Configure ESA Antivirus Scanning After Attachment Removed

Contents

[Introduction](#)

[Background Information](#)

[Problem Statement](#)

[Environment](#)

[Recommendation](#)

[Why Attachment Dropping Is Not Sufficient](#)

[Related Information](#)

Introduction

This document describes whether antivirus scanning remains necessary after attachment removal on Cisco Email Security Appliance (ESA).

Background Information

Antivirus scanning must remain enabled on the Cisco Email Security Appliance (ESA) even when attachment-dropping rules are enabled, because attachment removal does not reliably remove all malicious content from every message structure.

Problem Statement

Administrators can assume that removing attachments eliminates malware risk and makes antivirus scanning unnecessary. This document explains why antivirus scanning must still be used after attachment removal.

Environment

This guidance applies to inbound and outbound email messages processed by the Cisco Email Security Appliance (ESA).

Recommendation

Antivirus scanning is required for messages even when attachment-dropping rules are enabled on the Cisco

Email Security Appliance (ESA).

Keep antivirus scanning enabled for all applicable mail flows after attachment removal policies are configured.

- Scan inbound email because malicious content can remain in message parts that are not removed by attachment-dropping rules.
- Scan outbound email because messages can still contain malware after attachment removal processing.
- Expect attachment-dropping rules to reduce risk, not to replace antivirus scanning.



Note: Expected outcome: attachment removal can reduce exposure to some file-based threats, but antivirus scanning is still needed to detect malicious content that remains in the message. Scope: this guidance addresses whether antivirus scanning is still required after attachment removal; it does not describe all malware detection features on ESA.

Why Attachment Dropping Is Not Sufficient

Attachment dropping reduces risk but does not eliminate it.

- Attachment is not a strict technical definition.
- ESA evaluates RFC-defined MIME parts, not a universal attachment object.
- Messages can be constructed in ways that bypass attachment-dropping logic because the term "attachment" is not a precise technical definition.
- Because email content can be structured in different MIME formats, attachment-dropping rules do not reliably remove all malicious content.
- Outbound mail can still carry malware.

Related Information

For more information, see:

- ESA Message Filter Action Descriptions
- Working with Message Filters