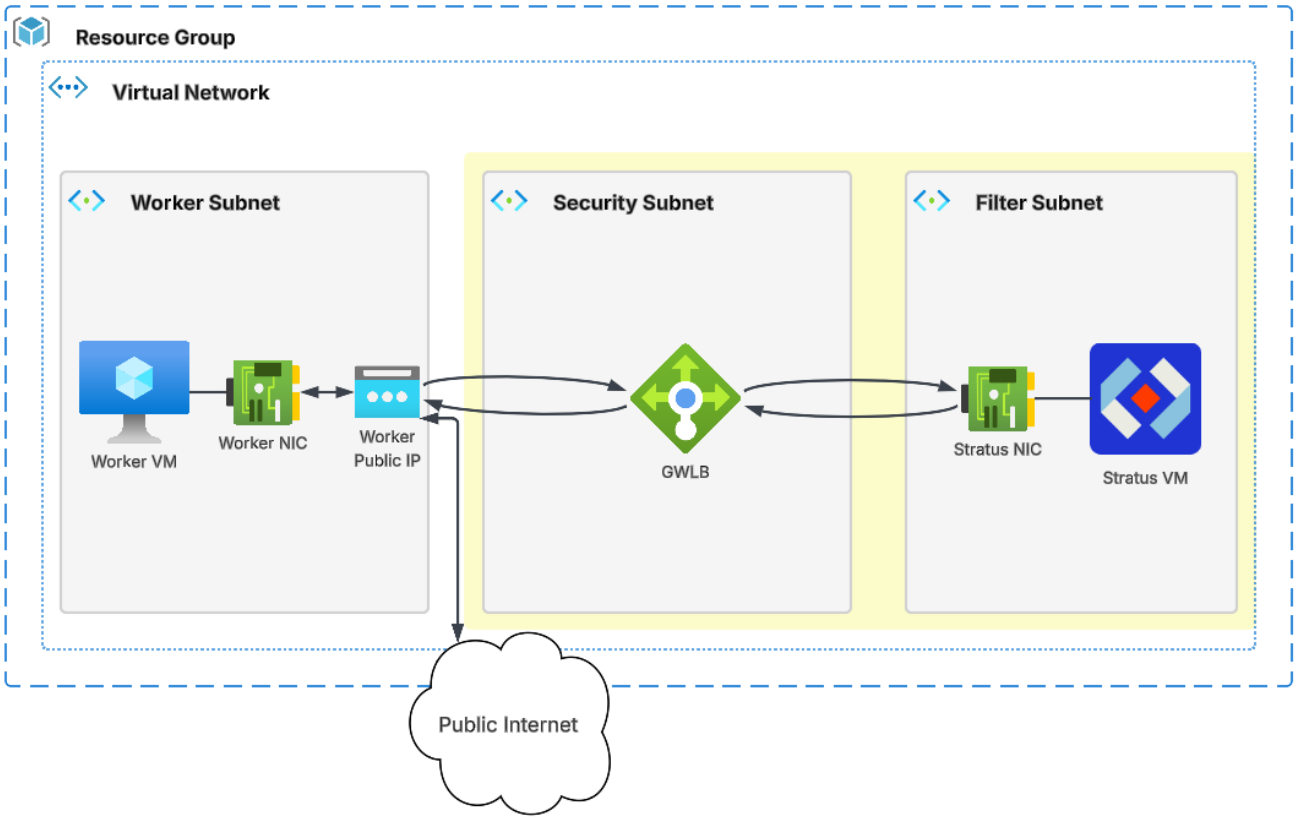
After deployment, customers can redirect traffic through Shield Stratus by:

- fronting workloads with the internal load balancer
- chaining existing load balancers to the GWLB
- routing inbound or outbound traffic through the filtering stack

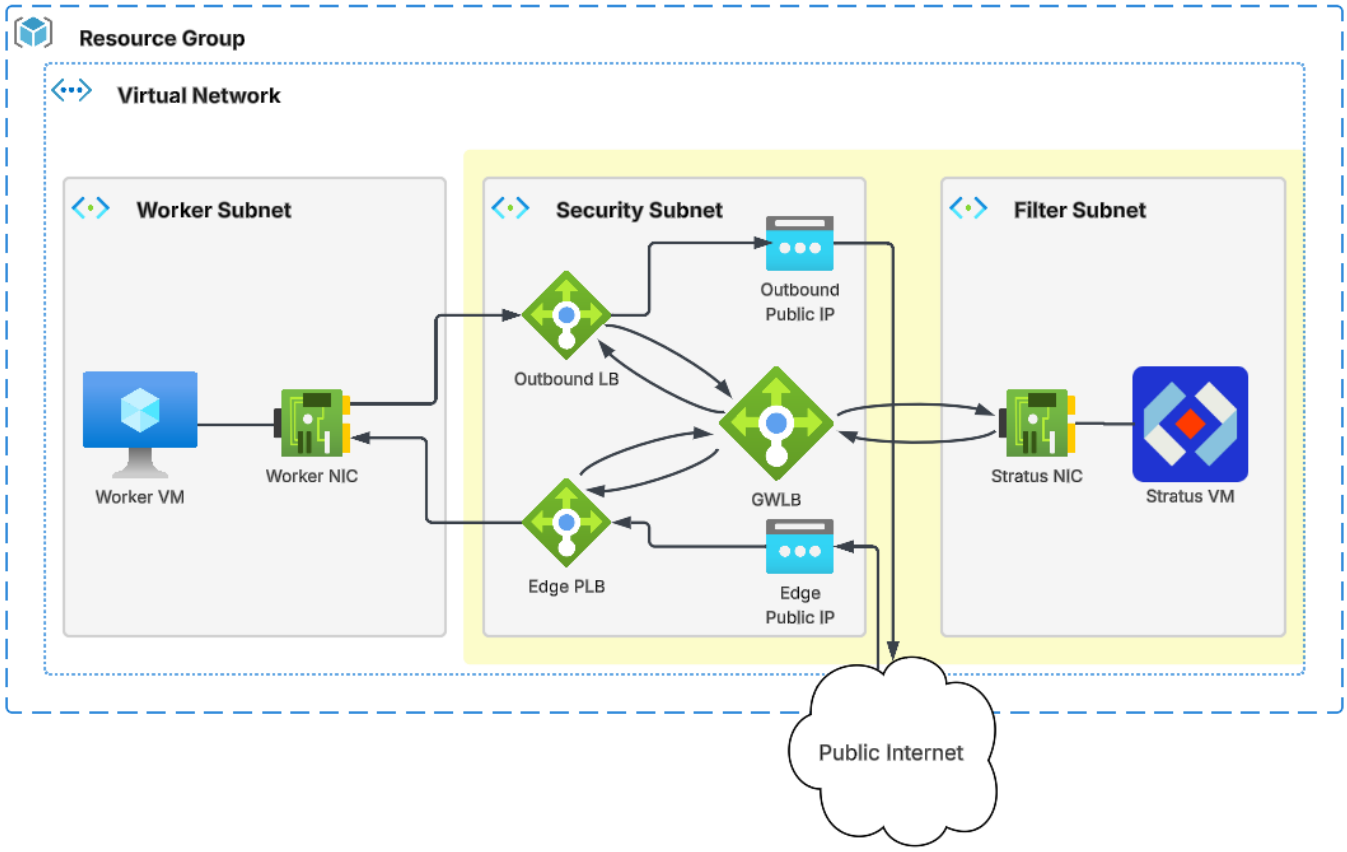
This option allows customers to **add inspection capability to an existing production network with minimal architectural changes.**

The following is an illustration of the architecture of the ARM Template 4 deployment. This template will deploy the security and filtering subnets within an existing VNet as highlighted in yellow. Deployment of the worker subnet and VMs is left to the user.

Template 4 example reference public worker deployment.



Template 4 example reference public worker deployment.



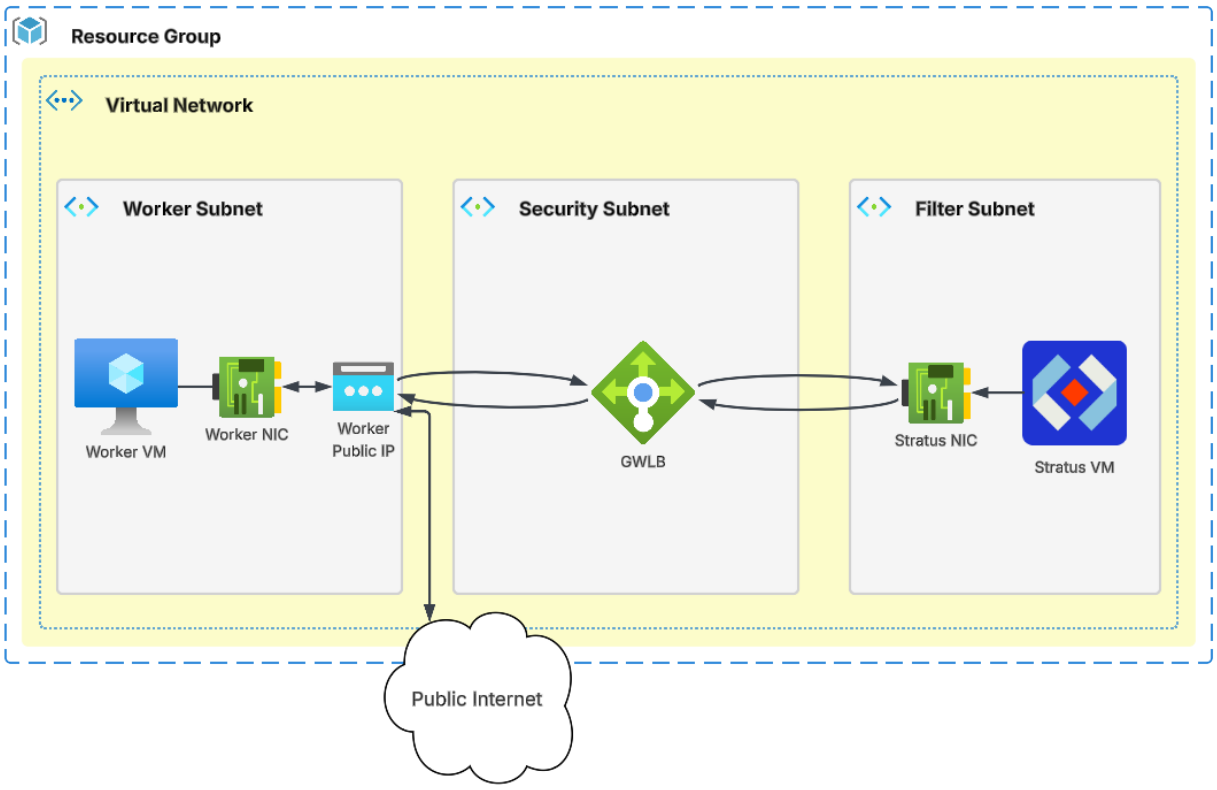
The following table lists the fields for ARM Template 4.

Template Variable	Label	Description
vmName	Shield Stratus VM Name	Name of the Intrusion Shield Stratus VM.
vmSize	Shield Stratus VM Size	Choose the VM size for the Stratus VM.
adminUsername	Admin username	Linux admin username to be created on the VM.
sshPublicKey	SSH public key	SSH public key to place in authorized_keys for the admin user (recommended).
vnetResourceId	Existing VNet resource ID	Resource ID of the EXISTING VNet. Example: /subscriptions/<sub>/resourceGroups/<rg>/providers/Microsoft.Network/virtualNetworks/<vnetName>
filterSubnetName	Filter subnet name	Subnet name for the sensor NIC.
filterSubnetCidr	Filter subnet CIDR	CIDR to assign to the filter subnet that will be created/updated in the existing VNet.
securitySubnetName	Security subnet name	Subnet name for the GWLB + security ILB frontend.
securitySubnetCidr	Security subnet CIDR	CIDR to assign to the security subnet that will be created/updated in the existing VNet.
sensorPrivateIP	Sensor private IP (optional static)	Optional static private IP inside the Filter subnet CIDR. Leave blank to use Dynamic allocation.
useNatGateway	Use NAT Gateway for sensor outbound internet	If enabled: the sensor NIC will NOT get a Public IP. A NAT Gateway (with a static Public IP) will be attached to the filter subnet for outbound internet.
createEdgePublicLB	Create Edge Public Load Balancer (SSH via GWLB)	If enabled, deploys an internet-facing Public Load Balancer fronted by a Public IP and chained to the Gateway Load Balancer.
createOutboundPublicLB	Create Outbound Public Load Balancer (worker egress)	If enabled, deploys a Public IP + Standard Load Balancer + outbound rule chained to the GWLB frontend. No NICs are attached by this template.
outboundAllocatedPorts	Allocated outbound SNAT ports per backend instance	Used by the outbound rule once backend NICs are attached later (8–64000).
outboundPipName	Outbound public IP name (optional)	Optional override for outbound Public IP resource name. Leave blank for default.
outboundLbName	Outbound load balancer name (optional)	Optional override for outbound Load Balancer resource name. Leave blank for default.
TechContact	Customer email to receive activation link (or existing customer API key)	Customer email to receive activation link (or existing customer API key)
DisplayName	Command Hub display name (optional)	Optional display name for the Shield Stratus instance in Intrusion Command Hub. Leave blank to use the default.
existingConfigSecretUri	Existing config secret URI (optional)	Optional: existing Key Vault Secret URI for Shield Stratus config. If set the template will not create the config secret.
enableKeyVaultPurgeProtection	Enable Key Vault purge protection	If enabled, purge protection is turned on for the Key Vault.
enableEncryptionAtHost	Enable Encryption at Host	If enabled, turns on Encryption at Host on the sensor VM.
healthPort	Health port (TCP)	TCP health probe port (1–65535).
vxlanPortInternal	VXLAN port (internal, UDP)	UDP port for the internal tunnel interface (1–65535).
vxlanVniInternal	VXLAN VNI (internal)	VNI for the internal tunnel interface.
vxlanPortExternal	VXLAN port (external, UDP)	UDP port for the external tunnel interface (1–65535).

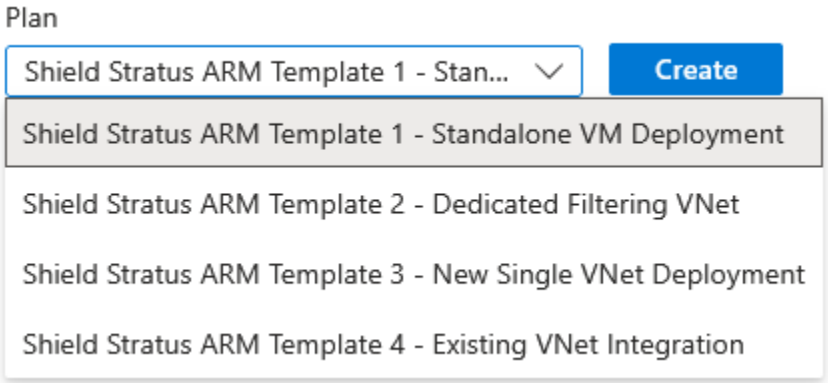
vxlanVniExternal	VXLAN VNI (external)	VNI for the external tunnel interface.

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

This example walks through the process of creating a new deployment of ARM Template #3, which create a fresh environment, starting with a new VNet. This includes a public worker VM with a public IP.

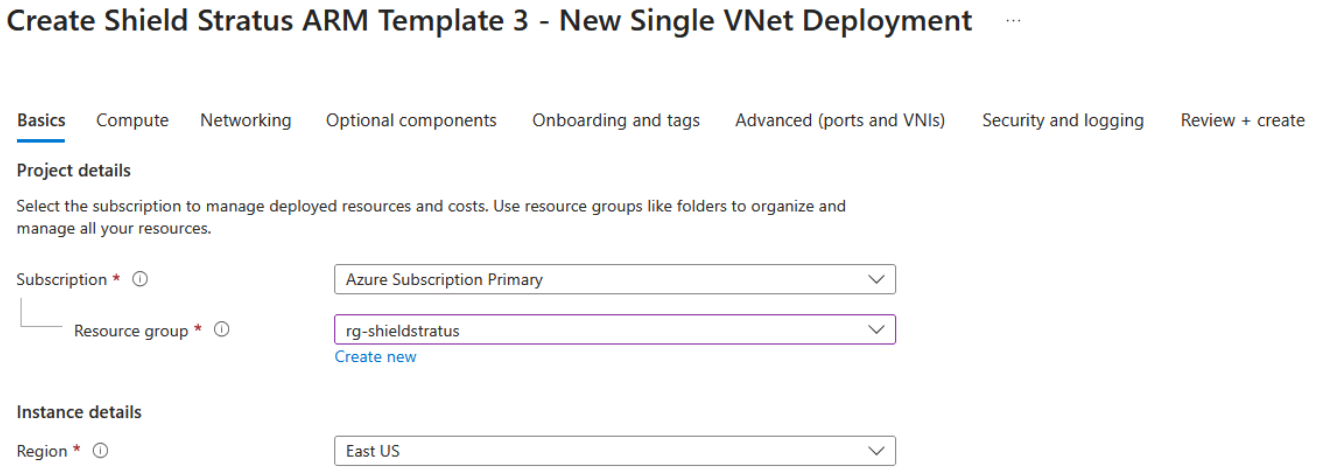


From the Azure Marketplace listing, select Shield Stratus **ARM Template 3– New Single VNet Deployment** and click **Create**.



The ARM template wizard will guide you through the process.

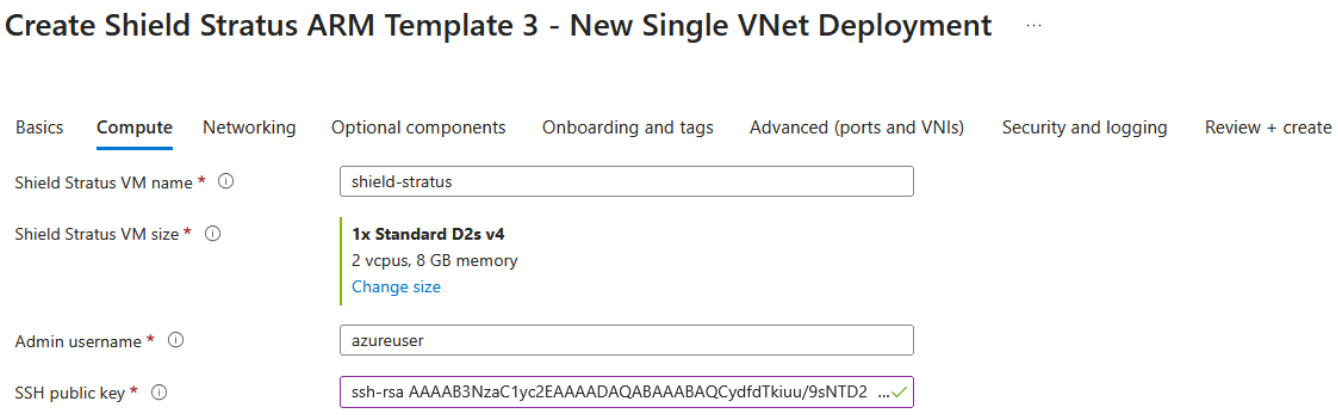
In the Basics section, select the Subscription, Resource group and region.



In the Compute section, give the stratus VM a name that it will be identified by in Azure.

You can change the default VM size of Shield Stratus.

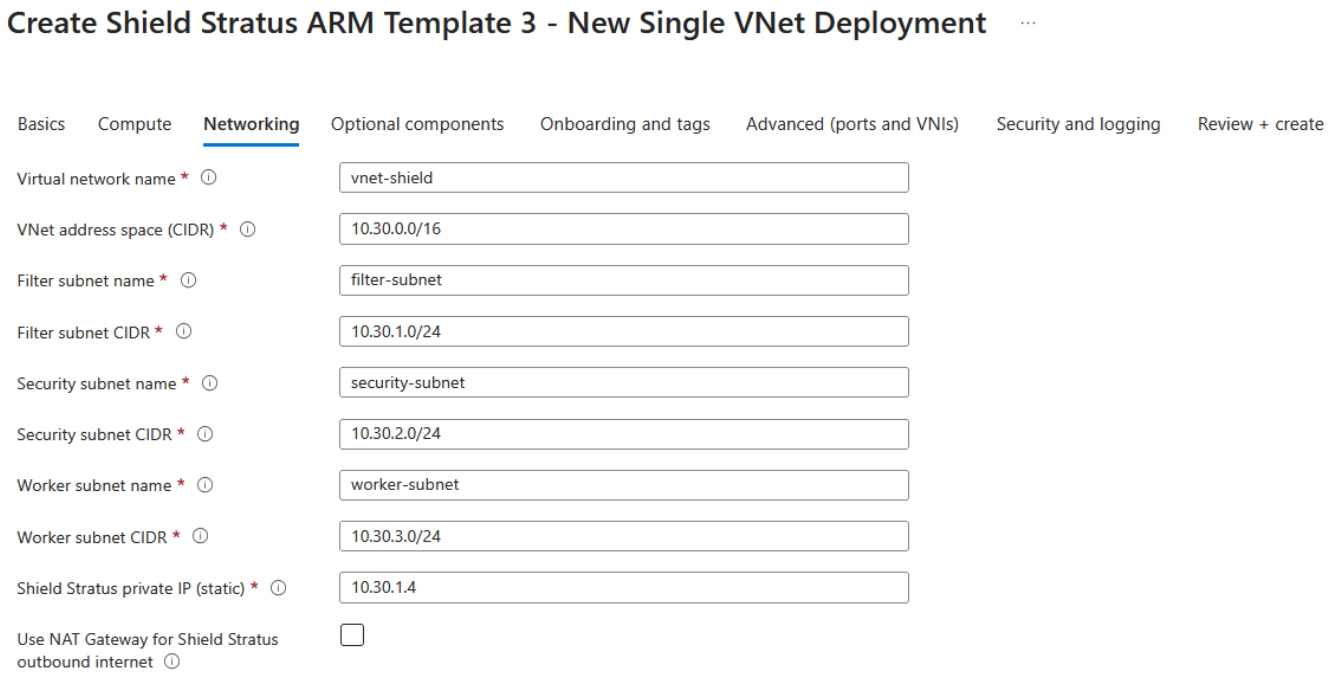
Additionally, you can paste an SSH public key that will be used for connectivity to the Worker VM.



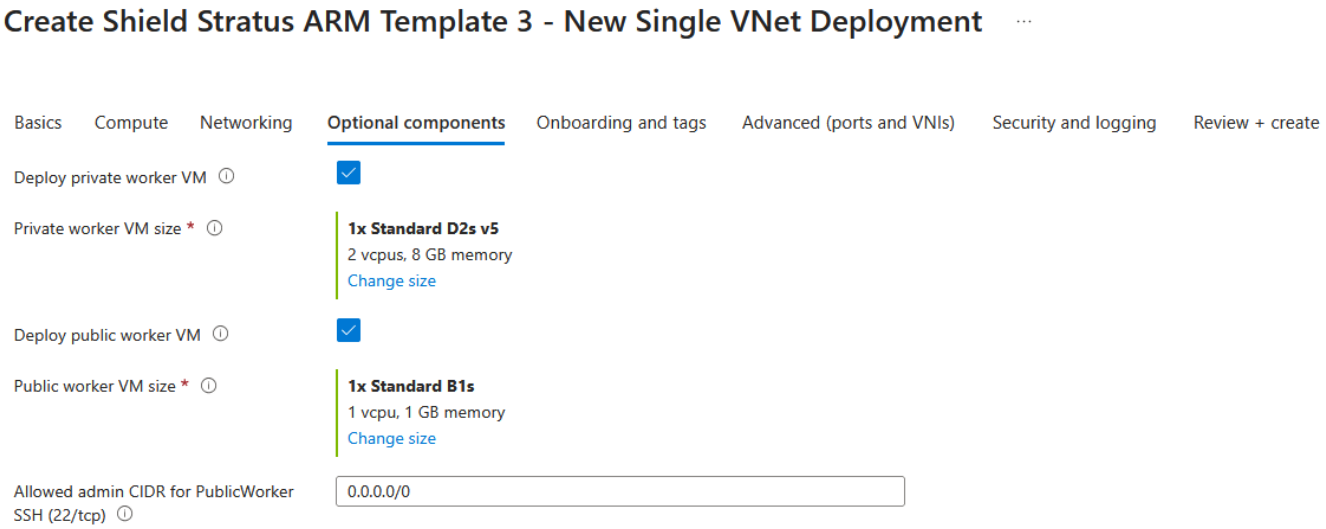
In the Networking section, specify the name of the virtual network to be created. This should not overlap any existing virtual network names.

You can specify the subnet names and CIDR addresses for the

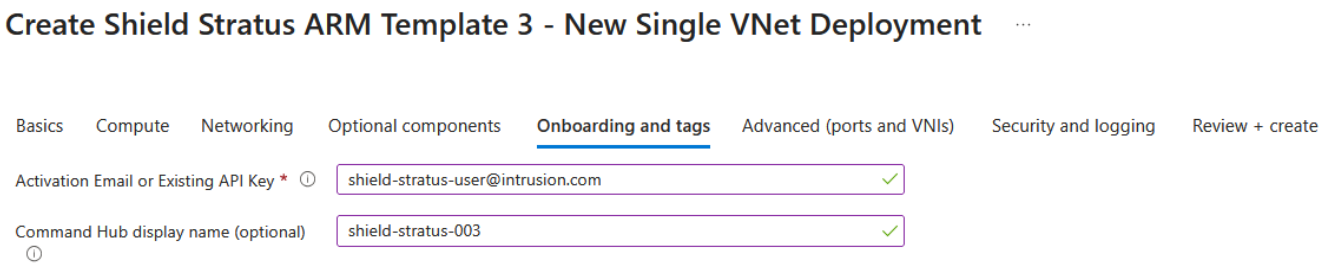
- Filter subnet – the subnet which houses the Shield Stratus VM
- Security subnet – the subnet which houses the GWLB for traffic inspection
- Worker subnet – a sample subnet that will contain a public or private example VM



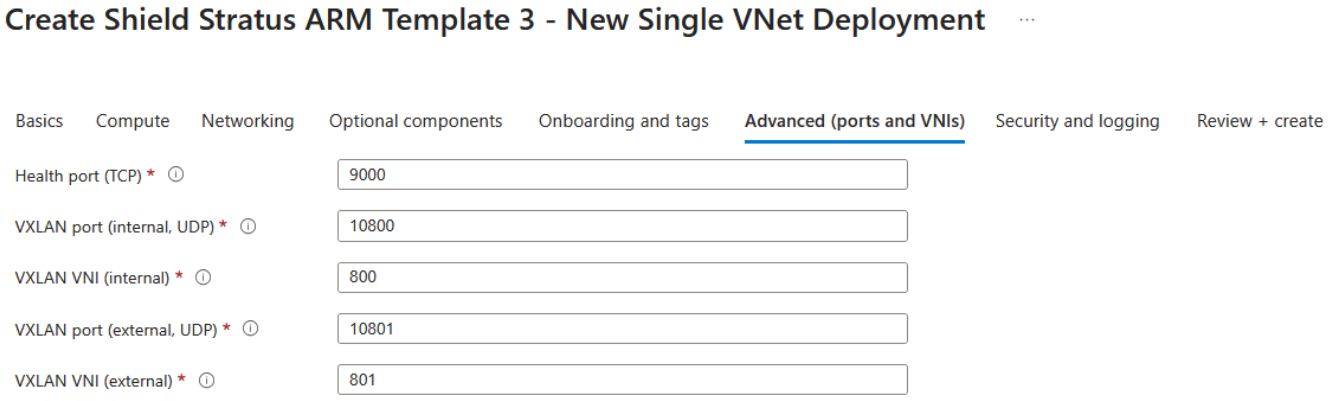
In the Optional Components, you can choose to deploy a public and/or private worker Ubuntu instance. These are not essential to Shield Stratus operation, but rather serve as examples for testing.



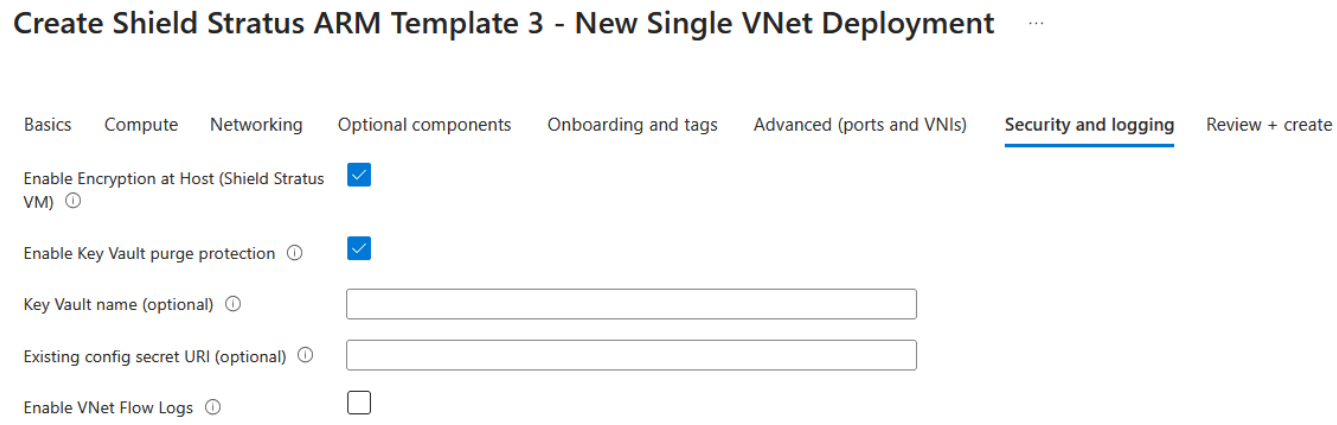
In the Onboard and Tags section, enter the email address to which you want to receive the activation email. Additionally enter the display name which you want this Stratus instance to appear as in Command Hub.



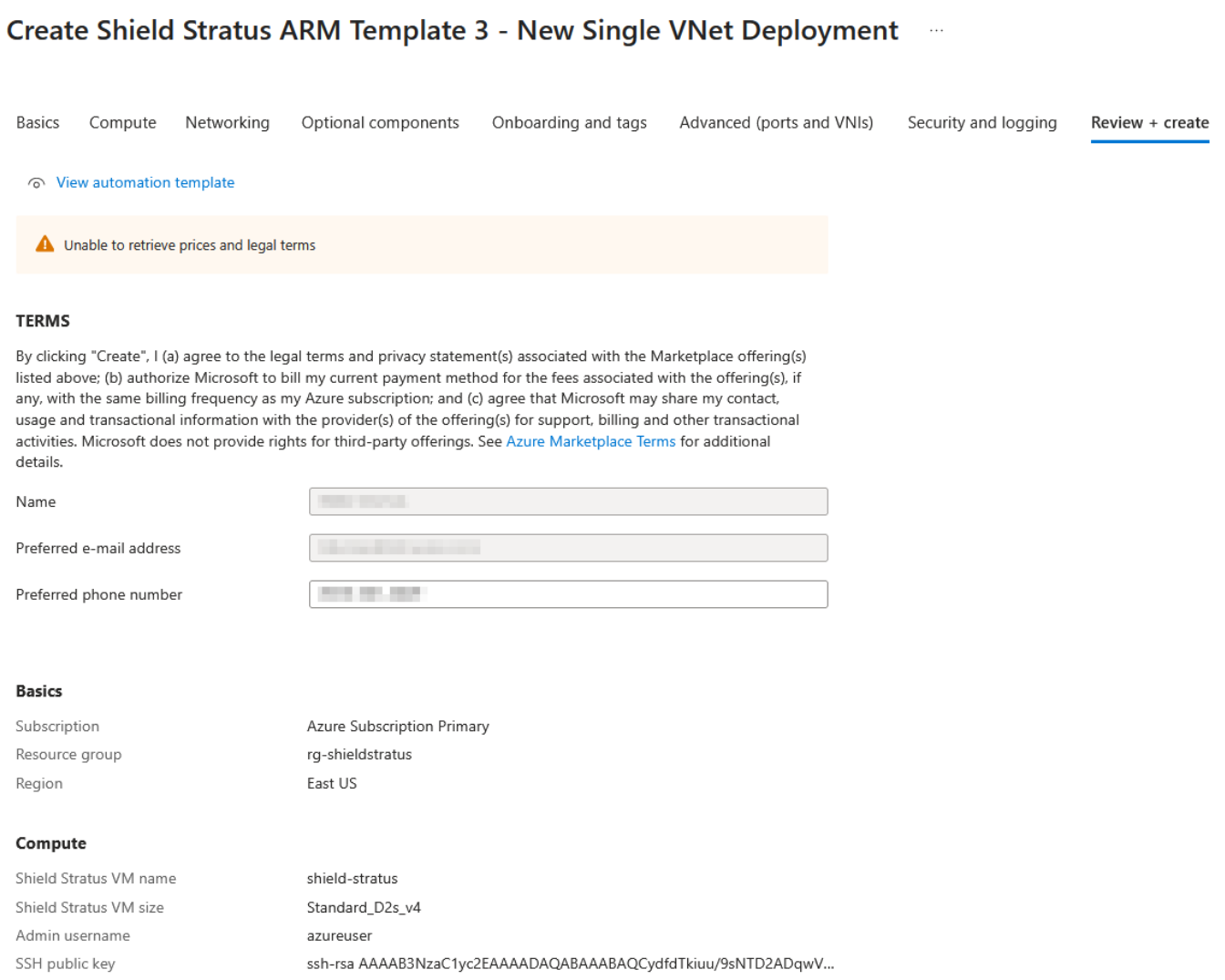
The Advanced (ports and VNIs) section can usually be left at the defaults. These are the ports used for communication between the GWLB and Shield Stratus instance.



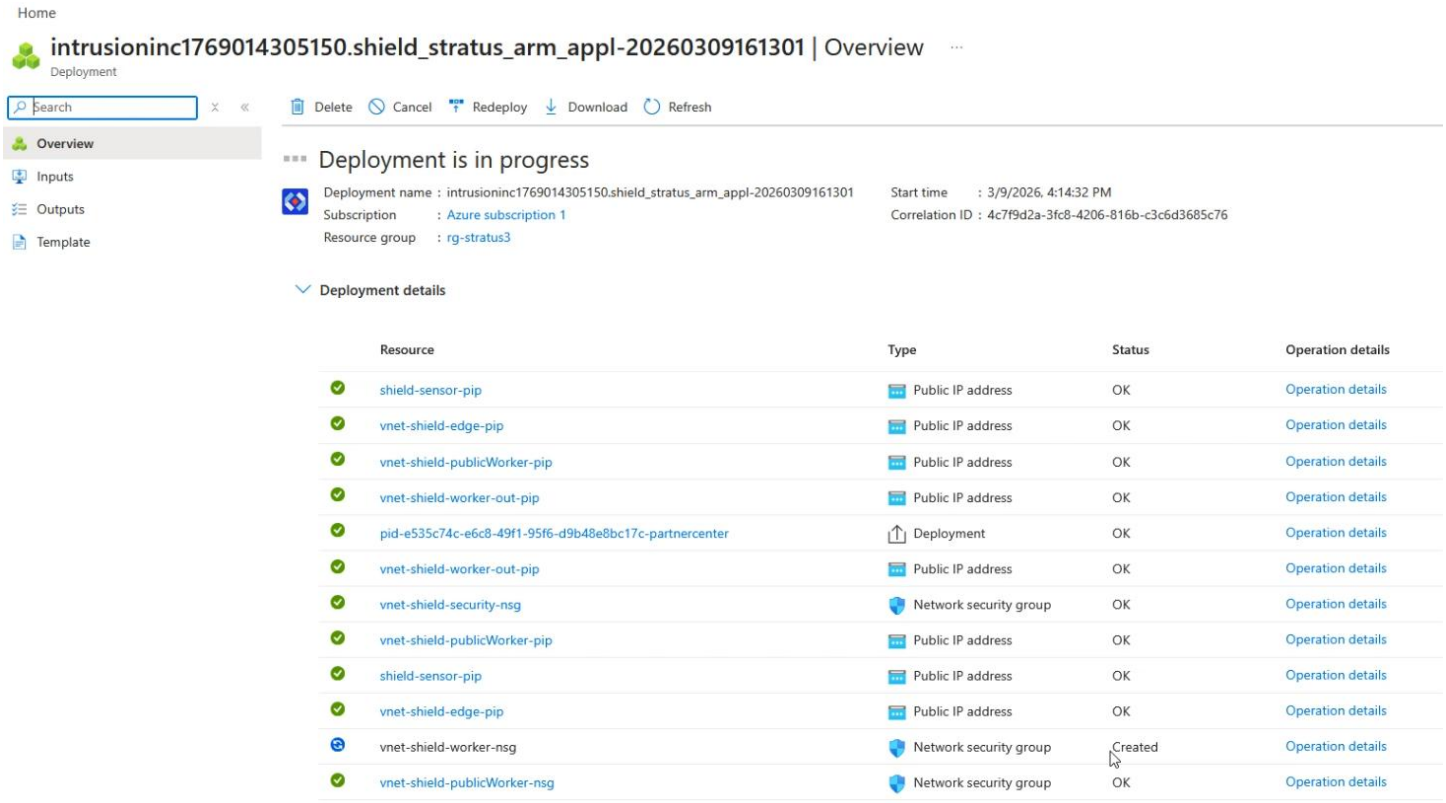
In the Security and logging section, you can define encryption settings for the VM. You can specify a key vault name which Stratus will use to store configuration settings.



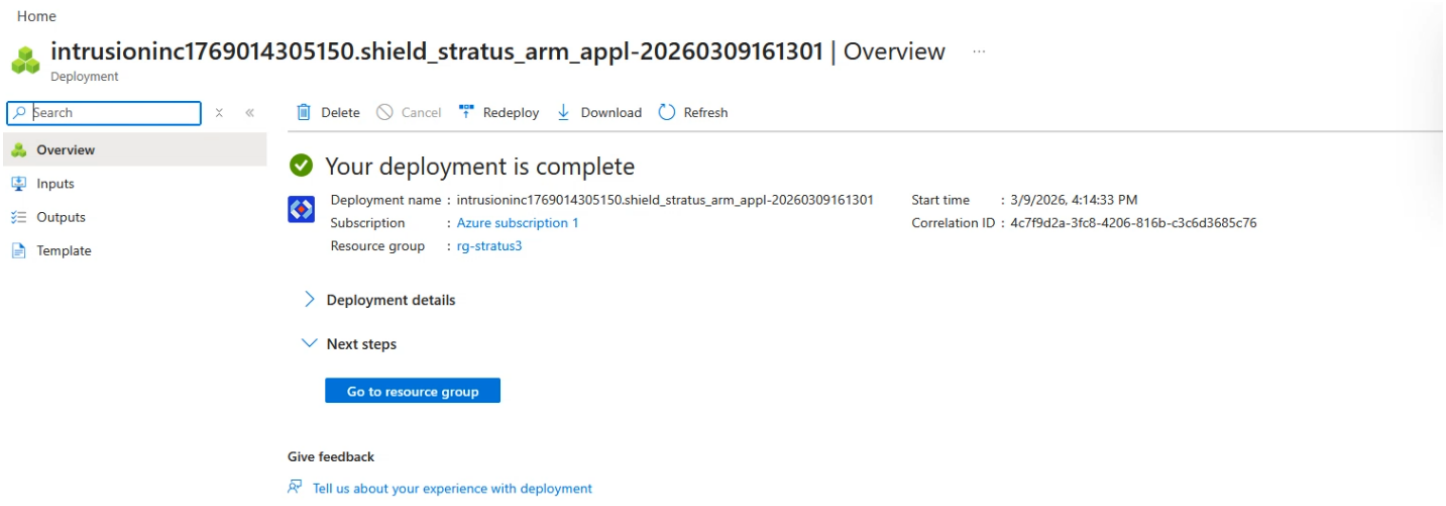
Finally, the Review and Create section previews the template configuration which will be deployed. This will warn of any pre-deployment errors that need resolving.



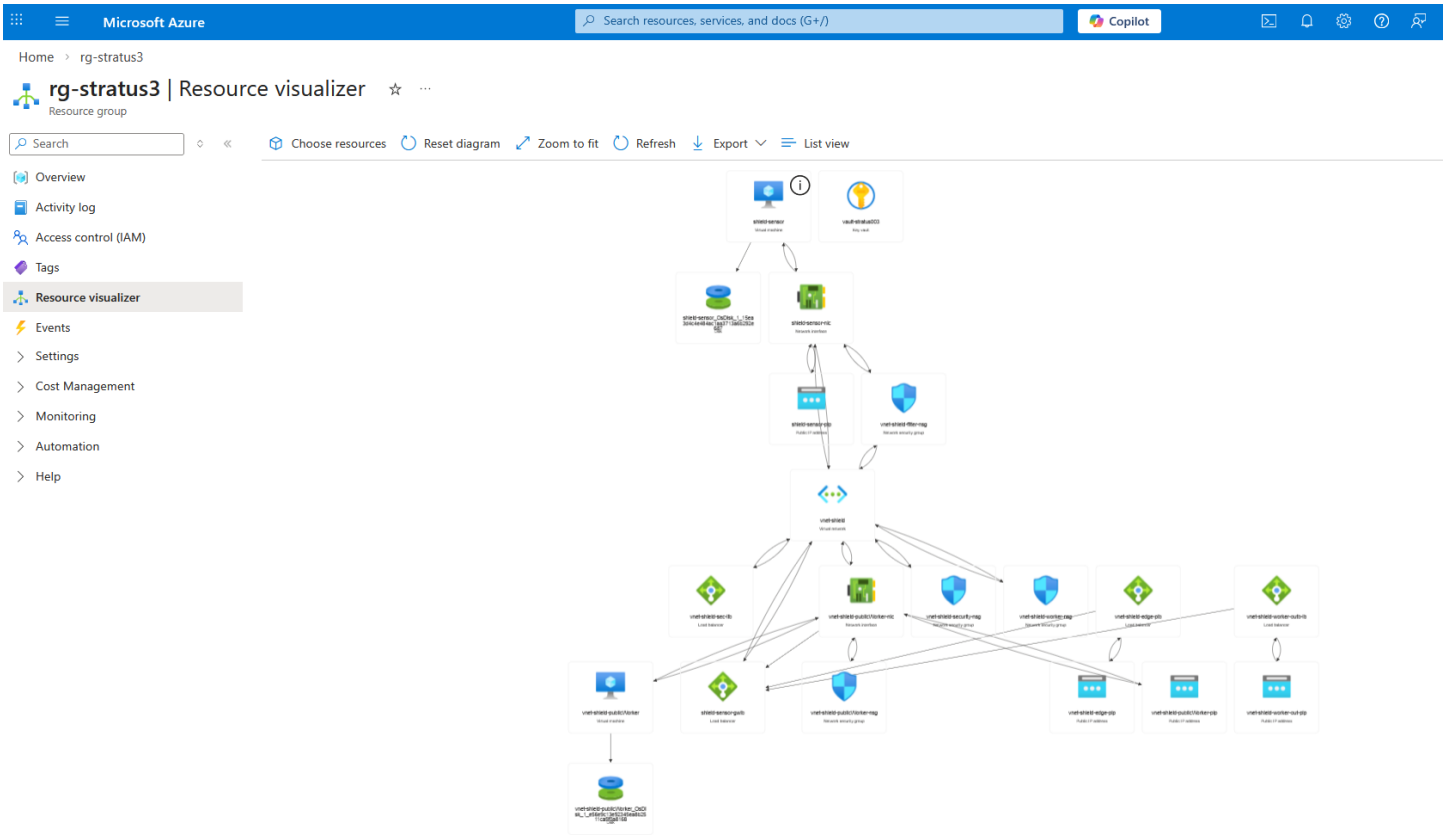
When you deploy, you will be presented with the ARM Template deployment screen which shows the list of resources being deployed and their deployment status. Look for any errors that appear here.



Finally, once successful, you will be presented with a message that the deployment is complete.



You may visualize the resources that were deployed by navigating to the Resource visualizer in the Azure Portla under the resource group in which Shield Stratus was deployed.



Activating Shield Stratus

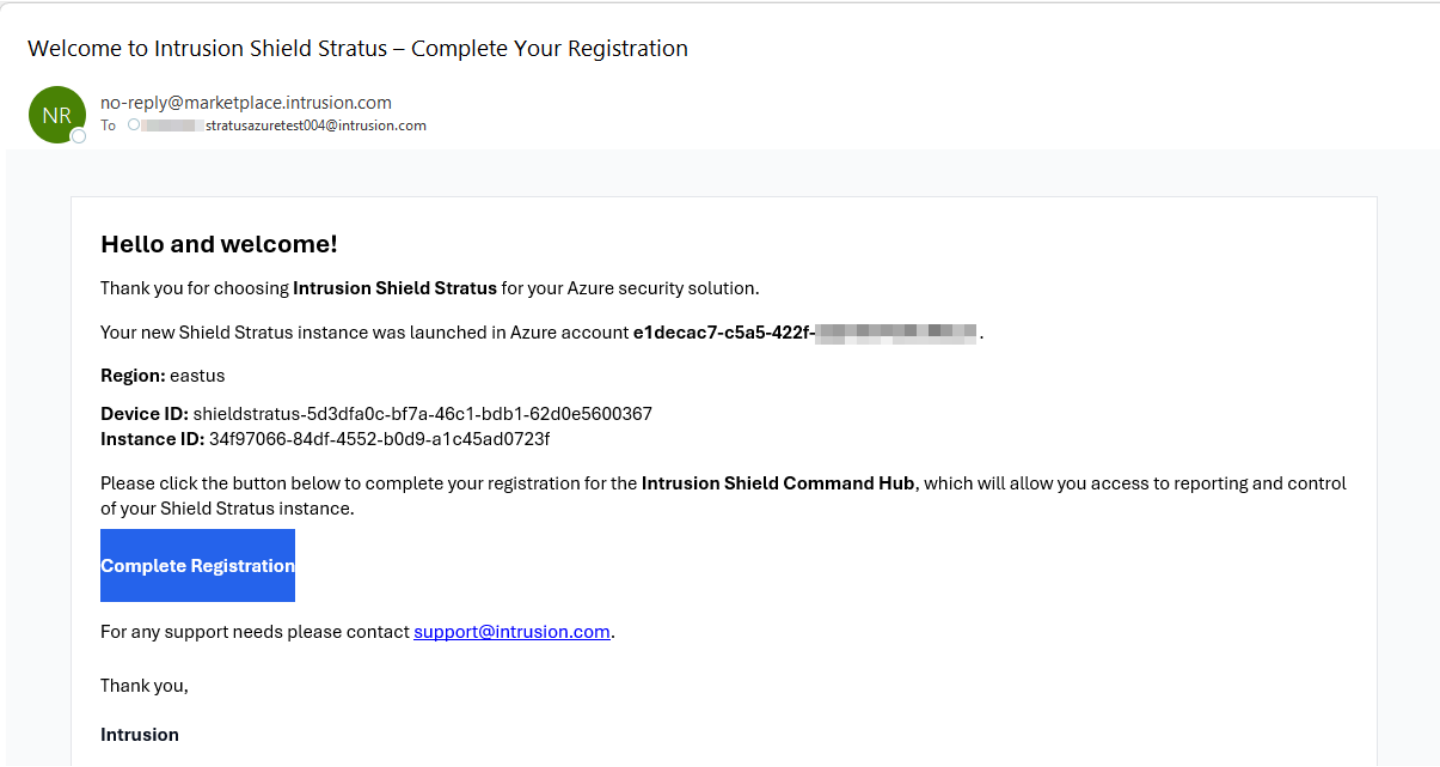
Although Shield Stratus is instantiated and will pass traffic by default, it will not filter or log traffic until it has been activated.

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

Creating an Intrusion Command Hub Account

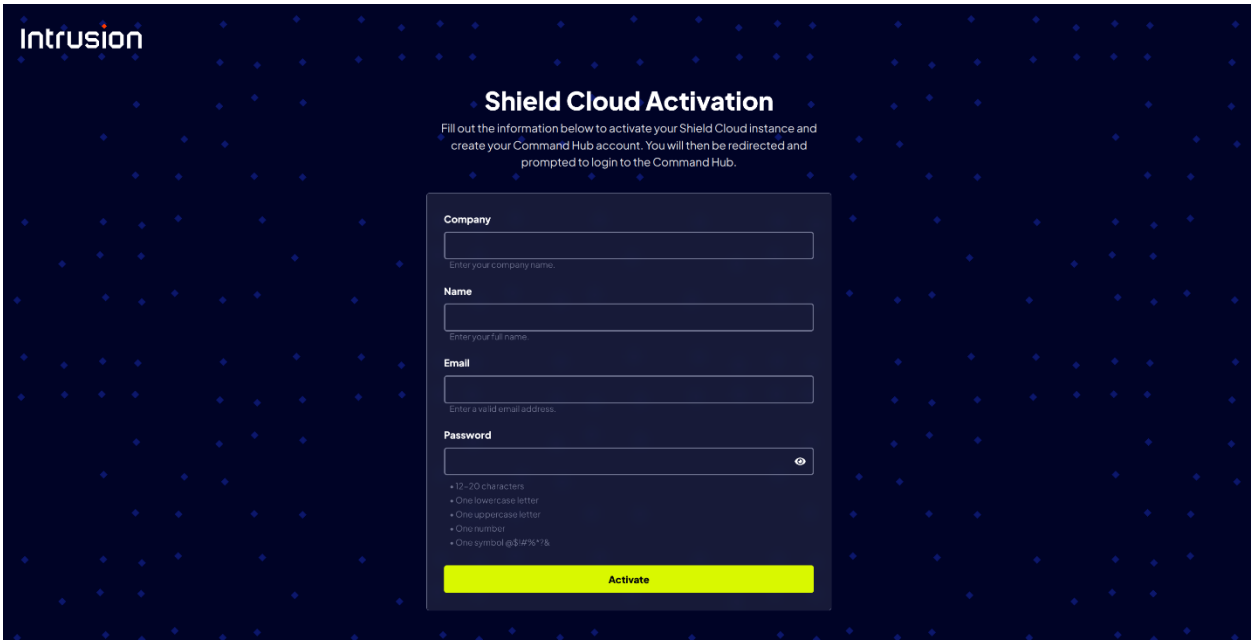
Shield Stratus detects whether an Intrusion Command Hub account has been registered for your Azure subscription. If a previous activation is associated with your Azure subscription, you may continue to use your previously setup credentials to login to the Command Hub.

If your Azure subscription 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.

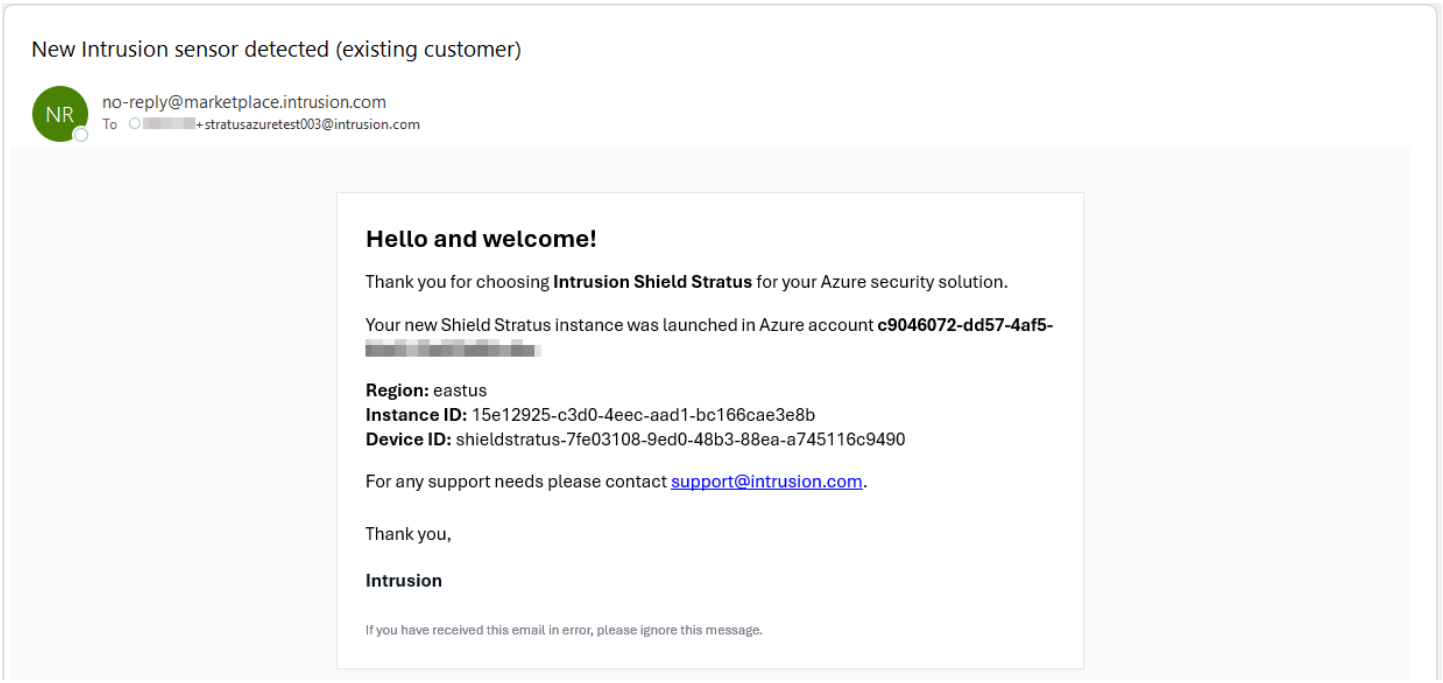
The email and password provided will serve as a login to Intrusion Command Hub.



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

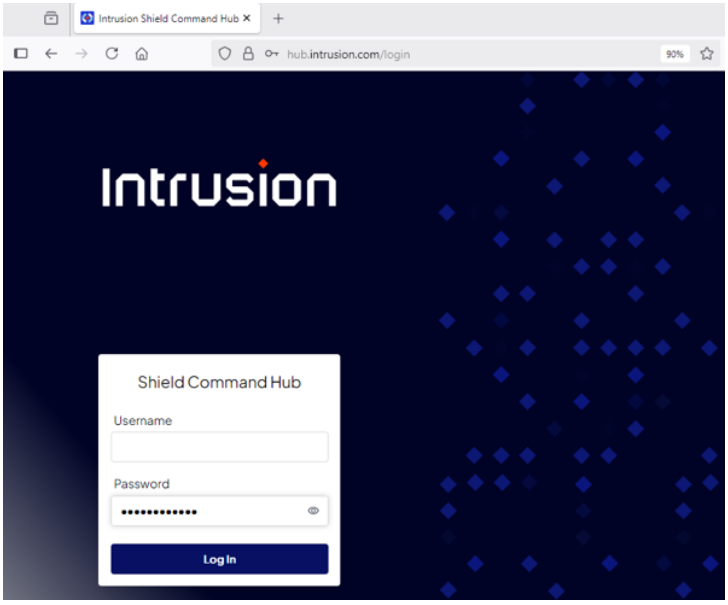
Additionally, this will trigger your Shield Stratus instance to register with this account within a few minutes.

If you have already registered previously with your Azure subscription, 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.

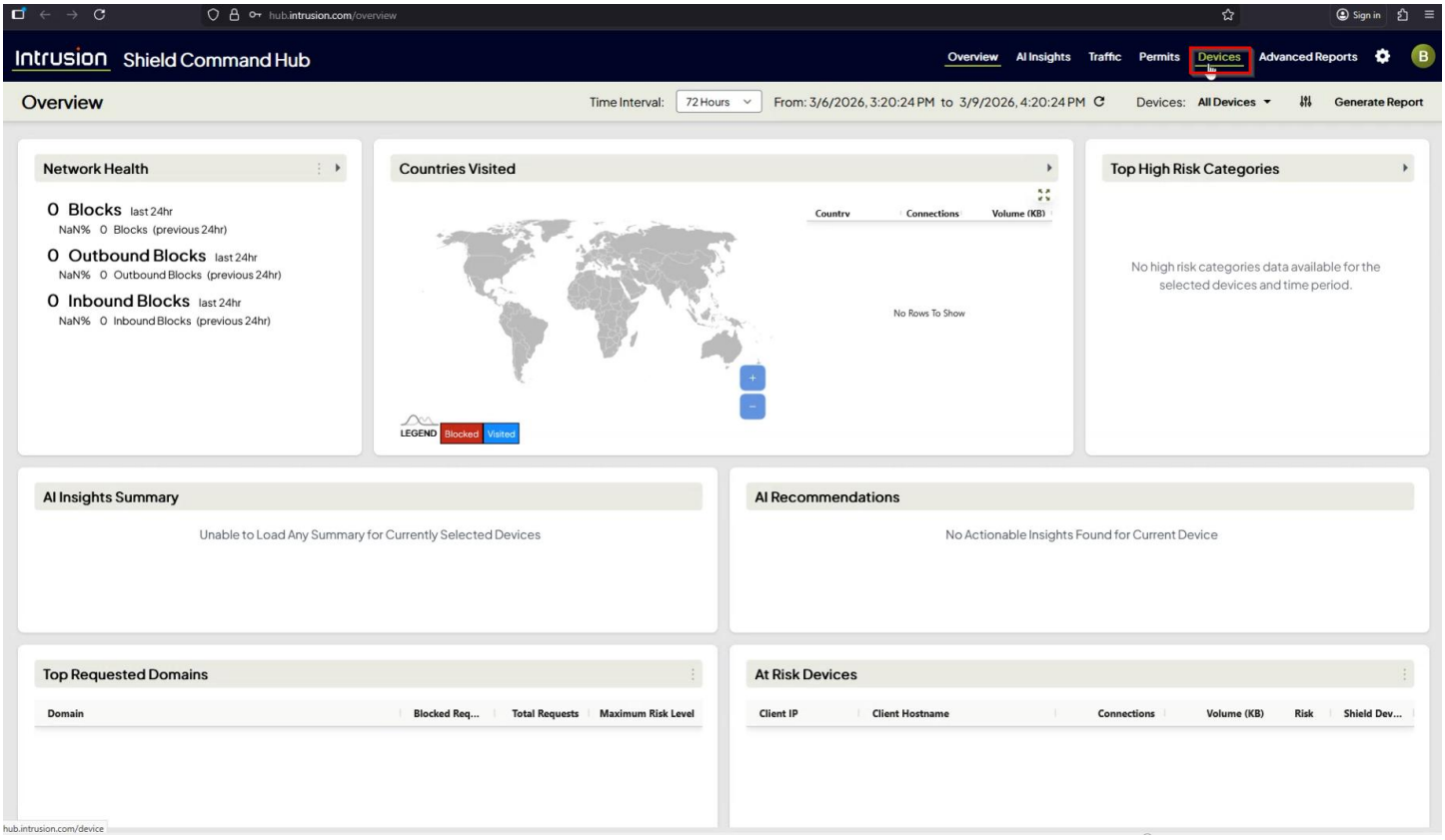


Intrusion Command Hub

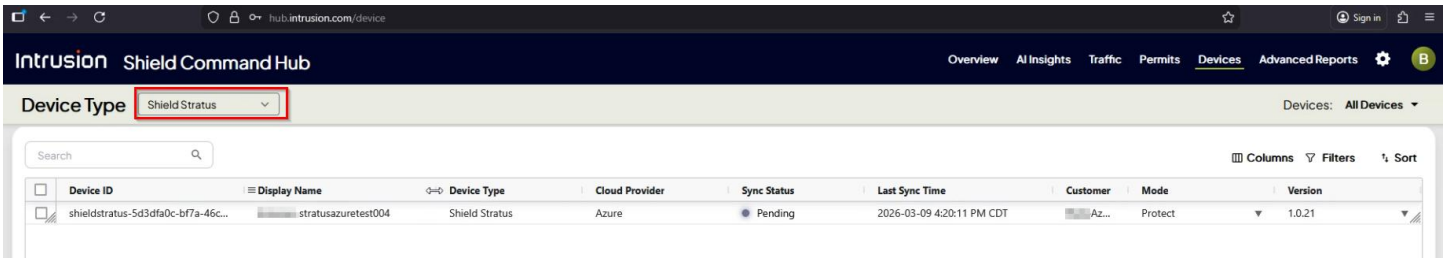
The Intrusion Command Hub (https://hub.intrusion.com) can be accessed with the newly created credentials. For more information, see Command Hub Management of Shield Stratus.



Once logged in, click on the Devices tab.



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



For more information, see Command Hub Management of Shield Stratus.

Configuring DNS Clients

By default, Azure VNets will enable DNS resolution from internal Azure resolvers from inside the VNet without traversing the GWLB. 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 VNet.

Testing

To verify that the Intrusion ATI is working, try resolving various domains from a VM protected by Stratus.

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.

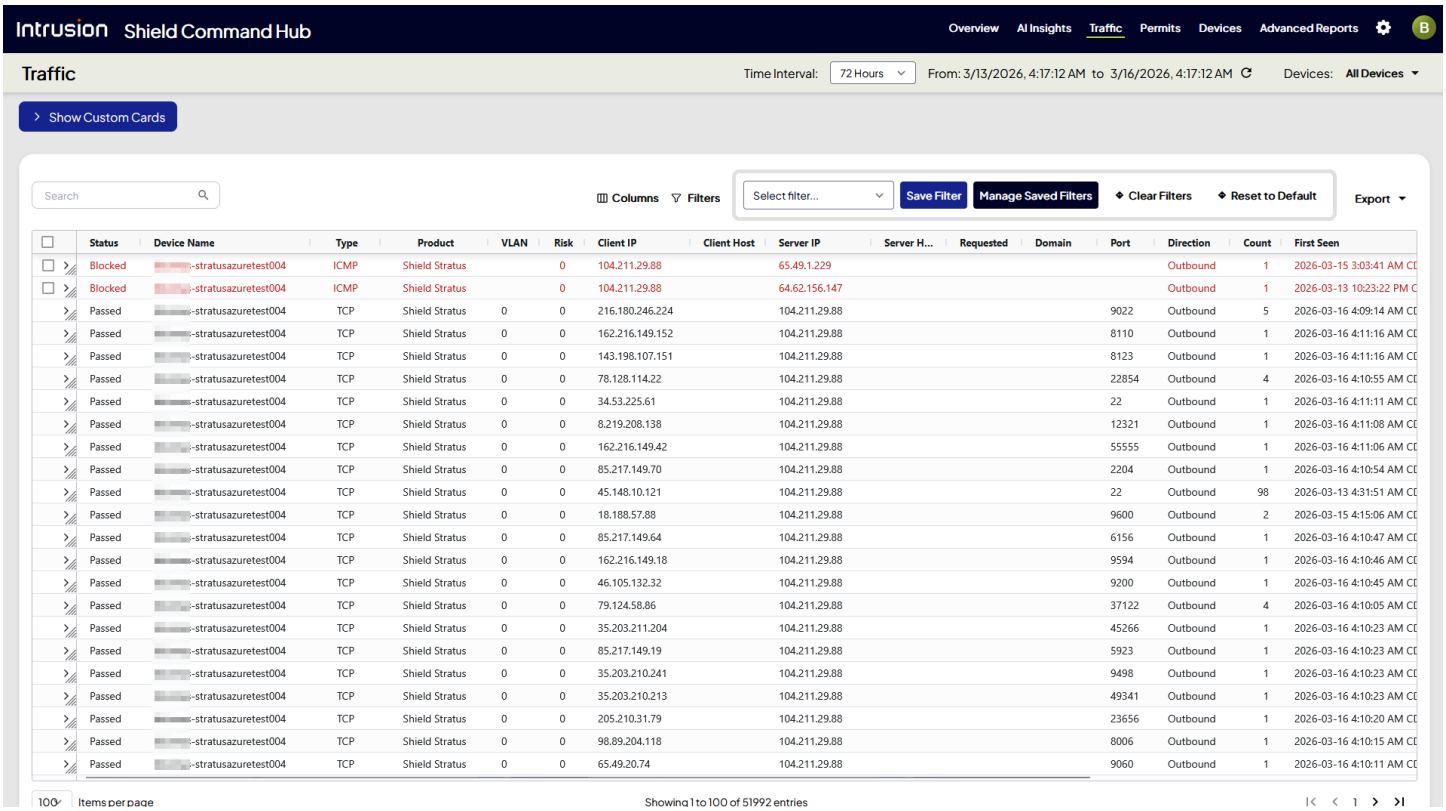
Reporting can be accessed via the Intrusion Shield Hub dashboard at https://hub.intrusion.com.

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 VNet. It shows a summary of DNS requests, TCP connections, UDP sessions and ICMP packets over a 72 hour period.



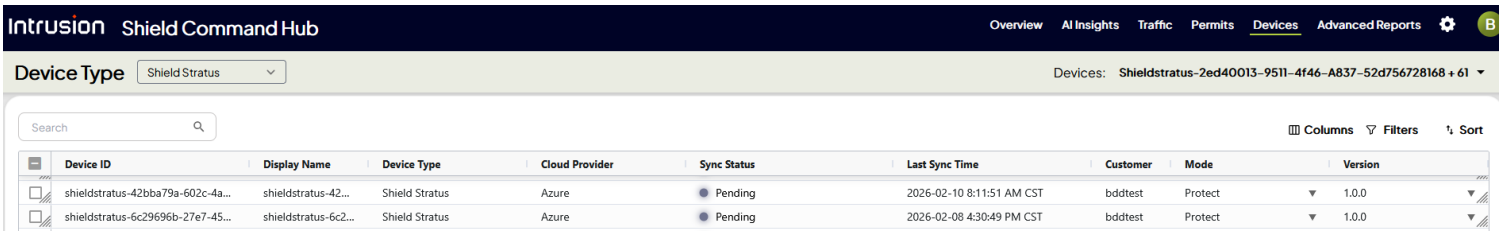
Traffic summaries are updated from Shield Stratus approximately every 15 minutes.

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

Managing Devices

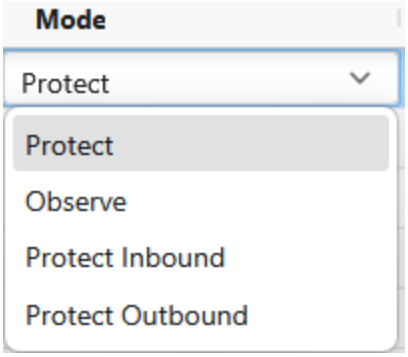
Shield Stratus devices appear in the **Devices** tab. From the **Device Type** dropdown, select **Shield Stratus** to see a list of devices registered to your account. The Devices tab allows users to select Device type and choose to modify a device if necessary.

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 • Pending – device has been registered but has not synchronized state • Sync Successful – device has synchronized status at least once
Last Sync	Read-only	The last synchronization time
Mode	Read-write	The provisioned mode of the Stratus instance • **Protect** – DNS and IP filtering are enabled. Traffic logging is enabled. • **Observe** – DNS and IP filtering are disabled but Traffic logging is still active • **Protect Inbound** – DNS and IP filtering only apply to inbound connections entering the VNet from the public Internet. Outbound connections are logged but not filtered. • **Protect Outbound** – DNS and IP filtering only apply to outbound connections leaving the VNet to the public Internet. Inbound connections are logged but not filtered.
Version	Read-write	Shield Stratus software version. Can be dynamically updated. Software updates typically take 1-2 minutes.

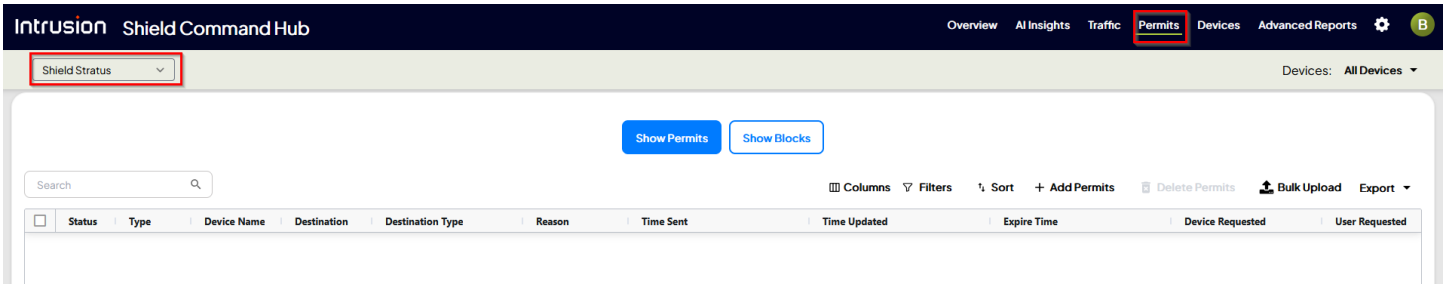

Mode
Protect
Protect
Observe
Protect Inbound
Protect Outbound

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.

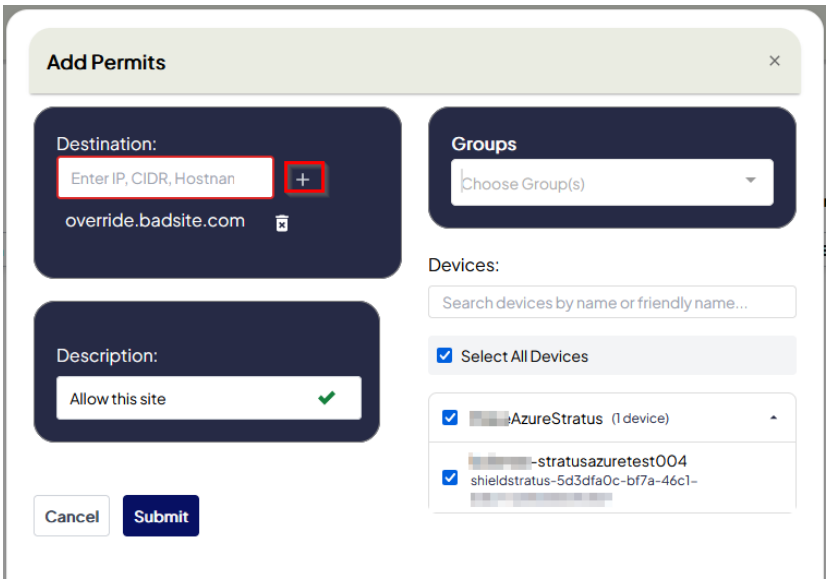


To add a new permit, click the **+ Add** button. The **Destination** can be an IP, CIDR range, or hostname. An individual Shield Stratus device can be selected, or a group can be selected.

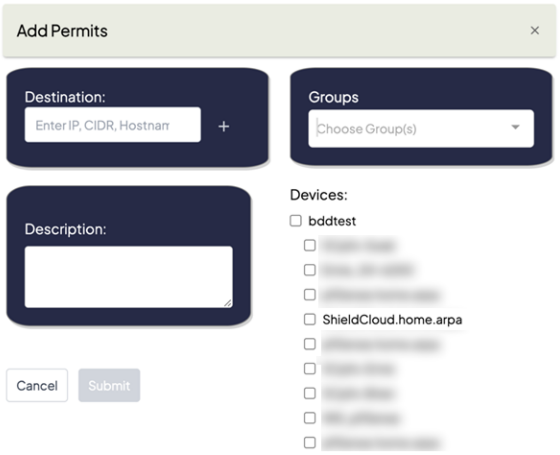
Populate with

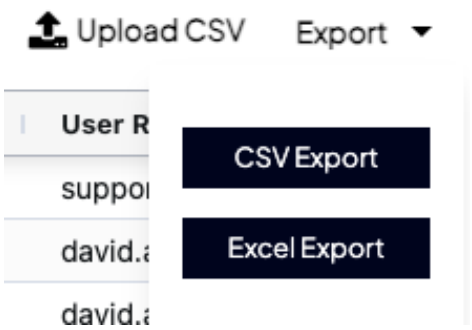
- **Destination** – a FQDN or IP address. Make sure to click the plus sign (**+**) after each one.
- **Description** – a required note for why you are unblocking
- **Devices** – one or more current Shield Stratus devices to which you want to apply the permit

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.





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

Frequently Asked Questions

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 instance type **Standard_D2S_v4**.

2. **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.

3. **Can I instantiate Shield Stratus without an ARM template?**

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

Command Hub

4. **How do I obtain an Intrusion Command Hub login?**

   Upon the deployment of a Shield Stratus instance for the first time in your Azure subscription, 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.

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

   Please contact Intrusion support.

6. **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

7. **Can Shield Stratus be deployed in High Availability mode in Azure?**

   Yes, multiple Shield Stratus can be associated with a Gateway Load Balancer backend pool, effectively supporting parallel processing of network flows. However, they will show up as separate devices in Command Hub that must be managed manually. Adding a new instance to the pool does not automatically inherit existing settings or permits.

Logging

8. **Does Shield Stratus support Azure Monitor Logs?**

   Currently Shield Stratus currently does not support Azure Monitor Logs.

Troubleshooting

1. **When deploying the ARM template, I receive an error that *securityProfile.encryptionAtHost* is not enabled.**

   For some Azure accounts, disk encryption is not enabled by default. This can be enabled using the following PowerShell script:

   ```
   az feature register --namespace Microsoft.Compute --name EncryptionAtHost
   ```

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 Stratus VM:

- 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)
- Intrusion 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.