NAME

postscreen − Postfix zombie blocker

SYNOPSIS

postscreen [generic Postfix daemon options]

DESCRIPTION

The Postfix **postscreen**(8) server provides additional protection against mail server overload. One **postscreen**(8) process handles multiple inbound SMTP connections, and decides which clients may talk to a Postfix SMTP server process. By keeping spambots away, **postscreen**(8) leaves more SMTP server processes available for legitimate clients, and delays the onset of server overload conditions.

This program should not be used on SMTP ports that receive mail from end−user clients (MUAs). In a typical deployment, **postscreen**(8) handles the MX service on TCP port 25, while MUA clients submit mail via the **submission** service on TCP port 587 which requires client authentication. Alternatively, a site could set up a dedicated, non−postscreen, "port 25" server that provides **submission** service and client authentication, but no MX service.

postscreen(8) maintains a temporary whitelist for clients that have passed a number of tests. When an SMTP client IP address is whitelisted, **postscreen**(8) hands off the connection immediately to a Postfix SMTP server process. This minimizes the overhead for legitimate mail.

By default, **postscreen**(8) logs statistics and hands off every connection to a Postfix SMTP server process, while excluding clients in mynetworks from all tests (primarily, to avoid problems with non−standard SMTP implementations in network appliances). This mode is useful for non−destructive testing.

In a typical production setting, **postscreen**(8) is configured to reject mail from clients that fail one or more tests. **postscreen**(8) logs rejected mail with the client address, helo, sender and recipient information.

postscreen(8) is not an SMTP proxy; this is intentional. The purpose is to keep spambots away from Postfix SMTP server processes, while minimizing overhead for legitimate traffic.

SECURITY

The **postscreen**(8) server is moderately security−sensitive. It talks to untrusted clients on the network. The process can be run chrooted at fixed low privilege.

STANDARDS

RFC 821 (SMTP protocol)
RFC 1123 (Host requirements)
RFC 1652 (8bit−MIME transport)
RFC 1869 (SMTP service extensions)
RFC 1870 (Message Size Declaration)
RFC 1985 (ETRN command)
RFC 2034 (SMTP Enhanced Status Codes)
RFC 2821 (SMTP protocol)
Not: RFC 2920 (SMTP Pipelining)
RFC 3207 (STARTTLS command)
RFC 3461 (SMTP DSN Extension)
RFC 3463 (Enhanced Status Codes)
RFC 5321 (SMTP protocol, including multi−line 220 banners)

DIAGNOSTICS

Problems and transactions are logged to **syslogd**(8).

BUGS

The **postscreen**(8) built−in SMTP protocol engine currently does not announce support for AUTH, XCLIENT or XFORWARD. If you need to make these services available on port 25, then do not enable the optional "after 220 server greeting" tests, and do not use DNSBLs that reject traffic from dial−up and

residential networks.

The optional "after 220 server greeting" tests involve **postscreen**(8)'s built−in SMTP protocol engine. When these tests succeed, **postscreen**(8) adds the client to the temporary whitelist, but it cannot not hand off the "live" connection to a Postfix SMTP server process in the middle of a session. Instead, **postscreen**(8) defers attempts to deliver mail with a 4XX status, and waits for the client to disconnect. When the client connects again, **postscreen**(8) will allow the client to talk to a Postfix SMTP server process (provided that the whitelist status has not expired). **postscreen**(8) mitigates the impact of this limitation by giving the "after 220 server greeting" tests a long expiration time.

CONFIGURATION PARAMETERS

Changes to main.cf are not picked up automatically, as **postscreen**(8) processes may run for several hours. Use the command "postfix reload" after a configuration change.

The text below provides only a parameter summary. See **postconf**(5) for more details including examples.

NOTE: Some **postscreen**(8) parameters implement stress−dependent behavior. This is supported only when the default parameter value is stress−dependent (that is, it looks like ${stress?{X}:{Y}}, or it is the $*name* of an smtpd parameter with a stress−dependent default). Other parameters always evaluate as if the **stress** parameter value is the empty string.

COMPATIBILITY CONTROLS

postscreen_command_filter ($smtpd_command_filter)
A mechanism to transform commands from remote SMTP clients.

postscreen_discard_ehlo_keyword_address_maps ($smtpd_discard_ehlo_keyword_address_maps)
Lookup tables, indexed by the remote SMTP client address, with case insensitive lists of EHLO keywords (pipelining, starttls, auth, etc.) that the **postscreen**(8) server will not send in the EHLO response to a remote SMTP client.

postscreen_discard_ehlo_keywords ($smtpd_discard_ehlo_keywords)
A case insensitive list of EHLO keywords (pipelining, starttls, auth, etc.) that the **postscreen**(8) server will not send in the EHLO response to a remote SMTP client.

TROUBLE SHOOTING CONTROLS

postscreen_expansion_filter (see 'postconf -d' output)
List of characters that are permitted in postscreen_reject_footer attribute expansions.

postscreen_reject_footer ($smtpd_reject_footer)
Optional information that is appended after a 4XX or 5XX **postscreen**(8) server response.

soft_bounce (no)
Safety net to keep mail queued that would otherwise be returned to the sender.

BEFORE-POSTSCREEN PROXY AGENT

Available in Postfix version 2.10 and later:

postscreen_upstream_proxy_protocol (empty)
The name of the proxy protocol used by an optional before−postscreen proxy agent.

postscreen_upstream_proxy_timeout (5s)
The time limit for the proxy protocol specified with the postscreen_upstream_proxy_protocol parameter.

PERMANENT WHITE/BLACKLIST TEST

This test is executed immediately after a remote SMTP client connects. If a client is permanently whitelisted, the client will be handed off immediately to a Postfix SMTP server process.

postscreen_access_list (permit_mynetworks)
Permanent white/blacklist for remote SMTP client IP addresses.

postscreen_blacklist_action (ignore)
The action that **postscreen**(8) takes when a remote SMTP client is permanently blacklisted with the postscreen_access_list parameter.

MAIL EXCHANGER POLICY TESTS

When **postscreen**(8) is configured to monitor all primary and backup MX addresses, it can refuse to whitelist clients that connect to a backup MX address only. For small sites, this requires configuring primary and backup MX addresses on the same MTA. Larger sites would have to share the **postscreen**(8) cache between primary and backup MTAs, which would introduce a common point of failure.

postscreen_whitelist_interfaces (static:all)
A list of local **postscreen**(8) server IP addresses where a non−whitelisted remote SMTP client can obtain **postscreen**(8)'s temporary whitelist status.

BEFORE 220 GREETING TESTS

These tests are executed before the remote SMTP client receives the "220 servername" greeting. If no tests remain after the successful completion of this phase, the client will be handed off immediately to a Postfix SMTP server process.

dnsblog_service_name (dnsblog)
The name of the **dnsblog**(8) service entry in master.cf.

postscreen_dnsbl_action (ignore)
The action that **postscreen**(8) takes when a remote SMTP client's combined DNSBL score is equal to or greater than a threshold (as defined with the postscreen_dnsbl_sites and postscreen_dnsbl_threshold parameters).

postscreen_dnsbl_reply_map (empty)
A mapping from actual DNSBL domain name which includes a secret password, to the DNSBL domain name that postscreen will reply with when it rejects mail.

postscreen_dnsbl_sites (empty)
Optional list of DNS white/blacklist domains, filters and weight factors.

postscreen_dnsbl_threshold (1)
The inclusive lower bound for blocking a remote SMTP client, based on its combined DNSBL score as defined with the postscreen_dnsbl_sites parameter.

postscreen_greet_action (ignore)
The action that **postscreen**(8) takes when a remote SMTP client speaks before its turn within the time specified with the postscreen_greet_wait parameter.

postscreen_greet_banner ($smtpd_banner)
The *text* in the optional "220−*text*..." server response that **postscreen**(8) sends ahead of the real Postfix SMTP server's "220 text..." response, in an attempt to confuse bad SMTP clients so that they speak before their turn (pre−greet).

postscreen_greet_wait (normal: 6s, overload: 2s)
The amount of time that **postscreen**(8) will wait for an SMTP client to send a command before its turn, and for DNS blocklist lookup results to arrive (default: up to 2 seconds under stress, up to 6 seconds otherwise).

smtpd_service_name (smtpd)
The internal service that **postscreen**(8) hands off allowed connections to.

Available in Postfix version 2.11 and later:

postscreen_dnsbl_whitelist_threshold (0)
Allow a remote SMTP client to skip "before" and "after 220 greeting" protocol tests, based on its combined DNSBL score as defined with the postscreen_dnsbl_sites parameter.

Available in Postfix version 3.0 and later:

postscreen_dnsbl_timeout (10s)
The time limit for DNSBL or DNSWL lookups.

AFTER 220 GREETING TESTS

These tests are executed after the remote SMTP client receives the "220 servername" greeting. If a client passes all tests during this phase, it will receive a 4XX response to all RCPT TO commands. After the client reconnects, it will be allowed to talk directly to a Postfi x SMTP server process.

postscreen_bare_newline_action (ignore)
The action that **postscreen**(8) takes when a remote SMTP client sends a bare newline character, that is, a newline not preceded by carriage return.

postscreen_bare_newline_enable (no)
Enable "bare newline" SMTP protocol tests in the **postscreen**(8) server.

postscreen_disable_vrfy_command ($disable_vrfy_command)
Disable the SMTP VRFY command in the **postscreen**(8) daemon.

postscreen_forbidden_commands ($smtpd_forbidden_commands)
List of commands that the **postscreen**(8) server considers in violation of the SMTP protocol.

postscreen_helo_required ($smtpd_helo_required)
Require that a remote SMTP client sends HELO or EHLO before commencing a MAIL transaction.

postscreen_non_smtp_command_action (drop)
The action that **postscreen**(8) takes when a remote SMTP client sends non−SMTP commands as specifi ed with the postscreen_forbidden_commands parameter.

postscreen_non_smtp_command_enable (no)
Enable "non−SMTP command" tests in the **postscreen**(8) server.

postscreen_pipelining_action (enforce)
The action that **postscreen**(8) takes when a remote SMTP client sends multiple commands instead of sending one command and waiting for the server to respond.

postscreen_pipelining_enable (no)
Enable "pipelining" SMTP protocol tests in the **postscreen**(8) server.

CACHE CONTROLS

postscreen_cache_cleanup_interval (12h)
The amount of time between **postscreen**(8) cache cleanup runs.

postscreen_cache_map (btree:$data_directory/postscreen_cache)
Persistent storage for the **postscreen**(8) server decisions.

postscreen_cache_retention_time (7d)
The amount of time that **postscreen**(8) will cache an expired temporary whitelist entry before it is removed.

postscreen_bare_newline_ttl (30d)
The amount of time that **postscreen**(8) will use the result from a successful "bare newline" SMTP protocol test.

postscreen_dnsbl_ttl (1h)
The amount of time that **postscreen**(8) will use the result from a successful DNS blocklist test.

postscreen_greet_ttl (1d)
The amount of time that **postscreen**(8) will use the result from a successful PREGREET test.

postscreen_non_smtp_command_ttl (30d)
The amount of time that **postscreen**(8) will use the result from a successful "non_smtp_command" SMTP protocol test.

postscreen_pipelining_ttl (30d)
The amount of time that **postscreen**(8) will use the result from a successful "pipelining" SMTP protocol test.

RESOURCE CONTROLS

line_length_limit (2048)
Upon input, long lines are chopped up into pieces of at most this length; upon delivery, long lines are reconstructed.

postscreen_client_connection_count_limit ($smtpd_client_connection_count_limit)
How many simultaneous connections any remote SMTP client is allowed to have with the **postscreen**(8) daemon.

postscreen_command_count_limit (20)
The limit on the total number of commands per SMTP session for **postscreen**(8)'s built−in SMTP protocol engine.

postscreen_command_time_limit (normal: 300s, overload: 10s)
The time limit to read an entire command line with **postscreen**(8)'s built−in SMTP protocol engine.

postscreen_post_queue_limit ($default_process_limit)
The number of clients that can be waiting for service from a real Postfix SMTP server process.

postscreen_pre_queue_limit ($default_process_limit)
The number of non−whitelisted clients that can be waiting for a decision whether they will receive service from a real Postfix SMTP server process.

postscreen_watchdog_timeout (10s)
How much time a **postscreen**(8) process may take to respond to a remote SMTP client command or to perform a cache operation before it is terminated by a built−in watchdog timer.

STARTTLS CONTROLS

postscreen_tls_security_level ($smtpd_tls_security_level)
The SMTP TLS security level for the **postscreen**(8) server; when a non−empty value is specified, this overrides the obsolete parameters postscreen_use_tls and postscreen_enforce_tls.

tlsproxy_service_name (tlsproxy)
The name of the **tlsproxy**(8) service entry in master.cf.

OBSOLETE STARTTLS SUPPORT CONTROLS

These parameters are supported for compatibility with **smtpd**(8) legacy parameters.

postscreen_use_tls ($smtpd_use_tls)
Opportunistic TLS: announce STARTTLS support to remote SMTP clients, but do not require that clients use TLS encryption.

postscreen_enforce_tls ($smtpd_enforce_tls)
Mandatory TLS: announce STARTTLS support to remote SMTP clients, and require that clients use TLS encryption.

MISCELLANEOUS CONTROLS

config_directory (see 'postconf -d' output)
The default location of the Postfix main.cf and master.cf configuration files.

delay_logging_resolution_limit (2)
The maximal number of digits after the decimal point when logging sub−second delay values.

command_directory (see 'postconf -d' output)
The location of all postfix administrative commands.

max_idle (100s)
The maximum amount of time that an idle Postfix daemon process waits for an incoming connection before terminating voluntarily.

process_id (read−only)
The process ID of a Postfix command or daemon process.

process_name (read−only)
The process name of a Postfix command or daemon process.

syslog_facility (mail)
The syslog facility of Postfix logging.

syslog_name (see 'postconf -d' output)
The mail system name that is prepended to the process name in syslog records, so that "smtpd" becomes, for example, "postfix/smtpd".

SEE ALSO

smtpd(8), Postfix SMTP server
tlsproxy(8), Postfix TLS proxy server
dnsblog(8), DNS black/whitelist logger
syslogd(8), system logging

README FILES

Use "**postconf readme_directory**" or "**postconf html_directory**" to locate this information.
POSTSCREEN_README, Postfix Postscreen Howto

LICENSE

The Secure Mailer license must be distributed with this software.

HISTORY

This service was introduced with Postfix version 2.8.

Many ideas in **postscreen**(8) were explored in earlier work by Michael Tokarev, in OpenBSD spamd, and in MailChannels Traffic Control.

AUTHOR(S)

Wietse Venema
IBM T.J. Watson Research
P.O. Box 704
Yorktown Heights, NY 10598, USA