kaspersky BRING ON THE FUTURE

Kaspersky® Web Traffic Security

Strategic defense against web-based threats

Kaspersky Web Traffic Security protects corporate IT networks from the dangers of the World Wide Web, while mitigating the risk of data leaks and helping increase productivity by governing internet use. Its breadth of features, versatility and responsiveness enable this application to safeguard a broad range of corporate scenarios speedily and effectively. Kaspersky Web Traffic Security is a core component of Kaspersky Security for Internet Gateway, and an integral part of our infrastructure-spanning Kaspersky Total Security for Business solution.

Highlights:

- Multi-layered anti-malware and anti-phishing protection
- Zero-hour threat protection
- Content filtering
- Ransomware blocking
- Web Control
- Scalable for high-loaded networks
- Backed by global threat intelligence from Kaspersky Security Network
- Role-based access to admin and web usage
- Microsoft Active Directory support
- Multi-tenancy for MSPs and diversified business units
- Monthly subscription licensing option
- Offered as a standalone application or a ready-to-use appliance
- Kaspersky Anti Targeted Attack integration for automated response

Key benefits

Cuts the risk of infection with combined protection and control

Stops incoming threats at gateway level so they never reach your endpoints, reducing the risk from social engineering based threats and vulnerability exploitation. Enables you to control and restrict the use of internet resources, minimizing user error-based incidents and the proliferation of shadow IT.

Boosts the effectiveness of your corporate gateway protection

With one of the most powerful stacks of protective technologies in the industry, superior detection rates and near-zero false positives, the application integrates into the Kaspersky solutions family, or can be used to add a significant performance boost to your current web gateway countermeasures.

Adapts to your requirements

Scales to your needs and corporate structure, supporting hierarchical deployment, multiple node and multi-tenant management and role based access control and delegation. Lean configuration options enable the processing of huge bandwidths in telco-type environments.

Stand-alone App or Software Appliance	Simplified deployment via an all-in one software appliance including its own pre-configured proxy server, or installed into your existing system as a stand-alone app – you choose. Either way, expect minimum hassle

Features

Multi-layered threat protection and control, powered by data science

Kaspersky's next-generation malware protection and control incorporates multiple proactive security layers, including:

Anti-malware

Industry-proven protection through proactive, machine learning powered detection, analysis and filtering technologies that identify and block malware threats including spyware, financial Trojans, ransomware, miners and wipers.

Real-time new threat detection

The Kaspersky Security Network infrastructure, powered by constantly updating intelligence from tens of millions of global users and our world-leading research, supports the real-time detection of potential threats even as they emerge, with minimal false positives.

Emulative sandboxing

Attachments are executed and analyzed in a safe emulated environment, protecting against even the most sophisticated, heavily obfuscated malware,

Script detection

Identifies and deals with scripts embedding malware into apparently harmless files heading for your endpoints, and those used in drive-by web-based attacks.

Reputation-based filtering

File and address reputations delivered by the constantly renewed Kaspersky Security Network cloud databases mean suspicious or unwanted files and internet resources can be blocked without the need for deeper analysis.

Advanced anti-phishing

Detection models support cloud-assisted protection from both known and unknown/zero hour online phishing through the neural network-based analysis of over 1,000 criteria – including pictures, language checks, specific scripting – combined with globally acquired data about malicious and phishing URLs and IP addresses.

Content filtering

File types known to be potentially problematic or irrelevant can be prohibited from transmitting - based on parameters including name, extension/type (Format Recognizer is used to spot files with spoofed extensions), size, MIME type (video, pictures etc) or hash.

Web control

Administrators can create rules blocking access to web resources based on pre-defined categories or their own lists, reducing risk and helping eliminate online user distractions. A Default Deny scenario can be implemented if required, restricting access to web resources not essential to the user or group's work.

Deployment Options

Choose between a stand-alone app[1] for integration into your current systems, or the simplicity of deploying a ready-to-use software appliance.

Our software appliance option features:

- All-in-one readiness: Everything needed to deploy a Secure Web Gateway (SWG) in just a few clicks – including a pre-configured proxy server.
- Management: The appliances' web interface includes everything needed to manage the incorporated proxy server, avoiding the hassle of a command line-based configuration process.
- Out-of-the box traffic monitoring: So-called 'SSL/TLS bumping' is pre-configured, requiring only a few simple administrative actions to start securing encrypted web traffic.

The standalone app allows for:

- Resource economy: No need for a whole separate workload; the app can be installed on a multi-functional server, alongside other apps.
- Tighter integration with existing configuration: In complex environments, the ability to install and configure the security app separately from other gateway components allows for greater efficiency.

Flexibility and Integration

Highly adaptable and almost infinitely scalable, Kaspersky Web Traffic Security is designed to integrate readily into your current IT infrastructure.

Security for ICAP-enabled system

Traffic can be secured on any device supporting the ICAP protocol – not just proxy servers.. This could include Network Attached Storages (NAS), or other systems that can't be protected by an internal security solution.

Two-way integration with Kaspersky Anti Targeted Attack

API-based integration with Kaspersky's targeted attack detection powerhouse provides extra context for the deeper analysis of advanced threats, as well as automatically blocking attack components and attacker activities over the internet – including the transmission of commands, further payloads and stolen data exfiltration.

SIEM integration

Enriches the content of your Security Information and Event Management (SIEM) system through exporting information in Common Event Format (CEF), together with widely used syslog.

Ideal for Managed Service Providers

Powerful web gateway protection services are made easier to administer on behalf of clients with:

- Multi-tenancy - assign dedicated areas ('workspaces') to each serviced client, and manage them separately, combining 'global' and 'local' policies as appropriate.
- Role-based Access Control – provide the level of control over their specific workspace that you deem appropriate to each serviced client.
- Subscription-based licensing complements monthly service charging and budgeting models.

Convenient management

Kaspersky Web Traffic Security offers a flexible yet easy-to use management system.

Centralized console

Control all your ICAP-capable systems' security, including proxies and storages, via a single-point web interface providing excellent visibility and manageability.

[1] Not available during BETA testing

Convenient dashboard

Everything needed to gauge the current state of corporate security at gateway level is collected into a single dashboard, giving an instant and complete overview of the situation, including urgent events.

Threat Event management

Threat analysis results are presented using an event-centric approach and show real-time activity. Users' internet behavior can also be analyzed.

Flexible rules configuration

A flexible but easy-to-use rules configuration system enables granular management of gateway security with minimal upskilling involved.

Active Directory integration

For the configuration and ongoing synchronization of role-based access rules and security policies with your network and infrastructure.

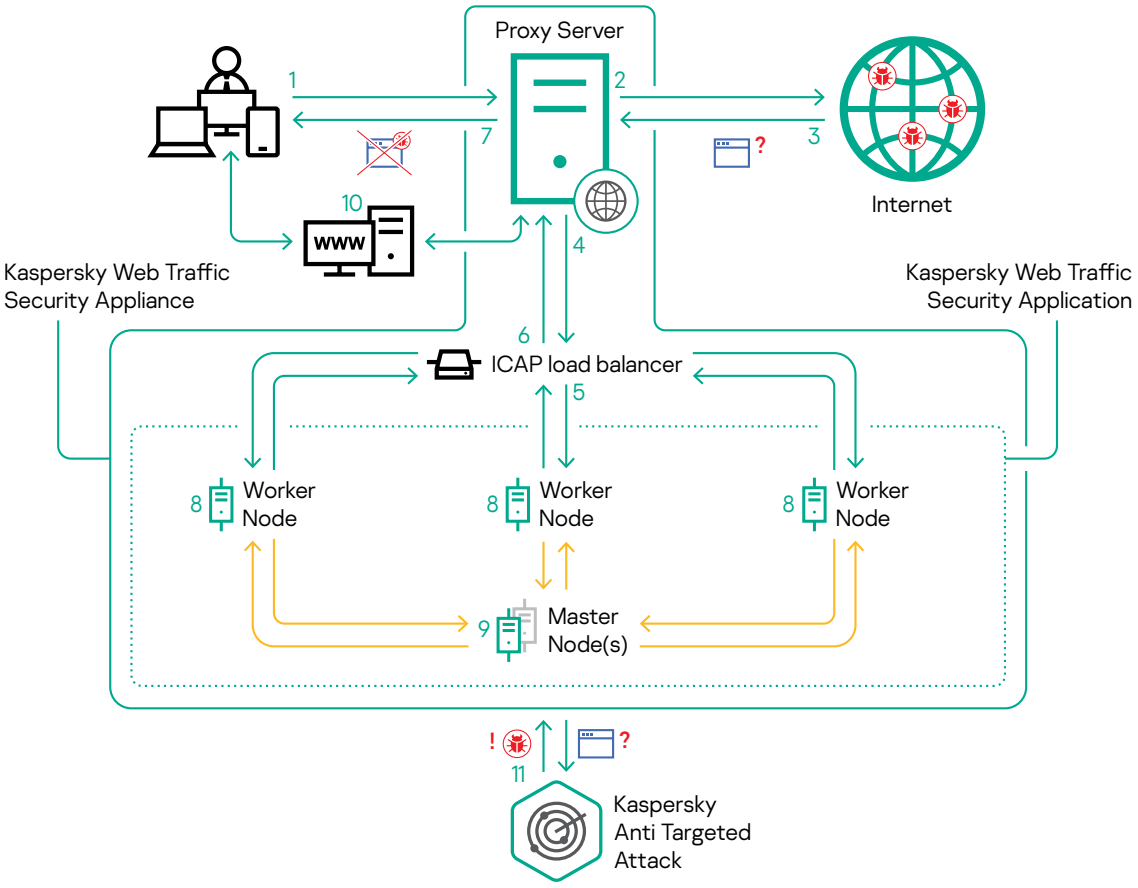
Role-Based Access Control (RBAC)

Different administrative roles can be defined, and separate rights and restrictions allocated to each – greatly assisting internal task delegation and the provision of appropriate levels of control to serviced clients.

Multi-tenancy

Assign dedicated areas ('workspaces') to different business units or clients and manage them separately, combining 'global' and 'local' policies as appropriate.

Kaspersky Web Traffic Security architecture



1. User requests information from the Internet through the corporate proxy server (via http(s), ftp).
2. Proxy server looks for the requested web resource.
3. Requested resources are sent to the proxy.
4. Through load balancer, proxy server sends objects to our system using ICAP.
5. Load balancer* chooses a working node and transmits objects for checking.
6. Worker node returns verdict to the proxy server.
7. Proxy server delivers proven safe web pages and objects, as well as verdicts about found threats to the user.
8. Worker nodes represent ICAP servers for object scanning, based on traffic processing rules. Default rule includes antimalware and anti-phishing check. URL categorization and content filtering are also available.
9. The central (master) node handles event data collection and management. It hosts the Kaspersky web interface for management of settings, and also provides dashboards for real-time monitoring of security events and system health.
10. Windows Domain Controller authenticates user or device on the proxy server via Kerberos or NTLM.
11. The results of the advanced analysis are used to block advanced threats' elements.

Hardware and software requirements

Minimum hardware requirements for Kaspersky Web Traffic Security 6.1 standalone application:
- CPU: Intel Broadwell or newer, 8 cores
- RAM: 16GB
- At least 8 GB available for swap
- 200 GB available on the hard drive to install the application and store temporary files and log files

Minimum software requirements for Kaspersky Web Traffic Security 6.1 standalone application:
- Squid version 3.5.x, 3.6 or higher.
- Ubuntu 18.04.2 LTS
- CentOS 7.6
- RHEL 7.6, 8
- Debian 10
- SLES 15
- Apache version 2.2, 2.4 or higher

To run the web interface of Kaspersky Web Traffic Security, one of the following browsers must be installed on the computer:
- Mozilla Firefox 67 or later
- Microsoft Internet Explorer 11 or later
- Microsoft Edge 44 or later
- Google Chrome version 75 or later

Additional requirements:
- Ngnix v.1.10.3, 1.12.2 or 1.14.0
- Haproxy v.1.5 for load balancing (needs to be configured separately)

Windows Server editions for LDAP integration:
- Windows 2012 R2 Standard
- Windows 2016 Standard
- Windows 2019 Standard

Minimum hardware requirements for Secure Web Gateway all-in-one appliance:
- CPU: Intel Broadwell or newer, 8 cores
- RAM: 16GB
- HDD: 200GB

Minimum software requirements for Kaspersky Web Traffic Security 6.1 secure web gateway software appliance (virtualization platform):
- VMware ESXi 6.5 Update 2 / 6.7 Update 1.
- Microsoft Hyper-V Server 2016 / 2019.

To run the web interface of Secure Web Gateway appliance, one of the following browsers must be installed on the computer:
- Mozilla Firefox 67 or later
- Microsoft Internet Explorer 11 or later
- Microsoft Edge 44 or later
- Google Chrome version 75 or later

Additional requirements:
- Haproxy v.1.5 for load balancing (needs to be configured separately)

How to buy

Kaspersky Web Traffic Security is an application activated in these products and solutions:
- Kaspersky Security for Internet Gateway
- Kaspersky Security for Storage
- Kaspersky Security for xSP
- Kaspersky Total Security for Business
- Kaspersky Anti-Virus for xSP

* installed and configured separately.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise

www.kaspersky.com

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tommorow.

Know more at kaspersky.com/transparency

Proven.
Transparent.
Independent.