Remote Filtering

Proprietary Hybrid Technology Requires No DMZ, VPN or PAC Files

iPrism's Remote and Mobile Filtering delivers comprehensive Web security using exclusive hybrid technology that makes deployment simple and seamless. Unlike any other remote Web filter, iPrism Remote Filter delivers powerful and flexible Internet protection to your remote employees without using your VPN, without requiring any deployments in your DMZ and without any PAC files, so remote users experience no browser latency. Using a combination of Windows or Mac Remote Filtering Client and a powerful elastic data center cloud service, iPrism Remote Filter delivers comprehensive Internet security to your off-premises users that includes flexible policy enforcement and robust reporting.

iPrism Remote Filtering Delivers Simplicity, Value and Performance:

Easy set-up and provisioning: Once you install the Remote Filtering Client software, you can manage and report on remote users easily from iPrism's browser-based central management console. And unlike solutions from other vendors, iPrism eliminates administrative burdens:

- No additional system modules to install off-box
- Eliminates the insecurity of copying users' directory service credentials off-premises
- No emails required to educate roaming users on self-provisioning

Secure Client-Based Hybrid Technology: Unlike other vendors that rely on PAC file-based hybrid solutions, iPrism uses lightweight, low-latency, tamper-proof and application-agnostic client software. This eases the burden on IT Admin resources:

- Eliminates the need to restrict users' workstation privileges
- No need to restrict application usage
- No changes to or restrictions on users' browser proxy settings

Accurate Off-Premises Policy Enforcement: The iPrism Remote Filtering client is location aware, which means you can apply and enforce the same or a different policy for roaming users, whether on- or off-premises relative to the corporate network. This also allows users to negotiate captive portals encountered at wireless hotspots such as airports, hotels, coffee houses and others.

Centralized Administration and Reporting: iPrism Remote Filtering offers centralized administration and reporting from your iPrism, so you can easily manage all employee Web surfing, regardless of location and time. Administration tasks, policy enforcement, drill-down reporting and real-time monitoring are stored and managed in the same manner for all users, and from the same single interface on your iPrism.

Bandwidth Conservation – No Latency: Unlike other remote Web filters, iPrism helps conserve your bandwidth, because there are no VPN tunnels and no deployments in your DMZ to hog network bandwidth so low latency is assured.

Distributed Data Center: iPrism uses a nationwide network of powerful, distributed data center cloud services so your users never encounter availability issues.

How iPrism Remote Filtering Works

iPrism's unique approach to remote and mobile filtering includes communications between the iPrism Web Filter and the iPrism Remote Client Software. The distributed in-the-cloud data center functions as a go-between, making sure your iPrism remains secure and conserving bandwidth. Each component has a role in assuring that iPrism performance and security are never compromised. All of the monitoring and filtering of your organization's Internet activities are handled by the iPrism, while the data center stores policies from the iPrism and applies them to the iPrism Remote Filtering Client in accordance with the policy you have established for that client. When a remote user accesses the Internet, the client software is connected to

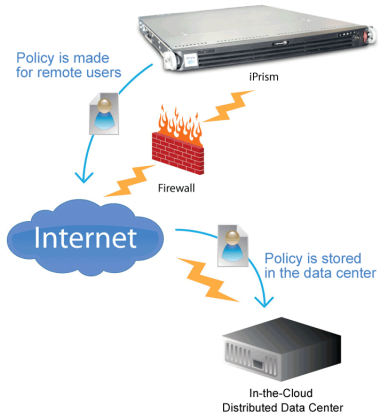
the data center and receives a disposition for the Web request based on its iGuard database URL rating and the remote client policy. The data center tells the client to block or allow a site and to monitor or not to monitor the user's Internet activity.

Periodically, the client sends logs of all your users' Internet activities on remote PCs or Macs to the data center. Your iPrism pulls these logs on-demand and adds them to the local iPrism reports database. This gives you a single source of management reports for all users whether on or off-premises. iPrism's unique technology allows you to compile reports from across your organization and drill down to a single user regardless of location.

The diagrams below illustrate the steps involved in iPrism's Remote Filtering:

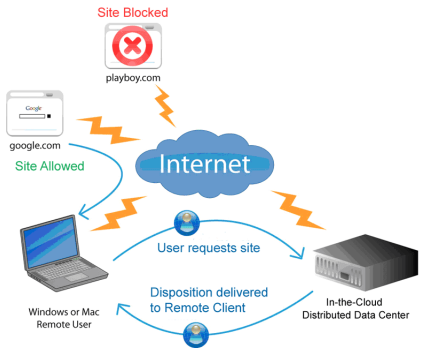
Step 1.
iPrism Establishes Policy

iPrism defines policies for your remote clients and pushes them to the distributed data center, where they are stored securely and confidentially.



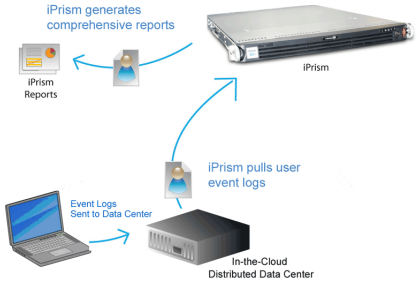
Step 2.
Remote User Browses the Internet and Policy is Enforced

The iPrism Remote Client requests Internet sites and gets the disposition of that request via the data center where policies and iGuard ratings are applied per client and sites are either allowed or blocked.



Step 3.
iPrism Sends Logs and Generates Reports

iPrism Remote Client captures browsing events into logs and pushes them to the SBS Data Center for temporary storage until iPrism retrieves them and uses them to generate reports for all users across your organization.



4225 Executive Sq., Ste. 1600
La Jolla, CA 92037-1487

Give us a call:
1-800-782-3762

Send us an email:
info@edgewave.com

For more info, visit us at:
www.edgewave.com