SMTP Inspector

SMTP Inspector Overview

Type	Inspector (service)
Usage	Inspect
Instance Type	Multiton
Other Inspectors Required	`stream_tcp`
Enabled	`true`

Simple Mail Transfer Protcocol (SMTP) enables a mail client to send messages to a mail server. SMTP issues commands to deliver a message to a recipient. An SMTP server uses TCP port 25 for insecure sessions or TCP port 587 for SMTP over SSL/TLS.

The `smtp` inspector detects SMTP traffic and analyzes SMTP commands and responses.

The `smtp` inspector identifies the command, header, and body sections of SMTP messages, and extracts and decodes multi-purpose internet mail extensions (MIME) attachments. MIME attachments may include multiple attachments and large attachments that span multiple packets.

The `smtp` inspector identifies and adds SMTP messages to the Snort allow list. When enabled, intrusion rules generate events on anomalous SMTP traffic.

You can configure the `smtp` inspector to:

- Log sender email ID, recipient email ID, email headers, and attachment filenames along with all generated events for the session.
- Normalize SMTP command lines by removing extraneous space characters. The `smtp` inspector normalizes the space (ASCII 0x20) or tab (ASCII 0x09) characters.

- Ignore TLS-encrypted traffic to improve performance.
- Ignore plain-text mail data to improve performance.

Best Practices for Configuring the SMTP Inspector

We recommend that you follow the guidelines from RFC 2821 to configure the `smtp` inspector's core configuration parameters:

- `max_command_line_len`: 512 characters
- `max_header_line_len`: 1024 characters
- `max_response_line_len`: 512 characters

SMTP Inspector Parameters

SMTP service configuration

The `binder` inspector defines the SMTP `service` configuration. For more information, see the Binder Inspector Overview.

Example:

```
[
    {
        "when": {
            "service": "smtp",
            "role": any
        },
        "use": {
            "type": "smtp"
        }
    }
]
```

alt_max_command_line_len[]

Specifies an array of SMTP command and an alternate maximum line length for the command. The alternate maximum line length overrides the value of the `max_command_line_len` for the SMTP command. You can enable rule 124:4 to generate events for this parameter.

Type: array

Example:

```
{
    "alt_max_command_line_len": [
        {
            "command": "AUTH",
            "length": 240
        }
    ]
}
```

alt_max_command_line_len[].command

Specifies a command string.

Type: string

Valid values: SMTP command

Default value: See Table 1: SMTP Commands and Default Alternate Command Lengths.

alt_max_command_line_len[].length

Specifies an alternate maximum command line length. Specify `0` to disable the detection of the command line length for a command.

Type: integer

Valid range: `0` to `4,294,967,295 (max32)`

Default value: See Table 1: SMTP Commands and Default Alternate Command Lengths.

Table 1: SMTP Commands and Default Alternate Command Lengths

Command	Length
ATRN	255
AUTH	246
BDAT	255
DATA	246
DEBUG	255
EHLO	500
EMAL	255
ESAM	255
ESND	255
ESOM	255
ETRN	500
EVFY	255
EXPN	255
HELO	500
HELP	500
IDENT	255
MAIL	260

Command	Length
NOOP	255
ONEX	246
QUEU	246
QUIT	246
RCPT	300
RSET	255
SAML	246
SEND	246
SIZE	255
SOML	246
STARTTLS	246
TICK	246
TIME	246
TURN	246
TURNME	246
VERB	246
VRFY	255
XADR	246
XAUTH	246
XCIR	246
XEXCH50	246
X-EXPS	246
XGEN	246
XLICENSE	246
X-LINK2STATE	246
XQUE	246
XSTA	246
XTRN	246

Command	Length
XUSR	246

auth_cmds

Specifies a list of SMTP commands that initiate the authentication exchange. Separate multiple SMTP commands with a space.

Type: string

Valid values: SMTP authentication exchange initiation commands

Default value: `AUTH XAUTH X-EXPS`

b64_decode_depth

Specifies the maximum number of bytes to extract and decode from each Base64 encoded MIME email attachment. You can specify an integer less than 65535, or specify 0 to disable decoding. Specify -1 to place no limit on the number of bytes to decode.

You can enable rule 124:10 to generate events for this parameter, and in an inline deployment, drop offending packets when decoding fails.

Type: integer

Valid range: `-1` to `65535`

Default value: `-1`

binary_data_cmds

Specifies a list of SMTP commands that initiate sending data and use a length value (in octets) after the command to indicate the amount of data to be sent. Separate multiple SMTP commands with a space.

Type: string

Valid values: Valid SMTP data send initiation commands that use a data length argument

Default value: `BDATA XEXCH50`

bitenc_decode_depth

Specifies the maximum number of bytes to extract from each non-encoded MIME email attachment. You can specify an integer less than 65535, or specify 0 to disable the extraction of the non-encoded MIME attachment. Specify -1 to place no limit on the number of bytes to extract. These attachment types include 7-bit, 8-bit, binary, and various multipart content types such as plain text, JPEG and PNG images, and MP4 files.

Type: integer

Valid range: `-1` to `65535`

Default value: `-1`

data_cmds

Specifies a list of SMTP commands that initiate sending data and use an end of data delimiter (<CRLF>.<CRLF>).

Type: string

Valid values: SMTP data send initiation command that uses an end of data delimiter.

Default value: `DATA`

decompress_pdf

Specifies whether to decompress `application/pdf` (PDF) files in MIME attachments.

Type: boolean

Valid values: `true`, `false`

Default value: `false`

decompress_swf

Specifies whether to decompress `application/vnd.adobe.flash-movie` (SWF) files in MIME attachments.

Type: boolean

Valid values: `true`, `false`

Default value: `false`

decompress_vba

Specifies whether to decompress Microsoft Office Visual Basic for Applications macro files in MIME attachments.

Type: boolean

Valid values: `true`, `false`

Default value: `false`

decompress_zip

Specifies whether to decompress `application/zip` (ZIP) files in MIME attachments.

Type: boolean

Valid values: `true`, `false`

Default value: `false`

email_hdrs_log_depth

Specifies the number of bytes of the email header to extract from the SMTP data. Specify 0 to disable extraction of the email header.

Type: integer

Valid range: `0` to `20480`

Default value: `1464`

ignore_data

Specifies whether to decode the email data section (except for MIME mail headers).

Type: boolean

Valid values: `true`, `false`

Default value: `false`

ignore_tls_data

Specifies whether to decode TLS-encrypted data.

Type: boolean

Valid values: `true`, `false`

Default value: `false`

log_email_hdrs

Specifies whether to decode and log the SMTP email header and all generated events for the session.

Type: boolean

Valid values: `true`, `false`

Default value: `false`

log_filename

Specifies whether to decode and log the MIME attachment filenames extracted from the `Content-Disposition` header within the MIME body, and all generated events for the session. If the message contains multiple MIME attachments, the SMTP inspector logs the filenames separated by a comma. The SMTP inspector logs no more than 1024 bytes.

Type: boolean

Valid values: `true`, `false`

Default value: `false`

log_mailfrom

Specifies whether to decode and log the sender's email address extracted from the SMTP `MAIL FROM` command, and all generated events for the session. If the message contains multiple senders, the SMTP inspector logs the senders separated by a comma. The SMTP inspector logs no more than 1024 bytes.

Type: boolean

Valid values: `true`, `false`

Default value: `false`

log_rcptto

Specifies whether to decode and log the recipient email addresses from the SMTP `RCPT TO` command, and all generated events for the session. If the message contains multiple recipients, the SMTP inspector logs the recipients separated by a comma. The SMTP inspector logs no more than 1024 bytes.

Type: boolean

Valid values: `true`, `false`

Default value: `false`

max_auth_command_line_len

Specifies the maximum number of bytes accepted for the SMTP authentication command line.

You can enable rule 124:15 to generate events, and in an inline deployment, drop offending packets. Specify 0 to disable alerts on SMTP `AUTH` commands, or omit `max_auth_command_line_len` parameter from your Snort configuration.

Type: integer

Valid range: `0` to `65535`

Default value: `1000`

max_command_line_len

Specifies the maximum number of bytes accepted for the SMTP command line.

RFC 2821, the Network Working Group specification on SMTP, recommends a maximum command line length of 512 bytes. Specify 0 to disable alerts on SMTP command line length, or omit the `max_command_line_len` parameter from your Snort configuration.

You can enable rule 124:1 to generate events, and in an inline deployment, drop offending packets.

Type: integer

Valid range: `0` to `65535`

Default value: `512`

max_header_line_len

Specifies the maximum number of bytes accepted for the SMTP data header line.

RFC 2821, the Network Working Group specification on SMTP, recommends a maximum data header line length of 1024 bytes. Specify 0 to disable alerts on SMTP data header line length, or omit the `max_header_line_len` parameter from your Snort configuration.

You can enable rules 124:2 and 124:7 to generate events, and in an inline deployment, drop offending packets.

Type: integer

Valid range: `0` to `65535`

Default value: `1000`

max_response_line_len

Specifies the maximum number of bytes accepted for the SMTP response line.

RFC 2821, the Network Working Group specification on SMTP, recommends a maximum response line length of 512 bytes. Specify 0 to disable alerts on SMTP response line length, or omit the `max_response_line_len` parameter from your Snort configuration.

You can enable rules 124:3 to generate events, and in an inline deployment, drop offending packets.

Type: integer

Valid range: `0` to `65535`

Default value: `512`

normalize

Specifies whether to normalize all commands, no commands, or a list of commands. You can specify the list of commands in the `normalize_cmds` parameter. The inspector checks for more than one space (ASCII 0x20) or tab (ASCII 0x09) character after a command.

Type: enum

Valid values:

- `none`
- `cmds`
- `all`

Default value: `none`

normalize_cmds

Specifies a list of SMTP commands to normalize. Separate multiple SMTP commands with a space.

Type: string

Valid values: SMTP commands

Default value: None

qp_decode_depth

Specifies the maximum number of bytes to extract and decode from each quoted-printable (QP) encoded MIME email attachment. You can specify an integer less than 65535, or specify 0 to disable decoding. Specify -1 to place no limit on the number of bytes to decode.

You can enable rule 124:11 to generate events, and in an inline deployment, drop offending packets.

Type: integer

Valid range: `-1` to `65535`

Default value: `-1`

uu_decode_depth

Specifies the maximum number of bytes to extract and decode from each Unix-to-Unix encoded (uuencoded) MIME email attachment. You can specify an integer less than 65535, or specify 0 to disable decoding. Specify -1 to place no limit on the number of bytes to decode.

You can enable rule 124:13 to generate events for this parameter, and in an inline deployment, drop offending packets when decoding fails (due to incorrect encoding or corrupted data, for instance).

Type: integer

Valid range: `-1` to `65535`

Default value: `-1`

valid_cmds

Specifies an additional list of SMTP commands which the SMTP inspector considers valid.

The SMTP inspector defines a list of default, valid SMTP commands: `ATRN AUTH BDAT DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SIZE STARTTLS SOML TICK TIME TURN TURNME VERB VRFY X-EXPS X-LINK2STATE XADR XAUTH XCIR XEXCH50 XGEN XLICENSE XQUE XSTA XTRN XUSR`.

You can enable rule 124:5 to generate events, and in an inline deployment, drop offending packets.

Type: string

Valid values: SMTP commands

Default value: None

xlink2state

Specifies how the SMTP inspector handles packets that are part of X-Link2State Microsoft Exchange buffer data overflow attacks (See CVE-2005-0560 for a description of the vulnerability). You can disable detection (`disable`), enable detection and generate alerts (`alert`), or enable detection and drop the offending packets (`drop`).

You can enable rule 124:8 to generate events for this parameter, and in an inline deployment, drop offending packets.

Type: enum

Valid values:

- `disable`
- `alert`
- `drop`

Default value: `alert`

SMTP Inspector Rules

Enable the `smtp` inspector rules to generate events and, in an inline deployment, drop offending packets.

Table 2: SMTP Inspector Rules

GID:SID	Rule Message
124:1	attempted command buffer overflow
124:2	attempted data header buffer overflow
124:3	attempted response buffer overflow
124:4	attempted specific command buffer overflow
124:5	unknown command

GID:SID	Rule Message
124:6	illegal command
124:7	attempted header name buffer overflow
124:8	attempted X-Link2State command buffer overflow
124:10	base64 decoding failed
124:11	quoted-printable decoding failed
124:13	Unix-to-Unix decoding failed
124:14	Cyrus SASL authentication attack
124:15	attempted authentication command buffer overflow
124:16	file decompression failed

SMTP Inspector Intrusion Rule Options

vba_data

Sets the detection cursor to the Microsoft Office Visual Basic for Applications macros buffer.

Syntax: `vba_data;`

Examples: `vba_data;`