iPrism Web Security

iPrism Datasheet

Comprehensive Web Security

EdgeWave's iPrism Web Security delivers unrivalled protection from Internet-based threats such as malware, botnets, viruses, spyware, circumvention tools, anonymous browsing, IM, P2P, and inappropriate content. As a self-contained appliance-based solution, iPrism offers universal interoperability on any platform and in any network environment and iPrism seamlessly integrates with your directory services to automate authentication for fast and easy deployment. Our exclusive cloud-based Remote Filtering assures policy enforcement without using VPN, DMZ deployments or PAC files. iPrism Social Media Security lets you monitor and filter popular Web 2.0 applications such as Facebook, Twitter, Google and others, allowing your users to have safe, policy-governed access.

iPrism Web Security has received numerous awards including, the Info Sec 2012, 2011 and 2010 Global Product Excellence Awards; SC magazines 2011 Innovator of the Year Award; five stars across the board recommended product status in the 2011 SC Magazine Group Test of Web Content Management Solutions; and 3 consecutive years of Technology & Learning Awards of Excellence.

iPrism Awards

Info Security Products Guide
2012
GLOBAL EXCELLENCE AWARDS
SC MAGAZINE
AWARDS of winner! EXCELLENCE TECH&LEARNING
Info Security Products Guide
2011
GLOBAL EXCELLENCE AWARDS
SC MAGAZINE RECOMMENDED
TECH&LEARNING WINNER AWARDS of EXCELLENCE 2009

Highlights

Multi-Layered Security Threat Protection – iPrism combines exclusive real-time botnet and malware defense, extensive URL database, application blocking, the Circumvention Defense Network, and granular policy creation to deliver comprehensive threat protection and enforcement for AUP and security policies.

Enterprise-Level Infrastructure Support – iPrism offers High Availability, VLAN Trunking support, virtual desktop support, email protocol filtering and certificate chain support.

Granular Policy Management and Control – iPrism has features that enhance policy management including Quotas and Warnings to help distribute bandwidth and optimize network performance, comprehensive directory integration, multi-user admin roles with SSO and comprehensive on-box reporting.

Innovative Cloud-based Services -- New iPrism Social Media Security allows safe Web 2.0 access, and iPrism Remote Filtering delivers policy-driven access to remote and roaming users.

Flexible Deployment Options -- iPrism technology is port-agnostic providing comprehensive coverage across your network. Choose from transparent bridge, transparent proxy, explicit proxy or multiple deployment schemes to fit the requirement of even the most complex or distributed network scenarios.

Features

Enterprise-Level Infrastructure Support

NEW Support for VLAN Trunking

Many organizations are using VLAN (virtual LAN) trunking configurations on their firewalls, which allows them to separate network traffic to virtual subnets, with the firewall enabling routing between VLAN's. This avoids the added expense of a Layer3 switch. iPrism supports multiple VLANs through a single appliance when it is installed on a "Trunked Port". This feature is easy to enable and allows simple centralized management and visibility of multiple VLAN traffic on a single iPrism.

Exclusive iPrism Cloud-Based Remote Filtering

iPrism's cloud-based Remote Filtering extends comprehensive, flexible Web security to your corporate laptop and other remote or roaming users with an exclusive cloud-based technology that makes deployment simple and seamless. Unlike any other remote filtering solution on the market, iPrism's proprietary technology delivers powerful Web security to your remote users without using your VPN and without adding any hardware in your DMZ or requiring browser-specific PAC files. Using a combination of iPrism Remote Filtering Client (for both Windows and Mac) and data center cloud service, iPrism delivers comprehensive Internet security that enforces your AUP and security policy, no matter where users are located.

NEW Email Protocol Filtering

As an added level of protection, iPrism supports email protocol filtering including SMTP, POP and IMAP and their secured versions. These protocols are used by internet email clients and iPrism's ability to filter them not only adds another layer of security, it is the first step in integrating our Web and email security solutions. This feature allows you to create policies governing user access to external email applications.

NEW High Availability

This feature allows two iPrisms to be connected together with the status of traffic on each one visible on both appliances. One iPrism acts as the "Primary" and the other is the "Secondary". Should the Primary iPrism become unavailable due to a hardware or system failure, the Secondary iPrism takes over seamlessly, connecting with the primary as a bridge. The Secondary iPrism become activated either because the Primary alerts it or a communications port, or the Primary iPrism disappears from the clustering environment. This configuration assures optimum performance when used in high availability or redundant networks with multiple firewalls.

NEW Certificate Chain Support

iPrism supports the ability to upload and install intermediary certificates, which adds security by eliminating the possibility that a root certificate could be compromised. Certificate Authorities, such as Thawte, provide the ability for administrators to install intermediary certificates in order to trust the certificates that are purchased from them. End entity certificates chained to an intermediate certificate represent the highest possible security solution for Certification Authorities and therefore their customers.

SSL Filtering

One of the most common forms of encryption is Secure Socket Layer (SSL), which requires the creation of a secure tunnel between the user (client) and the website (server). Once the tunnel is established, HTTPS traffic uses SSL encryption to transmit content through the tunnel. iPrism provides another layer of security over your Web traffic by allowing control of SSL traffic with a feature that detects and classifies the Server Name Indication (SNI) header information within the outbound Web request at the start of the SSL handshake. This lets you control where you will allow encrypted content to be sent, and avoids potential hacker incursions into your network via unfiltered SSL.

Seamless Virtual Desktop Support

iPrism's unique auto-login feature allows virtual desktop users to maintain their productivity without incessant authentication requests. iPrism's unique "session based" authentication technology lets you use Auto-login to simplify the authentication process without installing any software on your terminal or AD servers. This seamless integration is verified by iPrism's Citrix Ready status, which has confirmed iPrism's consistent policy application whether your users are Web surfing from their desktops or via Citrix or other terminal server systems.

Multiple Deployment Options

iPrism supports multiple deployment scenarios so you can choose the best option for your network configuration. Because iPrism has its own hardened and optimized OS, complete interoperability is assured. For more speed and less control, deploy iPrism in transparent bridge mode where proprietary kernel-level filtering combines the accuracy and security of pass-through filters with the speed and coverage of a pass-by or sniffer-type solutions, giving you the best of both worlds. In deployments where more control is required, deploy iPrism as a transparent proxy, where it work seamlessly in a wide range of networks involving mixed platforms, legacy systems and other variants. iPrism can also be deployed as an explicit proxy should your network configuration require it. iPrism h-Series appliances include a built-in, high-speed network failover circuit to mitigate introducing a single point of failure, and load balancing is supported as well as comprehensive reporting across your organization

Exclusive iPrism Cloud-Based Remote Filtering

iPrism's cloud-based Remote Filtering extends comprehensive, flexible Web security to your corporate laptop and other remote or roaming users with an exclusive cloud-based technology that makes deployment simple and seamless. Unlike any other remote filtering solution on the market, iPrism's proprietary technology delivers powerful Web security to your remote users without using your VPN and without adding any hardware in your DMZ or requiring browser-specific PAC files.

Granular Policy Management and Control

New iPrism Social Media Security

This new cloud-based service allows you to seamlessly monitor, filter and report on end-user interactions with social media applications through granular, policy-driven controls. Rather than taking an all-or-nothing approach to popular sites such as Facebook, Twitter, YouTube and others, this service enables real-time policy matching and enforcement across your organization.

Comprehensive Logging, Real-Time Monitoring and Reporting On-Box

iPrism's comprehensive on-box reporting, you can generate historical reports using a variety of available templates or you can customize reports to suit your needs. And you can assign designated users the right to run the Reports Manager, allowing you to use your IT resources more efficiently. Email alerts are generated when security problems are detected allowing you to quickly mitigate threats before they cause damage.

If you have multiple iPrisms deployed across your large enterprise and distributed network, the iPrism Enterprise Reporting Server (ERS) delivers comprehensive aggregate reports on all Web activity quickly and easily. See the iPrism ERS data sheet for details.

NEW Enhanced Custom Filters

iPrism adds more features to custom filtering allowing administrators to not only change the category rating of an iGuard database URL, but to also add properties to it. This granularity allows you to avoid events such as AV scanning and authentication requirements, or enforce safe search parameters. This feature also allows administrators to add query strings and top level domains to specific URLs.

NEW YouTube for Schools Support

iPrism continues support for educators with this feature, which allows access to the new YouTube for Schools channel, while blocking other unwanted YouTube content. Customers with a YouTube for Schools login will be able to enter those credentials in the Custom Filters function, and have their YouTube policies enforced. This enables schools to access valuable learning resources without worry.

Enhanced Directory Integration

Unlike some competitors, iPrism employs on-box user authentication rather than user identification giving you significant advantages. Because iPrism complies with Microsoft Best Practices and does not require a separate off-box agent, you achieve automated authentication with more security, less bandwidth drain and no latency. iPrism authentication incurs no OS conflicts and eases your administration duties by integrating seamlessly with all major network directories including Novell Netware Directory Services (NDS), Windows Active Directory (including one-way outgoing trust support) for Window 7 and also Mac clients using AD 2003/2008 and Mac OSX Snow Leopard. In addition, as an LDAP variant, it is possible to integrate iPrism Web Filter with OSX Server Open Directory (LDAP v2/v3).

Centralized, Multi-User Admin and Reporting with Granular Override Management and SSO

iPrism gives you the flexibility to define roles for policies, reports, and other facets of administration with eight pre-defined and customizable roles that you can delegate to any person within the organization (local or authenticated users). And unlike any other solution, iPrism has a granular override feature that allows you to delegate override privileges to a secondary administrator or even provide self-override roles to some end-users. iPrism's browser-based user interface offers single signon (SSO) access for comprehensive administration and reporting capabilities via any browser. In addition, multiple delegated administrators can log into the UI simultaneously for increased efficiency.

NEW Bandwidth Quotas and Warnings

iPrism gives you more control over bandwidth usage by allowing you to add policy attributes to Web profiles that limit bandwidth consumption for groups and/or individuals. With this feature, you simply add a policy attribute to any web profiles you choose and you can limit the total bandwidth consumed by users or groups. When a user gets near or exceeds the bandwidth quota, you receive a warning, and these Quotas and Warnings events are identified through both real-time monitoring and reporting. This new feature helps administrators establish limits on acceptable Web activity, which can ultimately decrease bandwidth usage.

Powerful Web Security

Anti-Circumvention and Anonymous Browsing Protection

Employees who try to get around your Web security measures by using circumvention tools, proxies or anonymizer websites, will have their attempts blocked at every turn by iPrism's multi-layered approach:

- **Dynamically-Detected Proxies** - Using deep packet inspection with real-time pattern rules, iPrism monitors and blocks websites or private servers leveraging script-based proxy tools, including PHProxy and CGIProxy, to anonymously redirect web requests.
- **Circumvention Defense Network (CDN)** - iPrism's unique CDN protects your organization from circumvention attempts by gathering intelligence on thousands of externally-hosted non-Web servers used to circumvent your network security by re-routing Web requests. We collect these IP addresses in the cloud and analyze them against known legitimate sites to mitigate false positives and immediately and continuously download the results to your iPrism. iPrism inspects outbound traffic and enforces monitoring and blocking of circumvention tools -- including UltraSurf, Tor and JAP clients – attempting to connect to their server networks
- **Active Domain IP Address Mapping and SSL Certificate Inspection** – Administrators always know where users are going on the Web because HTTPS traffic is enforced and reported using domain names, instead of IP addresses, in both transparent bridge and proxy mode deployments. This mapping feature blocks the ability to circumvent iPrism using IP addresses.
- **Anonymizers** – The iGuard analyst team continuously monitors message groups and other anonymizer listing sites for new anonymizer URLs, and updates the database hourly.

Application Filtering

iPrism offers application controls that reduce the risks associated with unsanctioned application communications. These applications, which include popular IM and P2P protocols, not only erode productivity and drain bandwidth; they can open serious security gaps where bot-related malware and viruses can invade your network. iPrism allows you to monitor and block IM and P2P applications such as Skype and FTP with a simple set-and-forget check box.

iGuard Database with iPrism Automated Rating Protocol (iARP)

The iPrism 100% human-reviewed iGuard database includes the iARP feature, which further refines Web filtering by sending your most frequently-accessed unrated URLs to the iGuard team automatically to be added to your and all our customers' database.

Outbound Anti-Botnet Protection

iPrism Web Security provides continuous defense against dangerous botnets by leveraging its unique botnet threat database to stop the "phone-home" mechanism that enables stealth, bot-related malware to steal identities or data and commit illegal or malicious actions within and outside your network.

EdgeWave h-Series Appliances

iPrism's powerful line of high-performance hardware offers a full range of appliances designed to deliver optimum performance and blazing Web security throughput speeds to organizations of all sizes no matter how big your pipeline. All of the h-Series models share a hardened and optimized OS for complete interoperability. Also, many h-Series models offer dual hot-swappable hard drives and power supplies for enhanced reliability

Model:	**25h**	**55h**	**105h**	**500h**		
Filtered Traffic Throughput	20 Mbps	50 Mbps	100+ Mbps	500+ Mbps		
Number of Workstations Supported	1-500	500-2500	1000-10,000	10,000 - 20,000		

EdgeWave

15333 Avenue of Science, San Diego, CA 92128.
www.edgewave.com

Toll Free: 800-782-3762
Email: info@edgewave.com

Phone: 858-676-2277
Fax: 858-676-2299