Release Notes

Intel Security Controller 2.0

Revision A

Contents

About this release

This release notes announces the launch of Intel® Security Controller virtual appliance version 2.0 software. In the release, you are provided several new features and enhancements for configuration and management of the Intel Security Controller virtual appliance.

The following table provides the compatible versions of the components for Intel Security Controller:

Release parameters	Versions
Intel Security Controller	2.0-3416
VMware NSX	6.1 or later
VMware vCenter Server	5.5 or later
VMware ESXi	5.5 or later
Openstack	Juno and Kilo

Intel Security Controller software version supports integration with the following products:

Table 1-1 Intel Security Controller compatibility matrix

Product	Versions supported
McAfee Network Security Platform Manager	• 8.1 — 8.1.3.4, 8.1.7.5, 8.1.7.13, 8.1.7.33 • 8.2 — 8.2.7.5, 8.2.7.24, 8.2.7.25, 8.2.7.27, 8.2.7.46, 8.2.7.71
McAfee Network Security Platform Sensor	8.1.7.17, 8.1.7.25
McAfee Next Generation Firewall	5.10 or later

New features

This release announces the new features as described in the sections below.

Integration with OpenStack

Intel Security Controller 2.0 announces support for integration with OpenStack as a virtualization provider. You will now be able to deploy IPS and next-generation firewall services on virtual machines in an OpenStack environment.

Intel Security Controller supports integration with the following versions of OpenStack:

- OpenStack Juno
- OpenStack Kilo
- OpenStack Liberty

If you are using OpenStack, the following distributions are supported:

- Redhat
- Mirantis
- HP
- Cononical (Ubuntu)
- Rakspace

For more information, see *Intel Security Controller 2.0 Product Guide*.

Integration with McAfee Next Generation Firewall

In this release, you are able to integrate **McAfee NGFW** with **Intel Security Controller** to provide next-generation firewall-based protection to virtual networks.

Intel Security Controller does not directly protect but orchestrates required actions by integrating with NSX or OpenStack, **SMC**, and **McAfee NGFW**. When you deploy the firewall service, Intel Security Controller orchestrates the automatic deployment of a Virtual Security System Container (VSS Container) instance in each ESXi host or OpenStack tenant.

A VSS Container instance is a Virtual Layer 2 Firewall Engine. Functionally, a VSS Container instance similar to **McAfee NGFW 5.10.0** Virtual Layer 2 Firewalls. However, it varies regarding deployment method, maintenance, and supported features.

When you deploy a security service, Intel Security Controller orchestrates inline inspection of traffic by the VSS Container instances. So all traffic related to the protected VMs is inspected for attacks. Should you migrate a VM to a different host within the same cluster, the VM is provided the same security services without the need to make any configuration changes.

Alarms and Alerts

You can now setup alarms that trigger alerts with this release. The alarms can be set for different types of failures like job failures, system failure, or appliance instance failures. Different severity levels can be defined for each type of failure, and also add an email notification to be sent out in case of a failure. To set an alarm, go to **Manage** | **Alarms**.

An alert is generated for every failure event that occurs. The description for the failure provides an easy way to troubleshoot the failure thereby reducing downtime. Alerts are generated with different severity level which depends on the severity level defined in the alarm. You can also acknowledge alerts that have been viewed so that you can filter alerts that require attention. To view the alerts generated, go to **Status** | **Alerts**.

Archives

With release 2.0, you can archive older jobs and alerts. Tasks related to the jobs are also archived. You can either set an auto schedule to archive the jobs and alerts, or manually trigger archiving whenever required. There are different options by which you can set a schedule for archiving. You can also download the previous archived files for analysis. To set up archiving, go to **Manage** | **Server** | **Archive**.

Security Groups

Several virtual environments do not allow you to define a security group to which you can deploy security services. Instead, when your assets and instances (which can be entire tenant networks or individual virtual machines) exist in a virtualization environment, Intel Security Controller 2.0 provides you the option to define a security group and deploy security services and policies to that group. This feature enables you to define which assets within OpenStack you want protected.

The **Security Groups** section is visible in the lower half when you navigate to **Setup** | **Virtualization Connector**.

Add a Security Group

When you click the **Add** button, the **Add Security Group** window appears. The order of elements that you must select are as follows:

1. Within this window, you must provide a name and select the appropriate tenant from OpenStack from the **Select Tenant** drop-down. All the tenants visible to the OpenStack administrator must be visible in the **Select Tenant** drop-down.

2. You must then select the region from the **Select Region** drop-down list. All regions available to the selected tenant must appear in this list.

3. Select the type of assets from the **Selection Type** options. You are presented with two choices:

   - **All Servers belonging to Tenant** – When you select this option, you are including every virtual machine instance present currently and virtual machines launched in the future. This is selected on behalf of that tenant for inclusion within the security group.

   - **By Type** – When you select this option, you have the following choices:

     - **VM** – choice of selecting individual virtual machines within the tenant. Any new network interface cards added to these servers will automatically be protected.

     - **NETWORK** – choice of selecting individual networks within the tenant. Any port connected to the network or added in the future is available to be included in the security group.

4. You must then select the items that are to be included from the available set.

Bind a Security Group to a policy

In order to protect your assets in a way that meets your security goals, you must use the appropriate policy by clicking the **Bind** button. When you click this button, the **Bind Policy to Security Group – <Tenant_Name>** window appears. In the Services section, you are provided a list of the **Distributed Appliances** configured on OpenStack.

1 Select the **Distributed Appliances** that meet your requirements by selecting the **Enabled** checkbox.

2 Choose the **Order** to specify the service function chaining to determine what order traffic is inspected in.

3 Select the **Inspection Policy** that you want Network Security Platform or McAfee NGFW to use to monitor traffic.

4 Select the **Failure Chaining Policy** as **FAIL_OPEN** or **FAIL_CLOSED** depending on your requirement and depending on which one is supported by your security service function.

5 Lastly, choose a dynamic deployment specification if this is applicable. To learn more about dynamic deployment specification, go to the section of these Release Notes, *Dynamic Deployment Specifications*.

Dynamic Deployment Specification

It is beneficial to learn about a Deployment Specification before learning about a Dynamic Deployment Specification. To learn about Deployment Specifications, go to the section, *Deployment Specifications*.

A Dynamic Deployment Specification is one that is created on demand to accommodate unique inspection requirements. Sometimes you might not want to create a Deployment Specification in advance. An example of such an instance is if you are a cloud service provider and are sharing your resources across several customers, you might have different service level objectives agreed on with different customers. In such circumstances, a customer to whom you have committed exclusive inspection to will not necessitate you to opt for sharing.

Clicking the hyper-link directs you to the **Dynamic Deployment Configurator** window in which you may select Dynamic Deployment Specifications that have been created.

In this window, you may click the **Create Dynamic Deployments** hyper-link to create a Dynamic Deployment Specification.

When you click this link, the **Add Dynamic Deployment Specification** window appears. In this window, perform the following steps:

1 Provide a name to the Dynamic Deployment Specification.

2 Select the tenant and region, from the OpenStack environment, from the drop-down lists.

3 Select the Management Network and the Inspection Network from the drop-down list.

4 Optionally, select the Floating IP Pool from the drop-down list.

Deployments

When you navigate to **Setup** | **Distributed Appliance** in the web-interface, you find a section in the lower-half of the **Distributed Appliance** screen known as the **Virtual Systems** screen. In release 2.0, you notice the **Deployments** button.

When you select an OpenStack-based **Distributed Appliance**, this button is enabled. If not, it is greyed out. When you click the **Deployments** button, you are routed to a sub-section known as the **Deployment Specification for Virtual System** section. Beside the name of the section, you are provided the **Virtual System** name and **Virtual Connector** that is used.

In this sub-section, you have the ability to create a deployment specification, which empowers you to mobilize the objective of your service deployment strategy. Since every implementation varies from another, you can employ a strategy that best suits your requirements. In the meanwhile, Intel Security Controller continually monitors the infrastructure to make sure that your objectives are implemented.

Examples of what you can achieve through a deployment specification are:

- deploy security services only on particular hosts or tenants
- provision more than one instance of a security service on a single host to load-balance traffic
- designate a set of hypervisor to have many security instances so as to handle all traffic flowing to and from VMs to pass through that host.

Creation of a deployment specification

When you click the **Add** button, the **Add Deployment Specification** window appears. In this window, you will need to follow the sequence of steps provided below:

1. Enter a name to identify the deployment specification within Intel Security Controller.
2. Select a tenant from the **Select Tenant** drop-down. All the tenants within a particular OpenStack deployment are visible in this drop-down list.
3. Select a region from the **Select Region** drop-down list. All the regions within a particular tenant are visible in this drop-down list.
4. Select the specific criterion from the **Selection Criterion** section that suits your service deployment strategy. The various options and their impact is described below:
    - **All (Hosts in selection Region)** – Deploy on one or more hosts that exist in and are added to the selected region. Intel Security Controller continually monitors infrastructure changes to implement your most recent requirements.
    - **By Availability Zone** – Deploy on one or more availability zones which appear in the list as defined in your OpenStack environment.

      In OpenStack, you have the ability logically organize compute hosts in groups. You can also consider creating a physical isolation from other availability zones by using a separate power source or network equipment.
    - **By Host Aggregates** – Deploy on one or more host aggregates which appear in the list as defined in your OpenStack environment.

      In addition to regions and availability zones, you can also create host aggregates in OpenStack. Host aggregates enable you to partition compute zones into logical groups for load balancing and instance distribution. You can use host aggregates to partition an availability zone into several groups of hosts that either share common resources, such as storage and network, or have a special property, such as trusted computing hardware.
    - **By Host** – Deploy on one or more hosts, across all regions within the tenant, which appear in the list. When you select this option, you have the option to deploy more than one instance of a security service.

    For more details about all of the above segregation constructs offered by OpenStack, refer to OpenStack Product Documentation.
5. Select the **Management Network**.

6 Select the **Inspection Network**.

> This network does not actually pass traffic through it and therefore does not require an IP address. It must be different from the network specified for the management network, or else you will receive an error.

7 Optionally, configure the **Select Floating IP Pool**, **Deployment Count**, and **Shared** checkbox.

Traffic Policy Mappings

When you navigate to **Setup** | **Distributed Appliance** in the web-interface, you find a section in the lower-half of the **Distributed Appliance** screen known as the **Virtual Systems** screen. In release 2.0, you find the **Traffic Policy Mappings** button, which when clicked on routes you to a sub-section known as the **Policy Mapping for Virtual Systems** with the **Virtual System** name beside it.

A traffic policy mapping refers to the inspection policy that is used for that virtual system. To add a traffic policy mapping, click the **Add** button. When you click **Add**, the **Add Policy Mapping** pop-up appears.

You will need to follow the sequence mentioned below:

1 Provide a name for the policy mapping within Intel Security Controller.

2 Click on the **Select Policy** drop-down list and select the appropriate policy. These policies are those that are configured in the security manager domain that you have selected while creating the **Distributed Appliance**.

3 Enter the **Tag**. The **Tag** refers to the ID of the inspection interface.

If two or policies exist in different domains of the security manager can have the same name, interfaces are automatically tagged with a unique ID in Intel Security Controller to distinguish them.

> This might not be relevant if this **Distributed Appliance** uses a McAfee NGFW security service since McAfee NGFW uses shared domains.

Email configuration

With release 2.0, you can now setup a SMTP server to receive emails when for critical failures. Depending on the alarms enabled, the email notification is sent to the email ID configured for that alarm. This helps you immediately troubleshoot all critical failures. To setup the SMTP server, go to **Manage** | **Server** | **Email**.

NAT details for network settings

Previously you could setup IP address for network settings. With this release, you can setup the NAT address for your network. To add the NAT address, go to **Manage** | **Server** | **Network**.

Enhancements

This release of Intel Security Controller version 2.0 provides the enhancements that are described at a high level in the sections that follow.

For more details on each of these features, refer to the *Intel Security Controller 2.0 Product Guide*.

UI enhancements

With release 2.0, you can now filter the tasks for jobs using the **Objects** column in **Tasks** section.

Virtualization Connector enhancements

The Virtualization Connector window has been enhanced with several features to support integration with OpenStack. When you log on to the Intel Security Controller web application and navigate to **Setup | Virtualization Connectors** and click the **Add** button, you are provided with options to choose the type of virtualization provider as either VMware or OpenStack.

If you select OpenStack to be your virtualization provider type, you can optionally set up an SDN Controller, which allows network programming capability and thereby separates the control plane from the data plane. You are able to steer or redirect traffic from the virtual machines to the inspection device, depending on the SDN controller you are using. You have three choices to select from. The following are the options, and the functionality and impact of each option:

- NSC (Network Security Controller) – A simple SDN controller used by used primarily to redirect traffic. It does not offer service function chaining, failure policy support, and off-box redirection.
- MIDO_NET – An full-service SDN controller developed by Midokura.
- NONE – Intel Security Controller can operate in a deployment-only mode in which it will not redirect traffic. Instead, your virtual network has its own infrastructure to redirect traffic. The only requirement is for the switching device to add an identifier which notifies the security service about which policy is to be used during traffic inspection.

Setting up an SDN Controller requires you to provide an IPv4 address and its relevant credentials unless you have selected **NONE**.

The other part of the configuration that is mandatory if you select OpenStack is the **Keystone** configuration. OpenStack Identity, code-named Keystone, is the identity management component in OpenStack. You must provide the IPv4 address, username, and password to the administrator tenant which must have sufficient privileges to query and perform all operations and must have to access other tenants in the environment.

In addition to the above settings, you also have the option to set up a RabbitMQ messaging broker by clicking the **Advanced Settings** button.

A message broker is used to translate messages from the formal messaging protocol of a sender into the formal messaging protocol of the receiver. In this context, it is used to translate messages between Intel Security Controller and OpenStack since each uses a unique messaging protocol.

RabbitMQ is an integral component of OpenStack. It is an open-source message broker software that implements Advanced Message Queuing Protocol. In this context, it is used to translate messages between Intel Security Controller and OpenStack since each uses a unique messaging protocol.

Security Groups enhancements

Within the **Virtualization Connector** window, you notice the **Security Groups** section in the lower-half of the window. Since the enhancements within this section are new features, refer the section, New features on page 2.

Service Function Catalog enhancements

To accommodate the need to deploy security instances on virtual machines that are present in OpenStack environments, every security service function must be uploaded to Intel Security Controller. In the same way that you upload security function software images (.ovf) for VMware-specific environments, you may upload equivalent software images (.qcow) images by going to **Setup | Service Function Catalog** and clicking **Auto Import.**

You can have .ovf and .qcow images of the same version of each security service function.

For more details, refer to the *Intel Security Controller 2.0 Product Guide*.

Distributed Appliance enhancements

Release 2.0 makes enhancements in the **Distributed Appliances** section to make deployment of a security service function, on OpenStack-based virtual machines, simple. Additionally, if you are integrating with McAfee NGFW, you have the option to select the appropriate **Manager Connector**.

When you log on to Intel Security Controller and navigate to **Setup** | **Distributed Appliance** and click the **Add** button, you are presented with **Add Distributed Appliance** window. However, if you are integrating with McAfee NGFW, you have the option to select the appropriate **Manager Connector**. Additionally, if you have imported an OpenStack-compatible image (.qcow) of a security software function, you are able to select this image from the **Service Function Definition** drop-down.

A requirement that is specific to OpenStack environments is selection of an appropriate **Encapsulation Type**. Traffic between the switch and the virtual security service is encapsulated depending on the what the security service supports. In this case VLAN is the only encapsulation type supported by virtual IPS, virtual NGFW, and virtual SNORT. The type of encapsulation is used to encapsulate and de-encapsulate each packet with a tag that represents the policy mapping that should be used for inspection by the relevant service. The tag can simply be header information which is specific to the security service.

Virtual Systems enhancements

Within the **Distributed Appliances** window, you notice the **Virtual Systems** section in the lower half of the window. Since the enhancements within this section are new features, refer the section, New features on page 2.

Resolved issues

There are no resolved issues in this release of the product.

Installation instructions

Intel® Security Controller

See the *Intel® Security Controller 2.0 Product Guide* for information about how to install the Intel Security Controller virtual appliance.

Security Management Center

For server requirements and information about how to install or upgrade the SMC, see *McAfee Next Generation Firewall 5.10.0 Product Guide*.

Virtual Security System

See the *Intel® Security Controller 2.0 Product Guide* for information about how the Virtual Security System instances are deployed.

VMware products

For information about how to install ESXi, vCenter Server, and NSX see the relevant VMware documentation at https://www.vmware.com/support/pubs/.

Openstack

For information about how to install OpenStack, refer to OpenStack documentation at http://docs.openstack.org/

Upgrade recommendations

See the *Intel® Security Controller 2.0 Product Guide* for information about how to upgrade the Intel Security Controller virtual appliance.

Known issues

For a list of known issues in this product release, see this Intel Security KnowledgeBase article — KB84920

Product documentation

Every McAfee product has a comprehensive set of documentation.

Find product documentation

1. Go to the McAfee ServicePortal at http://mysupport.mcafee.com and click **Knowledge Center**.
2. Enter a product name, select a version, then click **Search** to display a list of documents.

Intel Security Controller product documentation

Intel Security Controller 2.0 Product Guide

Copyright © 2015 McAfee, Inc. www.intelsecurity.com

Intel and the Intel logo are trademarks/registered trademarks of Intel Corporation. McAfee and the McAfee logo are trademarks/registered trademarks of McAfee, Inc. Other names and brands may be claimed as the property of others.