

# ESA FAQ: If attachments are dropped on the ESA, is it still required to do Anti-Virus scanning?



Document ID: 117832

Contributed by Nasir Shakour and Enrico Werner, Cisco TAC Engineers.

Jun 24, 2014

## Contents

### Introduction

If attachments are dropped on the ESA, is it still required to do Anti-Virus scanning?

## Introduction

This document describes whether it is required to Anti-Virus scan messages after attachments have been dropped on the Cisco Email Security Appliance (ESA).

## If attachments are dropped on the ESA, is it still required to do Anti-Virus scanning?

In general, it is always a good idea to scan for viruses. There is no strict definition for the term *attachment*, there are only MIME parts. It is common to use the term attachment, however, with an expectation that computers cannot tell what is meant by the term. What that actually means is that programmers must come up with a mapping between what users think of as attachments, and what is available to them in the message, which is controlled by the definitions of the Internet RFCs.

Refer to the ESA FAQ: On which specific parts of an email message do filter attachment rules apply on the ESA? Cisco document for a discussion of this definition.

For this reason, it is difficult to rigorously enforce *attachment* stripping, because there will always be alternative ways to construct a message that bypasses the engineers' best effort to implement the inexact term *attachment*. Also, even if you drop attachments on inbound mail, you might not be dropping attachments on outbound mail. ***Therefore it is good practice to scan outgoing email for viruses as well as incoming email.***

---

Updated: Jun 24, 2014

Document ID: 117832

---