VMware Carbon Black Cloud Host-based Firewall FAQ

Table of contents

VMware Carbon Black Cloud Host-based Firewall FAQ

Operation

What is VMware Carbon Black Cloud Host-based Firewall?

VMware Carbon Black Cloud Host-based Firewall enables security teams to further consolidate their security stack by integrating firewall management capabilities directly into their endpoint and workload protection platform. By including Host-based Firewall capabilities in the Carbon Black Cloud platform, SOCs can leverage a single platform for more use cases, increasing their overall efficiency and reducing the resources needed to run their SOC.

Carbon Black Cloud Host-based Firewall provides the following centralized management features:

- Consolidated view to manage firewall rules across assets through the Carbon Black Cloud console.
- Association of ordered (ranked) rule groups to security policies; rule groups can be reused across security policies.
- Rules are evaluated in order of user-defined precedence.
- Ability to test rules before enforcement.
- Count of behaviours blocked by Host-based Firewall policy.
- Visibility into security posture of assets through the Alerts and Investigate pages in the Carbon Black Cloud console.

What operating systems are supported?

- Windows 11 22H2
- Windows 11
- Windows 10 21H2 x64
- Windows 10 21H1 x64
- Windows 10
- Windows 8.1 x64
- Windows Server 2012 R2 x64
- Windows Server 2016
- Windows Server 2019

Please refer to the 3.9 Sensor Release notes.

What products are required to purchase VMware Carbon Black Cloud Host-based Firewall?

VMware Carbon Black Cloud Host-based Firewall will be available for purchase as an add-on to Endpoint Standard, Advanced, or Enterprise, or Workload Advanced or Enterprise. Customers must have Endpoint Standard or Workload Advanced as a minimum requirement.

Can customers with Enterprise EDR-only purchase VMware Carbon Black Cloud Host-based Firewall?

No, customers must have Endpoint Standard or Workload Advanced to run VMware Carbon Black Cloud Host-based Firewall as it is directly tied to the Policy page. This includes customers with any Endpoint bundle (Standard, Advanced, Enterprise) and customers with the Workload Advanced or Enterprise bundles.

Prevention

What is the workflow for using VMware Carbon Black Cloud Host-based Firewall?

Customers are asked to use the below workflow:

1. Set Default rule
2. Create rule groups and rules
3. Enable rules that you have confidence in
4. Enable Host-Based Firewall on the Sensor tab
5. Use the test rule action on rules that have not been enabled to build confidence, then enable them as well.

Refer to the Tech Zone demo video for more detail.

What is the hierarchy/order of precedence in the VMware Carbon Black Cloud Host-based Firewall rules?

The VMware Carbon Black Cloud Host-based Firewall rules are applied from top to bottom, and the first firewall rule that matches the traffic overrides all the other rules in the VMware Carbon Black Cloud Host-based Firewall rule base.

Can you change the default rule once set?

The Default Rule can only be changed when HBFW is disabled from the Sensor page. The recommended setting is to allow all as the default rule. If you want the rule base to include a default deny, add an any/any deny all rule above the default (this gives you control over the default rule).

Do Prevention permission policies supersede VMware Carbon Black Cloud Host-based Firewall blocking rules?

No. For combined policy simplicity, the block always takes precedence.

Does device quarantine take precedent over VMware Carbon Black Cloud Host-based Firewall rules?

Yes. The block always takes precedence.

Why do I get a 400 error when attempting to enable VMware Carbon Black Cloud Host-based Firewall in a policy, under sensor tab?

This is because you MUST enable a default rule (allow all or block all) PRIOR to checking the box.

Why am I restricted to using IP addresses for source/destination?

Support for domain names and FQDN is being evaluated for our Roadmap.

Can you copy rules between policies?

Yes, VMware Carbon Black Cloud Host-based Firewall allows you to copy rules between policies, simplifying and quickening management and adoption. The copy module will only populate policies where VMware Carbon Black Cloud Host-based Firewall is enabled.

Detection

How can Alerts be investigated?

Alerts can be viewed in a process tree visualization. Alert triage shows events that occurred during an attack in an easy-to-understand format. Click into individual events for additional process information and take action all from a single page.

The search fields in the investigate page have also been updated to allow for network-based searches – please refer to the in-console search guide.

Does VMware Carbon Black Cloud Host-based Firewall give information on Non-Alert Events?

Yes. Benign events can be searched across in a console with intuitive fuzzy search and filtering capabilities. Benign events are stored for, by default, 30 days on the Carbon Black backend.

Integration

Is there a VMware Carbon Black Cloud Host-based Firewall API?

Yes, you can use the Carbon Black Open API platform to integrate with a variety of security products, including SIEMs, ticket tracking systems, and your own custom scripts. please refer to our developer network for more information.

How do you send bulk alert and events data to a SIEM?

You can use Carbon Black Cloud Data Forwarders to send bulk data regarding alerts and endpoint events to external destinations such as an Amazon Web Services (AWS) S3 bucket. Refer to VMware Docs: Data Forwarder.

General

Are there tools or services available to help customers migrate firewall rules from their current solution to VMware Carbon Black Cloud Host-based Firewall?

Yes. We have developed a script to ease the transition of rules from their current HBFW to VMware Carbon Black Cloud Host-based Firewall. This tool is being managed through our Support team.

For access to this tool, customers will need to submit a support ticket.

What happens if you have Windows Defender FW rules in place, and then turn on VMware Carbon Black Cloud Host-based Firewall?

VMware Carbon Black Cloud Host-based Firewall will take it over and overwrite the pre-existing Windows Defender FW rules, thus providing single console visibility and control of both NGAV and HBFW. The Windows Defender FW rules you had in place can be restored if the VMware Carbon Black Cloud Host-based Firewall solution is disabled.

Summary and Additional Resources

Conclusion

This document provided answers to the most popular Carbon Black Cloud Host-based Firewall FAQs.

Authors and Contributors

This document was created by:

- Raj Sahota, Senior Technical Marketing Architect, Security Business Unit