SECURITY code

Continent WAF 2

Web application protection system with automated business logic analysis

- Virtual patching and protection against 0-day attacks
- Automated study of application business logic
- Ease of migration from free software by supporting ModSecurity rules
- Support for the WebSocket protocol at the business logic level
- Low level of false positives
- Ergonomic graphical interface

Continent WAF product line

Specifications	IPC-R1000 	IPC-3000L 
Efficiency, HTTP requests per second	up to 1 000	up to 3 000
Processor	Intel Xeon E-2276G	Intel Xeon E5-2680v4
RAM	Not less than 32 GB	Not less than 128 GB
Interfaces	8 x 10/100/1000BASE-T RJ45 4 x 10G SFP+	1 x 10/100/1000BASE-T RJ45 4 x 10GB SFP+

Key features

Traffic analysis

- Flexible configuration of application models:
  - Validation of the HTTP protocol;
  - Syntactic analysis of requests and responses;
  - Defining the business logic of an application;
  - Identification, authentication of users and session control.
- Automatic building of the application operation model.
- Analysis of deviations of user behavior from the standard scenario.
- Data analysis in the SSL tunnel.
- A package of pre-configured signatures.
- Support for ModSecurity format rules.
- Expanding the structures of transmitted data available for parsing.
- The ability to select various objects as a source of data analysis (IP address, session ID, etc.).
- Verification of the success of user actions and control of the sequence of actions (business logic level).

Management and monitoring

- Graphical representation of the web server request and response parsing model.
- Monitoring and managing the protection of multiple applications from a single console.
- Graphical display and editing of decision-making rules.
- The output of generalized statistics in real time.
- Aggregation and prioritization of information security event data.
- Automatic notification of the operator about information security events.
- The role model of access to the management console.
- Audit of the WAF operator's actions in the management console.
- Integration with the SIEM system using the syslog protocol.
- Updating ModSecurity rules according to OWASP Top 10.
- The ability to create lists of objects for further use in the rules.

Operating modes

- Monitoring mode.
- Reverse Proxy mode.
- Audit mode:
  - Analysis of web server activity logs.

Detecting attacks on web applications

- Detection of web application-specific attacks:
  - OWASP Top 10;
  - Brute-force attacks;
  - DoS at the application level;
  - Attacks on authorization and authentication mechanisms;
  - Automated attacks.
- Detecting anomalies in web server requests and responses.
- Anomaly detection based on the application operation model:
  - Matching with the model;
  - Deviation from the model.
- Detection of anomalies inside nested data transmitted over the HTTP protocol.

Application scenarios

Protecting complex web applications

Result:

- The costs associated with attacks on web applications are minimized.
- The risk of reputational losses during hacking of a corporate website has been reduced.
- Increased resistance of web applications to DoS attacks.
- Attempts of fraudulent actions by intruders have been prevented.
- The level of false positives has been reduced.

Protecting an organization's network from compromise through a website

Result:

- The risk of hacking the site is minimized.
- The risk of an attack on the corporate network through a hacked website has been reduced.

www.securitycode.net

115230, Moscow, 1st Nagatinsky proezd 10/1

E-mail: export@securitycode.ru
Tel.: + 7 (495) 982-30-20