Zorp

PROTECTION AT ALL LEVELS

In the frontline of technology

VIRUS FILTERING IN OVER 10 PROTOCOLS
RDP, SSH AND VNC CHANNEL CONTROL
SINGLE SIGN ON AUTHENTICATION

Zorp is a perimeter defense tool, developed for companies with extensive networks and high security requirements. Zorp inspects and analyzes the content of the network traffic to verify that it conforms to the standards of the network protocol in use (for example, HTTP, IMAP, and so on). Zorp provides central content filtering including virus- and spam-filtering at the network perimeter, and is capable of inspecting a wide range of encrypted and embedded protocols, for example, HTTPS and POP3S used for secure web browsing and mailing. Advanced authentication methods like Single Sign On and out-of-band authentication are supported as well. Zorp offers a central management interface for handling multiple firewalls, and an extremely flexible, scriptable configuration to suit divergent requirements.

Complete protocol inspection

In contrast with packet filtering firewalls, Zorp handles network connections on the proxy level. Zorp ends connections on one side, and establishes new connections on the other; that way the transferred information is available on the device in its entirety, enabling complete protocol inspection. Zorp has inspection modules for over 20 different network protocols and can inspect 100% of the commands and attributes of the protocols. All proxy modules understand the specifications of the protocol and can reject connections that violate the standards. Also, every proxy is capable to inspect the TLS or SSL encrypted version of the respective protocol.

Unmatched configuration possibilities

The more parameters of a network connection are known, the more precise policies can be created about the connection. Complete protocol inspection provides an immense amount of information - giving Zorp administrators unprecedented accuracy to implement the regulations of the security policy on the network perimeter. The freedom in customization helps to avoid bad trade-offs between effective business-processes and the required level of security.

Reacting to network traffic

Zorp can not only make complex decisions based on information obtained from network traffic, but is also capable of modifying certain elements of the traffic according to its configuration. This allows to hide data about security risks, and can also be used to treat the security vulnerabilities of applications protected by Zorp.

Supported protocols

- HTTP
- SOCKS
- SSL
- POP3
- TFTP
- SMTP
- MIME
- RSH
- Oracle SQL/Net8
- LDAP
- VoIP SIP
- SSH
- MS RPC
- FTP
- IMAP
- TELNET
- LPR
- RADIUS
- SOAP
- RDP
- VNC

Controlling encrypted channels

Zorp offers complete control over encrypted channels. The thorough inspection of embedded traffic can in itself reveal and stop potential attacks like viruses, trojans, and other malicious programs. This capability of the product provides protection against infected e-mails, or websites having dangerous content – even if they arrive in encrypted (HTTPS, POP3S, or IMAPS) channels. The control over SSH, SSL, and RDP traffic makes it possible to separately handle special features of these protocols, like port- and x-forwarding, or file- and printer sharing. Furthermore, the technology gives control over which remote servers can the users access by verifying the validity of the server's certificates on Zorp. That way the company security policy can deny access to untrusted websites or servers having invalid certificates.

Single Sign On authentication

Linking all network connections to a single authentication greatly simplifies user-privilege management and system audit. Zorp's single sign on solution is a simple and user-friendly way to cooperate with Active Directory. Existing LDAP, PAM, AD, TACACS, and RADIUS databases integrate seamlessly with Zorp's authentication module. Both password-based and strong (S/Key, SecureID, X.509, etc.) authentication methods are supported.

Centralized management system

The easy-to-use, central management system provides a uniform interface to configure and monitor the elements used in perimeter defense: Zorp devices, content vectoring servers, as well as clusters of these elements. Different, even completely independent groups of Zorp devices can be managed from the system. That way devices located on different sites, or at different companies can be administered using a single interface.

Stopping viruses at the network perimeter

Zorp provides a platform for antivirus engines. Using Zorp's architecture, these engines become able to filter data channels they cannot access on their own. Zorp's modularity and over 20 proxy modules enables virus filtering products to find malicious content in an unparalleled number of protocols, and their encrypted versions – for example, even in HTTP traffic transferred in an SSH tunnel.

Special features

- operates as a transparent proxy
- application-level protocol inspection
- authentication server and client
- user-level QoS
- SSO authentication on the network perimeter
- graphical management interface (Linux, Windows)
- VPN support
- load balance and HA clustering support
- content vectoring in over 10 protocols
- inspects encrypted and embedded protocols

Learn more

- Zorp homepage
- Request a demo
- Request a callback