SurfSecure – superior solution to provide secure Internet access for corporate clients of any size.

SurfSecure is a typical Secure Web Gateway (SWG). Gartner states SWGs should utilize URL filtering, advanced threat defense, legacy malware protection and application control technologies to defend users from internet-borne threats, and to help enterprises enforce internet policy compliance.

FEATURES

- ✓ categories based URL filtering;
- ✓ content filtering;
- ✓ protection from malicious code;
- ✓ HTTPs filtering;
- ✓ 3-level policy management (Enterprise, Security Group, User)
- ✓ administrator actions and user activities logging;
- ✓ reports on Internet activities of a company users;
- ✓ Active Directory and LDAP integration;
- ✓ SSO authentication;
- ✓ basic and advanced (deep packet analysis and precise protocol identification) application filters at the 7-th (application) layer of the OSI model;
- ✓ clustering - to provide redundancy or load balancing;
- ✓ integration with third-party systems via ICAP.

USE CASES

SurfSecure allows solving the most common challenges:

- ✓ protection from unintended use of Internet resources;
- ✓ protection from malware infection;
- ✓ protection from phishing websites;
- ✓ bandwidth or consumed traffic limitation, certain categories or individual websites restrictions, limitation of Internet usage time or other controls selectively applied to user groups, individual users or network nodes;
- ✓ downloads blocking by MIME file type;
- ✓ granular limitation of Internet activities for a variety of applications (instant messages, cloud- based applications, P2P file transfer, sites functions, etc.);

SurfSecure
Habankim str. 2, Haifa Israel
www.surfsecure.net
Email: office@sirfsecure.net

- ✓ monitoring of data sent over HTTP(S);
- ✓ protection from confidential data leakage;
- ✓ possibility to build a scalable fault-tolerant solution without using an external load balancer.

FUNCTIONALITY DESCRIPTION

✓ URL FILTERING

SurfSecure carries out real-time and highly precise classification of user queries to web sites by 80+ categoriesd. Real time classification data is provided by Symantec and Kaspersky Lab. The database is added with new URLs and is cleared from invalid links on a daily basis.

✓ WEB SURFING PROTECTION

SurfSecure ensures web traffic cleaned from known and unknown malicious codes (viruses, worms, Trojan horses, malicious scripts, etc.) utilizing multilevel anti-virus protection based on superior technology of Kaspersky Lab. SurfSecure blocks malware traffic, reduces the corporate network load, and streamlines capacity consumption. Independent anti-virus mechanisms, along with the proprietary unique heuristic engine ensure adequate protection from present-day security threats.

✓ SUPPORT OF VARIOUS AUTHENTICATION METHODS

Support for Kerberos, LDAP and NTLM allows transparent authentication of domain users of Active Directory and other directory services supported by SurfSecure. The user will not need to enter his login and password to access the network; the system will use his domain account data. User authentication in the system enables flexible implementation of web-filtering policies and reporting on information security policies implementation in the company.

✓ POLICY MANAGEMENT

SurfSecure's three-layer policy management mechanism allows administrators to define rules to access Internet resources for the whole organization, groups or individual users.

✓ APPLICATION TRAFFIC IDENTIFICATION AND BLOCKING

Today, most applications can bypass standard protection tools. SurfSecure allows identification and blocking of a multitude of applications, such as P2P clients, SMS clients, IM – Skype, ICQ, Mail Agent, GTalk, etc., video/audio streaming, VoIP, online games and many others, as well as built-in capabilities of multifunctional web sites. By blocking such applications, SurfSecure both reduces Internet channel bandwidth consumption and prevents intrusions into the network via those applications.

- ✓ LOAD BALANCING
  SurfSecure has built in load balancing mechanisms thus enabling system scalability through clustering without use of third-party load balancers. This eliminates the need to buy third-party appliances or replacing the current SurfSecure hardware platform with a more powerful one.

- ✓ DATA CACHING
  SurfSecure includes a built-in caching mechanism that reduces frequently used information access time, which gives better user experience and less Internet channel load.

- ✓ INSPECTION OF SECURE CONNECTIONS (HTTPS)

  HTTPS inspection enables full control over Internet activities of an account that is useful for web surfing control, detection of sophisticated hidden threats in files received from the Internet and confidential data leakage prevention. Encrypted traffic is analyzed via the deep packet inspection engine R&S PACE 2 from Rohde & Schwarz Cybersecurity.

- ✓ THIRD-PARTY SOLUTION INTEGRATION
  Integration through Internet Content Adaptation Protocol (ICAP) with any third-party solution that handles web traffic (DLP, Sandbox, etc.) ensures company data security and integrity.

- ✓ SCALABILITY
  Built-in load balancing mechanisms allow filtering system's performance increase up to any required level by adding an appropriate number of servers which requires minor changes into configurations and environment.

- ✓ USEABILITY
  SurfSecure has a user-friendly interface that is intuitive, safe and convenient for regular administration activities. Logs and statistics processing tools empower the administrator to get analytical reports generated on demand, and administration GUI allows to have a centralized control over Internet access policies for all web gateways of a company.

SurfSecure uses superior technology of:

KASPERSKY lab Symantec ROHDE&SCHWARZ Cybersecurity

SurfSecure
Habankim str. 2, Haifa Israel
www.surfsecure.net
Email: office@sirfsecure.net