What types of encryption does the encrypted() filter rule detect?

Document ID: 117884

Contributed by Scott Roeder and Enrico Werner, Cisco TAC Engineers.
Jul 08, 2014

Contents

Question

What types of encryption does the encrypted() filter rule detect?

In message filters, the encrypted() filter rule evaluates to TRUE for messages that are marked in their MIME type as either being PGP or S/MIME encoded.

For example, the following MIME headers would evaluate to TRUE for encrypted status:

```
Message-id: 41A37605.9080209@opus1.com
MIME-version: 1.0
Content-type: application/x-pkcs7-mime; name=smime.p7m
Content-transfer-encoding: base64
Content-disposition: attachment; filename=smime.p7m
Content-description: S/MIME Encrypted Message
```

The encrypted filter rule can only detect PGP and S/MIME encrypted data.

The encrypted filter rule does not evaluate to TRUE for messages that contain encrypted content. For example, it does not evaluate to TRUE for password protected ZIP files, or for Microsoft Word and Excel documents that include encrypted content.