What is new in Zorp Professional 7

March 04, 2024

Table of Contents

1. Preface

Welcome to Zorp Professional (Zorp) version 7 and thank you for choosing our product. This document describes the new features and most important changes since the latest release of Zorp. The main aim of this paper is to aid system administrators in planning the migration to the new version of Zorp. The following sections describe the news and highlights of Zorp 7.

This document covers the Zorp Professional 7 product and its related components.

The latest release of Zorp Professional focuses on performance, security and stability improvements, in order to ensure reliable and controlled connectivity of your network infrastructure, while also delivering unique security features based on Zorp's proxy technology.

Warning
Currently it is not possible to upgrade an existing Zorp installation to version 7. To preview and test Zorp 7, you have to perform a complete installation on a new hardware or a virtual machine.

2. Online Certificate Status Protocol (OCSP) stapling

Zorp Professional 7 supports the usage of Online Certificate Status Protocol (OCSP) stapling in servers in encryption policies. Online Certificate Status Protocol (OCSP) stapling is an alternative to the so far available Certificate Revocation Lists (CRL) in verifying the validity of certificates. The protocol is described in details in IETF RFC 6960. It is now also possible to define to what level of strictness the encryption policies shall check the revocation status of the certificates.

Online Certificate Status Protocol stapling provides the following benefits:

- The solution enables a more convenient solution of assigning server operators for keeping revocation information up-to-date instead of requiring that from clients.
- Due to the smaller size of the used traffic data during OCSP stapling compared to CRL processes, the network load is smaller as well.
- Clients can verify the revocation state of a certificate with minor overhead.

For more details, see *Section 11.2.5, Verification of certificate revocation state* in *Zorp Professional 7 Administrator Guide*.

3. Reusable Encryption policies

Zorp Professional 7 introduces Encryption policies that make encryption settings (including SSL/TLS settings, certificates, and so on) easily reusable between Services and firewall rules. Also, the Zorp SSL framework has been redesigned to make configuration easier and clearer, by allowing you to configure encryption settings based on the scenario you need, for example, ClientOnlyEncryption, ForwardStartTLS, and so on. For details, see *Chapter 3, The Zorp SSL framework* in *Zorp Professional 7 Reference Guide*, *Section 5.5, Module Encryption* in *Zorp Professional 7 Reference Guide*, and *How to configure SSL proxying in Zorp 7*.

4. Server Name Indication

Zorp Professional 7 supports the Server Name Indication (SNI) TLS extension, as described in *RFC 6066*. You can configure a mapping between hostnames and certificates, and if the peer sends an SNI request, Zorp automatically selects the matching certificate to show to the peer. For details, see *Section 5.5.18, Class SNIBasedCertificate* in *Zorp Professional 7 Reference Guide* and *Procedure 4.1, Configuring Server Name Indication (SNI)* in *How to configure HTTPS proxying in Zorp 7*.

5. Supported operating system

Zorp Professional 7 now supports the Ubuntu 18.04 LTS (Bionic Beaver) operating system with the kernel supplied by Canonical. This results in better hardware support and a wider selection of installable software components.

6. Single log message as connection summary

Zorp Professional 7 introduces a single log message that contains all relevant information about the traffic passing through the firewall. This results in better traceability of traffic and more consistent access to information. The previous behaviour is kept as a default and the new log message needs to be explicitly enabled via sysctl and Zorp Professional's logspec setting. To enable such log messages, you have to:

- Execute the following commands on your firewall hosts:

```
echo "net.netfilter.kzorp.log_session_verdict = 1" >
/etc/sysctl.d/61-zorp-session-log.conf
service procps restart
```

- Change the logspec of the host to at least `core.summary:4`.

7. Extended usage statistics on firewall rules

Zorp Professional 7 supports providing statistics counters for firewall rules using of the `kzorp-client` utility. Zone and rule-related statistics are also collected and saved to the `/var/lib/zorp/kzorp/` directory.

8. Session reuse in SSL and TLS connections

Starting with version 6.0, Zorp supports session reuse in SSL and TLS connections. Zorp supports both session identifiers (*RFC 8446*) and session tickets (*RFC 8446*). Note that session tickets can be used only in TLS connections. Unless explicitly disabled in the configuration of the Encryption policy (for details, see *Section 5.5, Module Encryption* in *Zorp Professional 7 Reference Guide*), Zorp attempts to use session tickets, and automatically falls back to using session identifiers if needed.

9. Session persistence in load balancing

Zorp’s HTTP proxy offers the ‘session persistence in load balancing’ feature, further enhancing Zorp’s load balancing capabilities by that.

With the help of this feature, the Round Robin chainer can identify connections by their session IDs and make sure that every connection with the same session ID is always addressed to the same server, so that the session persists.

10. Other changes and improvements

- The default number of processes (the number of CPU cores that the instance can maximally use) was decreased from 4 to 1. This change affects only newly created instances, existing instances are not modified.
- The Dispatcher's Rate Limit option has been moved to the Rule object. The Rate Limit functionality was not available since version 3.5, but is available again in version 6.0. For details, see *Procedure 6.5.7, Connection rate limiting* in *Zorp Professional 7 Administrator Guide*.
- Zorp Professional 7 now supports the RFC 5424 (IETF) syslog protocol for remote syslog destinations.
- Zorp Professional 7 now supports the TCP protocol for OpenVPN (SSL VPN) connections. For details, see *Procedure 16.4.2, Configuring SSL connections* in *Zorp Professional 7 Administrator Guide*.
- The deprecated PSSL class has been removed and converted to the new SSL configuration method.
- The deprecated VirusBuster search engine has been removed, configurations still using this engine have been updated to explicitly drop traffic with an error message referencing the removal.
- The Zorp Management Console version 7 no longer supports the Windows XP operating system, as it has reached its End of Life. You can use ZMC on Windows Vista and later.
- The **Zorp > Instance > Edit parameters > General > Thread stack limit** option has been removed. From now on, a Zorp process uses the default value of the stack size of the host (which is currently 8 Mb for Ubuntu 18.04 LTS). Zorp uses this memory only when it is actually needed by the thread, it is not allocated in advance, thus resident memory consumption and performance are not affected by the change.
- The behaviour of the `-1` (--no-syslog) Zorp process parameter has changed, it does not imply the foreground mode any more by default. In order to achieve the old behaviour, that is to imply the foreground mode as well, the `-1` process parameter has to be applied together with the `-F` (--foreground) parameter.