



## What is Surf-SeCure ?

Internet access has become an invaluable tool. It has also opened up a world of potential dangers, bandwidth hungry content and easy access to inappropriate material. Surf-SeCure is one of the most advanced dynamic multilayer Internet content filtering solutions, designed to provide easy and effective deployment of your organization's acceptable-use Internet policy. Surf-SeCure helps increase productivity, optimizes bandwidth consumption and reduces legal liability.

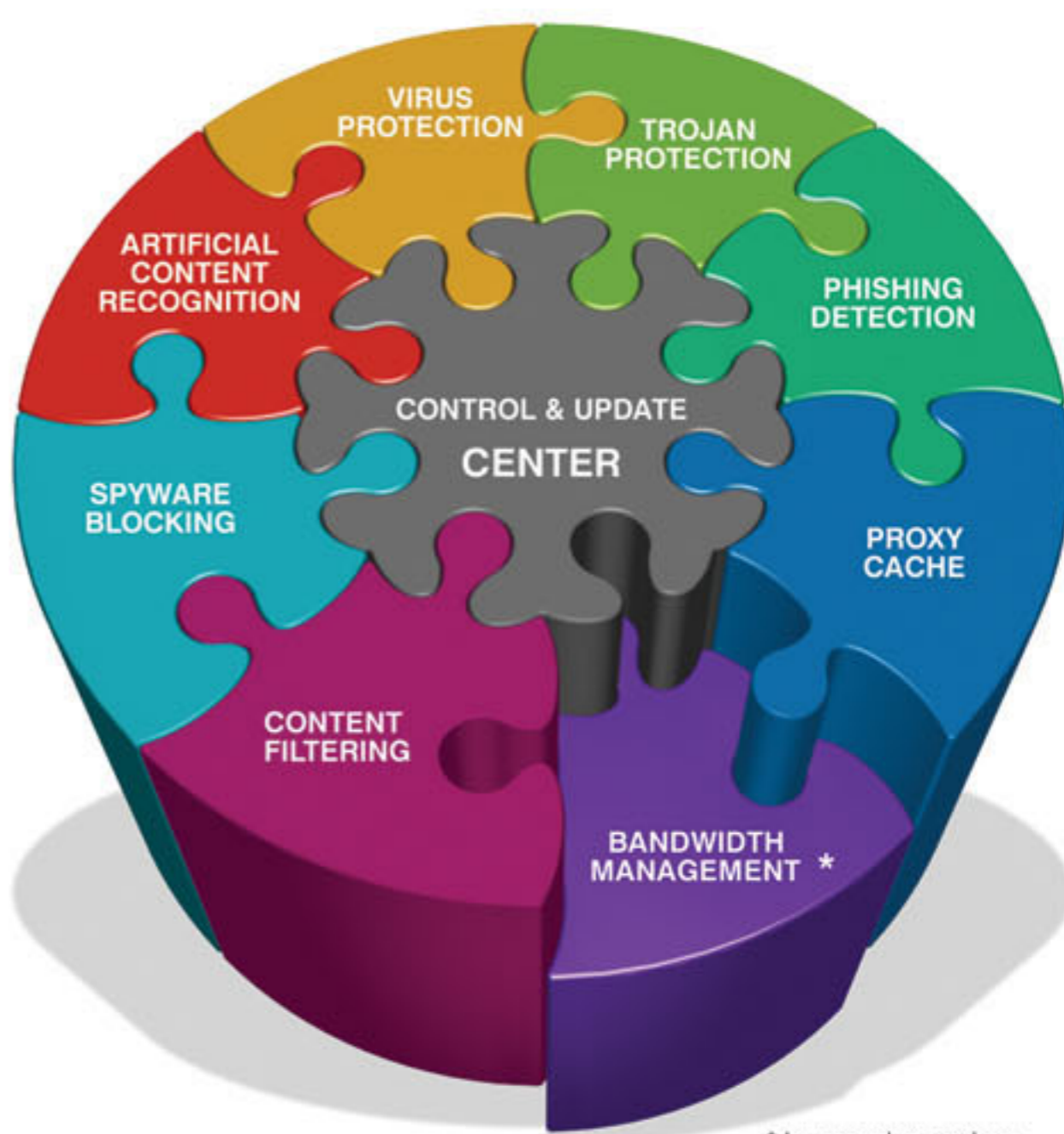
**Surf-SeCure** is a dedicated appliance that provides organizations with a Web-Surfing, Anti-Virus scanning engine and active URL filtering, based on PureSight's ACR™ technology.

**URL Filtering - ACR™** Active Content Recognition (ACR™) is the core technology that empowers **Surf-SeCure**, enabling **Surf-SeCure** to classify content on-the-fly. All HTTP traffic is screened by **Surf-SeCure**, to ensure compliance with organizational policies and to provide complete and reliable web coverage with unmatched recognition accuracy.

The World Wide Web consists of billions of web pages with millions more added each day. **Surf-SeCure's** dynamic content filtering server, sitting on the gateway (as bridge or gateway mode), works on-the-fly to cover the entire web, preventing all inappropriate content from entering your network.

**HTTP and FTP Anti-Virus filtering** **Surf-SeCure** scans all incoming content on any given port. Coupled with the F-Secure™ award winning anti-virus engine, the system provides full protection against known and unknown viruses and worms. F-Secure's engine is a combination of three engines: F-Secure, Kaspersky AVP and the Heuristic Orion engine.

**Proxy Server** **Surf-SeCure** can act as a proxy server (regular or transparent). This improves performance and saves bandwidth.

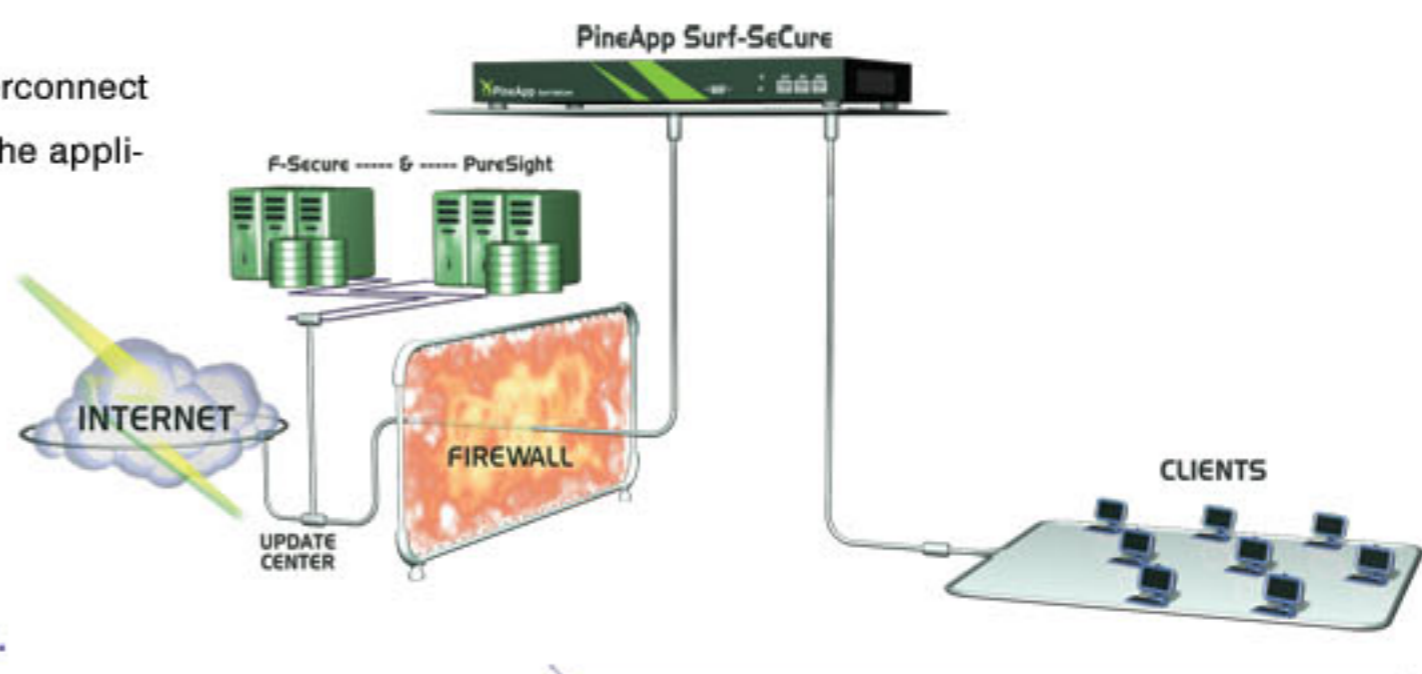


### Benefits:

- URL filtering and classification (24 categories) - uses PureSight's unique ACR™ technology.
- Anti-Virus – Three independent engines provide up-to-date protection against known and unknown Security threats.
- Filtering accuracy – Provides unfettered access to legitimate content and accurate management of inappropriate content.
- Immediate coverage of millions of new pages added every day.
- Language independent – Filters content of any language.
- Specific URL filtering – Known websites containing objectionable content may be added to a URL list so that specific problematic sites can be blocked or allowed.
- Informative logs and statistics – The system provides accurate logs and graphical statistics in an easy and readable manner.
- URL Caching - Once the site is classified, the site category is cached within memory, improving network performance.
- Automatic updates – The system is automatically updated on a daily basis which improves ACR™ accuracy.

### Implementation Methods:

- Bridge mode – Plug and Play, no need to configure or change the network configuration. Just plug-in the network cables and the unit is ready. The ability to bypass traffic in case of failure.
- Proxy mode – Selectively routing the traffic through the DMZ or the LAN.
- Transparent Proxy – Transparently filters and scans traffic without the need of changing configuration or IP's on the client's side.
- ICAP – Internet Content Adaptation Protocol – Ability to interconnect with 3rd party products such as firewalls and dedicated cache appliances.



- URL Filtering using Active Content Recognition.
- Spyware Blocking.
- NTLM authentication
- Content Filtering.
- Virus protection.
- Trojan protection.
- Phishing prevention.
- Proxy Cache.
- Reverse proxy \*
- P2P application control \*
- Bandwidth Management \*

\* In upcoming versions

