AI Security

13 July 2026

AI FACTORY FIREWALL

Getting Started Guide

CHECK POINT™

Check Point Copyright Notice

Important Information

Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Certifications

For third party independent certification of Check Point products, see the Check Point Certifications page.

Check Point AI Factory Firewall Getting Started Guide

For more about this release, see the home page.

Latest Version of this Document in English

Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format.

Feedback

Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments.

Revision History

Date	Description
13 July 2026	Updates for AI Factory Firewall v1.89: ■ *"Instructions for a Data Center Provider" on page 29* - added support for Smart-1 Cloud ■ *"Instructions for an End-Customer" on page 43* - added support for Smart-1 Cloud Removed: ■ Integrating AIFF with NVIDIA App Shield (its was replaced by NVIDIA DOCA Argus)
26 May 2026	Updates for AI Factory Firewall v1.87: ■ *"Terms" on page 7* ■ *"Introduction" on page 10* ■ *"Quick Start Guide for AI Factory Firewall" on page 18* ■ *"Instructions for an End-Customer" on page 43* ■ *"Instructions for a Data Center Provider" on page 29* ■ *"Configuration of Out-of-Band Management Network" on page 63* ■ *"Uninstalling the AIFF Container" on page 56* ■ *"Upgrading the AIFF Container" on page 53*
12 April 2026	Updates for AI Factory Firewall v1.86: ■ *"Terms" on page 7* ■ *"Quick Start Guide for AI Factory Firewall" on page 18* ■ *"Instructions for an End-Customer" on page 43* ■ Added support for Specific Workload Protection (*"Example Diagram - Specific Workload Protection" on page 66*)
23 March 2026	First release of this document for AI Factory Firewall v1.85

Table of Contents

Terms

Term	Definition
BlueField-3 (BF-3)	An NVIDIA product. It is a DPU - a network interface card with an additional general purpose processing unit. See this NVIDIA page for more information.
Host Server	A physical server, in which BlueField-3 is installed.
DPU	Data Processing Unit - a NIC with a general-purpose processing unit. This is essentially a small computer inside a NIC. The DPU is installed in a server and can pass traffic to / from it like any other NIC. The processing unit of the DPU can access the traffic flowing through it efficiently and provide additional functions using the general-purpose processor and other processors on it.
OFED	OpenFabrics Enterprise Distribution. These are the NVIDIA drivers for the Host Server.
DOCA	Data Center-on-a-Chip Architecture. A DPU software framework for packet handling and other tasks. See this NVIDIA page for more information.
BFB	BlueField-3 Bundle software. It includes firmware, a flavor of Ubuntu Linux and the DOCA library installed on it.
Virtual Function (VF)	Virtual Functions (VFs) are virtual interfaces that allow for fast and efficient packet transfer from the DPU to specific workloads (for example, Virtual Machines, containers) on the Host Server. See this NVIDIA page for more information about SR-IOV and Virtual Functions.

Term	Definition
Scalable Function (SF)	Scalable Functions (SFs) are virtual interfaces in the DPU that allow for efficient packet transfer within the DPU without using resources of the Host Server. AIFF requires a total of five Scalable Functions: ■ Two Scalable Functions for each of the two workload channels. ■ One Scalable Function for the management. In each workload channel, the AIFF Security Gateway monitors and controls traffic from the network-side Scalable Function to the Host Server-side, and vice versa.
SR-IOV	Single Root IO Virtualization is a technology that allows a physical PCIe device to present itself multiple times through the PCIe bus. This technology enables multiple virtual instances of the device with separate resources. See this NVIDIA page for more information about SR-IOV and Virtual Functions.
AIFF	AI Factory Firewall is a software Check Point Next Generation Firewall for a Data Processing Unit (DPU).
SMS	Check Point Security Management Server. An on-premises Management Server with a single Domain Management Servers. See the *Security Management Administration Guide* for your version.
MDSMS	Check Point Multi-Domain Security Management Server. An on-premises Management Server with multiple isolated Domain Management Servers. See the *Multi-Domain Security Management Administration Guide* for your version.
GPC	Group Policy Controller. A distribution point for Security Policies and configuration for AIFF Security Gateways in a Multi-Domain Security Management Server environment.

Term	Definition
SIC	Secure Internal Communication. Proprietary encrypted communication between the Check Point Management Server and managed devices.
CGC	CloudGuard Controller. A component on a Check Point Management Server that dynamically learns about objects and attributes in data centers, such as changes in subnets, security groups, virtual machines, IP addresses, and tags. In the AIFF environment, this component creates and enforces policies tailored to AI / Workload Cluster running on the Host Server. See the *CloudGuard Controller Administration Guide* for your version.
Data Center Provider (CSP / Enterprise)	A Cloud Service Provider (CSP) or an Enterprise who deploys dedicated management components per tenant that enable the tenant to define and manage the security policy of its AIFF Security Gateways.
End-Customer	A user who rents a Host Server with BlueField-3 from a Data Center Provider.

Introduction

This document describes the installation and functionality of Check Point AI Factory Firewall (AIFF).

See sk184795 for these:

- List of support features.
- Software downloads.
- Limitations.

Overview of the AIFF Product

Check Point AI Factory Firewall (AIFF) is a software Check Point Next Generation Firewall designed to protect the traffic of applications running on data center servers, typically AI models, but not limited to them.

The system enables Data Center Providers to support tenants in securing AI workloads within their infrastructure.

The system includes integrated security capabilities that protect each workload using a DPU-based SmartNIC located on the same server.

The security services primarily include the AIFF Security Gateway and can include additional components, such as Argus for application protection.

The Data Center Provider handles the orchestration of these services, while each tenant manages their own security policies within the system.

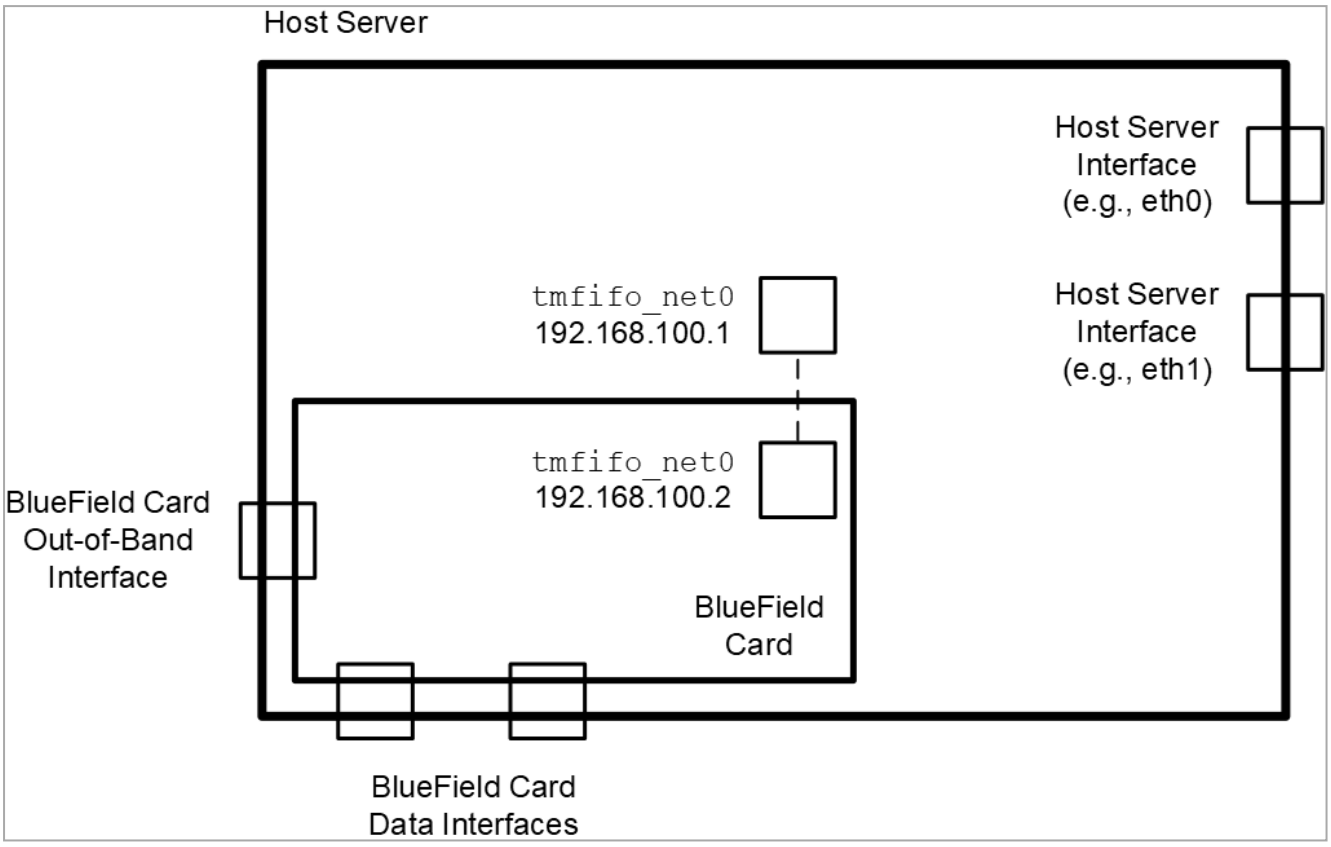
Each protected server has an NVIDIA© BlueField-3© (BF-3) Data Processing Unit (DPU) installed, on which the Check Point AIFF container is installed to protect the workloads' traffic going in and out of the server through that DPU.

By default, BlueField-3 acts just like a network interface card (NIC):

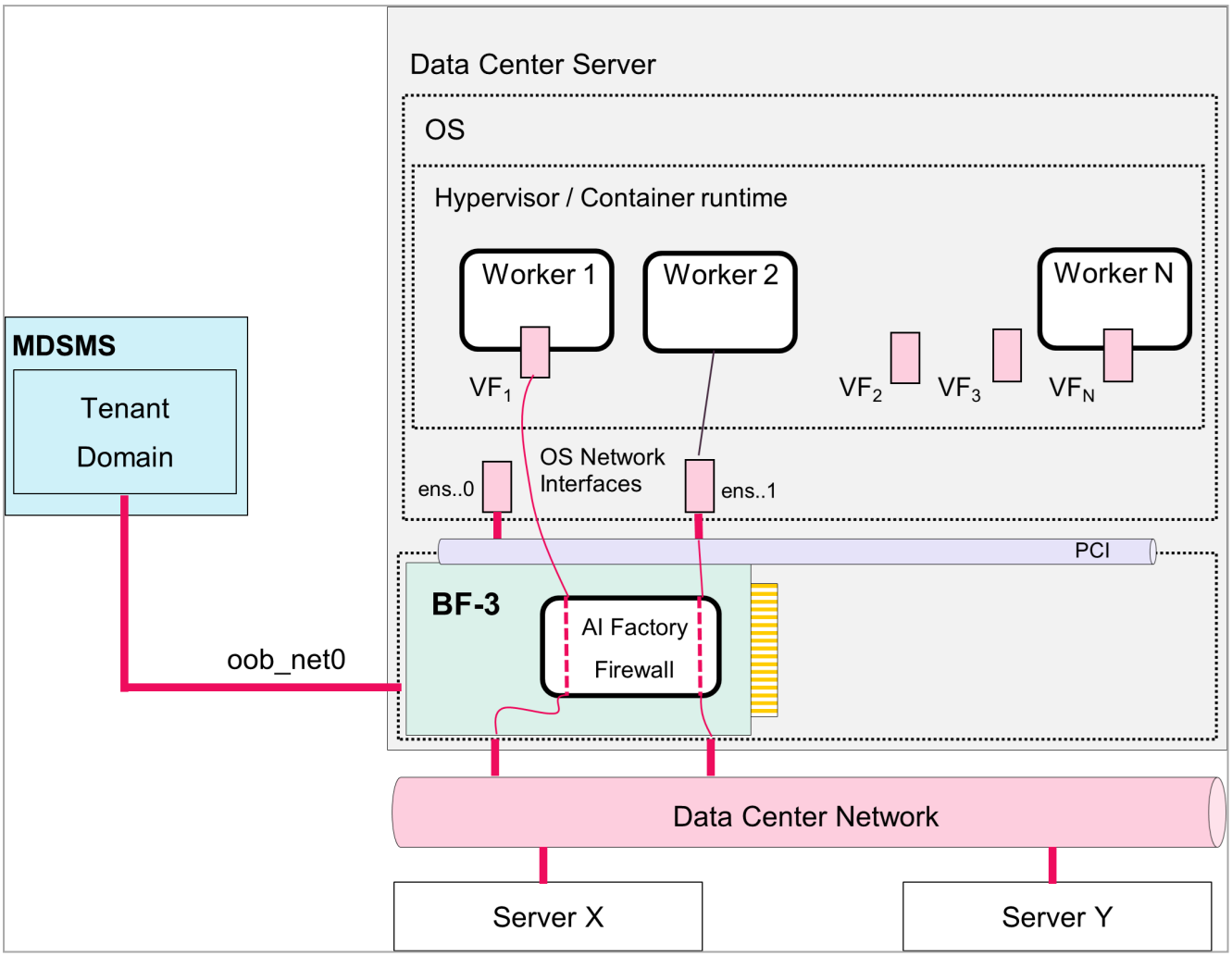
- When traffic arrives at the DPU's interfaces from the network, the corresponding OVS bridge forwards this traffic immediately to the Host Server.
- When traffic arrives at the DPU's interfaces from the Host Server, the corresponding OVS bridge forwards this traffic immediately to the network.

The AIFF is installed as "bump-in-the-wire", enforcing the user-defined policy on server workloads incoming / outgoing through BlueField-3.

Simplified diagram for BlueField-3 in a Host Server



Example diagram for AI Factory Firewall



Overview of the Check Point AIFF Deployment

Two roles are involved in deploying and using the AI Factory Firewall:

- The Data Center Provider.

  See *"Instructions for a Data Center Provider" on page 29*.

  The Data Center Provider owns the infrastructure.

  1. They install and configure the Check Point Management Server (Security Management Server or Multi-Domain Security Management Server).
  2. For each new tenant they run a script that creates an isolated management domain and connects it to a dedicated Group Policy Controller (GPC).
  3. They hand the tenant a configuration file (`zero_touch_parameters.json`) containing the credentials and parameters the tenant needs to proceed.

- The End-Customer.

  See *"Instructions for an End-Customer" on page 43*.

  The End-Customer owns the AI workloads.

  1. They install the AIFF security container onto the BlueField-3 DPU in their Host Server.
  2. They connect the AIFF to their management domain.
  3. They configure the security policy that governs their workloads' traffic.

Overview of the Check Point AIFF Environment

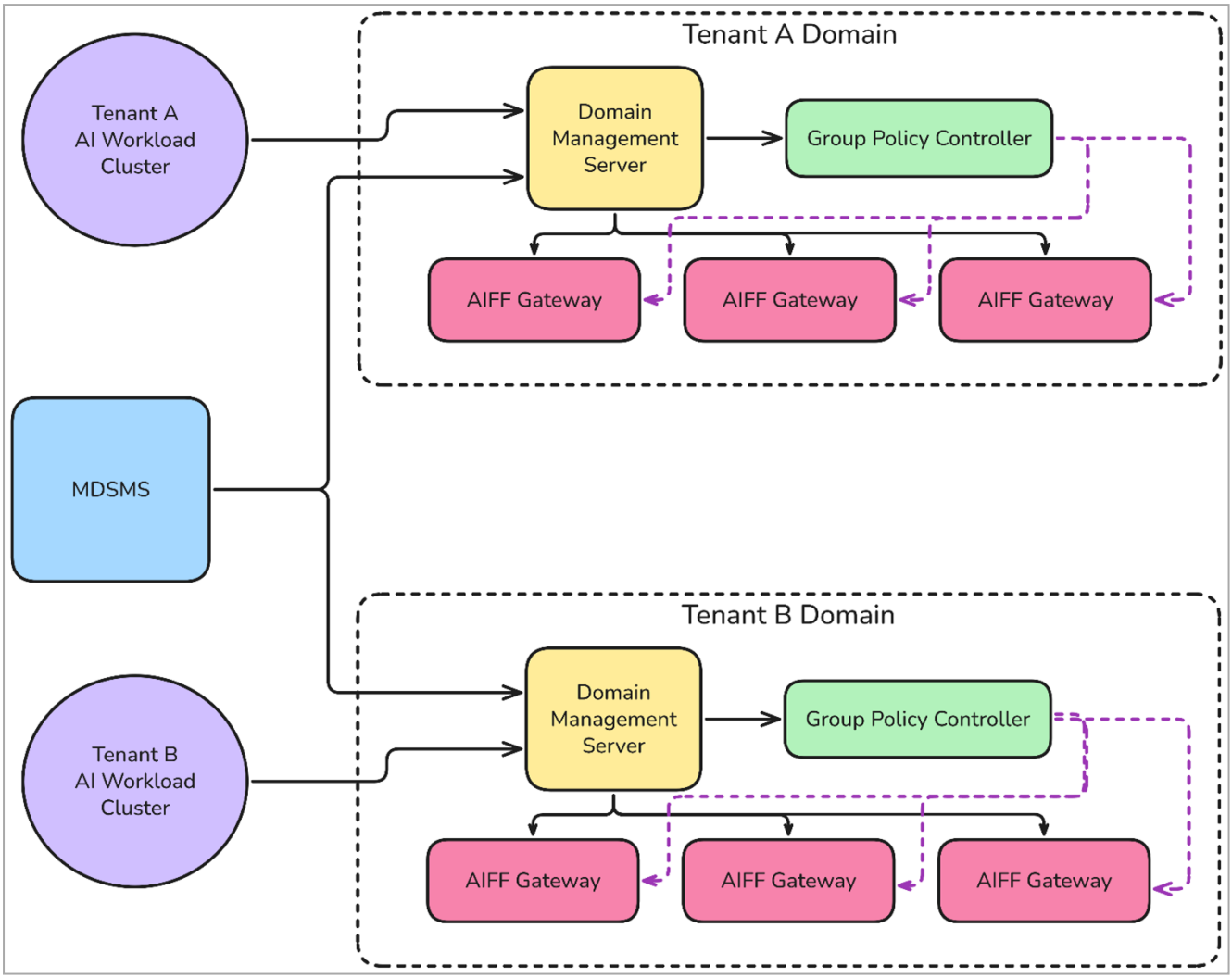
Simplified block-diagram for the AIFF environment:

This diagram shows a high-level multi-tenant cloud architecture from a Data Center Provider's perspective.

This diagram shows how multi-tenant workloads (End-Customers' workloads) are isolated and managed within a shared infrastructure.

The system includes shared infrastructure component - a Management Server (Security Management Server or Multi-Domain Security Management Server) that serves tenant Domains.

The architecture below is a container-orchestrated environment with policy-driven management and distributed gateway services, designed to scale across multiple tenants while maintaining security boundaries:



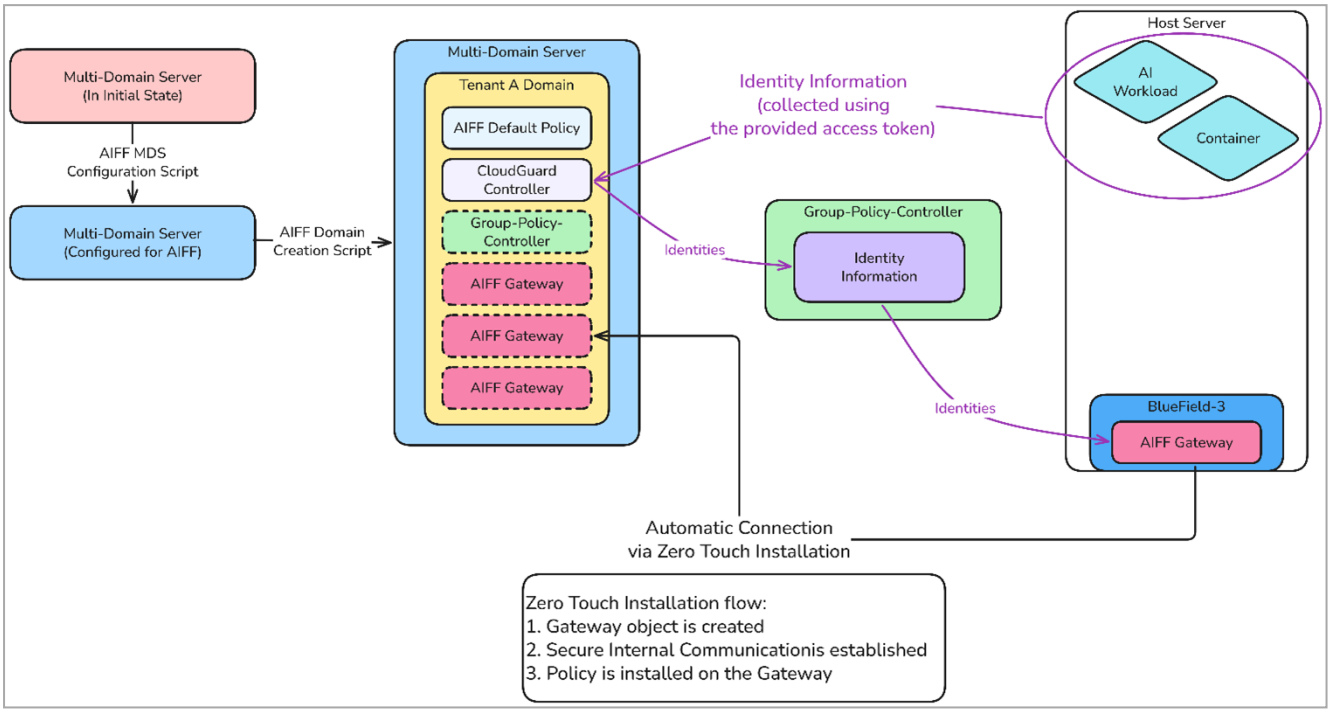
The workloads of each tenant are protected by AIFF containers that are installed using the Data Center Provider Kubernetes on the DPU of the relevant Host Servers. The Data Center Provider deploys dedicated management components per tenant (management Domain, Group Policy Controller) that enable the tenant to define and manage the security policy of its AIFF Security Gateways.

The policy can be object-based - the tenant workloads are deployed as containers on its Host Servers, and you can define policy rules based on the containers' names and labels.

The management system of the tenant connects to the tenant Kubernetes workload to discover the workload IP addresses that are in turn used by the AIFF Security Gateways to enforce the policy.

Detailed block-diagram for the AIFF environment:

This diagram describes the detailed deployment and configuration workflow for the multi-tenant system.



The workflow:

1. Install the Multi-Domain Security Management Server (MDSMS).
2. Run the one-time configuration script on the MDSMS.
3. Run the "Create Domain" script to create a new tenant Domain (in the diagram, "`Tenant_A_Domain`") and to configure several key components:
    - AIFF Default Policy for baseline policy.
    - Group Policy Controller (GPC) for sharing container identities with AIFF Security Gateways.
    - Identity Awareness (IDA) Client that the CloudGuard Controller uses to communicate with the Group Policy Controller (GPC).

If the Zero Touch flow was enabled during the installation, then after deploying the new AIFF Security Gateway:

1. The AIFF Security Gateway automatically connects to the tenant Domain using the internal Zero Touch script.
2. The AIFF Security Gateway automatically installs the policy configured in the Zero Touch policy name parameter.

This architecture demonstrates a policy-driven, automated deployment system where the Data Center Provider can efficiently provision and manage multiple tenant domains.

Overview of the AIFF Security Gateway Management

The management traffic for an AIFF Security Gateway can be one of these:

1. In-Band Management:

   In this scenario, we recommend configuring a dedicated underlay network for communication between the AIFF Security Gateways and the Security Management Server (both).

2. Out-of-Band (OOB) Management:

   Uses the interface "`oob_net0`" on the DPU card.

   See *"Configuration of Out-of-Band Management Network" on page 63*.

Overview of the AIFF Security Gateway Installation

The AIFF Security Gateway is installed over these:

1. Two pairs of Scalable Functions (SFs) for the traffic workloads it protects.
2. One SF for the management traffic.

When installing the AIFF Security Gateway, the administrator defines the internal network of BlueField-3, such that the requested workloads traffic will pass through the AIFF Security Gateway, while the rest of the traffic (if any) will skip it.

Such traffic scenarios can include the entire traffic from one network port to the Host Server on a specific channel (for example, between "`p0`" and "`pf0hpf`"), or specifically the traffic that goes to a specific worker in the Host Server through a Host Server Virtual Function (VF) representor (for example, "`pf0vf0`").

This is achieved with the OVS bridges, which connect the SFs with the actual interfaces of the DPU.

In the case of OOB management, there is a kernel bridge implementing the required connection.

The installation package of the AIFF provides a sample script, which configures the internal network of the Data Processing Unit card according to the required workloads and takes care of the management connection.

Quick Start Guide for AI Factory Firewall

Note - This procedure contains the instructions only for the latest version of the AI Factory Firewall package.

This is a quick procedure for deploying Check Point AI Factory Firewall (AIFF) on NVIDIA BlueField-3.

For complete procedures, see *"Instructions for a Data Center Provider" on page 29* and *"Instructions for an End-Customer" on page 43*.

This quick procedure assumes:

1. You are familiar with NVIDIA BlueField-3.
2. Your Host Server runs the Ubuntu operating system.
3. You are familiar with installing and configuring a Check Point Management Server.
4. You are familiar with installing and configuring a Check Point Security Gateway.

Procedure:

1. **On the Host Server - Install DOCA OFED.**

   Note - Skip this step if the required DOCA OFED version is already installed on your Host Server.

   See sk184795 > Section "Prerequisites" > "Prerequisites for a Data Center Provider" > row "Host Server with BlueField-3".

2. **On the Host Server - Enable and Start RShim.**

   Run these commands on the Host Server:

   ```
   sudo systemctl enable rshim
   sudo systemctl start rshim
   sudo systemctl status rshim
   ```

   Expected output:

   ```
   active (running)
   ```

3. **On the Host Server - Configure the Transmit Message FIFO (tmfifo) Networking.**

   Run these commands on the Host Server:

a. Edit the "`netplan`" script:

```
sudo nano /etc/netplan/50-cloud-init.yaml
```

Keep the existing Host Server configuration as-is and make sure the configuration contains this section:

```
tmfifo_net0:
      addresses:
      - 192.168.100.1/30
      dhcp4: false
```

b. Save the changes in the file and exit the editor.

c. Apply the configuration:

```
sudo netplan apply
```

d. Verify the configuration:

```
ip addr show tmfifo_net0
```

Expected output:

```
host tmfifo_net0 is 192.168.100.1/30
```

4. **On the Host Server - Flash a BlueField Bundle (BFB) to the DPU.**

Note - Skip this step if the required BFB version is already installed and configured on the DPU.

See sk184795 > Section "Prerequisites" > "Prerequisites for a Data Center Provider" > row "Host Server with BlueField-3".

5. **On the Host Server - Connect over SSH to BlueField-3 (over 'tmfifo').**

a. With the built-in SSH client, connect from the Host Server to BlueField-3:

```
ssh 192.168.100.2
```

The default credentials are:

- Username - `ubuntu`

- Password - `ubuntu`

b. After the first SSH login, follow the instructions on the screen.

Important - After changing the password, the SSH session disconnects automatically. Log in again with the new password.

6. **On the BlueField-3 - Configure Networking.**

a. Disable the "`cloud-init`" network configuration:

```
echo 'network: {config: disabled}' | sudo tee
/etc/cloud/cloud.cfg.d/99-disable-network-config.cfg >
/dev/null
```

b. Edit the BlueField-3 "`netplan`" script according to your environment:

```
sudo nano /etc/netplan/50-cloud-init.yaml
```

Example script:

```
network:
  version: 2
  renderer: NetworkManager
  bridges:
    oob_bridge0:
      interfaces:
        - oob_net0
      addresses:
        # This IP address is for direct SSH connection
        # to the MGMT interface of the BF-3 DPU
        - X.X.X.X/Y
      dhcp4: false
      nameservers:
        addresses:
        # These IP addresses are your DNS servers
(nameservers)
          - X.X.X.X
          - X.X.X.X
      routes:
        - metric: 1025
          to: 0.0.0.0/0
          # This IP address is your default gateway
          via: X.X.X.X

  ethernets:
    oob_net0:
      dhcp4: false

    tmfifo_net0:
      addresses:
        - 192.168.100.2/30
      dhcp4: false
```

c. Apply the "`netplan`" configuration:

```
sudo netplan apply
```

d. Configure the date and time in this format (in the UTC timezone):

```
sudo date -s "<YYYY-MM-DD HH:MM:SS>"
```

e. Writes the current system time to the hardware clock:

```
sudo hwclock -w
```

7. **Configure the Check Point Management Server and Group Policy Controller (GPC).**

   a. Use an existing Management Server (or install a new one with one of the supported versions).

      See sk184795 > Section "Prerequisites" > "Prerequisites for a Data Center Provider":

      - The row " Security Management Server (SMS)".
      - The row "Multi-Domain Security Management Server (MDSMS)".

   b. Install a valid Check Point license.

   c. If you are working with a Multi-Domain Security Management Server:

      Optional: In SmartConsole, provision at least one IP address.

      You **can** perform this optional step later with the "`config_MDS.py` script".

      Preferably, in the same network as the IP address of the Multi-Domain Security Management Server.

      i. Connect with SmartConsole to the **MDS** context.

      ii. Click the **Multi Domain** view.

      iii. Click the **Domains** page.

      iv. In the header row, right-click the Multi-Domain Server > click **Edit**.

      v. Click the **Multi Domain** page.

      vi. Refer to the **IP Range** section.

      Note - Both IP addresses are hosted on the same Multi-Domain Security Management Server.

   d. From sk184795 > section "Downloads", download the AI Factory Firewall package for a **Management Server** to your computer.

   e. Connect to the command line on the Management Server.

   f. Log in.

   g. If the default shell is Gaia Clish, then go to the Expert mode:

      ```
      expert
      ```

   h. Create the directory for the required scripts:

      ```
      mkdir /home/admin/MDM
      ```

i. Copy this AIFF package from your computer to the Management Server to the directory "`/home/admin/MDM/`".

j. Extract the archive package:

```
cd /home/admin/MDM
tar xvfz <Name of Archive Package>
```

k. If you are working with a Multi-Domain Security Management Server:

Configure a pool of IPv4 addresses for new Domains that manage AIFF Security Gateways:

```
python3 config_MDS.py [--ip_range="<Start IPv4 Address> -
<End IPv4 Address>"]
```

Note - If you already have an **IP Range** defined, then make sure there are enough IP addresses available for your AIFF domains and do **not** use the parameter "`--ip_range`".
To configure an IP Range, connect with SmartConsole to the **MDS** context > click the **Multi Domain** view > click the **Domains** page > in the header row, right-click the Multi-Domain Server > click **Edit** > click the **Multi Domain** page > refer to the **IP Range** section.

Example:

```
python3 config_MDS.py --ip_range="192.168.10.20 -
192.168.10.50"
```

l. Install and configure a new Group Policy Controller (GPC).

See sk184795 > Section "Prerequisites" > "Prerequisites for a Data Center Provider" > row Group Policy Controller (GPC).

m. On the Management Server, configure a new Domain and connect it to the Group Policy Controller (GPC).

   If you do **not** want to configure the Global AIFF policy, then **also** specify the parameter "`--no_global_policy`".

   i. On a Security Management Server, run:

   ```
   python3 createDomain.py --standalone --gw_ip="<IPv4 Address of GPC>" --gw_sic_pass="<SIC Activation Key for GPC>" [--no_global_policy]
   ```

   ii. On a Multi-Domain Security Management Server, run:

   ```
   python3 createDomain.py --name="<Name of New Domain>" --gw_ip="<IPv4 Address of GPC>" --gw_sic_pass="<SIC Activation Key for GPC>" [--no_global_policy]
   ```

n. On the Management Server, inspect the Domain configuration (you use these values in the next steps):

   ```
   cat ./<Name of Domain>/zero_touch_parameters.json
   ```

8. **On the BlueField-3 - Deploy AI Factory Firewall.**

   a. From sk184795 > section "Downloads", download the AI Factory Firewall package for the BlueField-3 DPU to your computer.

   b. With an SCP client, copy this AIFF package from your computer to the DPU to some directory (for example, create the directory "`/var/log/AIFF`").

      You can copy the package in one of these ways:

      - From your computer through the BlueField-3 Out-of-band Management - directly to the DPU.
      - From your computer through the regular Host Server interface and then from the Host Server to the DPU.

   c. With an SSH client, connect to the DPU.

   d. Go to the directory with the AIFF package:

   ```
   cd /var/log/AIFF/
   ```

e. Assign the 'execute' permission to the scripts:

```
sudo chmod +x AIFFctl
```

f. Start the installation:

```
./AIFFctl install
```

g. The script is interactive and prompts for all required values:

Note - The script saves all entered configuration values in the "`/etc/gwac/bf_standalone.conf`" file.
If you run the `AIFFctl` script again, it can automatically use these saved values to fill in the prompts.
This makes repeated deployments faster and consistent.

i. `Host interface 0:`

ii. `Host interface 1:`

iii. `DHCP for management network (y/n):`

If you entered "`n`":

- `AIFF static IP address:`
- `AIFF static IP prefix length (0-32): AIFF`
- `Default gateway IP address:`

iv. `Zero Touch provisioning (y/n):`

Important - Remember your choice.

- If you entered "`n`" (meaning, use an on-premises Management Server):

  `Enter Initial SIC key:`

  Important - Write down this key and keep it safe.

- If you entered "`y`" (meaning, use Zero Touch deployment):
  - `Management server IP:`

    Enter the value of "`domain_ip`" from the "`zero_touch_parameters.json`" file for your Domain
  - `Management API key:`

    Enter the value of "`mgmt_api_key`" from the "`zero_touch_parameters.json`" file for your Domain
  - `Server fingerprint:`

    Enter the value of "`mgmt_server_fingerprint`" from the "`zero_touch_parameters.json`" file for your Domain
  - `Domain name:`

    Enter the value of "`domain_name`" from the "`zero_touch_parameters.json`" file for your Domain
  - `Policy name:`

    Enter the value of "`aicp_policy_name`" from the "`zero_touch_parameters.json`" file for your Domain
  - `Use default blade configuration? [...] (y/n):`
    - If you entered "`n`":

      `Activate blade '[blade-name]'? (y/n):`

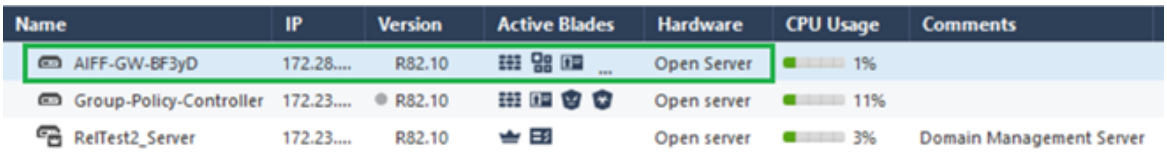
      Enter "`y`" or "`n`" to activate or disable the Software Blade specified in "`[blade-name]`".

h. Connect with SmartConsole to the applicable Domain.

i. From the left navigation panel, click **Gateways & Servers**.

The AIFF Security Gateway object must appear.

Example:



Instructions for a Data Center Provider

This section describes the required steps for a Data Center Provider to deploy the Check Point AIFF environment.

Prerequisites

See sk184795 > Section "Prerequisites" > "Prerequisites for a Data Center Provider".

Step 1 - Configure the Management Server

You can use one of these:

- On-Premises Management Server
- Smart-1 Cloud

Procedure for On-Premises Management Server

1. Use an existing Management Server or install a new one.

   See sk184795 > Section "Prerequisites" > "Prerequisites for a Data Center Provider":

   - The row "Security Management Server (SMS)".
   - The row "Multi-Domain Security Management Server (MDSMS)".

   See the *R82.10 Installation and Upgrade Guide* :

   - Chapter "*Installing a Security Management Server*" > Section "*Installing One Security Management Server only, or Primary Security Management Server in Management High Availability*".
   - Chapter "*Installing a Multi-Domain Server*" > Section "*Installing One Multi-Domain Server Only, or Primary Multi-Domain Server in Management High Availability*".
2. Install a valid Check Point license.
3. From sk184795 > section "Downloads", download the AI Factory Firewall package for a Multi-Domain Security Management Server to your computer.
4. Connect to the command line on the Management Server.
5. Log in.
6. If the default shell is Gaia Clish, then go to the Expert mode:

```
expert
```

7. Create the directory for the required scripts:

```
mkdir /home/admin/MDM
```

8. Copy this AIFF package from your computer to the Management Server to the directory "`/home/admin/MDM/`".

9. Extract the archive package:

```
cd /home/admin/MDM
tar xvfz <Name of Archive Package>
```

10. If you are working on a Multi-Domain Security Management Server, configure a pool of IPv4 addresses for new Domains that manage AIFF Security Gateways:

Note - If you are working on a Security Management Server, skip to *"Step 2 - Configure a new Tenant (GPC and Domain)" on page 33*).

Notes:

- You perform this step only one time.
- You can see the current pool in these ways:
  - Connect with SmartConsole to the **MDS** context > click the **Multi Domain** view > click the **Domains** page > in the header row, right-click the Multi-Domain Server > click **Edit** > click the **Multi Domain** page > refer to the **IP Range** section.
  - With the Management API command "`show mds`" (see *Check Point Management API Reference* (at the top, select the correct version)).
- All Domain Management Servers (that are assigned automatically) share this pool. The AIFF Security Gateway only draws IP addresses that are currently available in the pool when creating a new Domain.
- If you already have an **IP Range** defined, make sure there are enough IP addresses available for your AIFF domains and do **not** use the parameter "`--ip_range`" in syntax.

Syntax:

```
python3 config_MDS.py [--ip_range="<Start IPv4 Address> -
<End IPv4 Address>"]
```

Example:

```
python3 config_MDS.py --ip_range="192.168.10.20 -
192.168.10.50"
```

The "`config_MDS.py`" script:

a. Optionally, configures the specified IPv4 pool for new Domains.

Important - This script overwrites the current configured IP Range.

b. Initializes the Global Policy Assignment, so new Domains automatically inherit certain policy elements.

c. Configures the Service Group object called "`Kubernetes`" that contains the relevant service objects.

Procedure for Smart-1 Cloud

For information about Smart-1 Cloud, see the *Smart-1 Cloud Administration Guide*.

1. Use an existing Smart-1 Cloud tenant or create a new one.
2. In Smart-1 Cloud, create an API key as described in the Using the Settings > General > API & SmartConsole section of the *Smart-1 Cloud Administration Guide*.

   If you already have an API key, **no** need to create it again. Make sure you have it ready.
3. From sk184795 > section "Downloads", download the AI Factory Firewall package for a Multi-Domain Security Management Server to your computer.
4. Connect to the command line on your Group Policy Controller.
5. Log in.
6. If the default shell is Gaia Clish, then go to the Expert mode:

   ```
   expert
   ```
7. Create the directory for the required scripts:

   ```
   mkdir /home/admin/MDM
   ```
8. Copy this AIFF package from your computer to the Group Policy Controller to the directory "`/home/admin/MDM/`".
9. Extract the archive package:

   ```
   cd /home/admin/MDM
   tar xvfz <Name of Archive Package>
   ```

10. If you are working on a Multi-Domain Security Management Server, configure a pool of IPv4 addresses for new Domains that manage AIFF Security Gateways:

    Note - If you are working on a Security Management Server, skip to *"Step 2 - Configure a new Tenant (GPC and Domain)" on the next page*).

    Notes:
    - You perform this step only one time.
    - You can see the current pool in these ways:
      - Connect with SmartConsole to the **MDS** context > click the **Multi Domain** view > click the **Domains** page > in the header row, right-click the Multi-Domain Server > click **Edit** > click the **Multi Domain** page > refer to the **IP Range** section.
      - With the Management API command "`show mds`" (see *Check Point Management API Reference* (at the top, select the correct version)).
    - All Domain Management Servers (that are assigned automatically) share this pool. The AIFF Security Gateway only draws IP addresses that are currently available in the pool when creating a new Domain.
    - If you already have an **IP Range** defined, make sure there are enough IP addresses available for your AIFF domains and do **not** use the parameter "`--ip_range`" in syntax.

    Syntax:

    ```
    python3 config_MDS.py [--ip_range="<Start IPv4 Address> -
    <End IPv4 Address>"]
    ```

    Example:

    ```
    python3 config_MDS.py --ip_range="192.168.10.20 -
    192.168.10.50"
    ```

    The "`config_MDS.py`" script:

    a. Optionally, configures the specified IPv4 pool for new Domains.

       Important - This script overwrites the current configured IP Range.

    b. Initializes the Global Policy Assignment, so new Domains automatically inherit certain policy elements.

    c. Configures the Service Group object called "`Kubernetes`" that contains the relevant service objects.

Step 2 - Configure a new Tenant (GPC and Domain)

Procedure

1. Configure a new Group Policy Controller (GPC):

   Important - You must perform this step when you create a new Domain for a new tenant.

   a. Install a new Check Point Security Gateway (GPC).

      See sk184795 > Section "Prerequisites" > "Prerequisites for a Data Center Provider" > row Group Policy Controller (GPC).

      Steps for a Virtual Machine

      Note - The steps below are for VMware ESXi.

      i. In your virtualization platform, create a new Virtual Machine with the required hardware specifications.

         Do **not** power on the Virtual Machine yet.

      ii. In the Virtual Machine settings, add two network adapters:

         - The first network adapter appears in the Check Point Gaia OS as **eth0** (this procedure uses it as the external interface).
         - The second network adapter appears in the Check Point Gaia OS as **eth1** (this procedure uses as the internal interface).

         You can add more interfaces, if you need.

      iii. In the Virtual Machine settings, add the CD/DVD drive and select the Check Point ISO image.

      iv. Power on the Virtual Machine.

      v. In the Virtual Machine's BIOS, configure the CD/DVD drive as the first boot device.

      vi. Go through the Gaia installation wizard.

      vii. Wait for the ISO installation to complete and show the message about the reboot.

      viii. In the Virtual Machine settings, disconnect the CD/DVD drive.

      ix. In the console window, press Enter to reboot.

x. In the Virtual Machine's BIOS, configure the Hard Disk device as the first boot device.

xi. Wait for the Gaia OS to boot and show the login prompt:

```
login:
```

xii. Log in with these credentials:

Username: **admin**

Password: Enter the password you configured during the Gaia installation.

xiii. In VMware, connect a client computer to the first network adapter of the Virtual Machine that represents the external interface **eth0**.

On this client computer, configure the relevant interface with a static IPv4 address from the subnet that belongs to the external interface **eth0** (the default gateway is the IPv4 address of this interface **eth0**).

xiv. On the client computer, with a web browser connect to Gaia Portal on the Check Point Security Gateway (GPC):

```
https://<IPv4 Address of eth0>
```

Because Gaia Portal uses a self-signed certificate, your web browser will show a warning "`ERR_CERT_AUTHORITY_INVALID`".

Proceed with the connection.

Steps for a physical Check Point Appliance

i. Install a new Check Point Appliance.

See the relevant Getting Started Guide in sk96246 - Documentation For Check Point Appliances.

ii. Install the required Check Point image and reboot.

iii. Connect a cable from a client computer to the port **MGMT** on the Check Point Appliance.

On this client computer, configure the relevant interface with these settings:

- A static IPv4 address from the subnet that belongs to the port **MGMT**
- The default gateway is the IPv4 address of this port **MGMT**

iv. On a client computer, with a web browser connect to Gaia Portal on the Check Point Security Gateway (GPC):

```
https://192.168.1.1
```

Because Gaia Portal uses a self-signed certificate, your web browser will show a warning "ERR_CERT_AUTHORITY_INVALID".

Proceed with the connection.

v. Log in with these default credentials:

Username: **admin**

Password: **admin**

Steps for a physical open server

i. Install a new open server.

Follow the relevant documentation from your vendor.

ii. Install the required Check Point image and reboot.

iii. Connect a cable from a client computer to the interface, on which you configured an IPv4 address during the Gaia installation wizard.

On this client computer, configure the relevant interface with these settings:

- A static IPv4 address from the subnet that belongs to the relevant interface on the open server
- The default gateway is the IPv4 address of the relevant interface on the open server

iv. On a client computer, with a web browser connect to Gaia Portal on the Check Point Security Gateway (GPC):

```
https://192.168.1.1
```

Because Gaia Portal uses a self-signed certificate, your web browser will show a warning "ERR_CERT_AUTHORITY_INVALID".

Proceed with the connection.

v. Log in with these credentials:

Username: **admin**

Password: Enter the password you configured during the Gaia installation.

b. Follow the First Time Configuration Wizard.

Reference:
https://sc1.checkpoint.com/documents/R82.10/WebAdminGuides/EN/CP_R82.10_Gaia_AdminGuide/Content/Topics-GAG/Running-FTCW-in-Gaia-Portal.htm

You must configure these settings:

i. In the **Installation Type** window, select **Security Gateway and/or Security Management**.

ii. In the **Products** window:

- In the **Products** section, select only **Security Gateway**.
- In the **Clustering** section, clear **Unit is a part of a cluster, type**.

iii. In the **Dynamically Assigned IP** window, select the applicable option.

iv. In the **Secure Internal Communication** window, enter the applicable **Activation Key** (between 4 and 127 characters long).

Keep this activation key safe. You use it later on the Management Server.

c. In Gaia Portal, configure the applicable settings for your environment (additional administrator users, password security, and so on).

d. Install the valid Check Point license.

2. On the Management Server, configure a new Domain and connect it to the GPC:

   If you do **not** want to configure the Global AIFF policy, then **also** specify the parameter "`--no_global_policy`".

   - On an on-premises Security Management Server, run:

     ```
     python3 createDomain.py --standalone --gw_ip="<IPv4
     Address of GPC>" --gw_sic_pass="<SIC Activation Key for
     GPC>" [--no_global_policy]
     ```

     Example:

     ```
     python3 createDomain.py --standalone --gw_
     ip="172.23.53.78" --gw_sic_pass="MySICpswrd!@"
     ```

   - On an on-premises Multi-Domain Security Management Server, run:

     ```
     python3 createDomain.py --name="<Name of New Domain>" -
     -gw_ip="<IPv4 Address of GPC>" --gw_sic_pass="<SIC
     Activation Key for GPC>" [--no_global_policy]
     ```

     Example:

     ```
     python3 createDomain.py --name="New_Domain" --gw_
     ip="172.23.53.78" --gw_sic_pass="MySICpswrd!@"
     ```

   - To configure a Smart-1 Cloud tenant, run on your Group Policy Controller:

     ```
     python3 createDomain.py --cloud https://<Service_
     Identifier>.maas.checkpoint.com/<Mgmt_UID> --cloud_api_
     key <Your API Key> --gw_ip="<IPv4 Address of GPC>"
     ```

     You can see the "`<Service_Identifier>`" and "`<Mgmt_UID>`" in Smart-1 Cloud > **Settings** > **API & SmartConsole**.

     Example:

     ```
     python3 createDomain.py --cloud https://cloud-
     123.maas.checkpoint.com/456 --cloud_api_key aBcD789== -
     -gw_ip="172.23.53.78"
     ```

where:

Parameter	Description
<Name of New Domain>	Specifies the name of the Domain.
<IPv4 Address of GPC>	Specifies the IPv4 address of the GPC.
<SIC Activation Key for GPC>	Specifies the SIC Activation Key you configured on the GPC.
`--no_global_policy`	Specifies **not** to configure the Global AIFF policy.
`--standalone`	Configures a Security Management Server.
`--cloud_api_key`	Specifies the API Key you created in Check Point Portal.

The "`createDomain.py`" script:

a. Creates a new Domain with an IPv4 address from the configured IPv4 pool.

b. Configures an internal administrator user ("`<Name of New Domain>_admin`") with required permissions.

c. Connects the GPC to the new Domain (creates the corresponding Security Gateway object with the platform "Open Server").

d. Prepares the default policy called "`AIFF_Default_Policy`" for the AIFF Security Gateway object:

No	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	(empty)	Any	Any	Any	Kubernetes-Group	Accept	Log	Policy Targets
2	Parent rule for Domain's policy							
2.1	Clean Up	Any	Any	Any	Any	Drop	None	Policy Targets

This policy includes the Global Policy that is applied from the Multi-Domain Security Management Server through Global Assignment.

Note - You can edit this default Security Policy - **before** you deploy the AIFF Container on the DPU.

e. Create this file with the required variable values for the new Domain:

Note - The Data Center Provider must provide this file to the End-Customer.

- On an on-premises Security Management Server:

```
home/admin/MDM/standalone/zero_touch_
parameters.json
```

- On an on-premises Multi-Domain Security Management Server:

```
/home/admin/MDM/<Name of Domain>/zero_touch_
parameters.json
```

- On the Group Policy Controller (when you configure a Smart-1 Cloud tenant):

```
/home/admin/MDM/Cloud/zero_touch_parameters.json
```

Required variables:

- `MGMT_SERVER_IP`
- `mgmt_server_fingerprint`
- `mgmt_api_key`
- `domain_name`
- `aicp_policy_name`

3. If you configure a Smart-1 Cloud tenant, finish connecting the Group Policy Controller to Smart-1 Cloud:

a. From the file "zero_touch_parameters.json", copy the value of the variable "`auth_token`".

b. Connect to the command line on your Group Policy Controller.

c. Log in.

d. If the default shell is the Expert mode, then go to Gaia Clish:

```
clish
```

e. Connect the Group Policy Controller to Smart-1 Cloud:

```
set security-gateway cloud-mgmt-service on auth-token
<Value of 'auth_token'>
```

f. Connect with SmartConsole to your Smart-1 Cloud tenant. See the *Smart-1 Cloud Administration Guide*.

g. From the left navigation panel, click **Gateways & Servers**.

h. Double-click the Group Policy Controller object.

i. In the section **Establish secure communication**, click **Connect**.

j. Follow the steps on the screen to establish Secure Internal Communication (SIC).

4. In SmartConsole, examine the new Domain and the GPC:

a. Connect with SmartConsole to the Management Server.

If you are working with an on-premises Multi-Domain Security Management Server:

i. Connect to the context "**MDS**".

ii. From the left navigation panel, click **Multi Domain**.

iii. In the top panel, click **Domains**.

b. The GPC (and the new Domain) must appear on this page.

Example for a Multi-Domain Security Management Server:

- Domain:

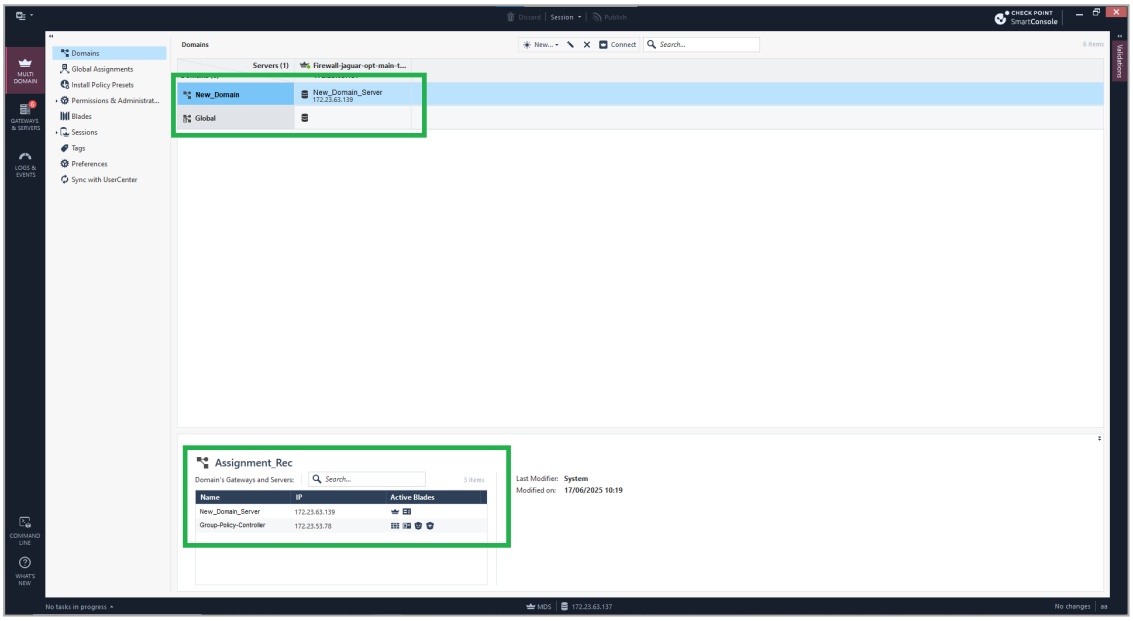
  Name: `New_Domain`

  IPv4: `172.23.63.139`

- GPC:

  Name: `Group-Policy-Controller`

  IPv4: `172.23.53.78`



Instructions for an End-Customer

Note - This procedure contains the instructions only for the latest version of the AI Factory Firewall package.

Prerequisites

1. See sk184795 > Section "Prerequisites" > "Prerequisites for an End-Customer".
2. See *"Creating a Virtual Function on the Host Server" on page 51*.

Step 1 - Configure the Host Server

Procedure

1. Make sure the Host Server does **not** use the network 192.168.100.x / 30 that is reserved for the DPU:

   A. Make sure that none of the Host Server interfaces are assigned an IP address from this network.

   B. Make sure there is no static route on the Host Server to this network.

   For more information, refer to the section "*Virtual Ethernet Interface*" in the NVIDIA BlueField-3 DPU documentation.
2. In the Host Server, install one or more BlueField-3 (DPU) cards.
3. On the Host Server, install the required DOCA OFED version.
4. On the DPU, install the required BFB version.

Step 2 - Configure the DPU (AIFF Security Gateway)

Procedure

1. On the Management Server, get the environment variables and their values for your Domain.

   Get this file from the Data Center Provider from the Management Server for your Domain:

- On a Security Management Server:

  ```
  home/admin/MDM/standalone/zero_touch_parameters.json
  ```

- On a Multi-Domain Security Management Server:

  ```
  /home/admin/MDM/<Name of Domain>/zero_touch_
  parameters.json
  ```

2. Copy these variables and their values from the "`zero_touch_parameters.json`" file you received from the Data Center Provider:
   - `MGMT_SERVER_IP`
   - `mgmt_server_fingerprint`
   - `mgmt_api_key`
   - `domain_name`
   - `aicp_policy_name`

   We recommend saving them aside for now. You use these parameters later during the installation of the AIFF Security Gateway (the "`AIFFctl`" script).

3. Get the Check Point AIFF package for the DPU:
   a. From sk184795 > section "Downloads", download the AI Factory Firewall package for the BlueField-3 DPU to your computer.
   b. Copy this AIFF package from your computer to the DPU.

      Follow one of these options:

      Option 1 - Through the BlueField-3 Out-of-band Management

      See *"Configuration of Out-of-Band Management Network" on page 63*.

      i. Configure an IP address on the "`oob_net0`" interface of the DPU.

         Make sure a computer with an SSH client and SCP client can reach this IP address.

ii. With the SSH client, connect from your computer to the IP address you configured on the "`oob_net0`" interface.

```
ssh <IP Address>
```

The default credentials are:

- Username - `ubuntu`
- Password - `ubuntu`

iii. On the DPU, create some directory for the AIFF package.

For example:

```
mkdir -v /var/log/AIFF
```

iv. With an SCP client, connect from your computer to the IP address you configured on the "`oob_net0`" interface.

The default credentials are:

- Username - `ubuntu`
- Password - `ubuntu`

v. Copy the AIFF package from your computer to the DPU to the new directory "`/var/log/AIFF`".

For more information, refer to the NVIDIA BlueField Platform Software Troubleshooting Guide.

Option 2 - Through the regular Host Server interface

i. Connect with an SCP client to one of the Host Server interfaces.

ii. Copy the AIFF package from your computer to the Host Server to some directory.

iii. With a built-in SCP client, copy the AIFF package from the Host Server to the DPU to the new directory "`/var/log/AIFF`":

```
scp -v /var/log/AIFF/<Name of package>
ubuntu@192.168.100.2:/var/log/AIFF/
```

The default credentials are:

- Username - `ubuntu`
- Password - `ubuntu`

4. On the DPU, install the AIFF package:

a. Go to the directory with the AIFF package:

```
cd /var/log/AIFF/
```

b. Assign the 'execute' permission to the scripts:

```
sudo chmod +x AIFFctl
```

c. Start the installation:

```
./AIFFctl install
```

Notes:

- The "`AIFFctl`" script:
  i. Verifies the environment prerequisites.
  ii. Prompts the user for the required installation parameters. See the prompts below.
  iii. Configures the internal networking of the BlueField-3, such that all of the required traffic passes through the Check Point Security Gateway.
  iv. Starts the AIFF Security Gateway Container.
  v. If you chose to use the Zero Touch installation, the script also:
    i. Creates the Security Gateway object.
    ii. Configures the Software Blades on the Security Gateway.
    iii. Connects the Security Gateway object to the Domain.
    iv. Installs the Security Policy whose name is specified in the parameter "`aicp_policy_name`" in the "`zero_touch_parameters.json`" file.
- The "`AIFFctl`" script saves all the entered configuration values in this file:
  `/etc/gwac/bf_standalone.conf`
  If you run the "`AIFFctl`" script again, it can automatically use these saved values to fill in the prompts.
  This makes repeated deployments faster and consistent.

The "`AIFFctl`" script is interactive and prompts for all required values:

i. `Host interface 0:`

   Use the default "`pf0hpf`" for entire workload protection for channel 0.

   Otherwise, use the relevant Host Server Virtual Function (for example, "`pf0vf0`") for specific workload protection. In this case, the script prompts you to enter the "`Host Interface 0 destination IP`", which is the IP address of the specific workload that uses this Virtual Function.

   See *"Example Diagrams of the Intra-DPU Network" on page 65*.

ii. `Host interface 1:`

   Use the default "`pf1hpf`" for entire workload protection for channel 1.

   Otherwise, use the relevant Host Server Virtual Function (for example, "`pf1vf0`") for specific workload protection. In this case, the script prompts you to enter the "`Host Interface 1 destination IP`", which is the IP address of the specific workload that uses this Virtual Function.

   See *"Example Diagrams of the Intra-DPU Network" on page 65*.

iii. `DHCP for management network (y/n):`

   If you entered "`n`":

   - `AIFF static IP address:`
   - `AIFF static IP prefix length (0-32): AIFF`
   - `Default gateway IP address:`

iv. `Zero Touch provisioning (y/n):`

   - If you entered "`n`":

     `Enter Initial SIC key:`

- If you entered "y" (meaning, use Zero Touch deployment):
  - `Management server IP:`

    Enter the value of "`MGMT_SERVER_IP`" from the "`zero_touch_parameters.json`" file for your Domain
  - `Management API key:`

    Enter the value of "`mgmt_api_key`" from the "`zero_touch_parameters.json`" file for your Domain
  - `Server fingerprint:`

    Enter the value of "`mgmt_server_fingerprint`" from the "`zero_touch_parameters.json`" file for your Domain
  - `Domain name:`

    Enter the value of "`domain_name`" from the "`zero_touch_parameters.json`" file for your Domain
  - `Policy name:`

    Enter the value of "`aicp_policy_name`" from the "`zero_touch_parameters.json`" file for your Domain
  - `Use default blade configuration? [...] (y/n):`
    - If you entered "`n`":

      `Activate blade '[blade-name]'? (y/n):`

      Enter "`y`" or "`n`" to activate or disable the Software Blade specified in "`[blade-name]`".

d. Wait for the installation script to finish.

   Note - This setup can take a few minutes, and it mostly runs in the background.

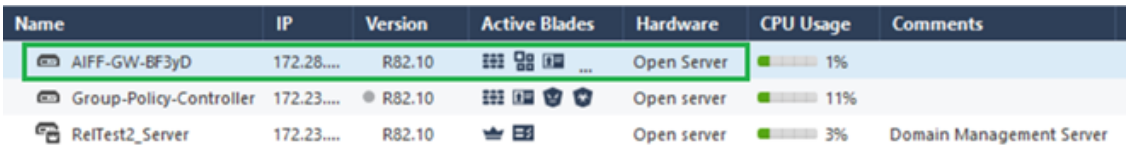
e. Connect with SmartConsole to the applicable Domain.

   If a Data Center Provider created the Domain for you, the Data Center Provider must provide the credentials for this Domain.

f. From the left navigation panel, click **Gateways & Servers**.

The AIFF Security Gateway object must appear.

Example:



Step 3 - Configure the Kubernetes Connection

Procedure

Follow the *R82.10 CloudGuard Controller Administration Guide* > Chapter "*Supported Data Centers*" > Section "*CloudGuard Controller for Kubernetes*":

1. Configure the applicable settings in Kubernetes.
2. In SmartConsole connected to the applicable Domain, configure the Kubernetes object.
3. Import objects from the Kubernetes: right-click the Data Center object and click **Import**.
4. Install the Access Control Policy on the AIFF Security Gateway.

Step 4 - Install Policy

Best Practice - Create the Access Control rules using your Data Center objects.

Installing policy on a specific AIFF Security Gateway

To install a policy on a specific AIFF Security Gateway:

1. Connect with SmartConsole to the Domain.

   If a Data Center Provider created the Domain, the Data Center Provider must provide the credentials for the Domain.
2. Click **Install Policy**.
3. Select **Access Control**.
4. Select **Threat Prevention**.

5. In the panel with the installation targets, select the **Group-Policy-Controller** object for any AIFF Security Gateways, on which you need to install this policy.
6. Click **Install**.

Note - To see the current policy name on a specific AIFF Security Gateway:

1. With an SSH client, connect to the IP address of the AIFF Security Gateway (as you see in SmartConsole).
2. Log in.
3. Run: `cpstat fw -f policy`
4. At the top of the output, refer to the row "`Policy name`".

Appendix

Creating a Virtual Function on the Host Server

Notes:

- If you wish the AIFF to protect **all** workloads (or for a PoC), you may skip this entire procedure and use the "*Entire workload protection*" on both channels.
- If you wish the AIFF to protect **specific** workloads, then on the Host Server you must create Virtual Functions (VFs) for these workloads (one VF for each channel).
  You configure an IP address for your workloads and use this information when the AIFF installation script (`AIFFctl`) prompts you for it.

This procedure enables SR-IOV for the BlueField-3 network function and creates one Virtual Function (VF) to be dedicated to a workload.

For reference, use NVIDIA DOCA Documentation > BlueField SR-IOV.

All low-level BlueField-3 configuration is performed using the Mellanox Firmware Tools (MFT).

Procedure:

1. Connect to the command line on the Host Server and log in.
2. Start the "MST" service:

   ```
   sudo mst start
   ```

3. Make sure the MST devices are available:

   ```
   sudo mst status -v
   ```

   In this output, locate the BlueField-3 network interface.

4. Identify the BlueField-3 network interface and the MST device.

   In our example, we use only channel 0:

   - Host Server Physical Function (PF) interface: `ens2f0`
   - MST device: `/dev/mst/mt41686_pciconf0`

   Important - Always make sure the BlueField-3 network interface and the MST device correspond to the same PCI function.

5. Check whether the SR-IOV support is already enabled for the identified BlueField-3 network interface:

```
sudo ls /sys/class/net/ens2f0/device/sriov_numvfs
```

   - If the file **exists**, then SR-IOV is already enabled. Skip to the next step.
   - If the file does **not** exist:
     a. Run these commands to enable SR-IOV for the identified the MST device:

```
sudo mlxconfig -e -d /dev/mst/mt41686_pciconf0 s PF_NUM_OF_VF_VALID=1
```

```
sudo mlxconfig -e -d /dev/mst/mt41686_pciconf0 s PF_NUM_OF_VF=1
```

     b. Reboot the Host Server (a full power cycle is required).

6. Create the Virtual Function (VF) for the identified BlueField-3 network interface:

```
echo 1 | sudo tee /sys/class/net/ens2f0/device/sriov_numvfs
```

   This creates one Host Server VF (in our example, "`ens2f0v0`") and a corresponding DPU VF representor (in our example, "`pf0vf0`").

7. Bring up the Host Server VF:

```
sudo ip link set ens2f0v0 up
```

8. Assign an IP address to the Host Server VF:

```
sudo ip addr add 20.20.20.8/8 dev ens2f0v0
```

9. Examine the VF on the Host Server:

```
sudo ip link show ens2f0v0
```

10. Examine the VF on the DPU:

```
sudo ip link show | grep pf0vf
```

At this point the VF exists, it is up, and has an IP address assigned.

Upgrading the AIFF Container

This section provides the steps to upgrade the AIFF container.

Warning - Schedule a maintenance window. When you install a higher version of the AIFF Container, the current AIFF Container stops.
Traffic starts passing again only after the new AIFF Container starts running again.

1. On the DPU, get the current version of the Check Point AIFF container:

   ```
   sudo crictl ps
   ```

   Refer to the column "`IMAGE`".

2. Get the latest Check Point AIFF package for the DPU:

   a. From sk184795 > section "Downloads", download the latest AI Factory Firewall package for the BlueField-3 DPU to your computer.

   b. Copy this AIFF package from your computer to the DPU.

   Follow one of these options:

   Option 1 - Through the BlueField-3 Out-of-band Management

   See *"Configuration of Out-of-Band Management Network" on page 63*.

   i. Configure an IP address on the "`oob_net0`" interface of the DPU.

   Make sure a computer with an SSH client and SCP client can reach this IP address.

   ii. With the SSH client, connect from your computer to the IP address you configured on the "`oob_net0`" interface.

   ```
   ssh <IP Address>
   ```

   The default credentials are:

   - Username - `ubuntu`
   - Password - `ubuntu`

iii. On the DPU, create some directory for the AIFF package.

For example:

```
mkdir -v /var/log/AIFF
```

iv. With an SCP client, connect from your computer to the IP address you configured on the "`oob_net0`" interface.

The default credentials are:

- Username - `ubuntu`
- Password - `ubuntu`

v. Copy the AIFF package from your computer to the DPU to the new directory "`/var/log/AIFF`".

For more information, refer to the NVIDIA BlueField Platform Software Troubleshooting Guide.

Option 2 - Through the regular Host Server interface

i. Connect with an SCP client to one of the Host Server interfaces.

ii. Copy the AIFF package from your computer to the Host Server to some directory.

iii. With a built-in SCP client, copy the AIFF package from the Host Server to the DPU to the new directory "`/var/log/AIFF`":

```
scp -v /var/log/AIFF/<Name of package>
ubuntu@192.168.100.2:/var/log/AIFF/
```

The default credentials are:

- Username - `ubuntu`
- Password - `ubuntu`

3. On the DPU, install the AIFF package:

a. Install the AIFF container:

```
/var/log/AIFF/AIFFctl install
```

b. Wait for the installation script to finish.

Note - This setup can take a few minutes, and it mostly runs in the background.

4. On the DPU, remove old unused AIFF packages:

```
sudo crictl rmi --prune
```

This command only deletes images that are not currently being used by a running or exited container.

Uninstalling the AIFF Container

This section provides the steps to uninstall the AIFF container and the corresponding Scalable Function (SF) settings.

Step 1 - Connect to BlueField-3

Procedure

1. Connect to the command line on the Host Server and log in.
2. Connect from the Host Server to the DPU's operating system over SSH:

   ```
   ssh ubuntu@192.168.100.2
   ```

   The default credentials are:

   - Username - `ubuntu`
   - Password - `ubuntu`
3. Go to the directory with the Check Point AIFF files:

   ```
   cd /var/log/AIFF
   ```

Step 2 - Uninstall the AIFF container

Procedure

Notes:

- When you remove the AIFF container:
  - No traffic will pass between the Scalable Function "`pf0sf0`" and the Scalable Function "`pf0sf1`".
  - No traffic will pass between the Scalable Function "`pf1sf0`" and the Scalable Function "`pf1sf1`".
- You remove the Scalable Functions and the OVS-switches created for them in the next step.

Warning - Traffic through the DPU will be blocked until you complete the next step to remove the Scalable Functions.

1. Run the script:

```
sudo ./AIFFctl uninstall
```

2. Examine the list of containers:

```
sudo crictl ps | grep AIFF
```

```
sudo crictl pods | grep AIFF
```

Expected output:

Empty.

Note - There should **not** be a container named "`AIFF`".

Troubleshooting Steps for a Data Center Provider

The "config_mds.py" script fails

Issue	Log File to Examine	Next Steps

■ Login failures.
■ Failure to configure an IP address.
■ Failure to configure an administrator. Failure to create an API key for the administrator.
■ Failure to configure API access settings.
■ Failure to configure Kubernetes objects.
■ Failure to configure the default policy package.
■ Failure to configure Access Control rules.
	On the MDSMS, examine this log file for API calls:
	`/home/admin/MDM/MDS_config_API.log`
	
	On the MDSMS, examine this general log file:
	`/home/admin/MDM/MDS_config.log`
		1. Examine the log files for the failure reason.
		2. Refer to the *Check Point Management API Reference* (at the top, select the correct version) to make sure the relevant API commands are executed with the required and correct parameters.
		3. Run the "`config_mds.py`" script again.

The "createDomain.py" script fails

Issue	Log File to Examine	Next Steps

■ Login failures.
■ Failure to configure a Domain.
	On the MDSMS, examine this log file for API calls:
	`/home/admin/MDM/createDomainApi.log`
	
	On the MDSMS, examine this general log file:
	`/home/admin/MDM/createDomain.log`
		1. Examine the log files for the failure reason.
		2. Refer to the *Check Point Management API Reference* (at the top, select the correct version) to make sure the relevant API commands are executed with the required and correct parameters.
		3. Run the "`createDomain.py`" script again.

■ Failure to configure the trusted client.
■ Failure to in Global Policy Assignment.
■ Failure to configure a Domain administrator.
■ Localhost failure.
	On the MDSMS, examine this log file for API calls:
	`/home/admin/MDM/createDomainApi.log`
	
	On the MDSMS, examine this general log file:
	`/home/admin/MDM/createDomain.log`
		1. Examine the log files for the failure reason.
		2. Connect with SmartConsole to the Multi-Domain Security Management Server to the "**MDS**" context.
		3. Manually execute the failed step in SmartConsole.

Issue	Log File to Examine	Next Steps

▪ Failure to configure the default policy package	On the MDSMS, examine this log file for API calls:
	`/home/admin/MDM/createDomainApi.log`
	
	On the MDSMS, examine this general log file:
	`/home/admin/MDM/createDomain.log`
		1. Connect with SmartConsole to the Multi-Domain Security Management Server to the "**MDS**" context.
		2. In SmartConsole, delete the new Domain.
		3. In SmartConsole, delete the new administrator.
		4. Close SmartConsole.
		5. Run the "`createDomain.py`" script again.

▪ Policy installation failure.	On the MDSMS, examine this log file for API calls:
	`/home/admin/MDM/createDomainApi.log`
	
	On the MDSMS, examine this general log file:
	`/home/admin/MDM/createDomain.log`
		1. Connect with SmartConsole to the new Domain.
		2. Manually install the policy called "`AIFF_Default`".

Troubleshooting Steps for an End-Customer

The Zero Touch Installation fails (AIFF Initialization)

Issue	Log File to Examine	Next Steps

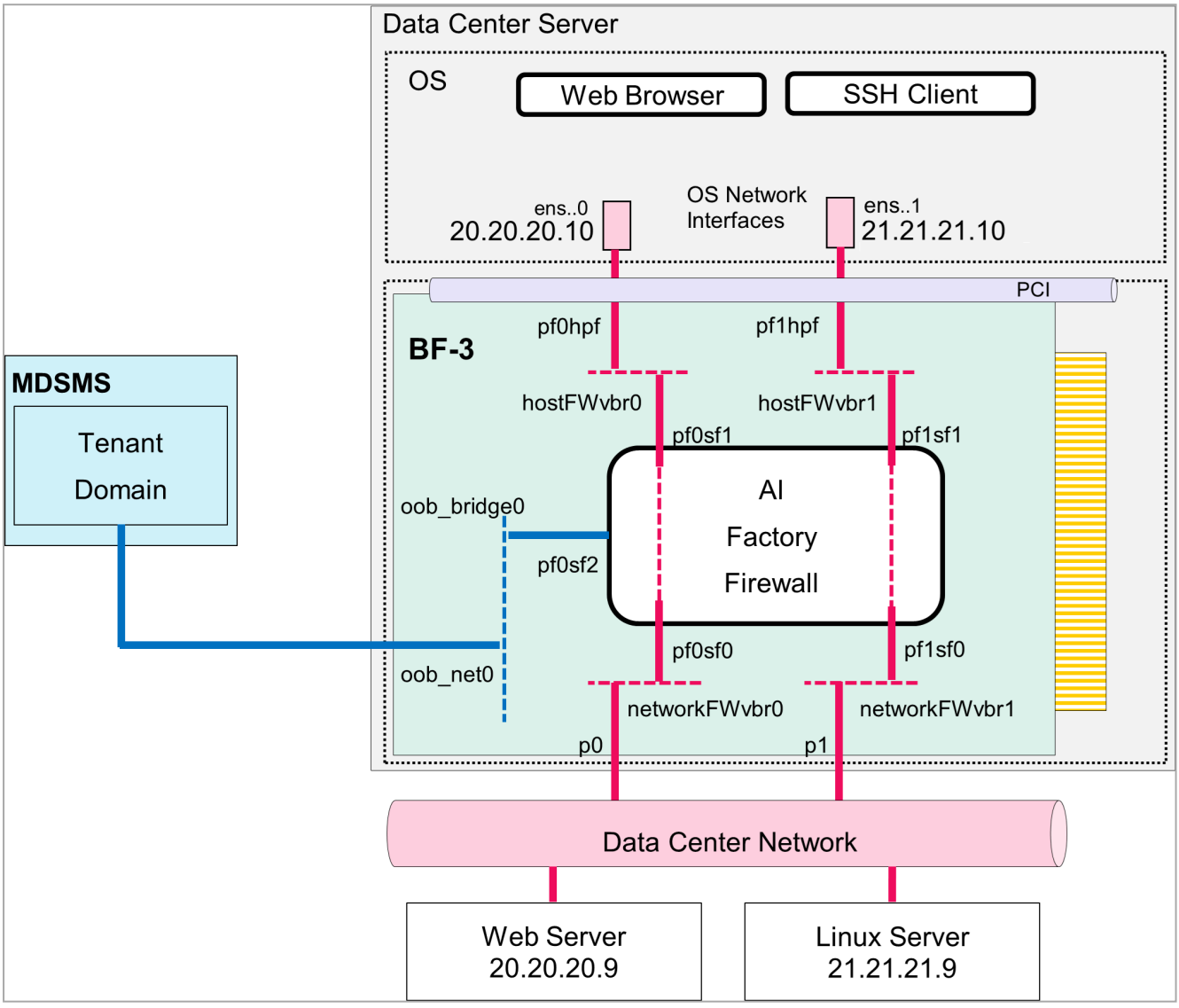
■ Missing executable or configuration files.
■ Missing environment variables.
■ Login failures.
■ Failure to create a Security Gateway object.
■ Failure to configure a Security Gateway object.
■ Failure to update the Topology in the Security Gateway object.
■ Policy installation failure.
	On the DPU, examine this Zero Touch log file:
	1. Get the Container ID:
	`sudo crictl ps`
	2. Show the log entries:
	`sudo crictl exec -it <Container ID> bash -c "cat -n /opt/CPsuite-R82.10/fw1/log/aicp/zero_touch.log"`
	
	In the AIFF container, examine this Zero Touch log file:
	`$FWDIR/log/aicp/zero_touch.log`
		1. Examine the log files for the failure reason.
		2. Ensure connectivity between the DPU and the Management Server.
		3. Refer to the *Check Point Management API Reference* (at the top, select the correct version) to make sure the relevant API commands are executed with the required and correct parameters.
		4. Make sure the software version of your container image is correct:
		`ctr -n k8s.io images import /var/log/AIFF/<Name of Container Package>`
		5. Reinstall the AIFF container using the latest available container package.

Policy Installation fails

Issue	Log File to Examine	Next Steps
Licensing issues.	Examine logs in SmartConsole.	1. Make sure a valid license is installed on the Multi-Domain Security Management Server. Contact your Data Center Provider. 2. Make sure a valid license is installed on the AIFF Security Gateway with this command: `cplic print` 3. Refer to the applicable troubleshooting in *Check Point Support Center*.

Configuration of Out-of-Band Management Network

Example Diagram



Procedure

Configure a bridge to connect the management port of the AIFF Security Gateway through the BlueField-3 interface "`oob_net0`" to the Check Point Management Server.

1. Connect the out-of-band interface (copper RJ45 connector) to a management network (for example, 192.168.17.0 / 24).

   You configure the corresponding interface "`oob_net0`" on the DPU in the next step.

   The management network must have a DHCP server, which the AIFF's management port will use to obtain an IPv4 address.

   Make sure the management network has access to the Management Server.

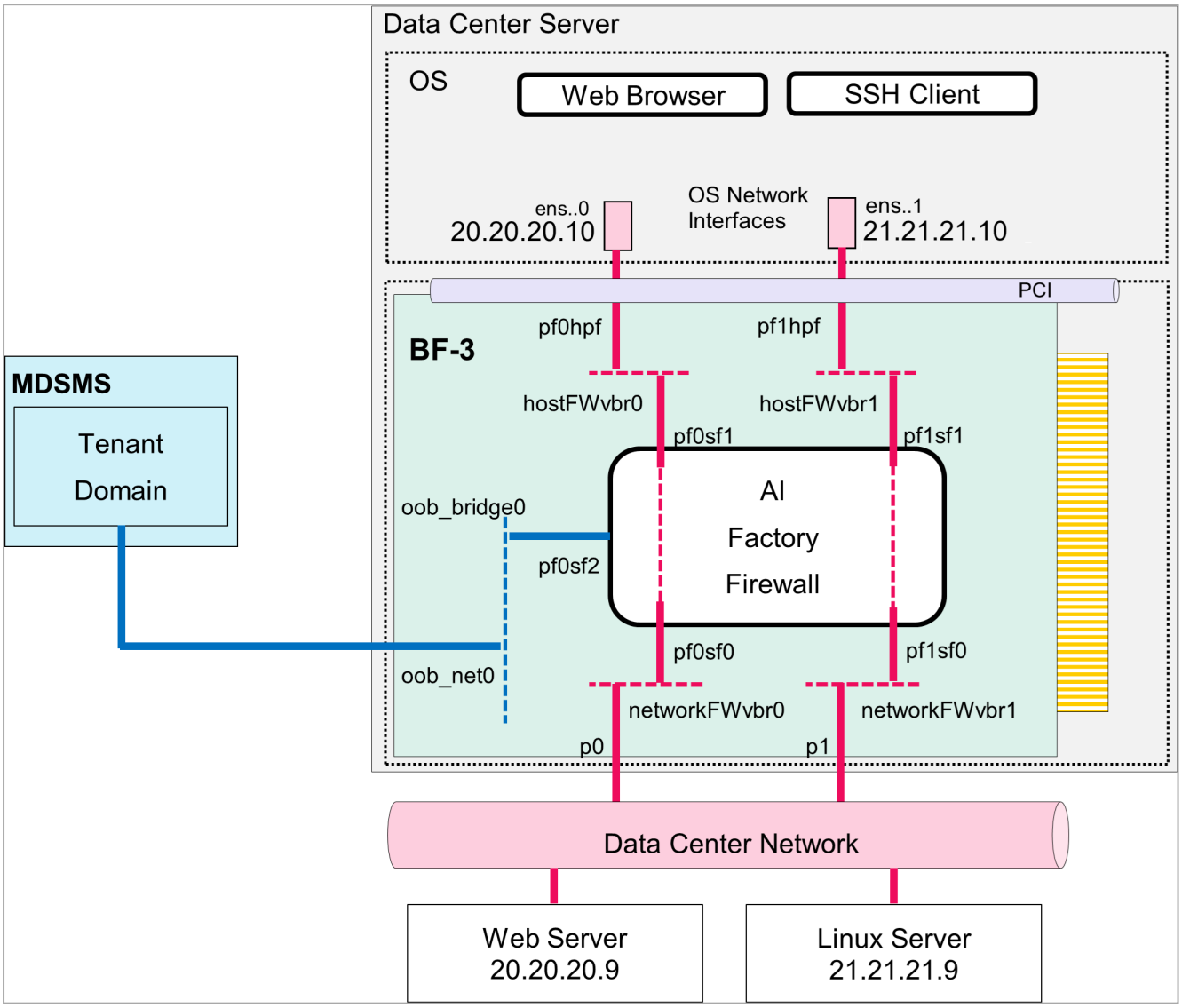
2. Create a persistent bridge (for example, "`oob_bridge0`").

   Add the BlueField-3 interface "`oob_net0`" to this bridge.

   Use the command "`netplan try`" to try the netplan and then apply the new netplan.

Example Diagrams of the Intra-DPU Network

Example Diagram - Entire Workload Protection with Out-of-Band Management



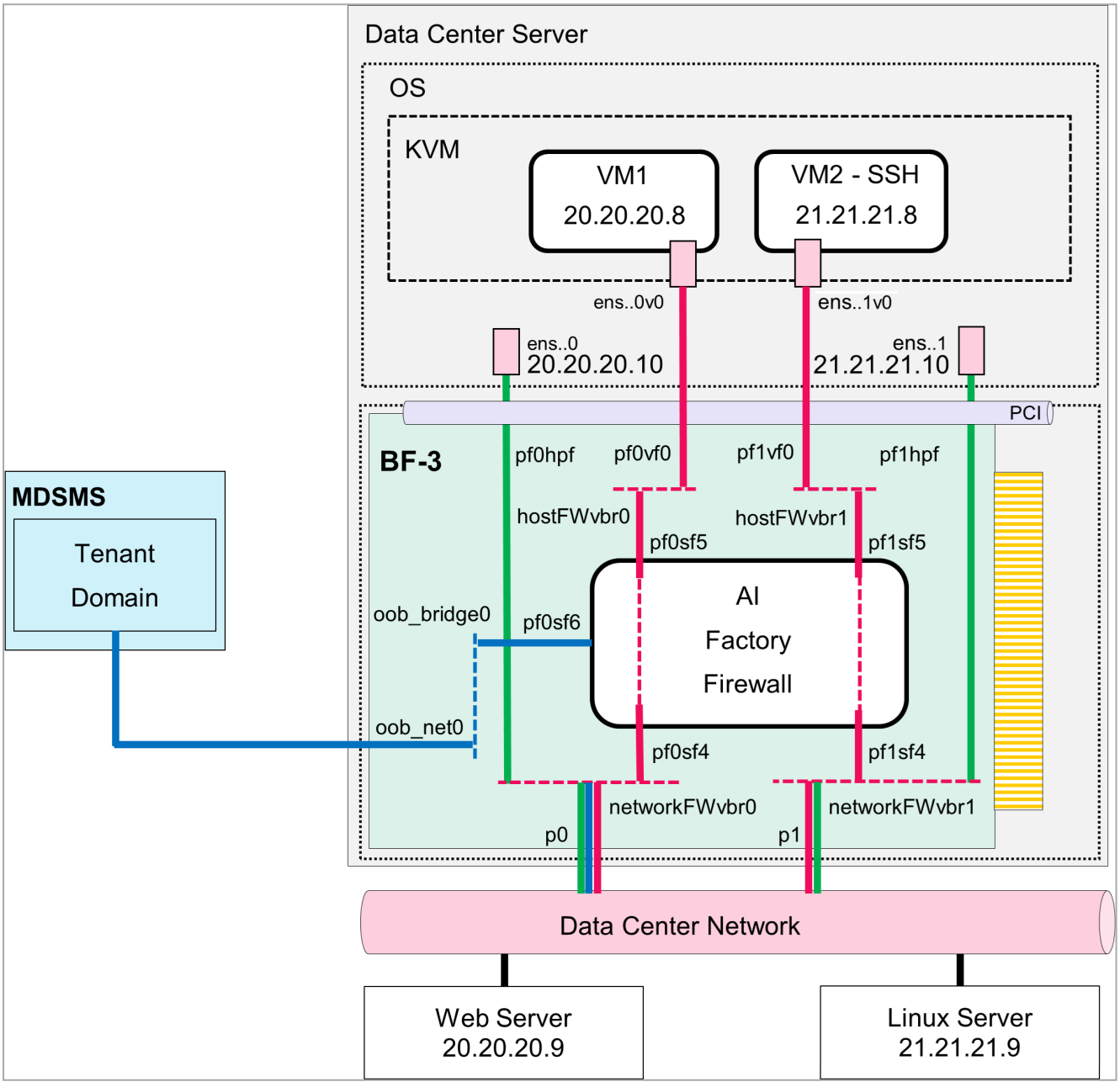
In this example diagram:

- The "Host Interface 0" is "`pf0hpf`".
- The "Host Interface 1" is "`pf1hpf`".

The Scalable Function (SF) pairs in this example diagram are:

- "`pf0sf0`" (Scalable Function for Data Center Network) and "`pf0sf1`" (Scalable Function for Host Server).
- "`pf1sf0`" (Scalable Function for Data Center Network) and "`pf1sf1`" (Scalable Function for Host Server).

Example Diagram - Specific Workload Protection



In this example diagram:

- The "Host Interface 0" is "`pf0vf0`" (representing Virtual Function 0 of "`ens...0`" - "`ens...0v0`").

  The "Host Interface 0" destination IP address is `20.20.20.8`.

- The "Host Interface 1" is "`pf1vf0`" (representing Virtual Function 0 of "`ens...1`" - "`ens...1v0`").

  The "Host Interface 1" destination IP address is `21.21.21.8`.

The Scalable Function (SF) pairs in this example diagram are:

- "`pf0sf4`" (Scalable Function for Data Center Network) and "`pf0sf5`" (Scalable Function for Host Server).
- "`pf1sf4`" (Scalable Function for Data Center Network) and "`pf1sf5`" (Scalable Function for Host Server).

Integrating AIFF with NVIDIA DOCA Argus

This section assumes that you are familiar with these products and how to configure them:

- NVIDIA DOCA Argus:
  - NVIDIA DOCA Argus Service Guide.
  - DOCA Argus Container Guide.
  - DOCA Container Deployment Guide.
- Check Point AI Factory Firewall:
  - *"Instructions for a Data Center Provider" on page 29*.
  - *"Instructions for an End-Customer" on page 43*.

This section describes only the specific steps to integrate these components.

Prerequisite

The AIFF Container must connect to the Internet to communicate with Check Point ThreatCloud.

Configuration Steps

Step 1 - In Check Point SmartConsole, configure the AIFF Security Gateway object

1. Connect with SmartConsole to the applicable Domain.
2. From the left navigation panel, click **Gateways & Servers**.
3. Double-click the AIFF Security Gateway object.
4. In the left panel, click the **General Properties** page.
5. On the **Threat Prevention** tab, select **Anti-Virus**.
6. In the **Anti-Bot and Anti-Virus First Time Activation** window:
   a. Select **According to the Threat Prevention Policy**.
   b. Click **OK**.
7. In the left panel, on the **Anti-Bot and Anti-Virus** page, leave the default settings.
8. Click **OK** to close the AIFF Security Gateway object.

Step 2 - In Check Point SmartConsole, configure the Threat Prevention Policy

1. From the left navigation panel, click **Security Policies**.
2. In the top panel, click **Threat Prevention** > **Custom Policy**.
3. In the **Action** column, you can select a different Threat Prevention Profile.
4. Install the Threat Prevention Policy on the AIFF Security Gateway.

Step 3 - Configure the Check Point AIFF Container

On the AIFF Container, it is necessary to configure the DOCA Argus log settings.

1. From the DOCA Argus Container's YAML configuration file (as defined in "`SERVICE_CONFIG_FILE`"), copy these settings:
   a. In the section "`volumes:`", copy the settings for "`name: logs-doca-app-shield-activity-report`".

   Example:

```
volumes:
- name: firewall-data
  hostPath:
    path: /opt/CheckPoint/AICloudProtect/data
    type: DirectoryOrCreate
- name: firewall-stat
  hostPath:
    path: /opt/CheckPoint/AICloudProtect/stat
    type: DirectoryOrCreate
- name: dev-vfio
  hostPath:
    path: /dev/vfio
    type: DirectoryOrCreate
- name: logs-doca-app-shield-activity-report
  hostPath:
    path: /var/log/doca_app_shield_activity_report
    type: DirectoryOrCreate
```

b. In the section "`volumeMounts:`", copy the settings for "`name: logs-doca-app-shield-activity-report`".

Example:

```
volumeMounts:
- name: firewall-data
  mountPath: /data
- name: firewall-stat
  mountPath: /stat
- name: dev-vfio
  mountPath: /dev/vfio
  readOnly: true
- name: logs-doca-app-shield-activity-report
  mountPath: /var/log/doca_app_shield_activity_report
```

2. On the AIFF Container, in the configuration file "`AIFF.yaml`":

   a. In the section "`volumes:`", configure the same settings for "`name: /var/log/doca_argus_activity_report`" as configured on the DOCA Argus Container.

   b. In the section "`volumeMounts:`", configure the same settings for "`name: /var/log/doca_argus_activity_report`" as configured on the DOCA Argus Container.

Step 4 - Configure the NVIDIA DOCA Argus Container

On the DOCA Argus Container, it is necessary to configure the AIFF log settings.

1. From the AIFF Container, from the configuration file "`AIFF.yaml`", copy these settings:

a. In the section "`volumes:`", copy the settings for "`name: logs-argus-activity-report`".

   Example:

```
volumes:
- name: logs-argus-service
  hostPath:
    path: /var/log/doca_argus
    type: DirectoryOrCreate
- name: logs-argus-activity-report
  hostPath:
    path: /var/log/doca_argus_activity_report
    type: DirectoryOrCreate
- name: conf-argus-config
  hostPath:
    path: /etc/doca_argus_config
    type: DirectoryOrCreate
```

b. In the section "`volumeMounts:`", copy the settings for "`name: logs-argus-activity-report`".

   Example:

```
volumeMounts:
  - name: logs-argus-service
    mountPath: /var/log/doca_argus
  - name: logs-argus-activity-report
    mountPath: /var/log/doca_argus_activity_report
  - name: conf-argus-config
    mountPath: /etc/doca_argus_config
```

2. On the DOCA Argus Container, in the YAML configuration file (as defined in "`SERVICE_CONFIG_FILE`"):

   a. In the section "`volumes:`", configure the same settings for "`name: logs-argus-activity-report`" as configured on the AIFF Container).

   b. In the section "`volumeMounts:`", configure the same settings for "`name: logs-argus-activity-report`" as configured on the AIFF Container.

c. In the section "`output:`", make sure the value of the parameter "`log_folder_path`" is **not** "`false`".

   Example:

```
output:
# Log events to stdout. Normally disabled for
production.
log_stdout: false
# Events will be logged to this file - 'false' to
disable
log_folder_path: /var/log/doca_argus_activity_report
...
```

d. In the section "`collection:`", make sure the values of all these parameters are "`true`":

   - In the section "`container:`":
     - `container_started: true`
     - `container_terminated: true`
   - In the section "`process:`":
     - `process_created: true`
   - In the section "`network_connection:`":
     - `network_connection_created: true`

Example Detection of a Malicious Process

1. A new process starts on the Host Server.
2. The DOCA Argus Container identifies that a new process started and reports it.

Example Log


```
{
  "vendor_name": "NVIDIA",
  "product_name": "DOCA_APPSHIELD",
  "product_version": "0.7.0",
  "message_type": "EVENT",
  "severity": "info",
  "schema_version": "1.0",
  "message_id": "803e912e2184a722dd57103c58ce9ac2f3d3b2a4",
  "occurred_message_timestamp_utc_ms": "1743940182060",
  "occurred_message_display_time_local_rfc3339": "2025-04-06T11:49:42.060+00:00",
  "occurred_message_display_time_utc_rfc3339": "2025-04-06T11:49:42.060Z",
  "bluefield_system_information": {
    "linux_version": "Linux BF3189 5.15.0-1050-bluefield #52-Ubuntu SMP Wed Jul 31
13:43:07 UTC 2024 aarch64 ",
    "ubuntu_linux_version": "22.04.5 LTS (Jammy Jellyfish)",
    "doca_version": "99.99.9999",
    "bluefield_networking_interfaces": {
      "0": {
        "bluefield_network_interface_name": "tmf1fo_net0",
        "bluefield_network_interface_mac_address": "XX:XX:XX:XX:XX:01",
        "bluefield_network_interface_ip_address": "fe80::21a:caff:feff:ff01,
192.168.100.2"
      },
      "1": {
        "bluefield_network_interface_name": "oob_bridge0",
        "bluefield_network_interface_mac_address": "XX:XX:XX:XX:XX:80",
        "bluefield_network_interface_ip_address": "fe80::9e63:c9ff:fe50:9380,
172.23.5.189"
      }
    }
  },
  "system_information": {
    "system_name": "baremetal"
  },
  "event_data": {
    "type": "process_created",
    "details": {
      "ns_net": "4026531840",
      "state": "RUNNING",
      "exit_time": "1743941490",
      "creation_time": "1741134640",
      "folder_path": "/usr/bin/containerd-shim-runc-v2",
      "ns_pid": "4026531836",
      "comm": "containerd-shim",
      "cmd_line_args": "/usr/bin/containerd-shim-runc-v2 -namespace k8s.io -id ba...15
-address /run/containerd/containerd.sock",
      "exec_id": "6",
      "file_size": "0",
      "ppid": "1",
      "ns_mnt": "4026531841",
      "cpu_cycles": "2828472434",
      "sha256": "N/A",
      "gid": "0",
      "sha1": "N/A",
      "pid": "5439",
      "uid": "0",
      "container_id": "ba...15"
    }
  }
}
```

3. The Check Point AIFF Container sends the process hash to the Check Point ThreatCloud database.
4. The process is identified as malware.
5. The Check Point AIFF Container sends a log to the Management Server.

   Example: