TREND MICRO

5.7

TREND MICRO™ Deep Discovery Inspector

Service Pack 2

AWS Deployment Guide

Breakthrough Protection Against APTs and Targeted Attacks

Endpoint Security

Network Security

Protected Cloud

TREND MICRO SMART Protection Network™

Document Part No.: APEM59149/201116

Release Date: December 2020

Protected by U.S. Patent No.: 8595840; 8925074; 7707635; 8505094

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Evaluate this documentation on the following site:

https://www.trendmicro.com/download/documentation/rating.asp

Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that Deep Discovery Inspector collects and provides detailed instructions on how to disable the specific features that feedback the information.

https://success.trendmicro.com/data-collection-disclosure

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Notice:

https://www.trendmicro.com/privacy

Table of Contents

Preface

Preface

This Guide introduces Trend Micro™ Deep Discovery™ Inspector 5.7 SP2.

Learn more about the following topics:

- *Documentation on page iv*
- *Audience on page v*
- *Document Conventions on page v*

Documentation

The documentation set for Deep Discovery Inspector includes the following:

TABLE 1. Product Documentation

DOCUMENT	DESCRIPTION
Administrator's Guide	The Administrator's Guide contains detailed instructions on how to configure and manage Deep Discovery Inspector, and explanations on Deep Discovery Inspector concepts and features.
AWS Deployment Guide	The AWS Deployment Guide contains information about requirements and procedures for planning deployment, deploying, and troubleshooting Deep Discovery Inspector deployment on AWS.
Installation and Deployment Guide	The Installation and Deployment Guide contains information about requirements and procedures for planning deployment, installing Deep Discovery Inspector, and using the Preconfiguration Console to set initial configurations and perform system tasks.
Syslog Content Mapping Guide	The Syslog Content Mapping Guide provides information about log management standards and syntaxes for implementing syslog events in Deep Discovery Inspector.
Readme	The Readme contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, known issues, and product release history.
Online Help	Web-based documentation that is accessible from the Deep Discovery Inspector management console. The Online Help contains explanations of Deep Discovery Inspector components and features, as well as procedures needed to configure Deep Discovery Inspector.

Document	Description
Support Portal	The Support Portal is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Support Portal, go to the following website: https://success.trendmicro.com

View and download product documentation from the Trend Micro Online Help Center:

https://docs.trendmicro.com/en-us/home.aspx

Audience

The Deep Discovery Inspector documentation is written for IT administrators and security analysts. The documentation assumes that the reader has an in-depth knowledge of networking and information security, including the following topics:

- Network topologies
- Database management
- Antivirus and content security protection

The documentation does not assume the reader has any knowledge of sandbox environments or threat event correlation.

Document Conventions

The documentation uses the following conventions:

TABLE 2. Document Conventions

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
Italics	References to other documents
`Monospace`	Sample command lines, program code, web URLs, file names, and program output
Navigation > **Path**	The navigation path to reach a particular screen For example, **File** > **Save** means, click **File** and then click **Save** on the interface
Note	Configuration notes
Tip	Recommendations or suggestions
Important	Information regarding required or default configuration settings and product limitations
WARNING!	Critical actions and configuration options

Chapter 1

About Deployment on AWS

This guide provides additional information that enables you to evolve from an on-premises Deep Discovery Inspector appliance to a Deep Discovery Inspector appliance on AWS. For more details about the Deep Discovery Inspector features and functions, see the *Deep Discovery Inspector Administrator's Guide* on https://docs.trendmicro.com/en-us/enterprise/deep-discovery-inspector.aspx.

Specialized Knowledge

This guide assumes familiarity with networking basics. This guide also requires a moderate level of familiarity with AWS. If you are new to AWS, visit the *Getting Started Resource Center* (https://aws.amazon.com/getting-started/) and *AWS Training and Certification* (https://aws.amazon.com/training/). These sites provide materials for learning how to design, deploy, and operate your infrastructure and applications on the AWS.

AWS Account

If you do not already have an AWS account, create one at https://aws.amazon.com by following the on-screen instructions. Part of the sign-up process involves receiving a phone call and entering a PIN using the phone keypad.

AWS automatically signs up your account for all AWS services. You are charged only for the services you use.

Cost and Licenses

In order to access and use the AMI version of the Deep Discovery Inspector virtual appliance, you must already have and continually maintain an active AWS Account on the AWS Marketplace and you are responsible for purchasing and maintaining through such AWS Account, your use of the Amazon Web Service platform/infrastructure that is required for your deployment of a Deep Discovery Inspector virtual appliance.

The Deep Discovery Inspector virtual appliance is offered as an AMI in the AWS Marketplace. Access to the AMI can be obtained by searching the AWS Marketplace console.

Chapter 2

Deployment Planning

Planning the Deployment

The following steps provide an overview for planning the deployment of Deep Discovery Inspector virtual appliances in an AWS environment.

Procedure

1. Review the architecture.

   For details, see *Architecture on page 2-3*.

2. Review the system requirements.

   For details, see *System Requirements on page 2-3*.

3. Choose a deployment option to integrate with Amazon VPC Traffic Mirroring.

   For details, see *Deployment Options on page 2-5*.

4. Prepare items before deploying Deep Discovery Inspector.

   For details, see *Items to Prepare on page 2-8*.

5. Deploy the Deep Discovery Inspector virtual appliance.

   For details, see *Deployment on page 3-1*.

6. Access the Deep Discovery Inspector virtual appliance management console.

   For details, see the *Deep Discovery Inspector Administrator's Guide*.

Architecture

The Deep Discovery Inspector virtual appliance supports deployment on an AWS EC2 environment and can scan as well as analyze mirrored packets from an AWS VPC traffic mirror.

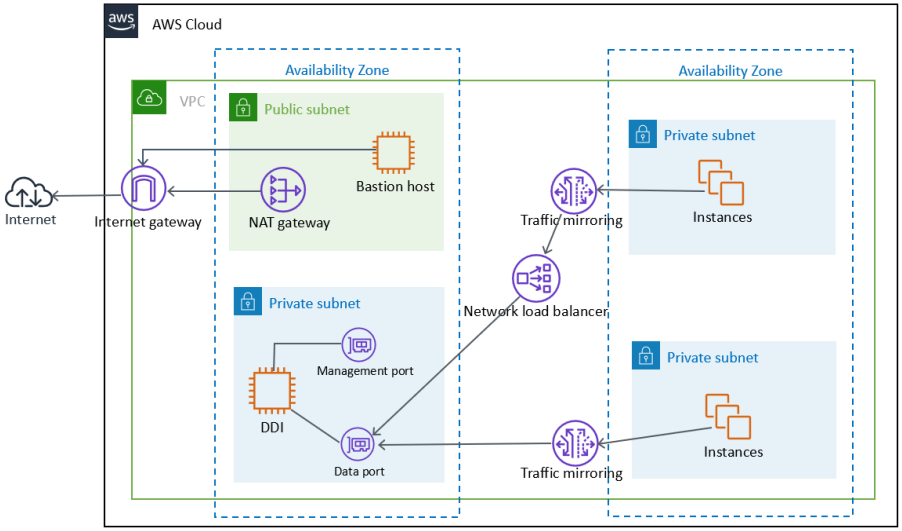


FIGURE 2-1. Deployment Architecture

System Requirements

Trend Micro recommends the following minimum specifications based on your licensed model's throughput.

Note

When using a Deep Discovery Inspector virtual appliance on AWS with Virtual Analyzer, only external Virtual Analyzers and Sandbox as a Service are supported.

Table 2-1. System Requirements

Throughput (Mbps)	AWS vCPU	AWS Memory (GiB)	AWS Storage (GiB)	AWS ENI (Elastic Network Interfaces)	Recommended AWS EC2 Instance Type
250	8	32	500	2	• t3.2xlarge • t3a.2xlarge • m5.2xlarge • m5a.2xlarge
500	8	32	500	2	• t3.2xlarge • t3a.2xlarge • m5.2xlarge • m5a.2xlarge
1000	16	64	1000	2	• m5.4xlarge • m5a.4xlarge

Note

T3 and T3a instances launch as unlimited mode by default. For more details about using unlimited mode or standard mode on the instance types, see https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/burstable-performance-instances.html.

For details about AWS EC2 instance types, see https://aws.amazon.com/ec2/instance-types/.

You can use non-recommended instance types as long as the instance type meets the minimum system requirements.

Deployment Options

By integrating with the Amazon VPC Traffic Mirroring feature, the Deep Discovery Inspector virtual appliance can provide a network security solution via two deployment options:

- **Option 1: Deploy the Deep Discovery Inspector virtual appliance as a traffic mirror target**

  Network traffic is mirrored from an ENI (Elastic Network Interfaces) mirror source to a data port of the Deep Discovery Inspector virtual appliance. This option depends on the settings of traffic mirror filter as shown in the figure below.

  Note

  If the Deep Discovery Inspector virtual appliance is attached to more than 1 data port, you can set each data port as traffic mirror target.

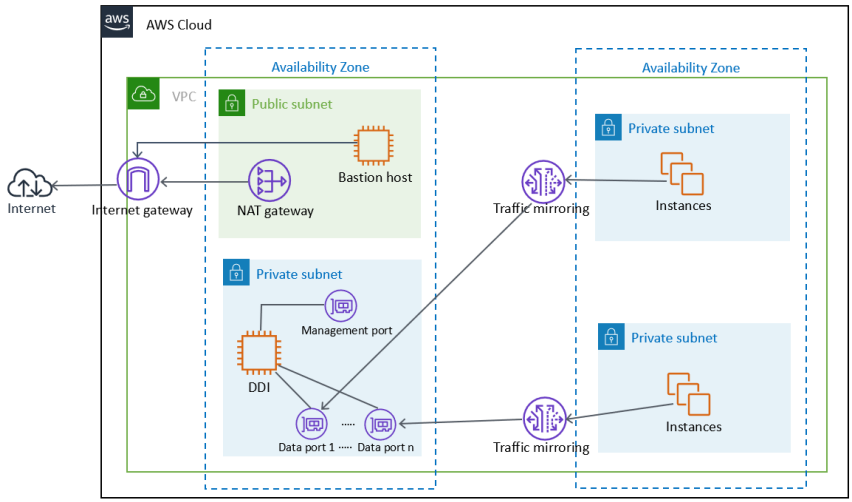


FIGURE 2-2. Option 1: Deploy the Deep Discovery Inspector virtual appliance as a traffic mirror target

- **Option 2: Deploy the Deep Discovery Inspector virtual appliance behind the NLB**

  Deploy the Deep Discovery Inspector virtual appliance in the target group behind the NLB (Network Load Balancer). Network traffic is mirrored to the NLB and the NLB forwards traffic to health instances belonging to the target group as shown in the figure below.

Note

The NLB only forwards the mirrored traffic to data port 1 of the Deep Discovery Inspector virtual appliance.

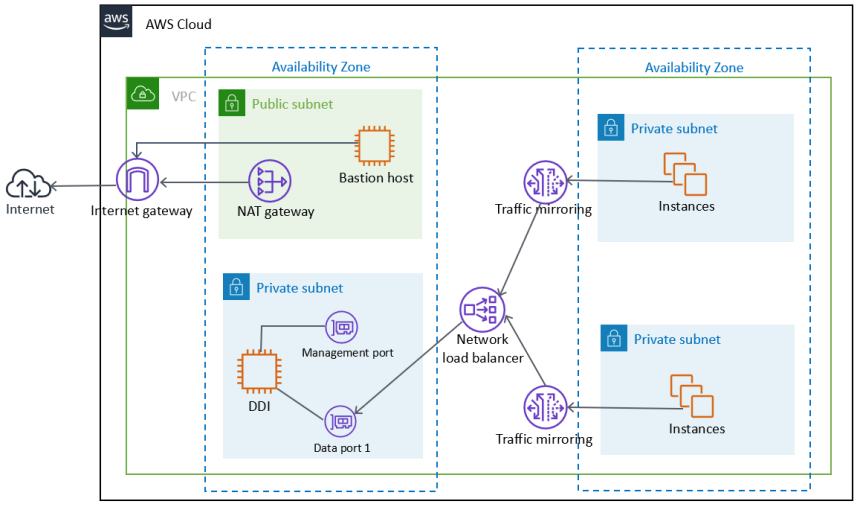


FIGURE 2-3. Option 2: Deploy the Deep Discovery Inspector virtual appliance behind the NLB

Considerations

The quota limitation enforced by AWS traffic mirrors has the following limitations for the deployment options:

- Maximum number of mirror sources per a non-dedicated instance type as target: 10
- Maximum number of mirror sources per a dedicated instance type as target: 100

Note

For more details about the limitation, see https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-considerations.html.

You are not limited to a particular deployment option. If you deploy a Deep Discovery Inspector virtual appliance as a traffic mirror target for early validation and later change to deploy a Deep Discovery Inspector virtual

appliance behind an NLB, then it is unnecessary to re-launch a new Deep Discovery Inspector virtual appliance after changing. In addition, advanced deployments can incorporate both deployment options at the same time in the VPC environment.

Items to Prepare

- **Deep Discovery Inspector AMI**

  AMI of the Deep Discovery Inspector virtual appliance from the AWS Marketplace

- **Deep Discovery Inspector Activation Code**

  Activation Code for the Deep Discovery Inspector virtual appliance

- **AWS VPC and subnet**

  A VPC configured with public and private subnets, according to AWS best practices, to provide you with your own virtual network on AWS.

  Note

  For details about creating a VPC and subnet, see https://docs.aws.amazon.com/vpc/latest/userguide/working-with-vpcs.html.

  Public subnets and:

  - Managed NAT gateways to allow outbound internet access for the Deep Discovery Inspector virtual appliance in the private subnets.

    Note

    For details about creating a NAT gateway, see https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html.

  Private subnets and:

- Management port and Data port of the Deep Discovery Inspector virtual appliance which can be in the same subnet or different subnets in your VPC.

- **AWS VPC Traffic Mirror**

  Traffic Mirroring is an AWS VPC feature that you can use to copy network traffic from an elastic network interface (ENI) of Amazon EC2 instances. The security and monitoring appliances can be deployed as individual instances, or as a fleet of instances behind a Network Load Balancer (NLB) with a UDP listener.

  Note

  For details, see https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-how-it-works.html.

  - One or more instances that create some network connections. The instances act as the traffic mirror sources.

    Important

    There is a limit on the size of the mirrored packet, and packets larger than 8947 bytes are always truncated. Ensure that your traffic mirror source's MTU size is set to equal or less than 8947 bytes. To check and set MTU on your AWS EC2 instance which you want to set as traffic mirror source, see https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/network_mtu.html#set_mtu and https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/network_mtu.html#set_mtu_windows.

  - Only instances powered by the AWS Nitro system can be traffic mirror sources. For details, see https://aws.amazon.com/blogs/aws/new-vpc-traffic-mirroring/.

  - (Optional) A Network Load Balancer, with the settings configured properly:

    - Target group

- Traffic mirror, with the settings configured properly:
  - Traffic mirror filter
  - Traffic mirror target
  - Traffic mirror session

Note

For details about creating a traffic mirror target and filter, and then using those resources to create a session, see https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-getting-started.html.

- **AWS EC2 Security Group**

Inbound/ Outbound Rule	Type	Protocol	Port	Source	Description
Inbound	HTTPS	TCP	443	CIDR that can reach your instance	For accessing the Deep Discovery Inspector virtual appliance management console
Inbound	SSH	TCP	22	CIDR that can reach your instance	For accessing the Deep Discovery Inspector virtual appliance pre-configuration console

Inbound/ Outbound Rule	Type	Protocol	Port	Source	Descriptio n
Inbound	Custom UDP	UDP	4789	CIDR of your mirror source or the NLB	For VXLAN traffic required by the AWS traffic mirror
Inbound	Custom TCP	TCP	14789	CIDR of NLB	(Optional) Implemente d by the Deep Discovery Inspector virtual appliance for answering the NLB health check.

Note

Outbound Rules in the default security group should allow all traffic. The Deep Discovery Inspector virtual appliance works well with the default outbound rules. The following exceptions may apply:

- For some organizations, whose policies may need more specific protocols and port numbers, see *Chapter 2: About Your System* in the *Deep Discovery Inspector Installation and Deployment Guide*.
- For some organizations, whose infrastructure may need an outbound proxy with domains allowed to access the internet, see https://docs.trendmicro.com/all/ent/ddi/v5.7/en-us/ddi_5.7_olh/access_trend_service.html for detailed addresses.

Chapter 3

Deployment

Deployment Overview

The following is an overview of the steps required to deploy a Deep Discovery Inspector virtual appliance and a VPC traffic mirror in your AWS environment.

1. Launch a Deep Discovery Inspector virtual appliance.

   For details, see *Launching a Virtual Appliance on page 3-2*.

2. (Optional) Configure the description for the virtual appliance network interfaces.

   For details, see *Configuring the Description for Network Interfaces on page 3-12*.

3. Choose one of the following options to deploy the AWS VPC traffic mirror.

   - Deploy a virtual appliance as a traffic mirror target

     For details, see *Deploying a Virtual Appliance as a Traffic Mirror Target on page 3-14*.

   - Deploy a virtual appliance behind an NLB

     For details, see *Deploying a Virtual Appliance Behind an NLB on page 3-22*.

Launching a Virtual Appliance

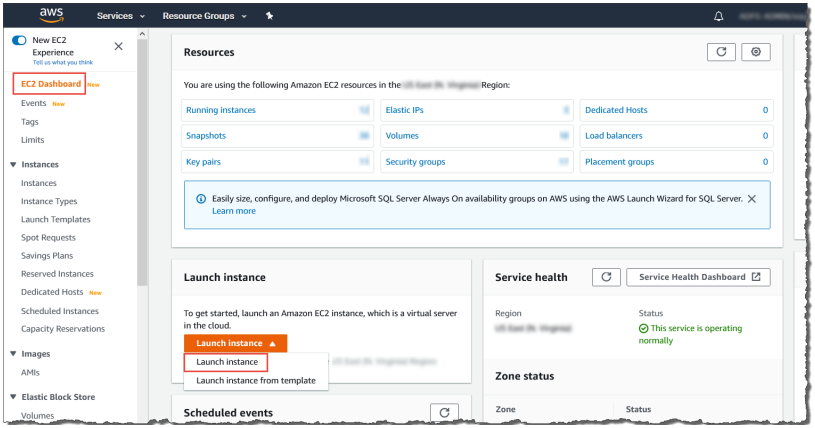
Procedure

1. Initiate the instance launch.

   a. Open the **Amazon EC2** console at https://console.aws.amazon.com/ec2/.

   b. In the navigation bar at the top of the screen, select a Region for the instance that meets your needs.

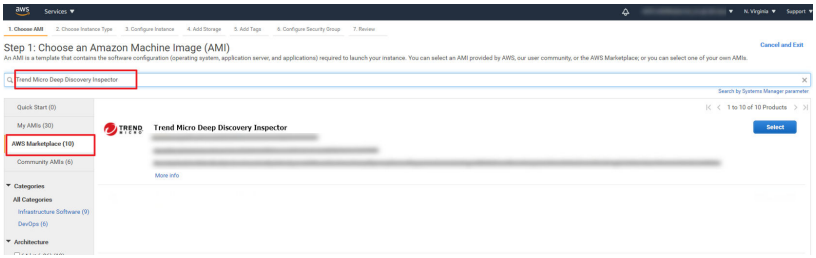
c. From the **Amazon EC2** console dashboard, select **Launch instance**.



2. Choose the AMI for Deep Discovery Inspector.

a. On the **Choose an Amazon Machine Image (AMI)** screen, select **AWS Marketplace** in the left pane.

b. In the search box, search for `Trend Micro Deep Discovery Inspector`.



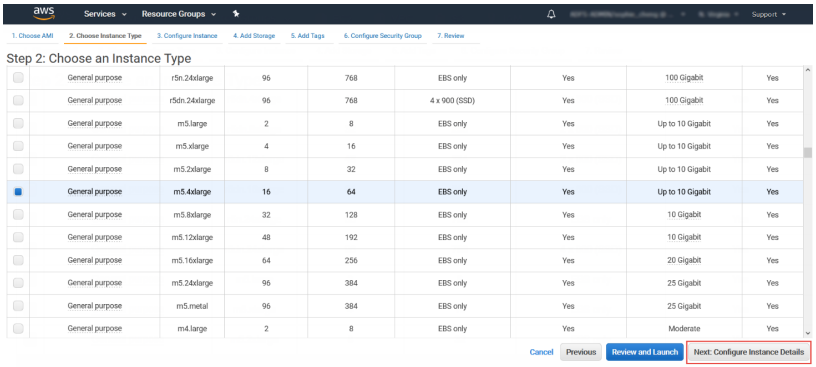
c. After the search results appear, click **Select** for **Trend Micro Deep Discovery Inspector <version>**.

3. Choose an Instance Type.

a. On the **Choose an Instance Type** screen, choose an instance type that meets the minimum specifications based on your licensed model's throughput.

For details, see *System Requirements on page 2-3*.

b. Choose **Next: Configure Instance Details** to configure your instance further.

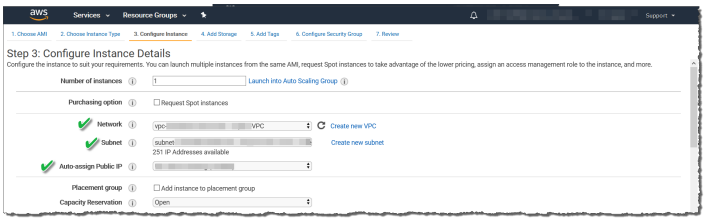


	General purpose	r5n.24xlarge	96	768	EBS only	Yes	100 Gigabit	Yes
	General purpose	r5dn.24xlarge	96	768	4 x 900 (SSD)	Yes	100 Gigabit	Yes
	General purpose	m5.large	2	8	EBS only	Yes	Up to 10 Gigabit	Yes
	General purpose	m5.xlarge	4	16	EBS only	Yes	Up to 10 Gigabit	Yes
	General purpose	m5.2xlarge	8	32	EBS only	Yes	Up to 10 Gigabit	Yes
	General purpose	m5.4xlarge	16	64	EBS only	Yes	Up to 10 Gigabit	Yes
	General purpose	m5.8xlarge	32	128	EBS only	Yes	10 Gigabit	Yes
	General purpose	m5.12xlarge	48	192	EBS only	Yes	10 Gigabit	Yes
	General purpose	m5.16xlarge	64	256	EBS only	Yes	20 Gigabit	Yes
	General purpose	m5.24xlarge	96	384	EBS only	Yes	25 Gigabit	Yes
	General purpose	m5.metal	96	384	EBS only	Yes	25 Gigabit	Yes
	General purpose	m4.large	2	8	EBS only	Yes	Moderate	Yes

4. Configure the Instance Details.

a. On the **Configure Instance Details** screen, change the follow settings.

- - **Network**: Select the VPC.
  - **Subnet**: Select the subnet into which to launch your instance. Select a subnet that is planned for the data port subnet.
  - **Auto-assign Public IP**: Select **Disable**. Trend Micro recommends that you deploy the Deep Discovery Inspector virtual appliance behind an AWS NAT gateway.



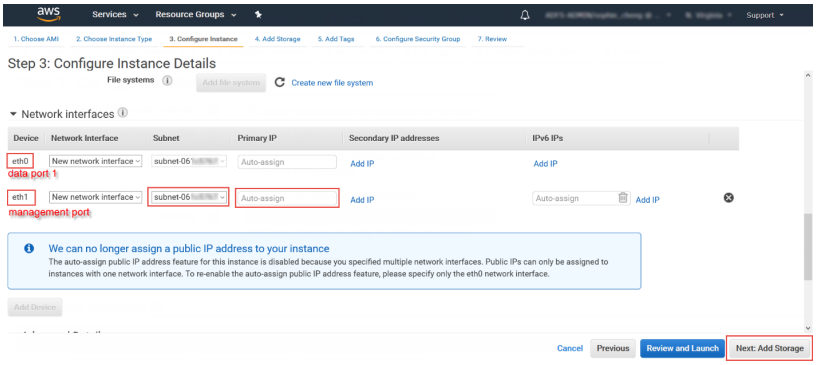
- **Network interfaces**: Add a secondary network interface for the Deep Discovery Inspector virtual appliance instance by choosing **Add Device**.

Important

The management port for Deep Discovery Inspector on-premises is fixed at the first NIC port (eth0 in Deep Discovery Inspector). In order to adapt into the AWS environment, the Deep Discovery Inspector virtual appliance has swapped port enumeration for the management port to port 1 (eth1) and data port to port 0 (eth0).

- Device eth0:
  - **Subnet**: The subnet has been configured in a previous step.
  - **Primary IP**: Type a private IPv4 address from the range of your subnet, or leave **Auto-assign** to let AWS choose a private IPv4 address for you.
- Device eth1:
  - **Subnet**: Select a subnet that is planned for the management port subnet.
  - **Primary IP**: Type a private IPv4 address from the range of your subnet, or leave **Auto-assign** to let AWS choose a private IPv4 address for you.

- **IPv6 IPs**: (Optional) Click **Add IP** and type an IPv6 address from the range of the subnet, or leave **Auto-assign** to let AWS choose an IPv6 address for you.



b. Click **Next: Add Storage** to specify the root volume size of your instance

5. Add Storage.

a. Specify the following settings on the **Add Storage** screen.

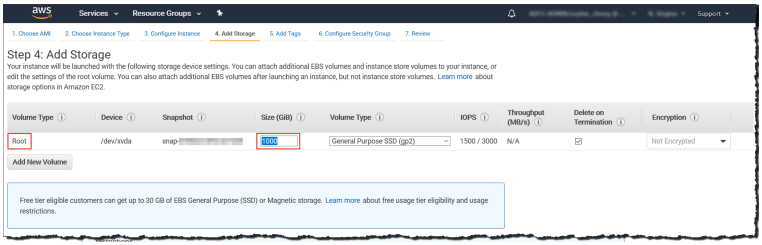
- **Size**: The storage size should meet the minimum specifications based on your licensed model's throughput.

  For details, see *System Requirements on page 2-3*.

  Note

  To enlarge the storage size, specify the storage size of the **Volume Type: Root**. The Deep Discovery Inspector virtual appliance only partitions the storage when the **Volume Type** is **Root**. The extra storage will not be used.

- **Volume Type**: Use the default value, **General Purpose SSD (gp2)**.



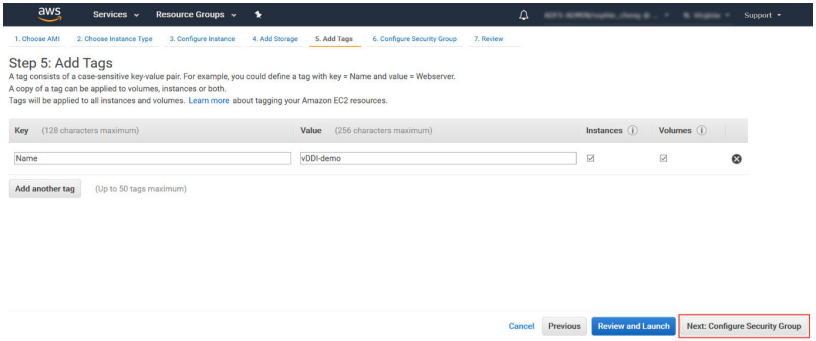
b. Click **Next: Add Tags** to add some custom tags.

6. Add Tags.

a. On the **Add Tags** screen, specify tags by providing the key and value combinations.

For example, for **Key** type `Name` and for **Value** type `vDDI-demo`.

b. Click **Next: Configure Security Group**.



7. Configure Security Group.

a. On the **Configure Security Group** screen, use a security group to define firewall rules for the Deep Discovery Inspector virtual appliance instance.

- To use existing security group, select **Select an existing security group**, and select your security group.
- To create a new security group, select **Create a new security group**.

b. Verify that your selected security group contains the following rules:

TABLE 3-1. Inbound Rules

TYPE	PROTOCOL	PORT RANGE	SOURCE	REASON
SSH	TCP	22	CIDR that can reach your instance	For accessing Deep Discovery Inspector virtual appliance Pre-Configuration console
HTTPS	TCP	443	CIDR that can reach your instance	For accessing Deep Discovery Inspector virtual appliance management console
Custom UDP	UDP	4789	CIDR of your mirror source or the NLB	For VXLAN traffic required by AWS traffic mirror
Custom TCP	TCP	14789	CIDR of NLB	Implemented by the Deep Discovery Inspector virtual appliance for answering NLB health check

Note

Outbound Rules: Rules in default security group allow all traffic. The Deep Discovery Inspector virtual appliance works well with default outbound rules. The following exceptions may occur:

- For some organizations, whose policies may need more specific protocols and port numbers, see *Chapter 2: About Your System > Ports Used by the Appliance* in the *Deep Discovery Inspector Installation and Deployment Guide*.
- For some organizations, whose infrastructures may need an outbound proxy with domains allowed to access the internet, see https://docs.trendmicro.com/all/ent/ddi/v5.7/en-us/ddi_5.7_olh/access_trend_service.html for detailed addresses.

c. Click **Review and Launch**.

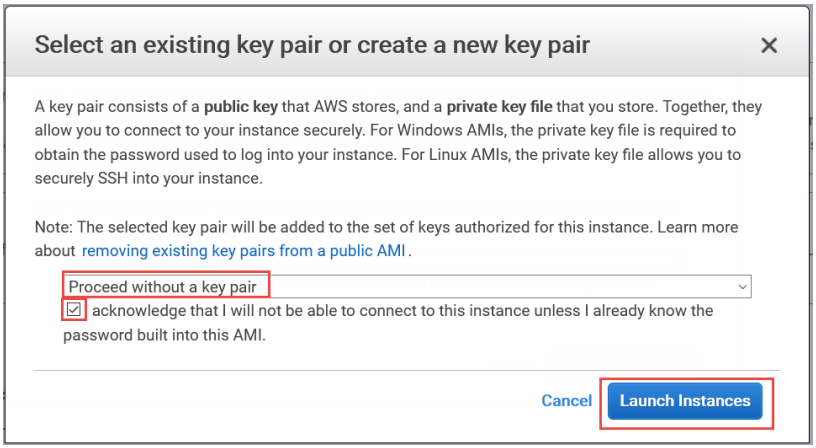
8. Review Instance Launch and select key pair.

a. On the **Review Instance Launch** screen, check the details of your instance, and make any necessary changes by choosing the appropriate **Edit** link.

b. Click **Launch**.

c. In the **Select an existing key pair or create a new key pair** dialog box, select **Proceed without a key pair**.

d. To launch your instance, select the acknowledgment check box, then click **Launch Instances**.



9. Wait for the Deep Discovery Inspector virtual appliance to become ready.

Note

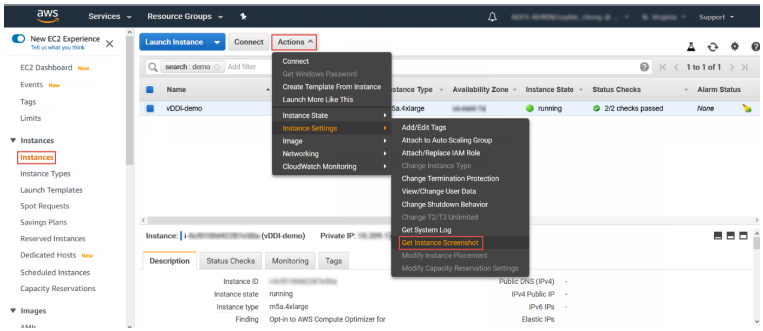
The Deep Discovery Inspector virtual appliance takes about 15 minutes to become ready.

a. View the Deep Discovery Inspector installation progress by using the following steps:

   i. In the left navigation page, click **Instances**.

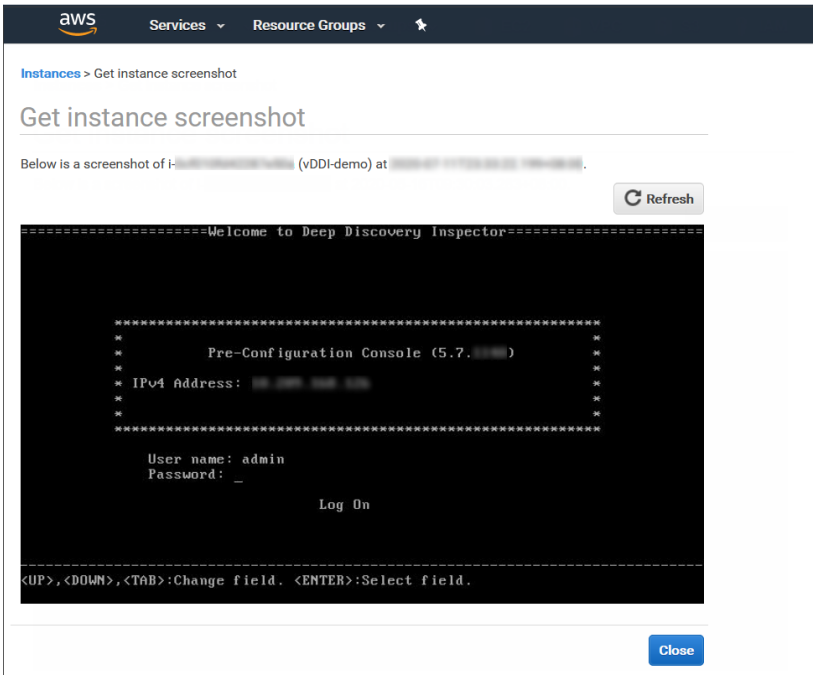
   ii. Select the Deep Discovery Inspector virtual appliance instance.

   iii. Select **Actions** > **Instance Settings** > **Get Instance Screenshot**.



For more details, see https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html.

b. When the Deep Discovery Inspector virtual appliance pre-configuration console appears, then Deep Discovery Inspector is ready.



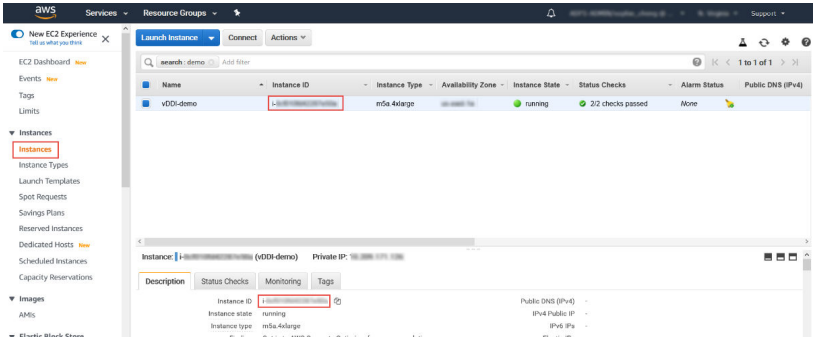
Configuring the Description for Network Interfaces

This task is optional. Trend Micro recommends setting the description for network interfaces of instances. When selecting one ENI from a long list of many ENIs, you can save time and avoid operation errors.

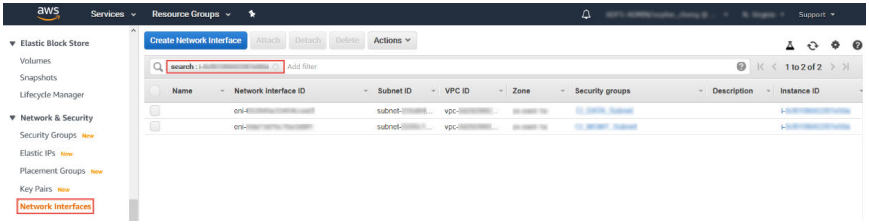
Procedure

1. Open the **Amazon EC2** console at https://console.aws.amazon.com/ec2/.
2. In the navigation pane, select **Instances** and copy the instance ID using the following steps.
   a. Search for the Deep Discovery Inspector virtual appliance that you created in *Launching a Virtual Appliance on page 3-2*.

b. Copy the value of **Instance ID**.



3. In the navigation pane, select **Network Interfaces** and find the network interfaces of the Deep Discovery Inspector virtual appliance by searching for the instance ID.



4. Select the network interfaces of the Deep Discovery Inspector virtual appliance and then select **Actions** > **Change Description**.

5. In the **Change Description** dialog box, type a description for the network interface, select **Save** and then perform the following steps:

   a. Set description of eth0 to `Data port 1`.

   b. Set description of eth1 to `Management port`.

Tip

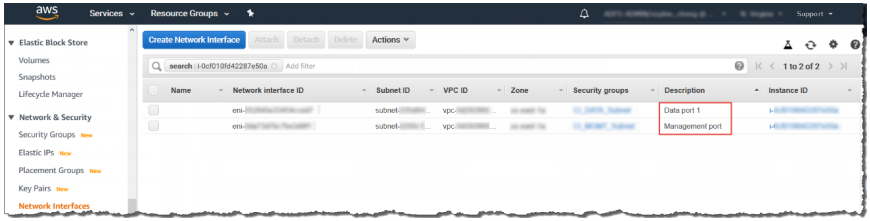
To view which interface is eth0 and which interface is eth1, perform the following:

a. Select the interface.

b. Click **Actions** > **Manage IP addresses**.

The port label appears.

c. Click **Cancel** to return to the previous screen.



Deploying a Virtual Appliance as a Traffic Mirror Target

Procedure

1. Configure the traffic mirror filter.

   For details, see https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-filters.html.

   a. Open the **Amazon VPC** console at https://console.aws.amazon.com/vpc/.

   b. In the **Region** selector, select the AWS Region that you used when you created the VPCs.

   c. On the navigation pane, go to **Traffic Mirroring** > **Mirror Filters**.

d. Select **Create traffic mirror filter**.

e. For **Name tag**, type a name for the traffic mirror filter.

   For example, type `demo-traffic-mirror-filter`.

f. (Optional) For **Description**, type a description for the traffic mirror filter.

   For example, type `demo-traffic-mirror-filter`.

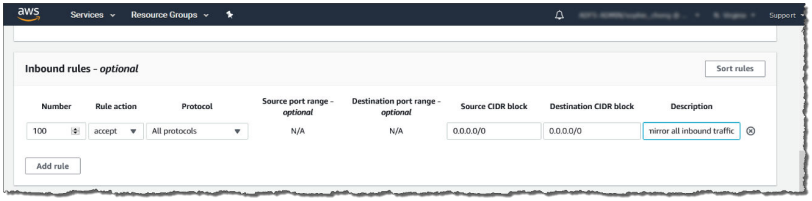
g. Select **amazon-dns**.

h. Add inbound rules. Select **Inbound rules** > **Add** > **rule**, and then specify the following information about the traffic mirror source inbound traffic:

- **Rule number**: Type a priority to assign to the rule.
- **Rule action**: Select the action to take for the packet.
- **Protocol**: Select the L4 protocol to assign to the rule.
- (Optional) **Source port range**: Type the source port range.
- (Optional) **Destination port range**: Type the destination port range.
- **Source CIDR block**: Type a source CIDR block.
- **Destination CIDR block**: Type a destination CIDR block.
- (Optional) **Description**: Type a description for the rule.

The following is an example of the values.

- Rule number: Use the default number
- Rule action: Select **accept**.
- Protocol: Select **All protocols**.
- Source CIDR block: Type `0.0.0.0/0`.
- Destination CIDR block: Type `0.0.0.0/0`.
- Description: Type `mirror all inbound traffic`.

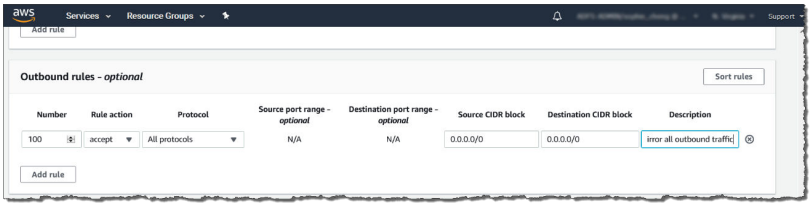


i. Add outbound rules. Select **Outbound rules** > **Add** > **rule**, and then specify the following information about the traffic mirror source outbound traffic:

- **Rule number**: Type a priority to assign to the rule.
- **Rule action**: Select the action to take for the packet.
- **Protocol**: Select the L4 protocol to assign to the rule.
- (Optional) **Source port range**: Type the source port range.
- (Optional) **Destination port range**: Type the destination port range.
- **Source CIDR block**: Type a source CIDR block.
- **Destination CIDR block**: Type a destination CIDR block.
- (Optional) **Description**: Type a description for the rule.

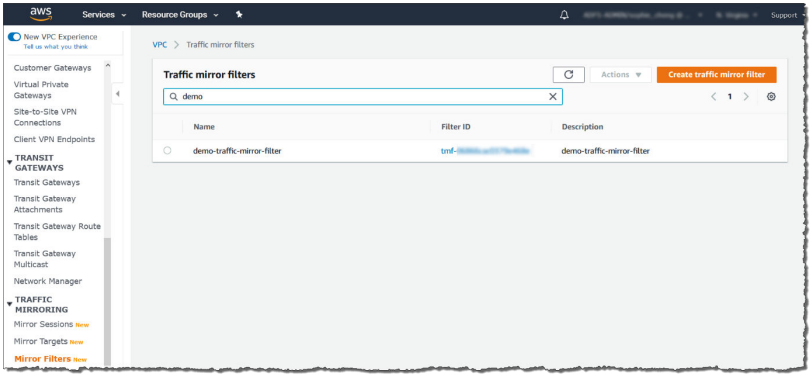
The following is an example of the values.

- Rule number: Use the default number
- Rule action: Select **accept**.
- Protocol: Select **All protocols**.
- Source CIDR block: Type `0.0.0.0/0`.
- Destination CIDR block: Type `0.0.0.0/0`.
- Description: Type `mirror all outbound traffic`.



j. Repeat the previous step for each inbound rule and outbound rule that you want to add.

k. Click **Create**.



2. Configure the traffic mirror target.

a. On the navigation pane, select **Traffic Mirroring** > **Mirror Targets**.

b. Select **Create Traffic Mirror Target**.

c. For **Name tag**, type a name for the traffic mirror target.

For example, type `demo-traffic-mirror-target`.

d. (Optional) For **Description**, type a description for the traffic mirror target.

For example, type `demo-traffic-mirror-target`.

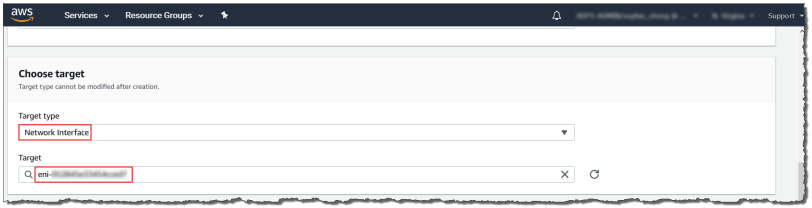
e. For **Target type**, select **Network Interface**.

f. For **Target**, select the Deep Discovery Inspector virtual appliance's eth0 (the data port that is connected to your subnet) as the traffic mirror target.

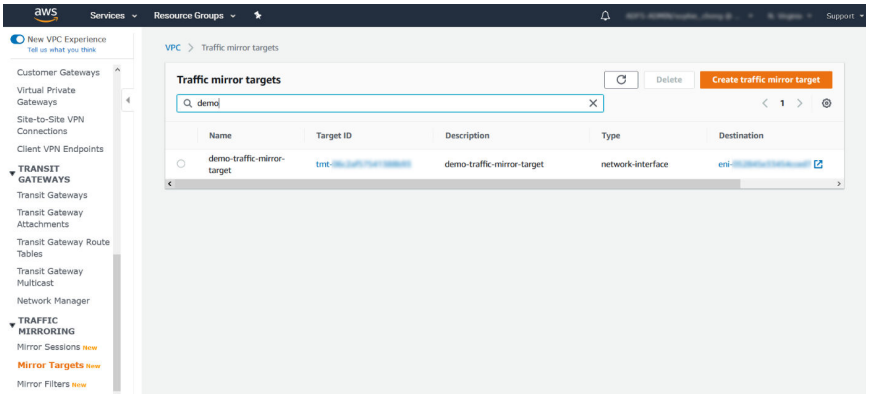
Note

You can select any other data port that you have attached on the Deep Discovery Inspector virtual appliance, such as eth2, or eth3.

Do not select the eth1 port that is used as the management port for the Deep Discovery Inspector virtual appliance.



g. Click **Create**.



3. Repeat the previous step to create a traffic mirror target for each Deep Discovery Inspector virtual appliance in your AWS environment.

4. Configure the traffic mirror session.

   a. On the navigation pane, select **Traffic Mirroring** > **Mirror Sessions**.

   b. Select **Create traffic mirror session**.

   c. For **Name tag**, type a name for the traffic mirror session.

      For example, type `demo-traffic-mirror-session`.

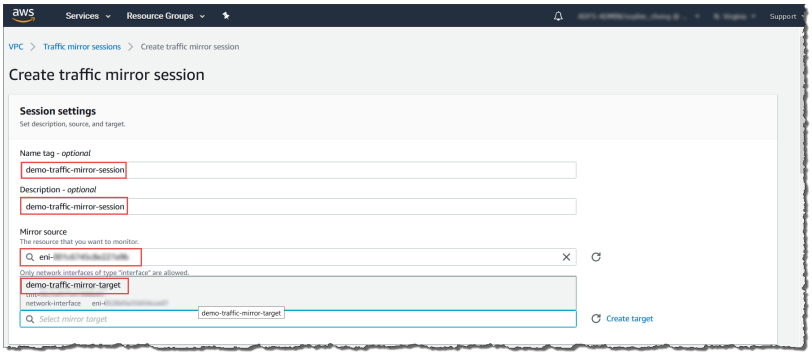
   d. (Optional) For **Description**, type a description for the traffic mirror session.

      For example, type `demo-traffic-mirror-session`.

   e. For **Mirror source**, select the network interface of the instance that you want to monitor.

   f. For **Mirror target**, select the traffic mirror target.

      For example, select **demo-traffic-mirror-target**.



g. Under **Additional settings**, perform the following:

- For **Session number**, type the session number `1`.

  The session number determines the order that the traffic mirror sessions are evaluated in both of the following situations:

  - When an interface is used by multiple sessions
  - When an interface is used by different traffic mirror targets and traffic mirror filters.

  Traffic is only mirrored one time. Use `1` for the highest priority. Valid values are 1-32766.

- (Optional) For **VNI**, type the VXLAN ID to use for the traffic mirror session.

  For details, see https://tools.ietf.org/html/rfc7348.

  If you do not specify a value, AWS assigns a random, unused number.

- (Optional) For **Packet Length**, type the number of bytes in each packet to mirror.

  If you do not want to mirror the entire packet, set **Packet Length** to the number of bytes in each packet to mirror. For example, if you set this value to 100, the first 100 bytes after the

VXLAN header that meet the filter criteria are copied to the target.

To mirror the entire packet, do not enter a value in this field.

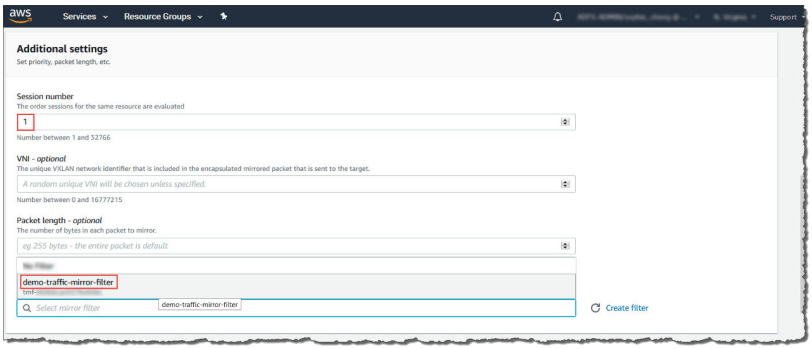
- For **Filter**, select the traffic mirror filter that determines what traffic gets mirrored.

  For example, select **demo-traffic-mirror-filter**.

- (Optional) Under the **Tags** section, add or remove a tag.

The following are example settings.

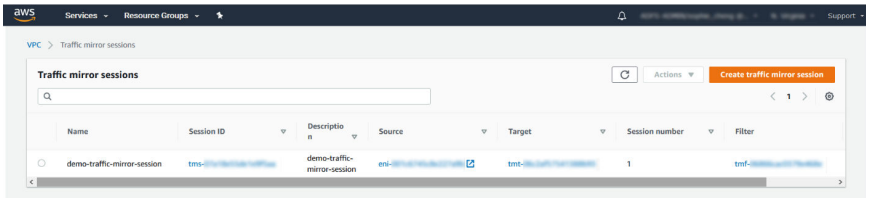
- For **Session number**, type the session number 1.
- For **VNI**, leave the value empty. AWS will assign a random number.
- For **Packet Length**, leave the value empty. AWS will mirror the entire packet.
- For **Filter**, select **demo-traffic-mirror-filter**.



h. Click **Create**.

Note

For more details, see *Working with Traffic Mirroring* at https://docs.aws.amazon.com/vpc/latest/mirroring/working-with-traffic-mirroring.html.



5. Repeat the previous step to create more traffic mirror sessions when there are multiple sources that you want to monitor.

Deploying a Virtual Appliance Behind an NLB

Procedure

1. Configure a load balancer and a listener.

   a. Open the **Amazon EC2** console at https://console.aws.amazon.com/ec2/.

   b. On the navigation pane, under **LOAD BALANCING**, select **Load Balancers**.

   c. Select **Create Load Balancer**.

   d. For **Network Load Balancer**, select **Create**.

   e. For **Name**, type a name for your load balancer.

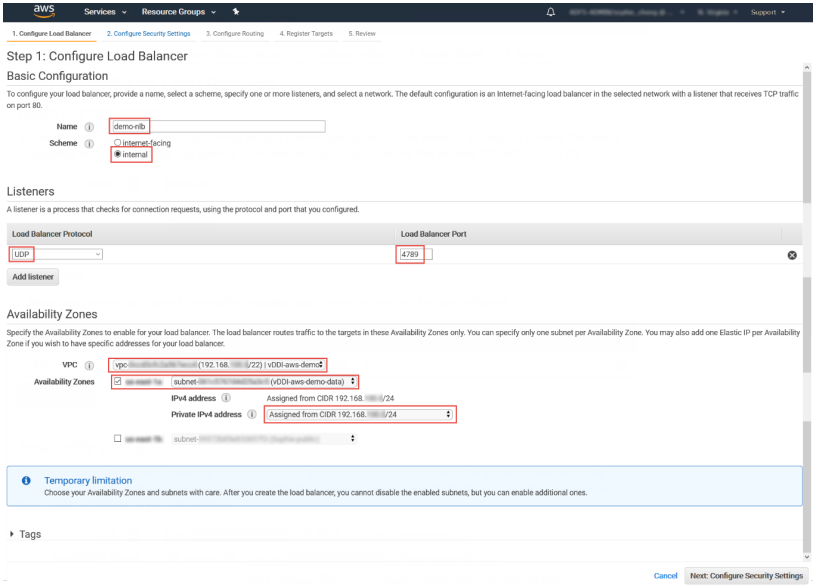
      For example, type `demo-nlb`.

   f. For **Scheme**, select **internal**.

   g. For **Listeners**, modify protocol to **UDP** and type `4789` for the port to receive mirrored traffic.

   h. For **Availability Zones**, select the VPC that you used for the Deep Discovery Inspector virtual appliance instance and select the subnet for the data port 1 (known as eth0) subnet.

i. For **IPv4 address**, you can select **Assigned from CIDR** to have AWS assign the address or select **Enter IP from CIDR** to specify the address.



j. Click **Next: Configure Security Settings**.

2. Configure the security settings.

   a. No changes are necessary in the **Configure Security Settings** screen.

   b. Click **Next: Configure Routing**.

3. Configure a target group.

   a. For **Target group**, keep the default, **New target group**.

   b. For **Name**, type a name for the target group.

      For example, type `demo-target-group`.

   c. For **Target type**, select **Instance**.

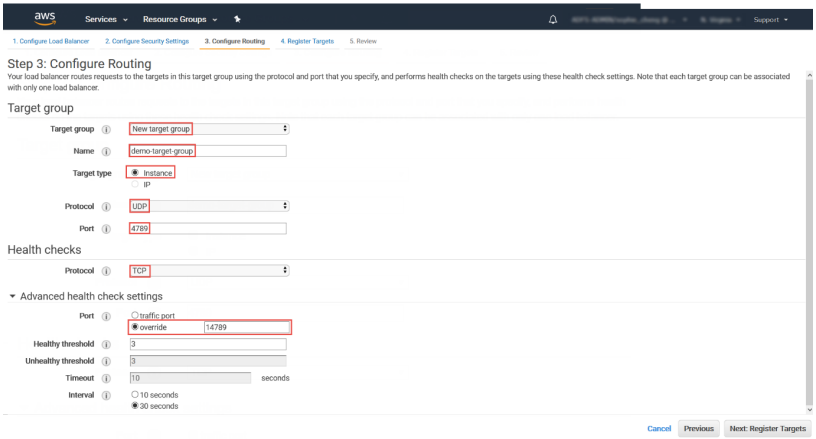
d. For **Protocol**, select **UDP**.

e. For **Port**, type `4789`.

f. For **Protocol** under **Health checks**, select **TCP**.

g. For **Port** under **Advanced health check settings**, select **override** and type `14789` for the port.

h. Leave other settings as default.



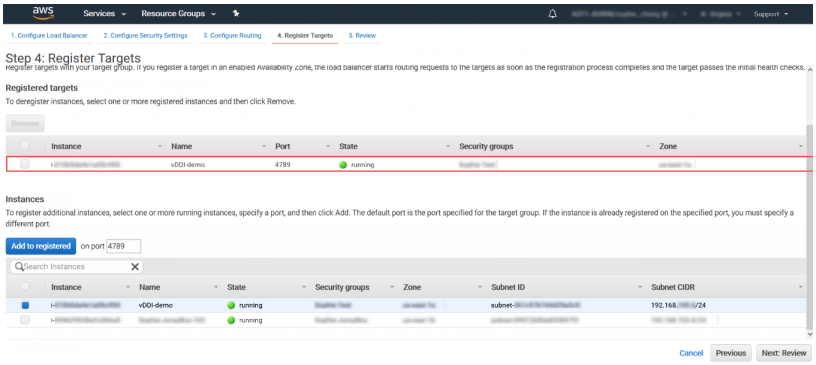
i. Click **Next: Register Targets**.

4. Register targets with the target group.

a. For **Instances**, select the Deep Discovery Inspector virtual appliance.

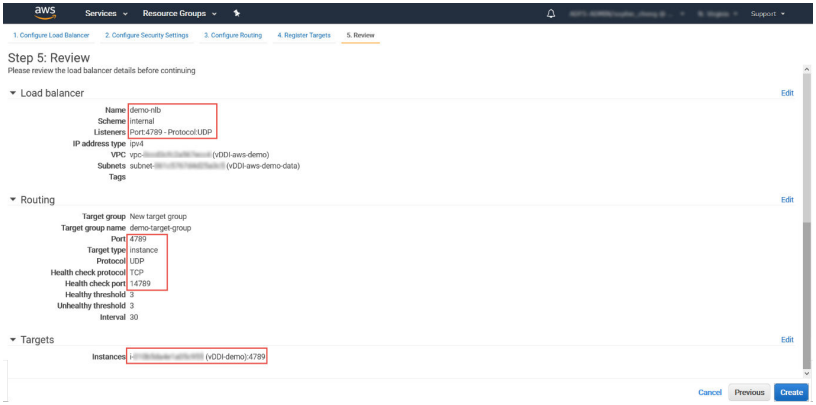
For example, select **demo-ddi**.

b. Keep the default instance listener port and select **Add to registered**.



c. Click **Next: Review**.

The **Review** screen appears.



5. Create the load balancer.

a. On the **Review** screen, click **Create**.

b. After the load balancer is created, click **Close**.

c. On the navigation pane, under **LOAD BALANCING**, select **Target Groups**.

d. Select the newly created target group.

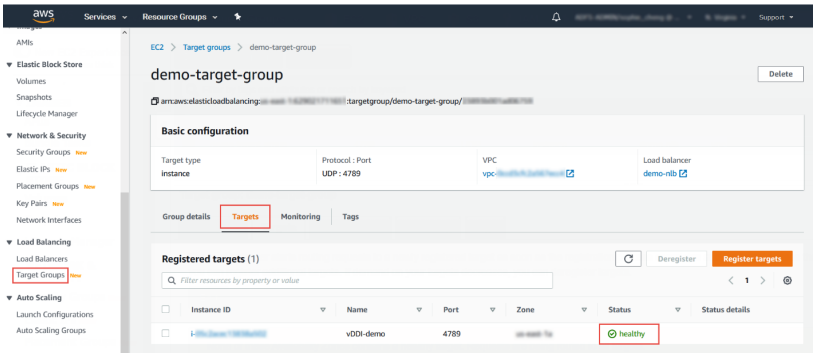
For example, select **demo-target-group**.

e. Select **Targets** and verify that your instances are ready.

Note

If the status of an instance is initial, it's probably because the instance is still in the process of being registered, or it has not passed the minimum number of health checks to be considered healthy. After the status of at least one instance is healthy, you can test your load balancer.

If the Deep Discovery Inspector virtual appliance is launched after the NLB was created, use **Register targets** to add the Deep Discovery Inspector virtual appliance to the NLB target groups. For more details, see https://docs.aws.amazon.com/elasticloadbalancing/latest/network/target-group-register-targets.html.



6. Configure the traffic mirror filter.

For details, see https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-filters.html.

a. Open the **Amazon VPC** console at https://console.aws.amazon.com/vpc/.

b. In the **Region** selector, select the AWS Region that you used when you created the VPCs.

c. On the navigation pane, go to **Traffic Mirroring** > **Mirror Filters**.

d. Select **Create traffic mirror filter**.

e. For **Name tag**, type a name for the traffic mirror filter.

   For example, type `demo-traffic-mirror-filter`.

f. (Optional) For **Description**, type a description for the traffic mirror filter.

   For example, type `demo-traffic-mirror-filter`.

g. (Optional) For **Network services**, select **amazon-dns**.

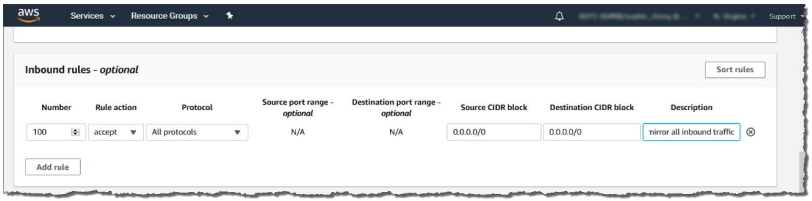
h. Add inbound rules. Select **Inbound rules** > **Add** > **rule**, and then specify the following information about the traffic mirror source inbound traffic:

- **Rule number**: Type a priority to assign to the rule.
- **Rule action**: Select an action to take for the packet.
- **Protocol**: Select a L4 protocol to assign to the rule.
- (Optional) **Source port range**: Type a source port range.
- (Optional) **Destination port range**: Type a destination port range.
- **Source CIDR block**: Type a source CIDR block.
- **Destination CIDR block**: Type a destination CIDR block.

- (Optional) **Description**: Type a description for the rule.

The following is an example of the values.

- **Rule number**: Use the default number
- **Rule action**: Select **accept**
- **Protocol**: Select **All protocols**
- **Source CIDR block**: Type `0.0.0.0/0`.
- **Destination CIDR block**: Type `0.0.0.0/0`.
- **Description**: Type `mirror all inbound traffic`.

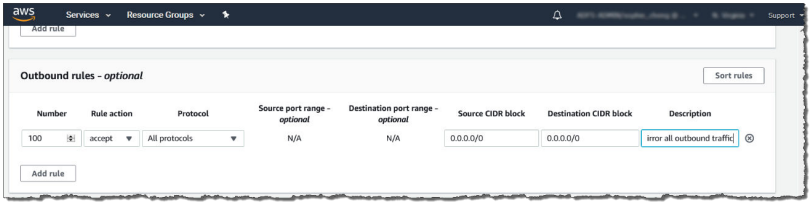


i. Add outbound rules. Select **Outbound rules** > **Add** > **rule**, and then specify the following information about the traffic mirror source outbound traffic:

- **Rule number**: Type a priority to assign to the rule.
- **Rule action**: Select an action to take for the packet.
- **Protocol**: Select a L4 protocol to assign to the rule.
- (Optional) **Source port range**: Type a source port range.
- (Optional) **Destination port range**: Type a destination port range.
- **Source CIDR block**: Type a source CIDR block.
- **Destination CIDR block**: Type a destination CIDR block.
- (Optional) **Description**: Type a description for the rule.

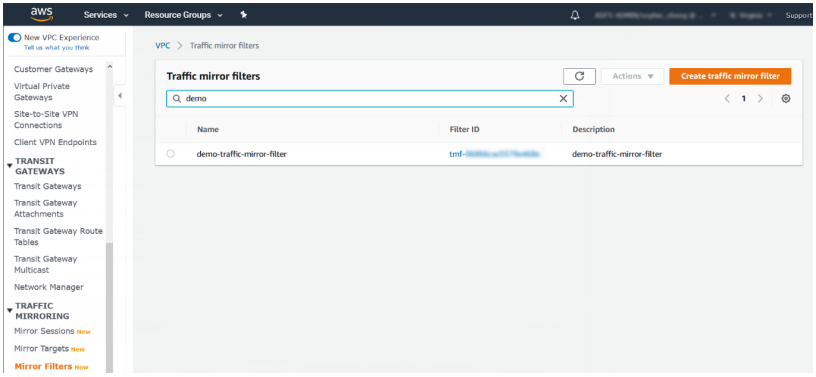
The following is an example of the values.

- **Rule number**: Use the default number
- **Rule action**: Select **accept**
- **Protocol**: Select **All protocols**
- **Source CIDR block**: Type `0.0.0.0/0`.
- **Destination CIDR block**: Type `0.0.0.0/0`.
- **Description**: Type `mirror all outbound traffic`.



j. Repeat the previous step for each inbound rule and outbound rule that you want to add.

k. Click **Create**.



7. Configure the traffic mirror target.

a. Open the **Amazon VPC** console at https://console.aws.amazon.com/vpc/.

b. In the **Region** selector, select the AWS Region that you used when you created the VPCs.

c. On the navigation pane, go to **Traffic Mirroring** > **Mirror Targets**.

d. Select **Create Traffic Mirror Target**.

e. For **Name tag**, type a name for the traffic mirror target.

For example, type `demo-traffic-mirror-target`.

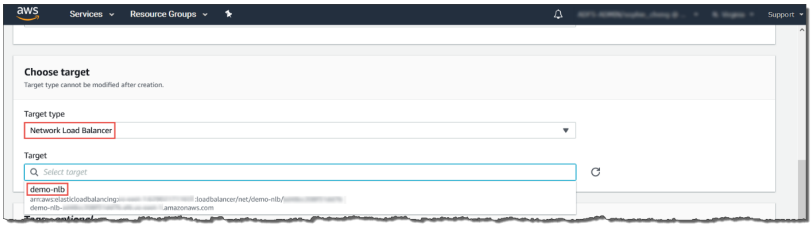
f. (Optional) For **Description**, type a description for the traffic mirror target.

For example, type `demo-traffic-mirror-target`.

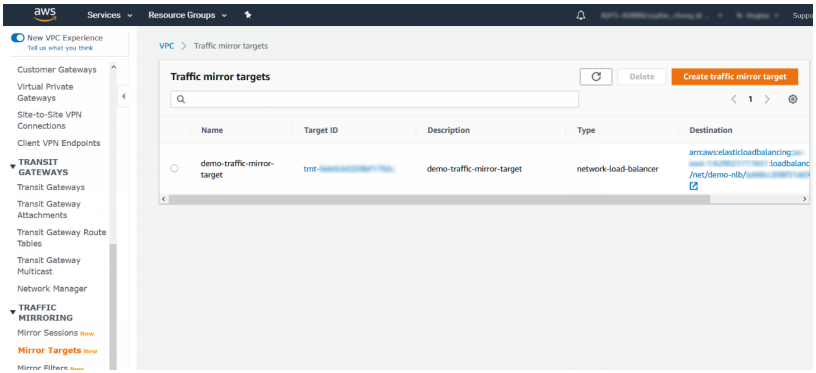
g. For **Target type**, select **Network Load Balancer.**

h. For **Target**, select a Network Load Balancer as the traffic mirror target.

For example, select **demo-nlb**.



i. Click **Create**.



8. Configure the traffic mirror session.

a. On the navigation pane, select **Traffic Mirroring** > **Mirror Sessions**.

b. Select **Create traffic mirror session**.

c. For **Name tag**, type a name for the traffic mirror session.

For example, type `demo-traffic-mirror-session`.

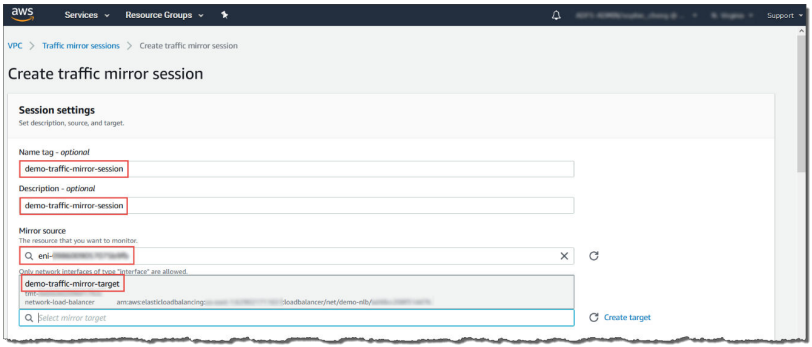
d. (Optional) For **Description**, type a description for the traffic mirror session.

For example, type `demo-traffic-mirror-session`.

e. For **Mirror source**, select the network interface of the instance that you want to monitor.

f. For **Mirror target**, select the traffic mirror target.

For example, select **demo-traffic-mirror-target**.



g. Under **Additional settings**, perform the following:

- For **Session number**, type the session number 1.

  The session number determines the order that traffic mirror sessions are evaluated in both of the following situations:

  - When an interface is used by multiple sessions.
  - When an interface is used by different traffic mirror targets and traffic mirror filters.

  Traffic is only mirrored one time. Use 1 for the highest priority. Valid values are 1-32766.

- (Optional) For **VNI**, type the VXLAN ID to use for the traffic mirror session.

  For details, see https://tools.ietf.org/html/rfc7348.

  If you do not specify a value, AWS assigns a random, unused number.

- (Optional) For **Packet Length**, type the number of bytes in each packet to mirror.

  If you do not want to mirror the entire packet, set **Packet Length** to the number of bytes in each packet to mirror. For example, if you set this value to 100, the first 100 bytes after the VXLAN header that meet the filter criteria are copied to the target.

To mirror the entire packet, do not enter a value in this field.

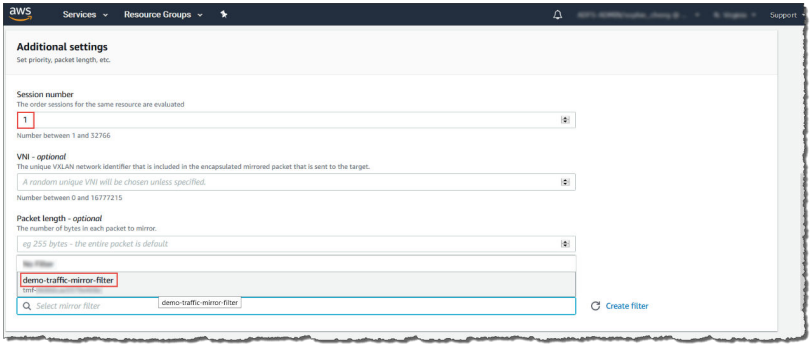
- For **Filter**, select the traffic mirror filter that determines what traffic gets mirrored.

  For example, select **demo-traffic-mirror-filter**.

- (Optional) Under the **Tags** section, add or remove a tag.

The following are example settings.

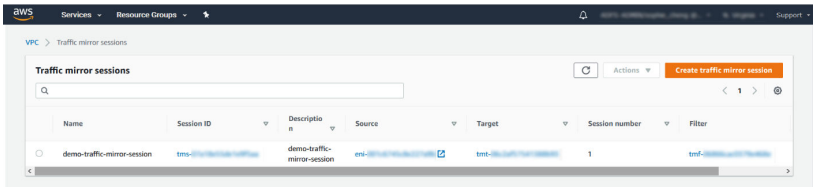
- For **Session number**, type the session number 1.
- For **VNI**, leave the value empty. AWS will assign a random number.
- For **Packet Length**, leave the value empty. AWS will mirror the entire packet.
- For **Filter**, select **demo-traffic-mirror-filter**.



h. Click **Create**.

Note

For more details, see https://docs.aws.amazon.com/vpc/latest/mirroring/working-with-traffic-mirroring.html.



9. Repeat the previous step to create more traffic mirror sessions when there are multiple sources that you want to monitor.

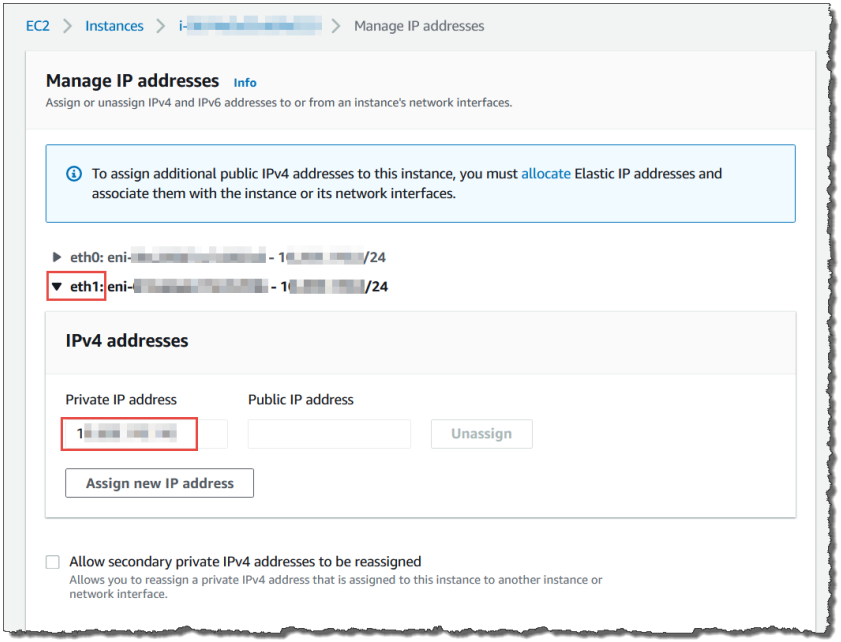
Chapter 4

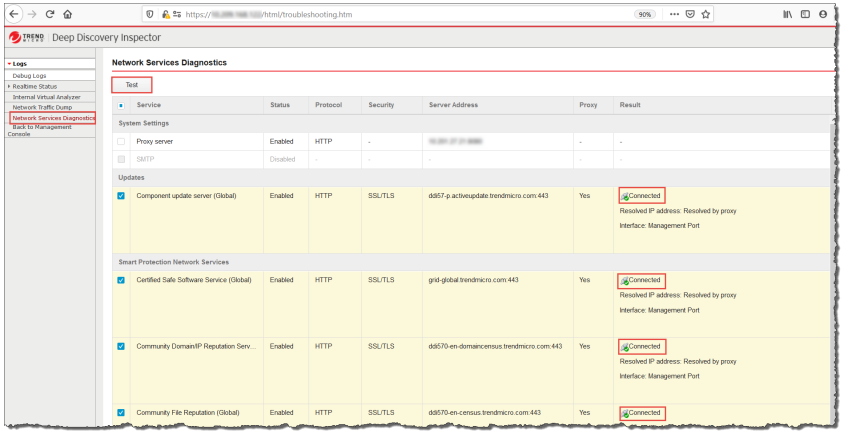
Deployment Testing and Troubleshooting

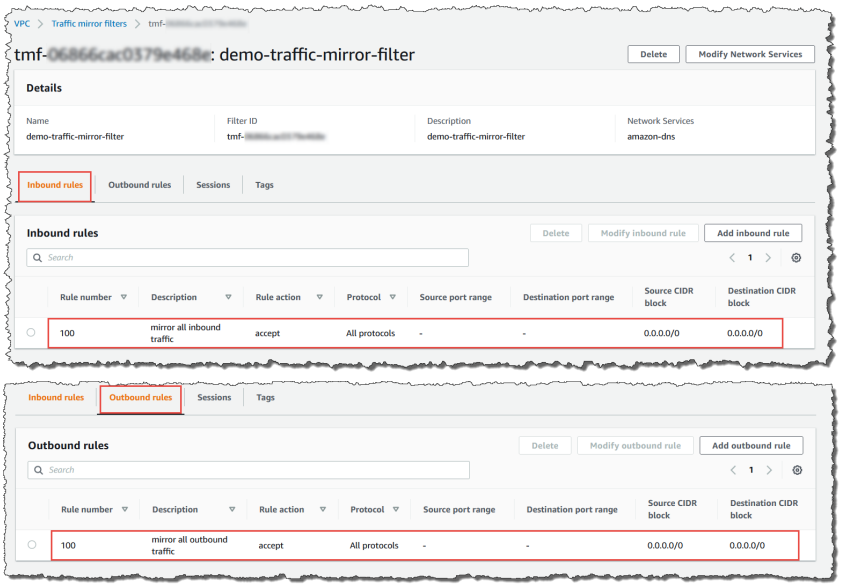
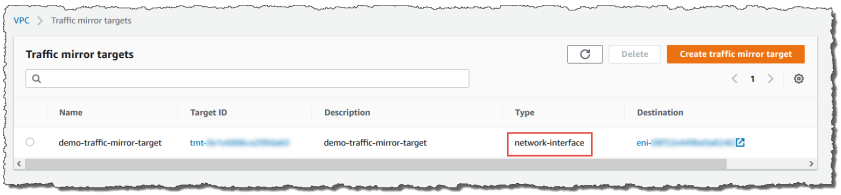
Checkpoints

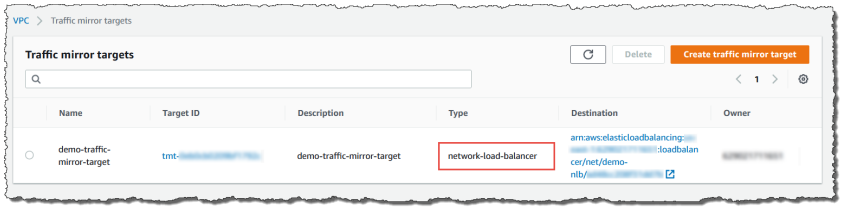
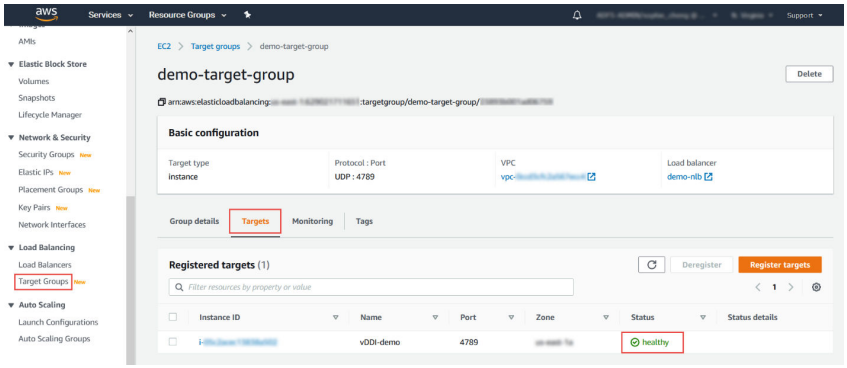
Pass the following checkpoints to ensure that the deployment is successful.

TABLE 4-1. Checkpoints

#	DESCRIPTION
1	Use an IPv4 address to log in to the management console of the Deep Discovery Inspector virtual appliance. You can find the management IP address on the Amazon EC2 console by following the steps below. 1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/. 2. In the navigation pane, select **Instances**. 3. Select the Deep Discovery Inspector virtual appliance. 4. Select **Actions** > **Networking** > **Manage IP Addresses**. 5. Expand **eth1**. The **Private IP Address** is the IP address of the management console for the Deep Discovery Inspector virtual appliance. 
2	Active the Deep Discovery Inspector appliance with the Activation Code.

#	Description
3	Update the components on the Deep Discovery Inspector appliance.
4	Follow the steps below to perform a network services diagnostic test on the Deep Discovery Inspector appliance and verify that all the tests are successful. 1. Go to `https://<virtual appliance IP address>/html/troubleshooting.htm` and click **Network Services Diagnostics**. 2. Select one or more enabled services and click **Test**. 3. When there are no connection issues, the result of all tested services is **Connected**. 

#	Description
5	Verify that the traffic mirror filter contains rules allowing the HTTP protocol in both inbound and outbound traffic. 
6	If you deploy Deep Discovery Inspector as the traffic mirror target, verify that the mirror target, for example **demo-traffic-mirror-target**, is configured with destination to the Deep Discovery Inspector virtual appliance. 

#	Description
7	If you deploy Deep Discovery Inspector behind the NLB, verify that the mirror target, for example **demo-traffic-mirror-target**, is configured with destination to the NLB. 
8	Verify that the mirror session, for example **demo-traffic-mirror-session**, is configured properly for the following fields: • Source • Target • Session number • Filter
9	If you deploy Deep Discovery Inspector behind the NLB, verify that the status of the registered instance in the target group, for example **demo-target-group**, is healthy. 

Testing the Deployment

You can perform the following steps to validate the Deep Discovery Inspector virtual appliance deployment:

Procedure

1. Perform an EICAR download on your test EC2 instance.

   The following example is for a Linux instance.

   Your testing EC2 instance must be configured as the traffic mirror source when Deep Discovery Inspector is deployed as a traffic mirror target and when Deep Discovery Inspector is deployed behind and NLB.

   In the example below, replace `hxxp` with `http`.

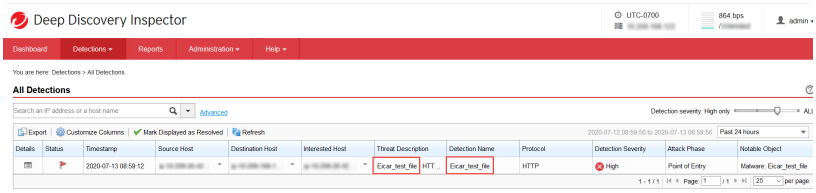
   ```
   ~$ curl -o /dev/null hxxp://2016.eicar.org/download/eicar.com
   ```

2. Verify the detection on the Deep Discovery Inspector virtual appliance.

   a. Log in to the management console of the Deep Discovery Inspector virtual appliance.

   b. Go to **Detections** > **All Detections**.

   c. Verify that the EICAR object was detected.

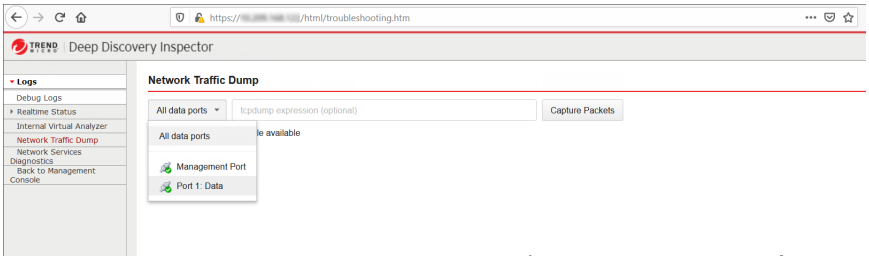


Troubleshooting the Deployment

The following are several tips for troubleshooting packet reception issues on Amazon EC2.

- Use the Deep Discovery Inspector virtual appliance Network Traffic Dump

  On the Deep Discovery Inspector virtual appliance, go to **Troubleshooting** > **Network Traffic Dump** and capture packets to check the data port's reception.



- Verify Network ACLs settings

  For details, see https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html.

- Verify Security Group settings

  For details, see https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html. For the traffic mirror target, the traffic mirror target requires the allowance of **VXLAN traffic (UDP port 4789)** from the traffic mirror source in the security groups that are associated with the traffic mirror target.

Note

If you are using deploying Deep Discovery Inspector behind an NLB, you may need to allow **custom traffic (TCP port 14789)** to the Deep Discovery Inspector virtual appliance in the security groups that are associated with the Deep Discovery Inspector virtual appliance.

Frequently Asked Questions

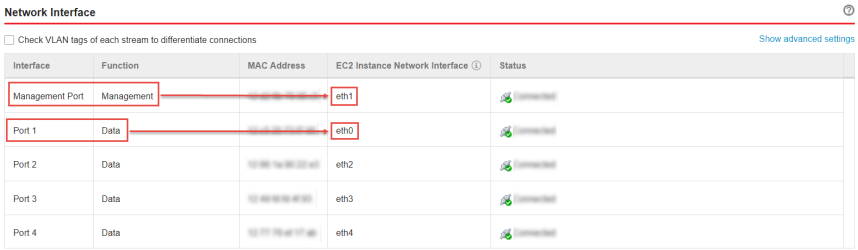
What are the changes on the Deep Discovery Inspector virtual appliance on AWS?

In order to adapt into the AWS environment, the Deep Discovery Inspector virtual appliance has some minor changes. These changes do not impact any major features and are described in the following list.

- Swapping port enumeration for management port

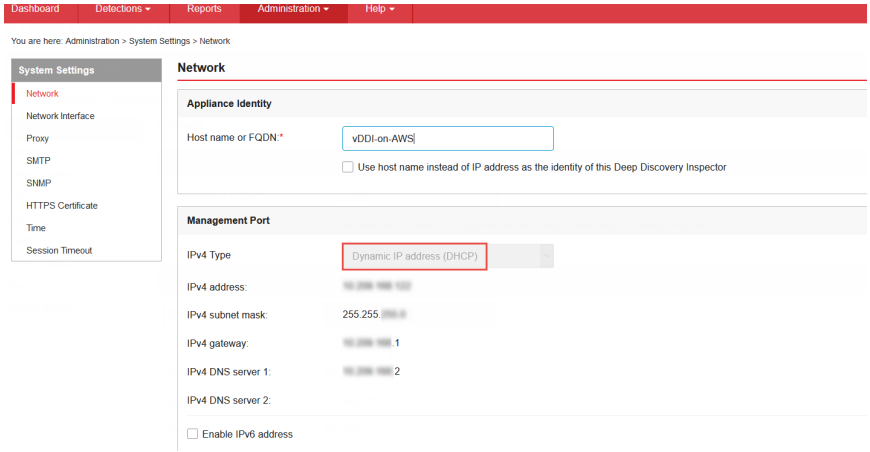
  The management port for Deep Discovery Inspector on-premises is fixed at the first NIC port (known as eth0). This change provides consistent information on Amazon EC2 console.

  The Deep Discovery Inspector virtual appliance swapped port enumeration for the management port to port 1 (known as eth1) and the data port to port 0 (known as eth0).



- IPv4 address for management port only supports DHCP

  Management ports configured as IPv4 only support DHCP. To modify the IPv4 address that is assigned, use the Amazon EC2 console.



To modify the IPv4 address that is assigned, perform the following steps on the Amazon EC2 console.

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.

2. In the navigation pane, select **Instances** and select the Deep Discovery Inspector virtual appliance.

3. Go to **Actions** > **Networking** > **Detach Network Interface**.

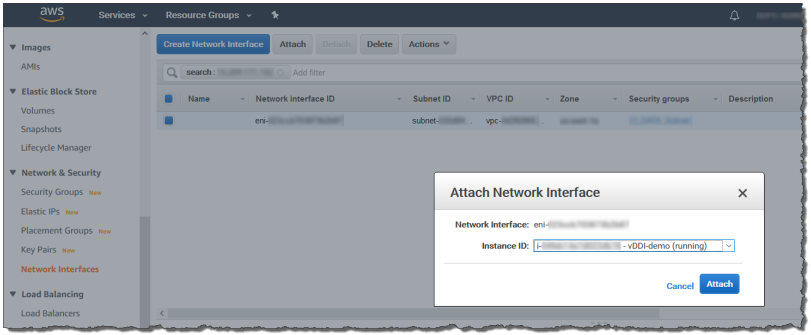
4. In the drop-down list, select **eth1** and click **Detach**.

5. In the navigation pane, select **Network interfaces**.

   You can create a network interface (For details, see https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html#create_eni) or find the IPv4 address that you want to attach to the management port of the Deep Discovery Inspector virtual appliance.

6. Select the network interface that you created or found in the previous step, and then click **Attach**.

7. Select the instance ID of the Deep Discovery Inspector virtual appliance, and then click **Attach**.



8. **Reboot** the Deep Discovery Inspector virtual appliance.

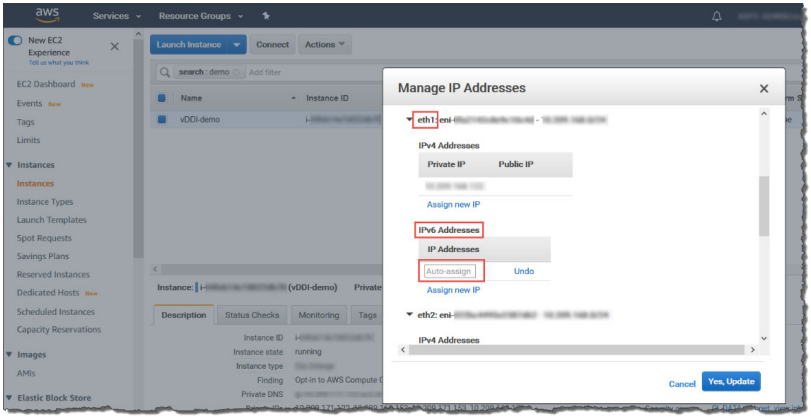
9. Verify that the management port (eth1) of the Deep Discovery Inspector virtual appliance is assigned to the new IPv4 address.

- IPv6 address for management port only supports DHCP

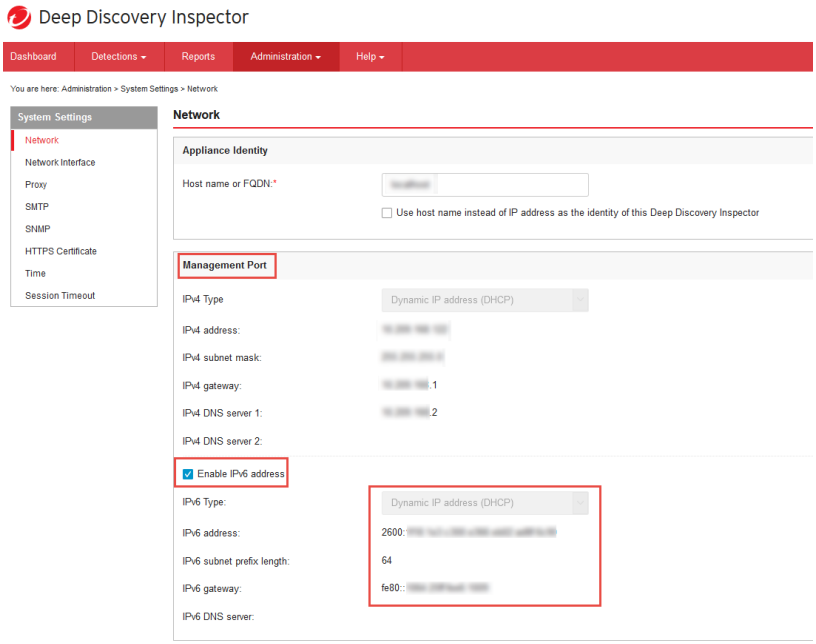
  On AWS, the IPv6 address is managed on the Amazon EC2 console. The Deep Discovery Inspector virtual appliance on AWS retrieves the IPv6 address automatically when IPv6 is assigned to a network interface on the Amazon EC2 console.

  To assign an IPv6 address, perform the following steps.

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. In the navigation pane, select **Instances**.
3. Select the Deep Discovery Inspector virtual appliance, and then select **Actions** > **Networking** > **Manage IP Addresses**.
4. For **eth1**, under **IPv6 Addresses**, select **Assign new IP**. You can specify an IPv6 address in the subnet range, or leave the **Auto-assign** value to let Amazon choose an IPv6 address for you.

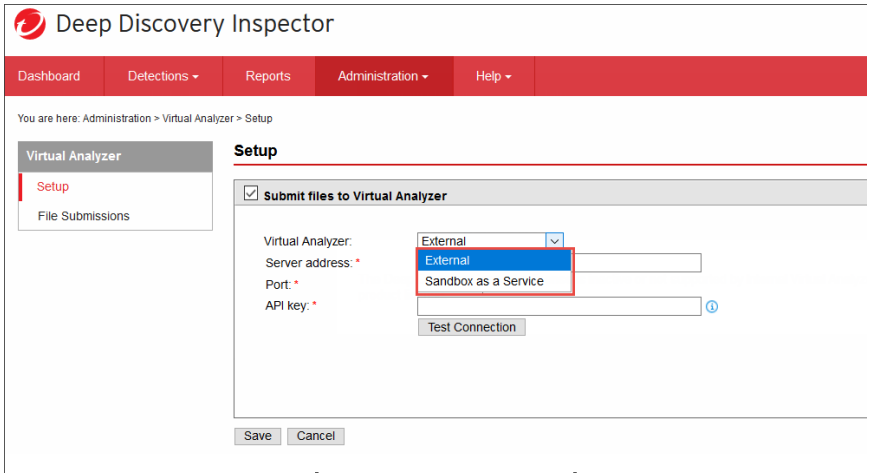


5. Click **Yes, Update**.
6. Log in to the management console of the Deep Discovery Inspector virtual appliance.
7. Go to **Administration** > **System Settings** > **Network**.
8. In **Management Port** section, select **Enable IPv6 address**.
9. Click **Save**.
10. **Reboot** the Deep Discovery Inspector virtual appliance.
11. Go to **Administration** > **System Settings** > **Network** and verify that the Deep Discovery Inspector virtual appliance is assigned an IPv6 address.



- No support for internal Virtual Analyzer

  When launching a Deep Discovery Inspector virtual appliance on AWS, only external Virtual Analyzer and Sandbox as a Service are supported.

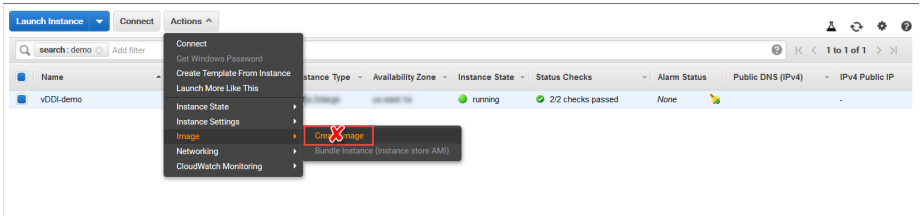


Does the Deep Discovery Inspector virtual appliance support AWS EC2 auto scaling?

No. The Deep Discovery Inspector virtual appliance does not support AWS EC2 auto scaling.

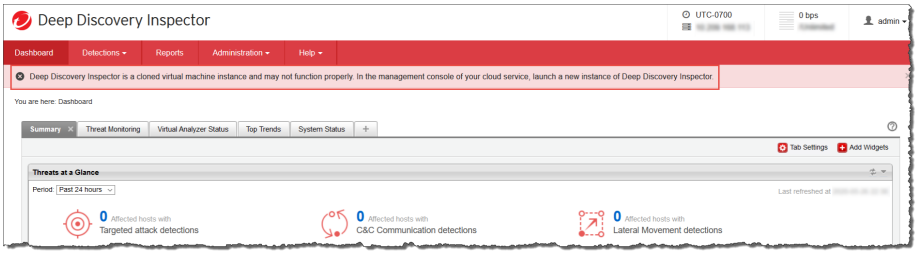
Does Deep Discovery Inspector support creating an Amazon Machine Image (AMI) from an EC2 instance of the Deep Discovery Inspector virtual appliance?

No. Deep Discovery Inspector does not support creating an AMI from an EC2 instance of the Deep Discovery Inspector virtual appliance.



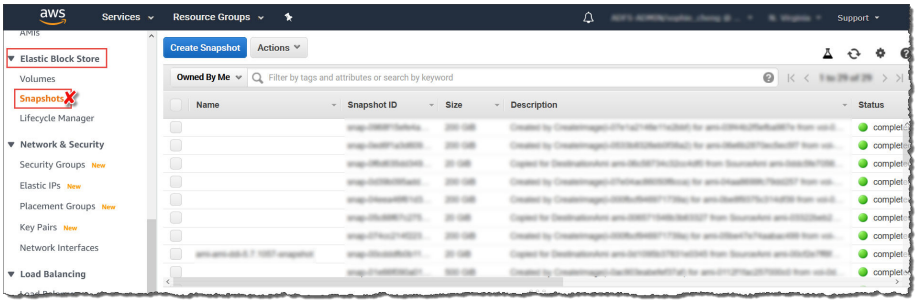
After installation, the Deep Discovery Inspector virtual appliance creates a UUID automatically and this UUID is used everywhere when communicating with Trend Micro global services. Creating a VM clone will corrupt the health status of bounded services.

If the Deep Discovery Inspector virtual appliance detects that the instance ID has changed, there is a warning message on the Deep Discovery Inspector virtual appliance management console.



Does Deep Discovery Inspector support creating an Elastic Block Store (EBS) snapshot from an EC2 instance of the Deep Discovery Inspector virtual appliance?

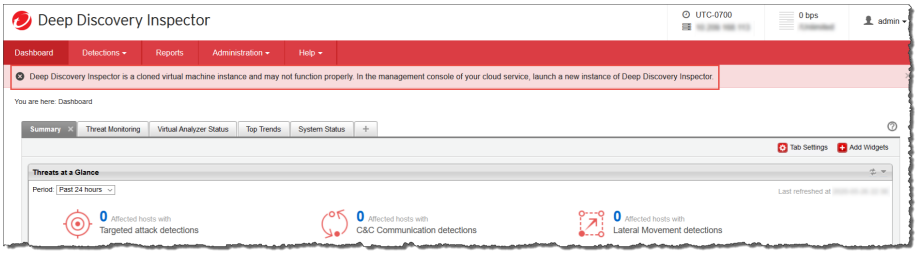
No. Deep Discovery Inspector does not support creating an EBS snapshot from an EC2 instance of the Deep Discovery Inspector virtual appliance.



After installation, the Deep Discovery Inspector virtual appliance creates a UUID automatically and this UUID is used everywhere when communicating

with Trend Micro global services. Creating a VM clone will corrupt the health status of bounded services.

If the Deep Discovery Inspector virtual appliance detects that the instance ID has changed, there is a warning message on the Deep Discovery Inspector virtual appliance management console.



TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: APEM59149/201116