SOLUTION NOTE

COST-EFFECTIVE PARENTAL CONTROL SOLUTIONS

Offer households comprehensive protection from dangerous online content

SUMMARY

While access to the Internet is almost a necessity, it can also offer content not necessarily appropriate for children or in line with preferred household values.

Besides the daunting task of monitoring what sites and content their children visit, parents also have to manage their children's device time consumption.

Parents want peace of mind with tools that enable them to protect children from the perils of online access—dramatically reducing the likelihood that children will be exposed to inappropriate images or videos and online threats. There are many excellent parental control apps and devices that help parents manage these problems. However, most parents lack the time and skills to manage security across multiple applications and solutions to cover all the devices and platforms in use. Also, how do parents protect children both at home and on mobile networks?

Today, there is a more robust and cost-effective way to provide a safe internet experience for your subscribers–using a DNS-based approach that offers several key benefits compared to traditional methods such as deep packet inspection. Infoblox Subscriber Services provides a cost-effective and scalable DNS-based approach that allows service providers to deliver value-added offerings, including comprehensive "set and forget" parental control solutions that shield young eyes from inappropriate content and block threats before they can cause damage, reducing risks from malware and other threats.

THE NEED FOR PARENTAL CONTROLS

Imagine that you are a child born within the last fifteen years. For you—the Internet has always existed. It's second nature for you to pop online to watch a video, to research a topic for homework, to chat with friends, play online games, or to post that ever-important video. Adults know the Internet can also hold dark content that should not be exposed to children. How can parents monitor what sites and content their children visit, let alone device time consumption?

CONVENTIONAL CONSUMER APPROACHES ARE COMPLEX AND LIMITED

If you perform an internet search, it's easy to see there are many excellent parental control apps and devices that help parents manage these problems. But it can be exhausting. How do non-technical parents choose and manage a solution that works across all the devices on the household network? Purchase expensive hardware? Perform complicated software downloads and installation across multiple device vendors and platforms? How will they efficiently manage this—and can they, across all of their devices? It's one thing to enable parental controls on a cell phone or a laptop, but what about a gaming system? Or an intelligent device that has no traditional operating system?

INCREASING GOVERNMENT REGULATION

There are increasing actions by regional and national governments devising plans on how best to regulate content to protect children online. According to Bloomberg, European and U.S. regulators are likely to ramp up enforcement of privacy laws, especially children's privacy, and wrap up probes of big technology companies. Recently, the U.K. government unveiled a plan that would provide the government more power to regulate internet content. In addition, the French government approved mandatory online pornography age checks.

LEGACY PROVIDER SOLUTION SCALABILITY PROBLEMS

Historically, many services providers have built value-added subscriber services using legacy approaches such as deep packet inspection (DPI) tools and proxies. It's a relatively simple concept to understand – all user traffic flows through the DPI tool, and pre-defined filtering and security policies are applied. But this approach brings up several issues.

Limited Scalability

Legacy approaches are not scalable because all subscriber traffic flows through the DPI tool or proxy. As the number of subscribers increases and resources move closer to the end-user, service providers cannot afford to deploy a linear number of legacy boxes at the problem.

Degraded Performance

Then there is performance. With traditional approaches that scale polynomial, the overall quality of experience (QoE) is negatively affected because all traffic is analyzed whether the user is a paid subscriber or not. Processing unnecessary traffic creates an impact that all subscribers feel, even though this interruption provides the subscribers with no value.

Limited Subscriber Reach

With legacy approaches, service providers typically focus on mobile users only and ignore fixed-access subscribers for value-added services because the bandwidth requires an excessive number of proxies. This is important for those service providers that offer wireless and wireline services – they are effectively forced to segment their subscribers and not provide the same service to wired and wireless subscribers simultaneously.

A BETTER APPROACH

Many service providers often overlook or fail to realize that DNS provides a more straightforward, more cost-efficient means for deploying value-added subscriber services. DNS is part of the core DDI infrastructure that their networks rely on every day. DDI is shorthand for integrating DNS, DHCP (Dynamic Host Configuration Protocol) and IPAM (IP address management) into a unified service or solution. DDI services play a central role in all communications over an IP-based network. The elements of DDI can be harnessed in service provider network infrastructures to bolster security, improve performance, and increase subscriber revenue streams. DNS-based deployment options provide the foundation for such value-added security services as Safe Internet, parental controls, and advertisement blocking, among others.

Applied strategically, DNS and its companion services can also significantly reduce network management and security complexity as CSPs confront the challenges of digital transformation. Today's networks are rapidly becoming more cloud-dependent and decentralized. In traditional architectures, all device connections route through statically configured, centralized data centers rapidly shifting outwards toward the network edge. DNS and other DDI services can serve as universal enforcement points that enable service providers to extend security to all endpoints regardless of their location. A DNS-based approach eliminates the complications and the cost of replicating centralized security stacks across the far reaches of a provider's network while enhancing network manageability, security and visibility.

INFOBLOX SUBSCRIBER SERVICES

Infoblox offers a complete end-to-end solution for subscriber services—the proxy, portal, DNS, policy managers, on-premises databases, logging management and threat intelligence. Infoblox Subscriber Services is a highly scalable DNS-based platform for delivering a comprehensive portfolio of value-added services, like parental controls, Safe Internet, and ad blocking for mobile and fixed-wireline access. It leverages a component-based approach with open interfaces (APIs). This approach enables CSPs to select the most efficient integration strategy for their IT footprint and optimize value-added service offerings by integrating them via API communications with existing OSSs and BSSs.

CSPs can leverage Infoblox's deep networking expertise and decades of investment to build out these new service offerings. Our product experts and engineers can help with critical features, including DDI management, device discovery, DNS cache acceleration, load balancing, automation, and extensive DNS security capabilities.

NETWORK-LEVEL PARENTAL CONTROLS

Infoblox provides network-level parental control offerings in an easy-to-use, self-service solution that requires no software downloads or complicated management for different types of devices. Parents gain comprehensive security and control to protect young users and their devices from web threats like malware and phishing and allow parents to personalize their children's Internet access settings to match the family's preferences and values.

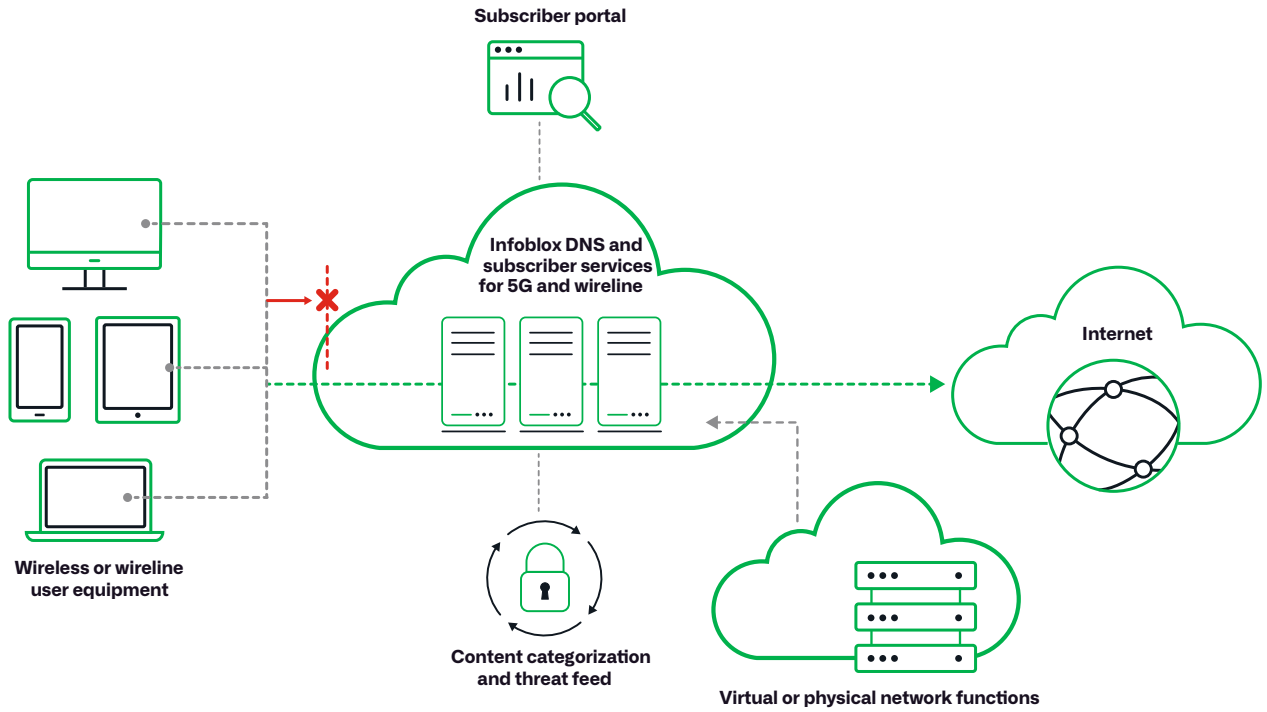
- Parents can access the user interface from any web browser and gain a centralized view of complete household Internet usage. They can establish separate user profiles for each household member and apply policies based on age or per device, leveraging pre-defined content categories to dial in the desired level of protection.
- Besides controlling content, parents can also establish time constraints. Is bedtime 9 pm on school nights? The Infoblox solution provides a simple way to control when children can use the Internet and shut down access on an established schedule.
- Since the solution works at the network level, parents can manage Internet access both inside and outside the home across all devices, including computers, tablets, mobile phones—and even game consoles. If parents suspect their child is being exposed to harmful content, they can instantly pause Internet access to review the situation. Plus, it's easy to extend access past bedtime for holidays and special occasions.
- CSPs can also build on basic parental controls to extend the solution to include additional per-fee services. For example, subscribers can be offered enhanced security protection by third-party security tools such as device clean-up services and IoT device security options.

EASIER ATTACH

With the user-friendly and white label subscriber portal, CSPs can present branded and differentiated opt-in offers that are simple to attach, personalize and use. With no software to download and install, subscribers are in complete control to configure and manage the solution across all their devices with little operator intervention. By enabling opt-out controls, CSPs can provide free or bundled parental control services by default to large groups of subscribers, providing them the choice and the means to discontinue the service if desired.

GREATER DEVICE REACH

Besides better scalability, the Infoblox DNS-based approach contains segmentation features that can distinguish between subscribers and non-subscribers, freeing providers to offer convergent subscriber services for both fixed and mobile access. This capability dramatically improves revenue potential for CSPs and provides differentiation against competitors. The Infoblox solution supports devices with associated telephone numbers such as cell phones and tablets to protect both wireline and wireless devices completely.



PREDICTABLE ROI

With Infoblox, CSPs can leverage their existing DNS infrastructure and investments, turning DNS from a network utility into a revenue-generating service. In place of the hardware-intensive, stand-alone solutions found in DPI tools or proxies that analyze all network traffic, the Infoblox DNS-based approach reduces network impact because only the traffic from specific customers is analyzed. Infoblox also minimizes the up-front investment with a scalable solution and a pay-as-you-grow licensing model, so providers only pay for the number of subscribers using the service.

MAINTAINS SPEED AND PERFORMANCE

Infoblox allows CSPs to leverage powerful DNS-caching capabilities to provide a much better first-connection experience. Designed to handle the "perfect storm" of future 5G and edge-based applications that require ultra-low latency of 50 microseconds on average, Infoblox DNS cache acceleration enables DNS query rates of up to 5 million queries per second. Through centralized management, network administrators can quickly instantiate, implement and auto-scale network services, and manage those services more efficiently through a unified family of devices.

LOWER ADMINISTRATIVE BURDEN

Infoblox provides a pre-built and user-friendly self-service portal accessible anywhere, enabling subscribers to personalize the service to match their preferences, values, and business needs. CSPs can customize the portal to fit branding and color schemes and expose new features to subscribers as their offerings evolve. The service also provides a user-friendly white-label administrative portal. Customer agents can view subscriber account details for assistance and troubleshooting, allowing them to see reporting on service activity, filtering trends and security threat activity. Agents can also manage manual subscriber onboarding, handle global policy settings and policy category groups, and set subscriber/user password rules (e.g., length and expiration).

CONCLUSION

With Infoblox, CSPs can use the DNS they already have to deliver cost-effective value-added parental controls. Infoblox Subscriber Services provides a scalable, resource-efficient, DNS-based way to protect the network and subscribers. It turns DNS into a powerful tool for building value-added security services, blocking threats at the source while maintaining high levels of speed and performance. Its lightweight footprint is easy to deploy and manage as an offering to existing fixed and wireless Internet services.

To learn more, visit www.infoblox.com/sp or contact your local Infoblox representative today.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20230918v1