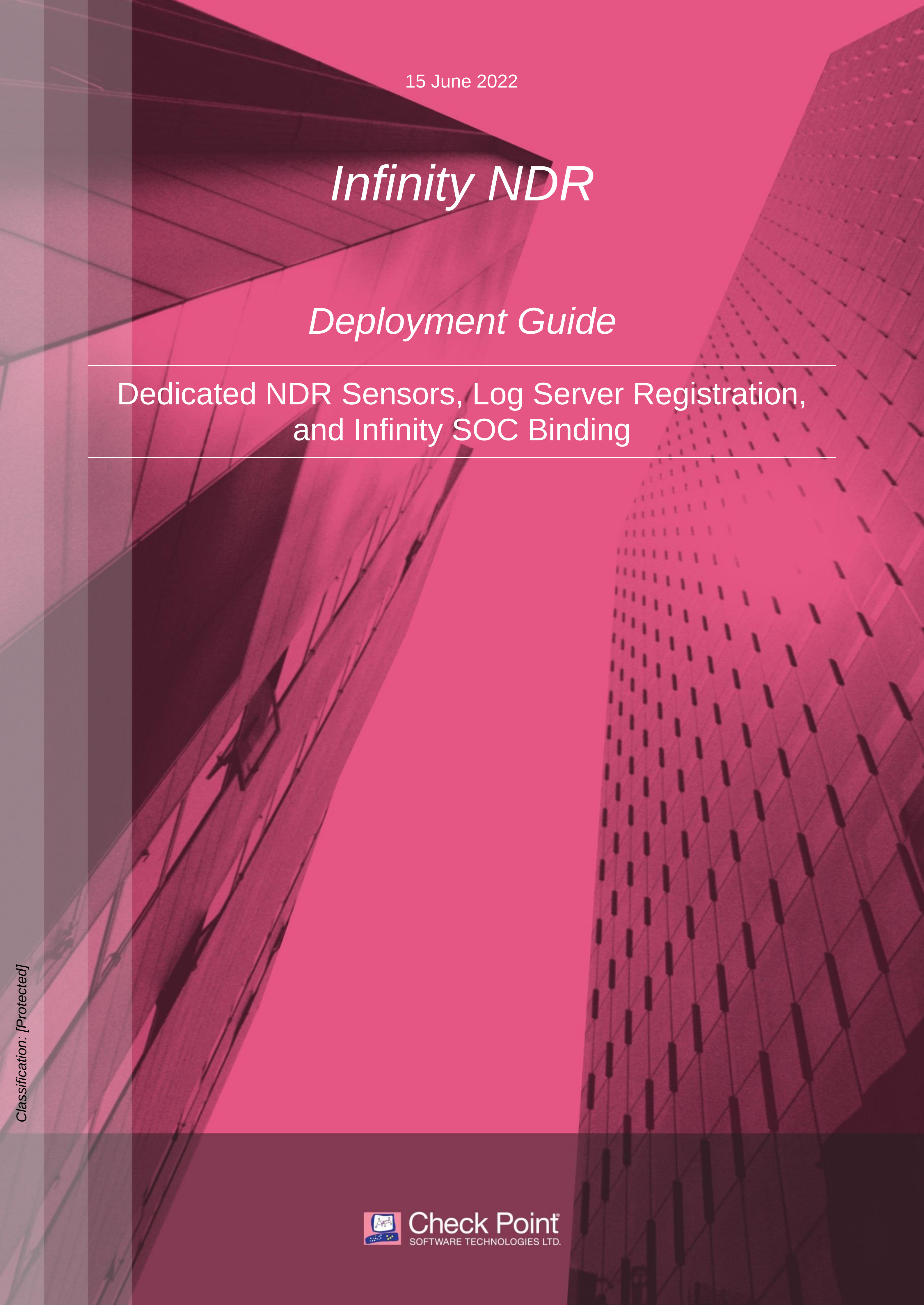


15 June 2022

Infinity NDR

Deployment Guide

Dedicated NDR Sensors, Log Server Registration, and Infinity SOC Binding

Classification: [Protected]

© 2022 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the Copyright page http://www.checkpoint.com/copyright.html for a list of our trademarks.

Refer to the Third Party copyright notices http://www.checkpoint.com/3rd_party_copyright.html for a list of relevant copyrights and third-party licenses.

Introduction

Check Point Infinity NDR is a comprehensive technology stack for Network Detection and Response. It consists of a back end service front-ended by a Web portal, hosted at https://now.checkpoint.com; and network sensors deployed on premises or in cloud environments.

The Check Point Infinity NDR operational concept is composed of the following flows:

- **Network traffic is analyzed by sensors, which generate analytical results in the form of logs**
- **Logs are transmitted to the NDR cloud for storage and analysis**
- Behavioral Analytics AI engines process the logs and generate analytical conclusions
- Human analysts are provided with event visualization tools for further data comprehension
- Data anomalies are incriminated through correlation with ThreatCloud intelligence and application risk scoring
- Analytical conclusions are published in the form of threat indicators and tags
- Threat indicators are also received from third party threat intelligence sources
- Indicators are applied by enforcement points and matched to network traffic, taking DETECT or PREVENT action

This article focuses on the deployment of sensors for the Infinity NDR application. You can achieve network visibility within minutes, with easy, intuitive deployment and minimal configuration effort, and with no impact on business traffic. There is no requirement for nor contention with other Check Point products to be present in the monitored environment.

Table of Contents

Infinity NDR Registration

Registering a Customer Domain

The Infinity NDR application is served at now.checkpoint.com. It is independent of the Infinity Portal. Infinity NDR maintains its own user and access authorizations repository.

Infinity NDR tenants are identified as ‘domains’. Each domain defines a set of objects, including sensors (that send logs to the Infinity NDR portal, stamped with the domain’s name); reports; user authorizations for accessing the domain; Intel indicators (IOCs); etc.

In order to create a domain, submit a new domain request via https://register.now.checkpoint.com/register. The Company Name you will enter will become the new domain name. It is recommended to subscribe to product news, as this will enable Check Point to notify you on maintenance alerts and security events as well. Once the request is approved, you will receive a confirmation email with a link to create your new Infinity NDR domain.

Access to Infinity NDR Portal

If this is your first domain on the portal, you will first be required to register user credentials for your new user account. This process installs a certificate in your browser, that will be used to identify and authenticate you to Infinity NDR on subsequent logins.

The certificate is generated on the portal, downloaded to your endpoint, and imported into your browser. Follow these steps to register the certificate:

a. You will be prompted for a password. This password will be used to encrypt your certificate when stored on disk. Enter the same password twice, and remember it for the next step.

b. Download the certificate to your endpoint by clicking “Download”.

c. It is recommended NOT to double-click the certificate object once downloaded. Doing so will launch the operating system’s certificate import wizard, and some browsers will not recognize it until they are completely restarted, typically requiring an endpoint reboot.

d. Instead, open browser Settings, go to Security > Management Certificates, and click “Import”.

e. Browse for the certificate on your disk and select it.
(In the browsing window you might be required to change the file type to "Personal Information Exchange" Or to "All files" in order to see your new downloaded certificate.)

f. The certificate should be loaded into the Personal certificate store (normally the default).

g. Complete the import process.

h. Sign into the Infinity NDR portal by pointing your browser to https://now.checkpoint.com. Click “Sign In”, and you will be prompted to select your certificate for accessing the portal.

i. Select the new domain you created above from the pull-down menu.

Forcing Chrome Browser Refresh

If after importing your new certificate into your browser you are not prompted for the certificate when trying to sign in, you might need to restart your browser in order to load the certificate into its Personal certificate store. The following procedure was tested to force Chrome browser on Windows to stop and refresh. Please make sure to save your work, use the history settings to relaunch all tabs.

a. Close all Chrome open instances

b. Use the "Windows Key" to search for "PowerShell". Hover over "Windows PowerShell" - right click on the PowerShell to select "Run as administrator".

c. Use the command "get -process -name Chrome | stop -process" to force-stop all Chrome related processes so the certificate will be activated.

Infinity NDR Sensors

Overview

Infinity NDR ingests network artifacts in the form of log records. Each record contains log fields that are extracted by a network sensor from the network traffic, including source and destination IP addresses, ports, amount of data transferred, URLs, application categorization, risk categorization, user identity, etc. In order to close the NDR Loop, threat indicators are delivered back to the sensor by the Infinity NDR Intel facility.

Supported sensor types include Check Point Security Gateways (Quantum, CloudGuard, and Quantum Spark), and Check Point Harmony Endpoint. Threat indicators can also be delivered to 3rd party devices.

Sensors can be NDR-Managed, in which case they are managed from a Management Server hosted by the Infinity NDR application. This means that you do not need to install a Management Server; nor SmartEvent; nor SmartConsole; nor provision policy. A non NDR-Managed sensor sends its logs to a Management Server or Log Server; Check Point Log Exporter is used to forward the logs to Infinity NDR for processing. In the non NDR-Managed case, the sensor must also be configured separately to subscribe to Infinity NDR Intel feeds.

Check Point Quantum NDR Sensors

You can easily convert any Check Point Quantum Security Gateway appliance into an NDR-Managed Infinity NDR sensor. The appliance’s control layer is then slaved to the Infinity NDR application, and all control layer communications, including policy, logs, ThreatCloud queries, NTP, DNS, etc. are tunneled over a mutually-authenticated SSL VPN tunnel to the Infinity NDR cloud. Traffic inspection is normally achieved via Monitor Mode interfaces attached to switch mirror ports. Inline deployment (Bridge Mode) is also supported – with fail-open network interfaces.

In NDR mode, the appliance applies Check Point’s real-time advanced SNBT threat detection engines on the mirrored network traffic, including: IDS/IPS, Application fingerprinting, Anti-Virus and Anti-Bot, and Threat Emulation (evasion-resistant sandboxing). Analytical conclusions are transmitted as log records to the Infinity NDR back end for further analysis.

Check Point CloudGuard NDR Sensors

The same NDR mode conversion process that is used for Quantum NDR sensors can also be applied on CloudGuard and Open Server Gaia installations.There are some differences in interface naming and licensing but the underlying SNBT functionality is the same on these sensors. However, virtualization impacts data layer attachment. In particular:

- Fail-open interfaces are unavailable – therefore inline deployment is not supported, only Monitor Mode
- CloudGuard for VMware ESX deployments operate similarly to physical appliances, via mirroring
- CloudGuard for AWS is provisioned automatically from the Infinity NDR application, using AWS Lambda serverless computing to manage cloud-native traffic mirroring APIs. The CloudGuard Network Security instance is deployed out of band for its Compute capabilities, with no impact to business traffic
- CloudGuard for GCP operates similarly to AWS, however mirroring is currently manually provisioned
- Alternatively for all environments, a CloudGuard Network Security instance can be deployed and converted into NDR mode; and traffic mirroring provisioned on a separate device (e.g. Check Point CloudGuard Network Security configured with a Mirror and Decrypt policy) over VXLAN

Log Server Registration

If you have a Check Point Management Server or Log Server that is collecting logs from Check Point Security Gateways and/or Check Point Harmony Endpoint, you can easily enable log export to Infinity NDR for NDR visualizations and analytics. The server is considered non NDR-Managed.

Preparing an Infinity NDR Sensor

Overview

This section details the process of converting a Check Point Quantum Security Gateway appliance into an NDR-Managed Infinity NDR sensor. The same process can be used for preparing a CloudGuard or Open Server-based Infinity NDR sensor.

Installing Check Point R81.10

Clean-install Check Point R81.10 on the appliance as a Quantum (or CloudGuard) Security Gateway, applying the latest R81.10 Jumbo Hotfix Accumulator. See sk170416 for detailed installation instructions.

Note - You do not need to install a Security Management Server. This function will be handled by Infinity NDR. Do not install the gateway as a Standalone (with Management) – this is not supported.

Determining Configuration Settings

In the process of installing the gateway, you will be provisioning the following configuration settings:

- Complete the First Time Wizard (FTW), establishing a routing path to the Internet, including:
  - Static IP address or DHCP on the appliance's Mgmt interface (eth0 on virtual instances)
  - Default gateway (if not using DHCP)
  - A DNS server IP (if not using DHCP) for initial domain name resolution
  - Proxy (if needed to connect out to the Internet)
  - Use any value for SIC activation key – this value will not be used but must be entered

- License - if you've reverted to factory defaults, the appliance should have a 14 day evaluation license. A paid-for Quantum appliance will automatically pull its license from the User Center. Otherwise install an evaluation license, or for a CloudGuard installation, a BYOL license.

- If preparing the appliance off-site (recommended), and the networking configuration is different from the target environment (e.g. different static IP address), you will later need to change the Mgmt interface's configuration. Before you do so, make sure that the registration sequence on the Infinity NDR portal has completed. Leave the appliance connected to the portal for about 15 minutes for engine updates to complete downloading.

Note - Once the registration process completes successfully, you will not be able to access the appliance remotely using SSH, WebUI. This is because the Infinity NDR sensor's control plane is tunneled over SSL VPN to the Infinity NDR portal and can only be managed from the Infinity NDR application. In addition, the admin password is automatically randomized.

See below, *Accessing the Sensor's Gaia Portal*, for post-registration maintenance.

Infinity NDR Sensors for VMware ESX Considerations

Installation on VMware ESX follows the same process as for a physical appliances, with the following caveats:

- At least 100GB disk space should be allocated for the sensor VM

- Allocate at least 2GB RAM per each processing core, with a minimum of 8GB RAM altogether

Required Access to the Infinity NDR Application Portal

Coordinate with the customer the following access rule authorizations:

- If there is a firewall on the path to the Internet, it must allow TCP port 443 connectivity from the appliance’s Mgmt interface to IP addresses 35.156.213.136, as well as to 18.196.115.85 (portal.now.checkpoint.com), and 35.157.19.226 (feeds.now.checkpoint.com).
- The NDR sensor authenticates to the Infinity NDR application portal using mutually-authenticated TLS; therefore if the customer is using HTTPS Inspection on the outbound path, you must request an exemption for the Infinity NDR appliance’s management traffic.
- An HTTPS Inspection exemption will also be required for user access to the Infinity NDR application portal at https://now.checkpoint.com.

Network Interfaces for Traffic Inspection

In most cases, you will be deploying the Infinity NDR sensor appliance passively, connected to one or more customer network switch’s mirroring (SPAN) ports. It is best to provision the monitor-mode interfaces on the appliances ahead of time. Identify which interfaces on the appliance will be used for this purpose, ensuring that they match the customer’s networking connections (i.e. fiber or copper) and speeds.

In some cases customers find challenges with provisioning SPAN ports[1]. An alternative connectivity option is inline bridge (bump in the wire). This is an easy-to-provision configuration, however it does not provide the East/West visibility that monitor-mode can. Its primary advantages are the ability to deliver on-box prevention, as well as inline HTTPS Inspection and Threat Extraction. Inline bridge deployment with Infinity NDR sensors is supported only when using a Check Point Quantum Security Gateway fitted with a fail-open network interface.

When a fail-open NIC is fitted, it should be installed in the appliance’s bay 1. A two port fiber fail-open NIC is automatically provisioned with a single two-interface bridge. A four port copper fail-open NIC provides two bridges. The odd-numbered interfaces on the card (eth1-01, and if available, eth1-03) are to be connected to the internal networking device, and the even-numbered interfaces to the external device. The bypass mode can be toggled from the Infinity NDR application portal’s Sensors tab, via Actions > BYPASS.

Notes – A common mistake is to connect the fail-open interface to a switch mirror (SPAN) port, instead of using it as a bridge. This can result in high CPU consumption and sensor instability.

Another problematic configuration is management-over-bridge: the appliance’s Mgmt interface is connected to an internal network, and the management traffic to the Infinity NDR portal is passed back through the appliance’s bridge. This configuration is supported, but results in the appliance disconnecting from Infinity NDR every time the fail-open NIC bypass mode is toggled. It is therefore recommended to connect Mgmt to a network segment on the external side of the Infinity NDR sensor.

When processing traffic from multiple interfaces, it is important to prevent a situation whereby the appliance sees the same packet twice (or more) from multiple interfaces, as this can result in sensor instability. This scenario can occur if multiple interfaces are seeing network segments that pass packets between them, without intervening NAT. For example, two internal networks that are not segmented by a NATing Security Gateway. In contrast, a valid deployment is to mirror a DMZ, and an internal network segment. Or, for the appliance to bridge between the firewall and the ISP router; and to monitor a SPAN port off a core switch. While each packet might indeed be seen twice by the appliance, egress hide-NAT on the firewall means that the two packets’ source IP addresses and ports are different.

Lights Out Management (LOM)

In some rare situations, an Infinity NDR sensor might lose its control connection to the cloud, and therefore can no longer be accessed from the Infinity NDR application. In these cases, a LOM module can be used to remotely reboot the appliance, or even provide access to the console interface. LOM configuration is peformed from the Gaia CLI, and must therefore be performed before the appliance is registered. See sk92652 for more details.

[1] See *Appendix A – SPAN Port Configuration* for command sequences used on common network switches.

Defining the Sensor on the Infinity NDR Application Portal

After all preparations have been completed, you may now proceed to sensor deployment.

1. Login to the Infinity NDR application portal and access the customer domain.

2. You will be directed to the Sensors tab, as there long as there are no sensors on the domain.

3. From the lefthand menu, select **Management** --> **Sensors** --> Click **New** (top middle).

4. For a Quantum Security Gateway appliance, select **Physical** and enter the appliance's MAC in colon-separated six tuple notation (e.g. 00:1C:7F:12:34:56). The MAC is printed on a pullout label on the appliance's front panel. In addition, it is the same as the appliance's Mgmt interface's MAC address.

5. When installing a CloudGuard Network Security Gateway or Open Server, select **Virtual** instead; a virtual MAC will be automatically generated to uniquely identify the sensor.

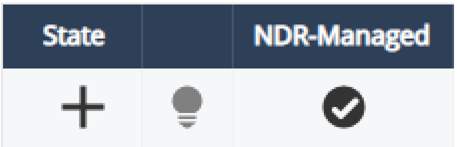
6. Enter a description/name for the sensor. Select the correct time zone. Then click ADD in the lower right corner of the new sensor form.

The sensor entry will now be displayed in the Sensors table with the following icons:

- State: "+", signifying that the sensor entry has been "Created".

- Connected indicator (lightbulb) is gray; this will turn green when the sensor establishes the TLS tunnel to the Infinity NDR portal.

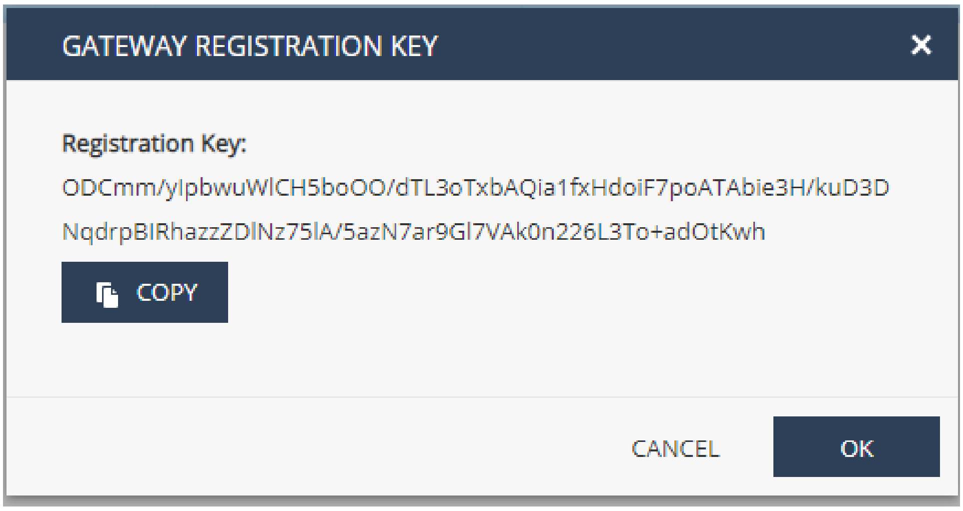
- NDR-Managed – the Infinity NDR application will be managing this gateway



State		NDR-Managed
+	💡	✓

7. Select the sensor entry (it will be highlighted in blue) and select "Generate Registration Key" from the Actions… menu.

The registration key will appear in a new pop-up window in the portal, e.g.:



GATEWAY REGISTRATION KEY

Registration Key:

ODCmm/ylpbwuWlCH5boOO/dTL3oTxbAQia1fxHdoiF7poATAbie3H/kuD3D
NqdrpBIRhazzZDlNz75lA/5azN7ar9Gl7VAk0n226L3To+adOtKwh

8. Copy the registration key for use on the appliance.

Registering the Appliance

1. In expert mode on the appliance, run a command as follows using the `<registration key>` obtained from the Infinity NDR application portal in step 5 above:

```
curl_cli -f -s -S --cacert $CPDIR/conf/ca-bundle.crt
https://portal.now.checkpoint.com/static/install.sh | bash /dev/stdin
--token <registration key> --monitor eth1 --monitor eth2-01
```

Note - Configure at least one interface in monitor-mode. In the example above, both eth1 and eth2-01 are set as monitor interfaces.

2. The machine will reboot automatically, and connect to Infinity NDR using the registration key.

3. On the Infinity NDR application portal, the Connected lightbulb will turn green; then the State icon will start turning signifying policy installation. Finally, the State icon will become a check mark (✓) – “Activated”.

Accessing the Sensor’s Gaia Portal

When an NDR-Managed sensor is activated and connected, it can be monitored and controlled only from the Infinity NDR application portal. Its resource consumption state (CPU, memory, disk) can be viewed by any user on the domain on which it’s registered, via the MANAGEMENT > System Monitor tab.

A user with Domain Administrator role on the domain will receive an additional option in the MANAGEMENT > Sensors tab’s Actions menu: “OPEN GAIA PORTAL”. Selecting the sensor and clicking this option will pop up the appliance’s Web UI in a new browser tab. This is intended to allow administrators to change interface mappings, view appliance status, and apply jumbo hotfix packages.

Infinity NDR Log Server Registration

Overview

Customers that already have a Check Point log server can send their logs to the Infinity NDR application using Check Point Log Exporter (sk122323), in addition to or instead of deploying dedicated Infinity NDR sensors. The Log Exporter configuration is packaged by the Infinity NDR application, and then downloaded to the customer’s log server and executed with a single command.

Prerequisites

- The Log Server must be running version R80.30 or higher

- If there is a firewall on the path to the Internet, it must allow TCP port 443 connectivity from the appliance’s Mgmt interface to IP addresses 35.156.213.136, 3.120.103.74, and 18.196.115.85 (portal.now.checkpoint.com).

- The Log Server authenticates to the Infinity NDR application portal using mutually-authenticated TLS; therefore if the customer is using HTTPS Inspection on the outbound path, you must request an exemption for the log export traffic from the Log Server

- An HTTPS Inspection exemption will also be required for user access to the Infinity NDR application portal at https://now.checkpoint.com

- In order for Infinity NDR to be effective, you should enable Extended Logging for the Application Control and URL Filtering blades on your Check Point gateways. Additional recommended blades include: IPS, Anti-Bot, Anti-Virus, and Threat Emulation.

Defining the Sensor on the Infinity NDR Application Portal

1. Login to the Infinity NDR application portal and access the customer domain.

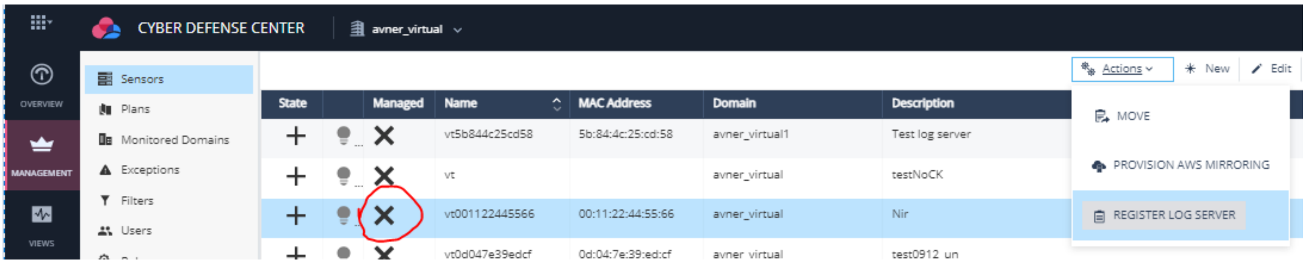
2. You will be directed to the Sensors tab, as long as there are no sensors on the domain.

3. From the lefthand menu, select **Management** --> **Sensors** --> Click **New** (top middle).

4. Deselect "NDR-Managed" – to create an "unmanaged" sensor. Do not enter a MAC.

5. Enter a description/name for the sensor. Select the correct time zone. Then click ADD in the lower right corner of the new sensor form.

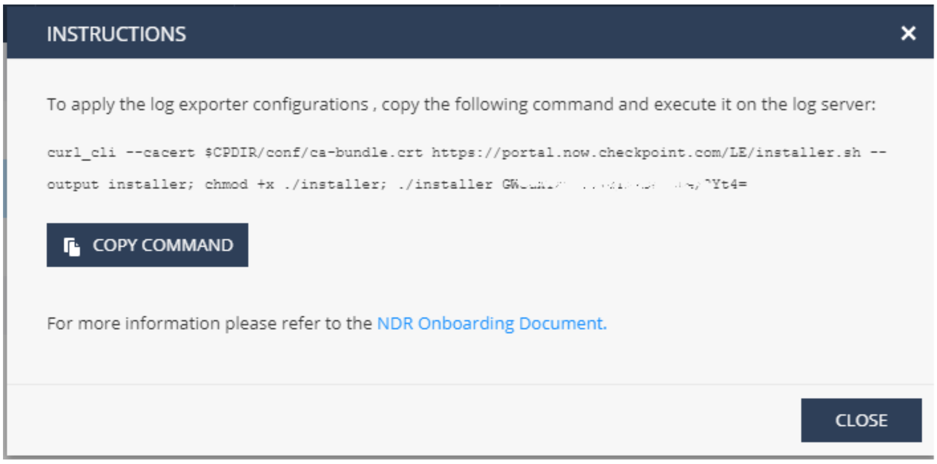
6. Click on the new sensor entry that you created in order to select it, and select "REGISTER LOG EXPORTER" from the Actions menu.



State		Managed	Name	MAC Address	Domain	Description
+	●	✕	vt5b844c25cd58	5b:84:4c:25:cd:58	avner_virtual1	Test log server
+	●	✕	vt		avner_virtual	testNoCK
+	●	✕	vt001122445566	00:11:22:44:55:66	avner_virtual	Nir
+	●	✕	vt0d047e39edcf	0d:04:7e:39:ed:cf	avner_virtual	test0912_un

7. On the confirmation pop up window click "CONTINUE".

8. COPY COMMAND to copy the personalized script to your clipboard:



To apply the log exporter configurations , copy the following command and execute it on the log server:

```
curl_cli --cacert $CPDIR/conf/ca-bundle.crt https://portal.now.checkpoint.com/LE/installer.sh --
output installer; chmod +x ./installer; ./installer GW[redacted]Yt4=
```

For more information please refer to the NDR Onboarding Document.

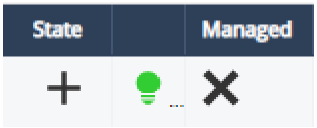
Registering the Log Server

1. Login to the Check Point log server in Expert Mode.

2. Paste the personalized script and hit "Enter".

3. If everything is working correctly, the script will execute cleanly and wish you a good day. If there is any error message, please contact the Check Point Infinity NDR team with the error details.

4. Once logs start flowing to NDR, the lightbulb icon next to the sensor will turn green:



Check Point Infinity NDR for AWS

Overview

Infinity NDR automatically deploys a Check Point CloudGuard Network Security instance in Monitor Mode into the customer's AWS VPC, via an AWS CloudFormation stack. The stack registers Lambdas (serverless compute instances) that use cloud-native APIs to provision cloud vendor traffic mirroring, in order to selectively mirror network traffic for analysis and threat detection. Deployment is quick and intuitive, and takes minutes. There is no need for network security expertise because the sensors do not require any configuration and do not influence traffic flow; there is no need to create complicated policy rules.

Terminology

Before you use this solution, you should make yourself familiar with these AWS terms and services:

- VPC
- Region and Availability Zone (AZ)
- EC2
- Traffic Mirroring
- Elastic Network Interfaces (ENI)
- Elastic Load Balancing (ELB/NLB)
- Lambda
- CloudFormation
- CloudWatch
- Identity and Access Management (IAM)

If you are new to AWS, see Getting Started with AWS.

Scoping and Costs

The customer's AWS estate is allocated to accounts, regions, and VPCs. The Check Point Infinity NDR solution monitors network traffic between, into, and out of EC2 compute instances. Each EC2 instance is defined in a single VPC and AZ, and communicates using one or more ENIs.

NDR uses cloud-native AWS Traffic Mirroring in order to receive network traffic for inspection. A CloudGuard Network Security (CG NS) instance is provisioned as an NDR sensor via CloudFormation stack. An AWS Network Load Balancer (NLB) is also provisioned in front of the CG NS. Traffic mirroring is configured for a specific VPC and AZ, by creating mirroring sessions from all ENIs that match a mirroring policy, to the NLB. The NLB routes the mirrored traffic to the NDR sensor.

Traffic Mirroring is priced by AWS on a per-mirrored ENI basis at approximately $11/month per ENI. (This pricing varies across different AWS regions.) Infinity NDR instance costs are dependent on the sustained rate of mirrored traffic sent to the sensor (larger amount of mirrored traffic requires larger Infinity NDR instance size). These two factors are the major contributors to the cost of the Infinity NDR solution. The other components (lambda compute, NLB, etc.) are typically comparatively negligible, assuming that the mirrored ENIs and the mirroring target (the NDR instance) are in the same AZ.

Resources Required on the AWS Account

Step 1: Preparing the customer's AWS account

1. Make sure you know which VPCs and AZs you will be mirroring, and have sufficient IAM permissions to provision the NDR components. Missing permissions will cause the deployment to fail, with indicative error messages being output to the AWS Console.

2. Use the region selector in the navigation bar to select the AWS region, where you want to deploy the NDR instance on AWS.

3. You will need an SSH key pair in your preferred region.

4. If necessary, request a service limit increase for the AWS resources that you plan to use.
   By default this guide uses:
   - c5.xlarge for the Infinity NDR instances

5. The Infinity NDR instance is intended to be deployed into an existing VPC with existing workloads. Accordingly, customers must deploy into an existing VPC and create 2 subnets for use by Infinity NDR. These subnets must be in the same Availability Zone within the region:
   - 1 internal subnet to be used for the Infinity NDR instance's interface to receive traffic mirroring
   - 1 external subnet with Internet access for the instance to send logs to the Infinity NDR portal

6. The external subnet should present a route out to the Internet. If it is placed behind a network gateway, the Infinity NDR instance can be allocated a local AWS IP address. Otherwise, an Elastic IP (EIP) should be configured for the Infinity NDR instance for direct outbound access.

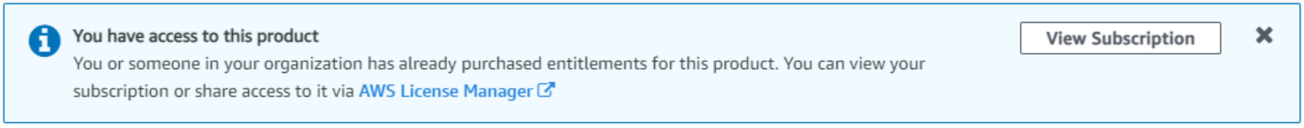
Step 2: Subscribing to CloudGuard Network Security in AWS Marketplace

In order to deploy a Check Point CloudGuard NDR Sensor, you must first subscribe your AWS account to Check Point CloudGuard Network Security with these steps:

1. Log in to AWS Marketplace.
   (You must have aws-marketplace:Subscribe IAM permission.)

2. Select the BYOL licensing option for the Check Point CloudGuard Network Security:
   CloudGuard Network Security with Threat Prevention & SandBlast BYOL

3. If the account is already subscribed, you will see at the top of this AWS Marketplace page that the AWS account is already entitled, as follows:



You have access to this product

You or someone in your organization has already purchased entitlements for this product. You can view your subscription or share access to it via AWS License Manager

4. Otherwise, select **Continue** to subscribe.
5. Select **Accept Terms** to confirm that you accept the AWS Marketplace license agreement.

Launch in AWS

After all preparations have been completed, you may now proceed to sensor deployment.

9. Login to the Infinity NDR portal portal and access the customer domain.

10. You will be directed to the Sensors tab, as there are no sensors on the domain.

11. From the lefthand menu, select **Management** --> **Sensors** --> Click **New** (top middle), then select **Virtual** and enter a description/name for the sensor. Select the correct time zone. Then click ADD in the lower right corner.

12. Select the new sensor entry, and click on **Actions** --> **LAUNCH IN AWS**.

13. This action generates a registration key for the new virtual sensor, and launches an AWS CloudFormation template in a new browser tab. It will first redirect you to login to your AWS account.

Note – Customers' AWS credentials are NOT provided to the Infinity NDR application portal nor in any way received or stored by Check Point Software Technologies.

Infinity NDR CloudFormation Template

1. **AWS General Configuration**

   The following parameters must all be filled in before creating the stack:

   a. **Stack Name**: will be automatically generated based on the sensor name. You may change this name if desired, e.g. to identify the AZ in which the sensor is instantiated.

      If relaunching the stack due to some error, e.g. missing IAM permissions, it is recommended to change this name to avoid resource collision in case the previous stack has not completed automated cleanup operations.)

   b. **VPC** where you want to deploy the Infinity NDR instance.

   c. **Availability zone**: an Infinity NDR instance should be deployed in each monitored AZ in order to avoid AWS inter-AZ network traffic mirroring costs.

   d. **AZ External subnet**: This subnet should have access out to the Internet (either directly or routed via other networks).

      In particular, the network should support TCP port 443 traffic to the following IP addresses: 3.64.14.68 and 35.156.213.136. If there is an outbound proxy, it must exempt HTTPS traffic inspection to these addresses.

   e. **AZ Internal subnet**: The mirrored traffic will be delivered to an Infinity NDR instance's VXLAN endpoint on this subnet. It may be the same as the AZ External subnet.

Note - Make sure the selected subnets are compatible with the selected availability zone.

2. **Infinity NDR Sensor Configuration**

   The following parameters must all be filled in before creating the stack:

   a. **EC2 Instance type**: AWS instance size used for the NDR sensor instance.

      The default is **c5.xlarge**. An oversized sensor will be more expensive in terms of AWS costs. On the other hand, an undersized sensor will provide reduced visibility due to uninspected connections, and in extreme cases will become unstable and disconnect from the Infinity NDR back end.

      The primary sizing consideration is the volume of traffic mirrored to the sensor for inspection. See Appendix A for guidelines on estimating traffic volumes in AWS, using AWS CloudWatch, where customers do not have this data handy.

      For a rough guide on choosing the instance type:

AWS instance type	**c5.large**	**c5.xlarge**	**c5.2xlarge**	**c5.4xlarge**	**c5.9xlarge**
# vCores	2	4	8	16	32
Max total traffic/sec	~0.5 Gbps	~1 Gbps	~2 Gbps	~4 Gbps	~8 Gbps

   b. **EC2 key name**: AWS security key pair for SSH access to the Infinity NDR instance. Normally this key is not used, but some key pair must be entered to allow instance deployment. There is no default.

   c. **Allocate EIP?** By default this attribute is set to "No", as in most customer VPCs, the Infinity NDR EC2 instance that is created on the AZ External subnet will receive an internal AWS IP address and a default gateway for outbound connectivity. Set this to "Yes" if you require an AWS Elastic IP to be allocated on the instance for direct Internet access.

Procedure for Resizing an Infinity NDR Sensor on AWS

For an activated sensor (in “✓” state), in case it is undersized or oversized and you need to change instance Type, follow these steps to relaunch it with the new size:

1. On AWS, delete the stack. This will clean up all resources consumed by the Infinity NDR solution.
2. On the Infinity NDRapplication   portal - on the MANAGEMENT > Sensors tab
    a. Select the sensor entry (it will be showing as “Disconnected” (grey lightbulb icon)
    b. Click on **Actions -->** **X DEACTIVATE**
    c. Click on **Actions -->** **LAUNCH IN AWS**
3. Fill in the CloudFormation Template with the new parameters.

Note – It is recommended to verify that the old stack has completed deletion before launching the new one; or to manually modify the stack name to avoid named collisions on deployed AWS resources.

3. CG NDR Configuration – Advanced

The following parameters all have valid default values and do not require modification. They provide for advanced Infinity NDR sensor configuration.

a. **Expiration period**: Time after which the stack is automatically deleted, releasing all AWS resources allocated for this stack. Defaults to “No expiration”.

b. **Include EC2 Instances with the following tags (default all)**: May be used to constrain the set of mirrored EC2 instances, using a comma-separated list of Key=Value AWS tags.

c. **Exclude EC2 Instances with the following tags (default none)**: May be used to further constrain the set of mirrored EC2 instances.

d. **Monitor all ENIs**? For multi-homed EC2 instances, setting this parameter to “No” will only monitor the main ENI.

e. **VXLAN ID**: VTEP number for mirroring sessions. Normally set to default value of “1”.

f. **VPC scan interval**: Defaults to 10 minutes.

g. **Version**: Do not change.

h. **Registration key**: Do not change.

4. Confirmation and Stack Creation

Check the acknowledgement and click “Create stack”. The CloudFormation Template (CFT) spins up the Infinity NDR instance in your selected VPC and AZ, and runs two lambda functions that provision AWS traffic mirroring. It will typically take up to 20 minutes before you start seeing logs on the Infinity NDR application portal. The sensor’s display on the portal will change to a green lightbulb icon with a “✓” state. CFT progress can be tracked in the AWS Console, including any relevant error messages.

5. **AWS Resources Provisioned by the CFT**

   a. A security group is created for each ENI:
      - Internal ENI: allow incoming vxlan (udp 4789), reject outbound
      - External ENI - allow incoming ssh/https (tcp 22/443), allow outbound

   b. AWS Traffic Mirroring sources and sessions for each mirrored ENI.

   c. AWS Network Load Balancer (NLB), defined as the mirroring target, routes mirrored traffic to the NDR sensor instance over the defined VXLAN on the AZ Internal subnet.

   d. Two lambda functions that automatically configure AWS traffic mirroring. An EC2 instance creation event on the VPC will trigger its evaluation against the mirroring policy (include and exclude lists). In addition, the VPC will be scanned on the defined scan interval, and any deleted EC2 instances will result in cleanup of the corresponding mirroring sources and sessions. These invocations are controlled by EventBridge rules.

   e. Elastic IP if enabled in the CFT.

Note - If you delete the stack from the AWS Console **-** this will clear up all related resources in your VPC, including the Infinity NDR CloudGuard Network Security instance, the lambda functions, and the traffic mirroring sessions.

Mirroring Additional VPCs

The “LAUNCH IN AWS” CFT provisions traffic mirroring for a specified VPC and AZ, and mirrors the traffic to a load balancer and Infinity NDR sensor. An alternative “PROVISION AWS MIRRORING” CFT is provided which does not create the latter two instances. Rather, it accepts the mirroring target as a parameter. This is intended to allow reuse of a single deployed Infinity NDR sensor for mirroring traffic from multiple VPCs. As long as the sensor and the mirrored traffic are defined in the same Availability Zone, there are no additional AWS costs due to inter-VPC or even inter-account traffic mirroring.

Note – It is not recommended to mirror across AZ boundaries (even though there is no technical limitation). AWS costs will grow significantly if traffic is mirrored between different AZs.

In order to provision mirroring on a different VPC:

1. From the lefthand menu, select **Management -->** **Sensors -->** Click **New** (top middle), then deselect **Managed** and enter a description/name for the sensor. Select the correct time zone. Then click ADD in the lower right corner.

2. Select the new sensor entry, and click on **Actions -->** **PROVISION AWS MIRRORING**.

3. This action launches an AWS CloudFormation template in a new browser tab. It will first redirect you to login to the customer’s AWS account. Ask the customer to enter his AWS account number and access credentials in order to access his AWS Console.

4. The CFT parameters are equivalent to those of LAUNCH IN AWS, with the following exceptions:

   - As no sensor is deployed, the CFT omits the following parameters: AZ External Subnet, AZ Internal Subnet, the entire CG NDR Configuration section, Version, Registration key

   - A Traffic Mirror Target parameter is added. Enter an Infinity NDR load balancer’s mirror target ID (e.g. ‘tmt-xxxxxx’).

5. Check the acknowledgement and click “Create stack”.

Traffic Mirroring Include/Exclude Lists

Traffic mirroring include and exclude lists are handled by the Infinity NDR Cloud Formation template which is deployed per sensor from the Infinity NDR portal. You can include comma-separated key value pairs in the CFT to indicate whether you'd like to include or exclude that instance from traffic mirroring. For example:

- MYTAG=DOMIRROR,MYOTHERTAG=INSTANCE
- CKP_TYPE = Sensor

Be sure to apply these tags to each instance according to whether you'd like to include or exclude them from traffic mirroring.

If you'd like to update your traffic mirroring include/exclude tags after initial CFT deployment, simply issue a CFT Stack update to revise the tags or to apply a different tag scan interval.

1. Find the CloudFormation Stack used to deploy your sensor, and select the "**Change Sets**" tab, then click on "**Create Change Set**".

2. Choose to Use the current template and click "**Next**".

3. Change the Include or Exclude tags as applicable and/or change the VPC Scan interval. When satisfied, click "**Next**".

4. Leave all stack options as-is (do not make any changes) and click "Next".

5. At the review screen, verify all parameters, then acknowledge the stack capabilities and click "**Create Change Set**".

6. Give the change set a name and click "**Create Change Set**" to make the changes to the applicable Infinity NDR sensors.

Sensor Deactivation on Stack Deletion

If you choose to delete the Cloudformation Stack which deployed your NDR Sensor, and relaunch in AWS from the Infinity NDR application portal, you will also need to first deactivate the sensor on the portal. This is because the Infinity NDR back end is not aware that the sensor was deactivated, only that it is disconnected.

On the MANAGEMENT > Sensors tab, select the relevant sensor, and X DEACTIVATE from the Actions menu.

Users and Access Control

Domains

The “domain” is the fundamental object collection on Infinity NDR. All objects are associated with a domain. This includes sensors, logs, packet captures, indicators, views, insights, reports, etc.

Authorizations

Each domain defines a set of user authorizations, viewed and edited via MANAGEMENT > Users. A user’s authorization on the domain defines a Role for the user’s access to the domain.

Users

The user object itself is created the first time an authorization is created on any domain, naming the user’s email address. The user is independent of any domain. The user’s email address is used both as the user’s unique identity, and for the purpose of communicating with the user, e.g. for reports and notifications.

The user receives an email with a link. Clicking on the link provisions the user object and generates a certificate with the user’s email address as the CN. This certificate is downloaded to the user’s endpoint and installed with a user-defined security level.

When the user logs in using his certificate, the Infinity NDR application verifies his or her certificate, retrieves the user’s domain authorizations, and matches them to the requested domain and service. Unauthorized requests will be rejected. Both authorized and unauthorized requests are audited and can be viewed on the MANAGEMENT > System Events tab.

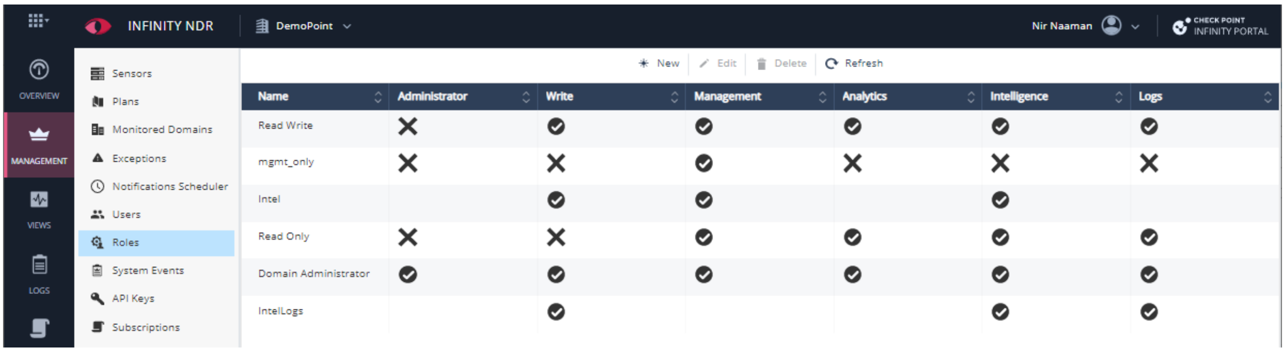
Note – Deleting a user record from MANAGEMENT > Users will not revoke the user’s certificate – only the user’s authorizations to the domain. If a user is left with no authorizations to any domain, the user account will be eventually deleted by automated cleanup services, and the user certificate revoked.

Note – MANAGEMENT > Users > Actions > REISSUE CREDENTIALS can be invoked on a user entry by any user with Write authorizations. This triggers an email with a reissue link to be sent to the target user’s email address; if the user receives the email and click the link, a new certificate will be generated and provided for download.

Roles

A Role defines a set of permissions that enable Infinity NDR services. Currently-supported permissions can be seen on the MANAGEMENT > Roles tab. These include:

- **Administrator** – required for sensitive services such as user authorizations, monitored domains, and input feed management
- **Write** – allows modifications to objects on the domain
- **Management** – controls access to the MANAGEMENT tab and its services
- **Analytics** – controls access to the VIEWS and INSIGHTS tabs and their services
- **Intelligence** – controls access to the INTEL tab and its services
- **Logs** – authorizes the user to view logs on the domain



Name	Administrator	Write	Management	Analytics	Intelligence	Logs
Read Write	✗	✓	✓	✓	✓	✓
mgmt_only	✗	✗	✓	✗	✗	✗
Intel		✓	✓		✓	
Read Only	✗	✗	✓	✓	✓	✓
Domain Administrator	✓	✓	✓	✓	✓	✓
IntelLogs		✓			✓	✓

Permissions are grouped under named roles. By default, each domain includes the “Read Only”, “Read Write”, and “Domain Administrator” roles. Additional roles can be defined as required.

For example, the Read Only role provides access to all tabs, but does not allow the user to manage user authorizations or modify any objects. The Intel role depicted above will allow the user to view and modify indicators, but not logs. The Infinity NDR application will display a tailored menu for a user in the Intel role, omitting OVERVIEW, VIEWS, LOGS, REPORTS, and INSIGHTS. Thus such a user would only see MANAGEMENT and INTEL.

Monitored Domains

An authorized Domain Administrator can create a new domain from the MANAGEMENT > Monitored Domains tab. This creates a monitored subdomain, that can be accessed by all users authorized to the monitoring domain. The monitored domain will be added to the domain drop-down menu for these users.

The role construct is also used when provisioning monitoring relationships between domains. The monitored domain defines the permissions that the users authorized to the monitoring domain will receive on the monitored domain’s objects. Effective permissions will be the intersection (i.e. minimum) of the user’s permissions on both domains.

For example, suppose domain X is monitoring domain Y, with Read Only role. A user is authorized as a Domain Administrator on X. His effective permissions on access to Y’s objects and services will be Read Only Domain Administrator. If the user is authorized to both X and Y, access to Y’s objects and services will be controlled using the more specific role assignment, i.e. the authorization on the Y domain.

When the monitoring relationship is created in the context of creation of a subdomain, the Domain Administrator role is used for the relationship.

Establishing a Monitoring Relationship between two Domains

The monitoring relationship between monitoring and monitored domains can also be created between any two arbitrary domains, even if the two domains were originally created independently. This is achieved as follows:

- A Domain Administrator on the monitored domain clicks “* New” on the MANAGEMENT > Monitored Domains tab, and specifies a Monitoring Domain Name. A contact name and email should be provided, as well as a role selected for the monitoring relationship.

- The request will show up on the monitoring domain. A Domain Administrator for that domain must Approve the request before it takes effect.

For example, in order to allow the Check Point Managed Detection and Response (MDR) service to monitor your domain, enter “Check_Point_MDR” as the Monitoring Domain Name. Once the monitoring request is approved by the MDR team, the MDR service will automatically start using Infinity NDR APIs to pull insights and logs from Infinity NDR to MDR, and to deliver threat indicators to enforcement points for prevention.

A Domain Administrator on either monitoring or monitored domain can break the relationship by deleting it.

Appendix A – SPAN Port Configuration

HP/Aruba Switches

See: https://community.arubanetworks.com/community-home/digestviewer/viewthread?MID=25100

1. Create the session and assign the local mirroring port (where your IDS is connected):
   a. ***mirror*** *session-#* ***port*** *exit-port-# [name name-str]*
   b. e.g.: *mirror 1 port 11*

*session-# = value from 1 to 4

2. Assign the monitored ports, vlans or mac addresses to any of the created local port mirroring sessions:
   a. ***interface*** *{port | trunk | mesh}* ***monitor all {in | out | both} mirror*** *{session-# | name-str} [{session-# | name-str}] [{session-# | name-str}] | [{session-# | name-str}] [no-tag-added]*
      i. e.g.: interface 28 monitor all both mirror 1

   OR

   b. ***vlan*** *vid-#* ***monitor all {in | out | both} mirror*** *{session-# | name-str} [{session-# | name-str}] [{session-# | name-str}] [{session-# | name-str}]*
      i. *e.g.: vlan 32 monitor all both mirror 1*

Cisco Switches

See: https://www.cisco.com/c/en/us/td/docs/switches/metro/me3600x_3800x/software/release/15-3_2_S/configuration/guide/3800x3600xscg/swSPAN.pdf

1. Enter the switch configuration mode
   a. configure terminal

2. Create the monitoring session
   a. ***monitor session*** *{session_number}* ***type local***
   b. e.g.: monitor session 1 type local

3. Designate the source port with 'both' for ingress and egress
   a. ***source interface interface_type*** *{list(,) or give range(-) of interfaces}* ***both***
   b. e.g.: source interface gigabitethernet 2/1 both
   c.
4. Designate the destination port
   a. ***destination interface interface_type*** *{list(,) or give range(-) of interfaces}* ***both***
   b. e.g.: destination interface gigabitethernet 2/4

5. Enable the SPAN session
   a. no shutdown

Example all together:
```
Switch# configure terminal
Switch(config)# monitor session 1 type local
Switch(config-mon-local)# source interface gigabitethernet 2/1
Switch(config-mon-local)# destination interface gigabitethernet 2/4
Switch(config-mon-local)# no shutdown
```

Appendix B – Binding w. Infinity SOC

Overview

Infinity SOC provides the following tools for an SOC analyst that augment Infinity NDR:

- SOC certainty (INSIGHTS) – Machine Learning (ML) based AI engine that processes Anti-Virus and Anti-Bot logs from Infinity NDR sensors and customers' Check Point Security Gateways, and accurately pinpoints real attacks from millions of daily logs and alerts. This enables you to quickly respond to the most severe threats with automated triage.

- Threat intelligence research (INVESTIGATE) - Use exclusive ThreatCloud and Open Source Intelligence (OSI) investigation tools developed by the Check Point Research Team and used daily to expose and investigate the world's most dangerous and sophisticated cyber-attacks.

- If a compromised network host is detected, allows you to download a lightweight remediation agent, available for Windows, MacOS, and Linux operating systems.

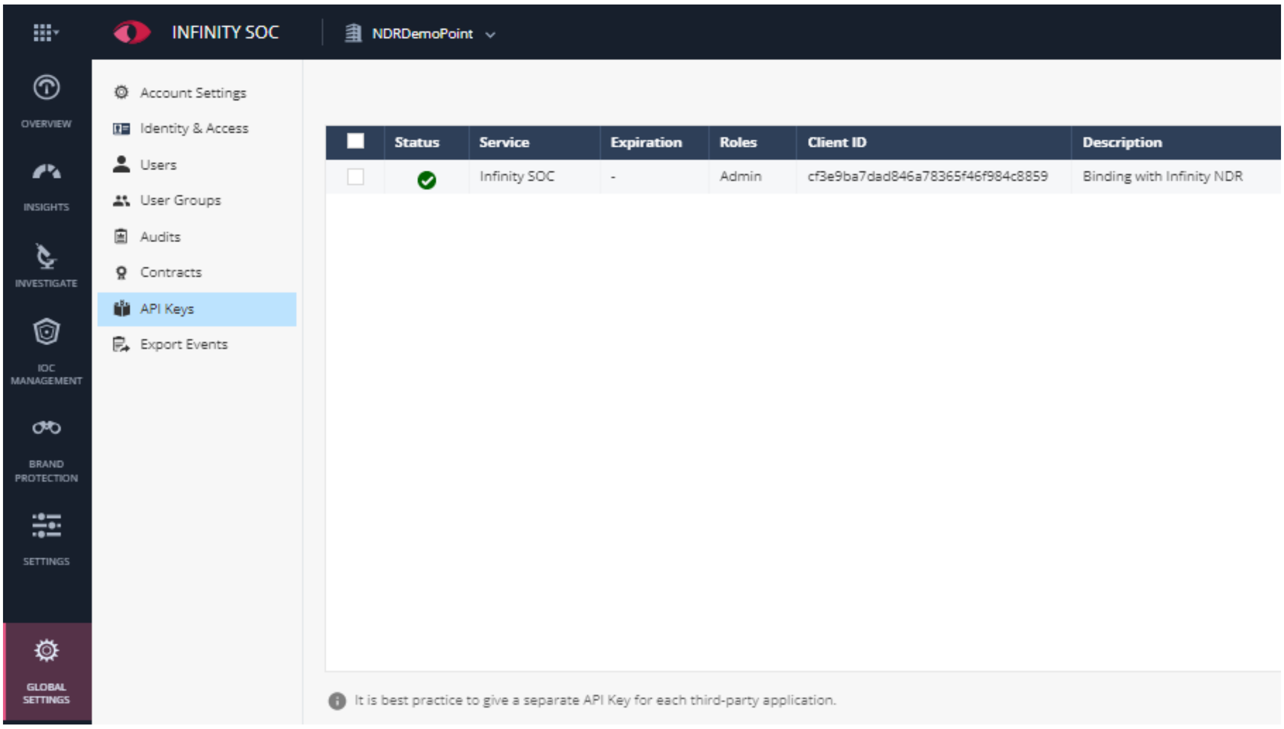
Note – Infinity SOC and Infinity NDR are bundled together commercially, however they are served from separate portals. Infinity SOC is published on the Infinity Portal: portal.checkpoint.com.

Creating an Infinity SOC API Key

1. Login to the Infinity Portal and select INFINITY-VISION SOC as the application.

2. On GLOBAL SETTINGS > API Keys, click "* New", select "Infinity SOC" as the Service, and optionally enter a Description (e.g. "Binding with Infinity NDR"). Click CREATE.

3. Infinity SOC will output two values: a Client ID, and an Access Key. Copy these values aside – once you close the window, it will not be possible to retrieve the Access Key.



□	Status	Service	Expiration	Roles	Client ID	Description
□	✓	Infinity SOC	-	Admin	cf3e9ba7dad846a78365f46f984c8859	Binding with Infinity NDR

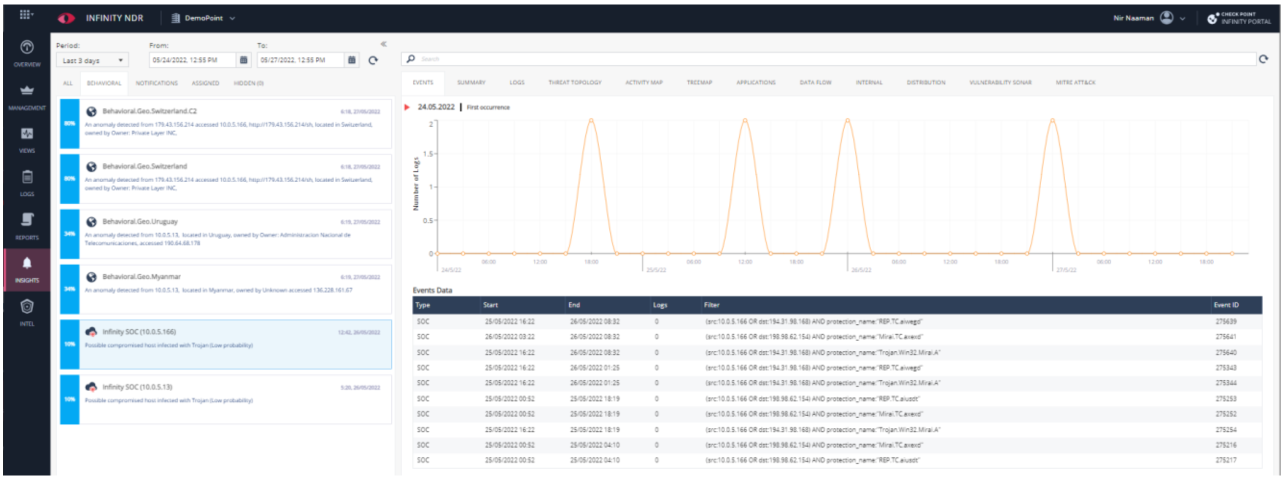
It is best practice to give a separate API Key for each third-party application.

Importing the Infinity SOC API Key into Infinity NDR

1. Login to the Infinity NDR application portal and access the customer domain.

2. On the MANAGEMENT > API Keys tab, click "* New", select "Infinity SOC" as Type, and enter the previously-copied Client ID and Access Key from Infinity SOC.

3. Infinity SOC Insights are then pulled automatically into Infinity NDR, adding to Infinity NDR's native Behavioral Analytics AI engines. This allows the Infinity SOC insights to be contextually visualized using all of Infinity NDR's advanced threat visualization capabilities.



Behavioral.Geo.Switzerland.C2 — 6:18, 27/05/2022
An anomaly detected from 179.43.156.214 accessed 10.0.5.166, http://179.43.156.214/sh, located in Switzerland, owned by Owner: Private Layer INC.

Behavioral.Geo.Switzerland — 6:18, 27/05/2022
An anomaly detected from 179.43.156.214 accessed 10.0.5.166, http://179.43.156.214/sh, located in Switzerland, owned by Owner: Private Layer INC.

Behavioral.Geo.Uruguay — 6:19, 27/05/2022
An anomaly detected from 10.0.5.13, located in Uruguay, owned by Owner: Administracion Nacional de Telecomunicaciones, accessed 190.64.68.178

Behavioral.Geo.Myanmar — 6:19, 27/05/2022
An anomaly detected from 10.0.5.13, located in Myanmar, owned by Unknown accessed 136.228.161.67

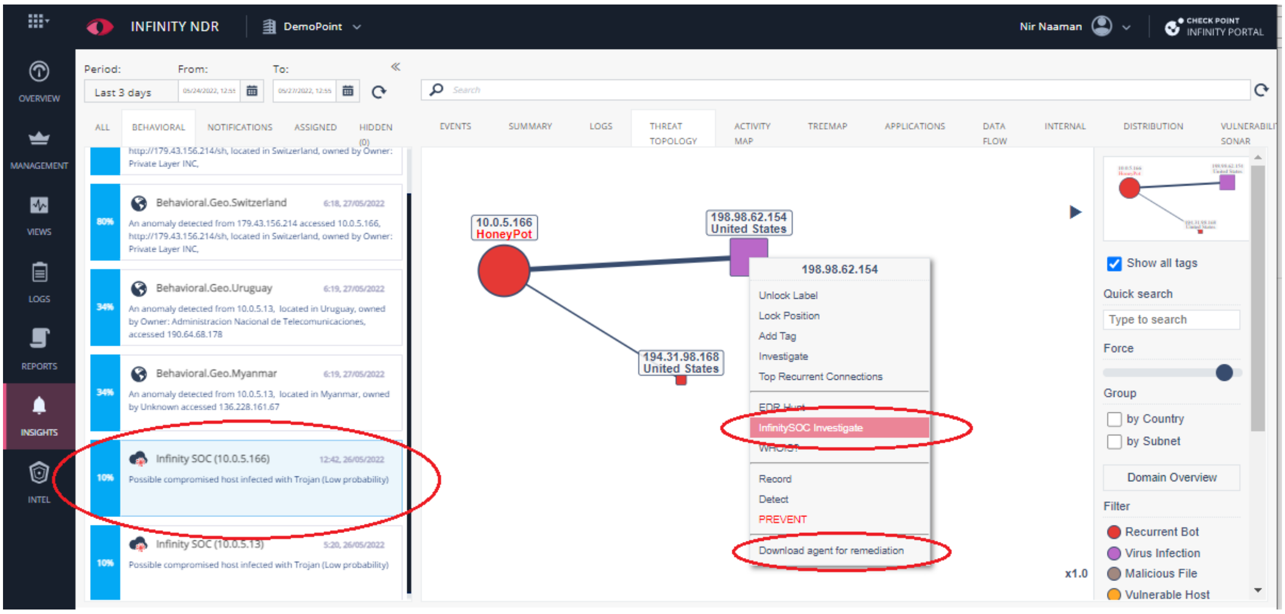
Infinity SOC (10.0.5.166) — 12:42, 26/05/2022
Possible compromised host infected with Trojan (Low probability)

Infinity SOC (10.0.5.13) — 5:20, 26/05/2022
Possible compromised host infected with Trojan (Low probability)

Events Data

Type	Start	End	Logs	Filter	Event ID
SOC	25/05/2022 16:22	26/05/2022 08:32	0	(src:10.0.5.166 OR dst:194.31.98.168) AND protection_name:"REP.TC.aiwegd"	275639
SOC	26/05/2022 03:22	26/05/2022 08:32	0	(src:10.0.5.166 OR dst:198.98.62.154) AND protection_name:"Mirai.TC.axexd"	275641
SOC	25/05/2022 16:22	26/05/2022 08:32	0	(src:10.0.5.166 OR dst:194.31.98.168) AND protection_name:"Trojan.Win32.Mirai.A"	275640
SOC	25/05/2022 16:22	26/05/2022 01:25	0	(src:10.0.5.166 OR dst:194.31.98.168) AND protection_name:"REP.TC.aiwegd"	275343
SOC	25/05/2022 16:22	26/05/2022 01:25	0	(src:10.0.5.166 OR dst:194.31.98.168) AND protection_name:"Trojan.Win32.Mirai.A"	275344
SOC	25/05/2022 00:52	25/05/2022 18:19	0	(src:10.0.5.166 OR dst:198.98.62.154) AND protection_name:"REP.TC.aiusdt"	275253
SOC	25/05/2022 00:52	25/05/2022 18:19	0	(src:10.0.5.166 OR dst:198.98.62.154) AND protection_name:"Mirai.TC.axexd"	275252
SOC	25/05/2022 16:22	25/05/2022 18:19	0	(src:10.0.5.166 OR dst:194.31.98.168) AND protection_name:"Trojan.Win32.Mirai.A"	275254
SOC	25/05/2022 00:52	25/05/2022 04:10	0	(src:10.0.5.166 OR dst:198.98.62.154) AND protection_name:"Mirai.TC.axexd"	275216
SOC	25/05/2022 00:52	25/05/2022 04:10	0	(src:10.0.5.166 OR dst:198.98.62.154) AND protection_name:"REP.TC.aiusdt"	275217

4. In addition, Infinity NDR allows you to download the Infinity SOC remediation agent from the NDR console, as well as pivot back to Infinity SOC for ThreatCloud and Open Source investigation.



http://179.43.156.214/sh, located in Switzerland, owned by Owner: Private Layer INC.

Behavioral.Geo.Switzerland — 6:18, 27/05/2022
An anomaly detected from 179.43.156.214 accessed 10.0.5.166, http://179.43.156.214/sh, located in Switzerland, owned by Owner: Private Layer INC.

Behavioral.Geo.Uruguay — 6:19, 27/05/2022
An anomaly detected from 10.0.5.13, located in Uruguay, owned by Owner: Administracion Nacional de Telecomunicaciones, accessed 190.64.68.178

Behavioral.Geo.Myanmar — 6:19, 27/05/2022
An anomaly detected from 10.0.5.13, located in Myanmar, owned by Unknown accessed 136.228.161.67

Infinity SOC (10.0.5.166) — 12:42, 26/05/2022
Possible compromised host infected with Trojan (Low probability)

Infinity SOC (10.0.5.13) — 5:20, 26/05/2022
Possible compromised host infected with Trojan (Low probability)

Appendix C – Known Limitations

- Infinity NDR only supports sensors that can run Check Point Gaia R81.10. This list currently excludes:
  - Quantum Spark SMB appliances (Embedded Gaia)
  - Quantum Maestro-orchestrated appliances
- Threat Extraction results are not included in the Security Checkup reports
- Infinity NDR supports registration of customer-managed log servers for processing of the logs from the customer's standard security gateways (i.e. not dedicated NDR sensors) by Infinity NDR's Behavioral Analytics AI engines and its threat visualization functionality. However, note that report generation is not supported for these logs.