Secure Connectivity for the Modern Hybrid Workforce

Introduction

The shift to remote working and hybrid networks (on-premises and Cloud solutions) has significantly transformed the cybersecurity landscape. Traditional network security models, which rely on on-premises firewalls and VPNs, struggle to effectively secure a distributed workforce.

WatchGuard FireCloud Internet Access, the initial release of WatchGuard's Secure Service Edge (SASE) strategy, addresses the challenges of securing remote workers as they access the Internet and Cloud applications from various locations around the globe. This solution extends the robust protections of Firebox firewalls to remote employees, enhances the user experience, and unifies security policies worldwide, greatly simplifying management.

The Challenge: Securing the Distributed Workforce

The expansion of remote and hybrid workforces has created new security challenges, including inconsistent security policies across different networks, increased attack surfaces due to unsecured home and public networks, performance bottlenecks associated with traditional VPN solutions, and complex management requirements for IT teams. As organizations move towards Cloud-based applications and services, there is a critical need for a security solution that ensures seamless and secure connectivity, regardless of location.

Solution Overview: WatchGuard FireCloud Internet Access

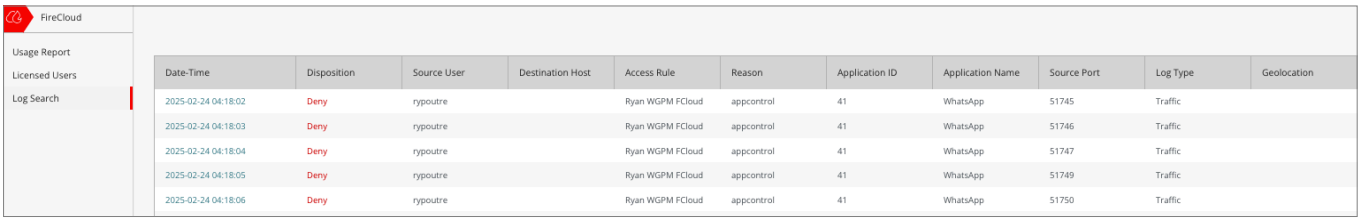
FireCloud Internet Access is a Cloud-delivered SASE solution designed to secure remote workers, regardless of location, as they access the Internet and Cloud applications. Built on a global network of points of presence (PoPs), it provides consistent security enforcement and optimized performance. Its capabilities include firewall-as-a-service, which offers Cloud-delivered firewall protection; a secure web gateway that includes URL filtering, malware scanning, and application control; and DNS filtering, which blocks malicious domains and prevents DNS-based attacks.

Key Features and Benefits

Enhanced Security

FireCloud Internet Access provides proactive threat prevention by blocking malware, ransomware, and phishing attempts before they reach users. It enforces global security policies, ensuring users and devices only access approved websites and applications and minimizing the chances of malware infection.

- **Web Blocking and Content Filtering:** The shift to remote working and hybrid networks (on-premises and Cloud solutions) has significantly transformed the cybersecurity landscape. Traditional network security models, which rely on on-premises firewalls and VPNs, struggle to effectively secure a distributed workforce.



Date-Time	Disposition	Source User	Destination Host	Access Rule	Reason	Application ID	Application Name	Source Port	Log Type	Geolocation
2025-02-24 04:18:02	Deny	rypoutre		Ryan WGPM FCloud	appcontrol	41	WhatsApp	51745	Traffic	
2025-02-24 04:18:03	Deny	rypoutre		Ryan WGPM FCloud	appcontrol	41	WhatsApp	51746	Traffic	
2025-02-24 04:18:04	Deny	rypoutre		Ryan WGPM FCloud	appcontrol	41	WhatsApp	51747	Traffic	
2025-02-24 04:18:05	Deny	rypoutre		Ryan WGPM FCloud	appcontrol	41	WhatsApp	51749	Traffic	
2025-02-24 04:18:06	Deny	rypoutre		Ryan WGPM FCloud	appcontrol	41	WhatsApp	51750	Traffic	

Figure 1. FireCloud log UI filtered blocked traffic view

- **Geolocation Filtering:** FireCloud's unique geolocation feature allows administrators to detect and control network traffic based on geographic locations. By enabling geolocation filtering, organizations can block access to or from specific countries or regions, reducing exposure to potential cyber threats originating from high-risk locations. This feature enhances security by restricting connections to only trusted geographical areas, further strengthening the organization's defense against cyberattacks.
- **Botnet Detection and Network Blocking:** FireCloud provides advanced network-blocking capabilities, including botnet detection and intrusion prevention. The Botnet Detection feature maintains an updated list of known botnet IP addresses and automatically adds them to the Blocked Sites List, preventing users from connecting to malicious domains. Additionally, FireCloud's Intrusion Prevention Service (IPS) utilizes real-time signature-based detection to safeguard against network attacks such as spyware, SQL injections, cross-site scripting, and buffer overflows. Administrators can configure IPS settings to take appropriate actions when threats are detected, ensuring proactive network protection.

Simplified Deployment and Management

FireCloud security policies enhance Firebox policies with centralized management in WatchGuard Cloud. Administrators can configure and enforce security policies from a single interface, simplifying management by using consistent policy structures and terminology across both Firebox and FireCloud.

Administrators easily push the FireCloud agents to target devices from the WatchGuard Cloud. Once security settings are saved, they are automatically deployed to all WatchGuard-hosted points of presence (PoPs) worldwide, guaranteeing consistent policy enforcement regardless of the user's location.

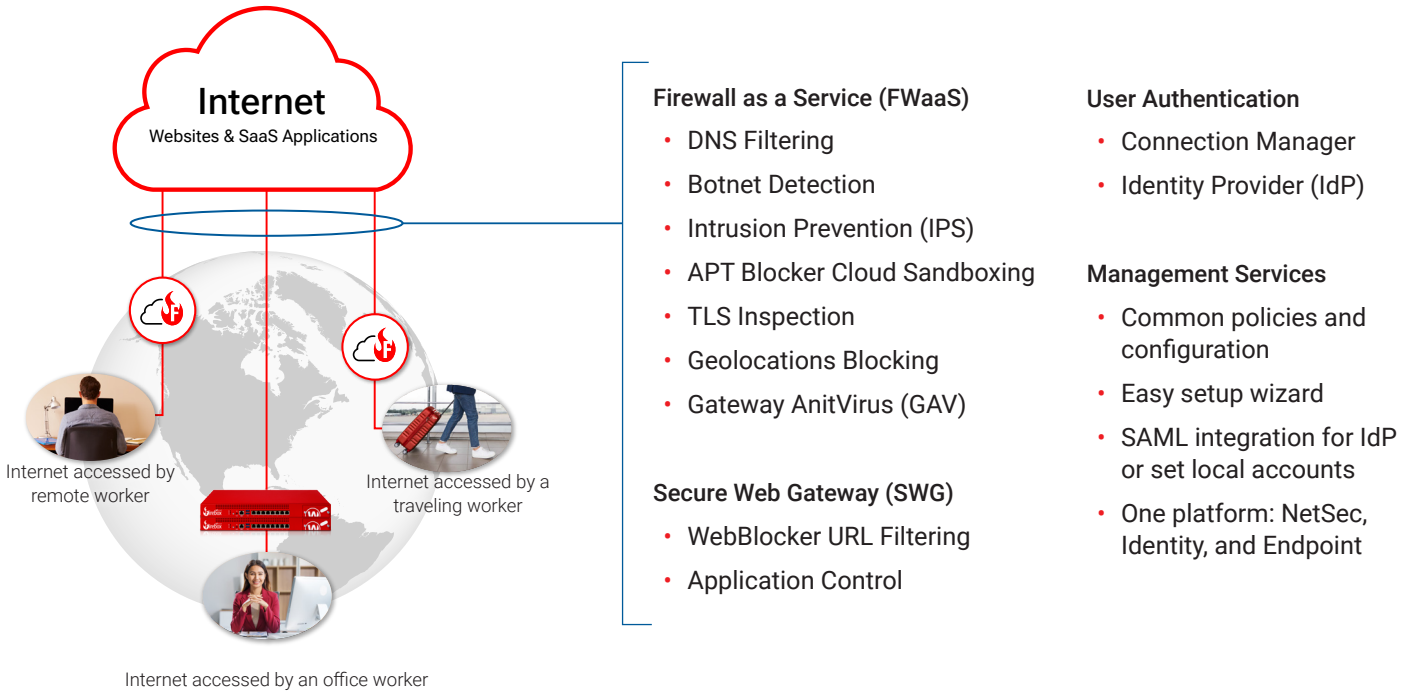


Figure 2. FireCloud Internet Access extends Firebox protections to remote workers

Improved User Experience

Optimized routing through a global network of PoPs reduces latency, ensuring seamless access to Cloud-based applications and services. The scalable architecture allows businesses to handle increasing bandwidth demands effortlessly. Employees can transition between office and remote environments without disruptions to their connectivity or security protections.

Dashboards and Reporting

FireCloud Reporting provides comprehensive insights into network activity, security events, and user connections through an intuitive dashboard. The FireCloud Usage Report delivers real-time and historical data, enabling administrators to monitor traffic patterns, enforce security policies, and optimize performance.

- **Security Analysis Views:** The Security tab offers detailed data on network threats and blocked traffic. Administrators can explore specific security events, including blocked attacks displayed in a line graph showing the frequency of attack attempts and blocked malware threats intercepted by FireCloud. Zero-day malware identified by APT Blocker is highlighted, along with a breakdown of blocked URL categories by WebBlocker. Reports also identify the top blocked applications, blocked user requests, and most-frequently blocked destinations and communication protocols. Geolocation Filtering presents a geographic breakdown of blocked traffic by country, allowing administrators to assess security actions based on location.

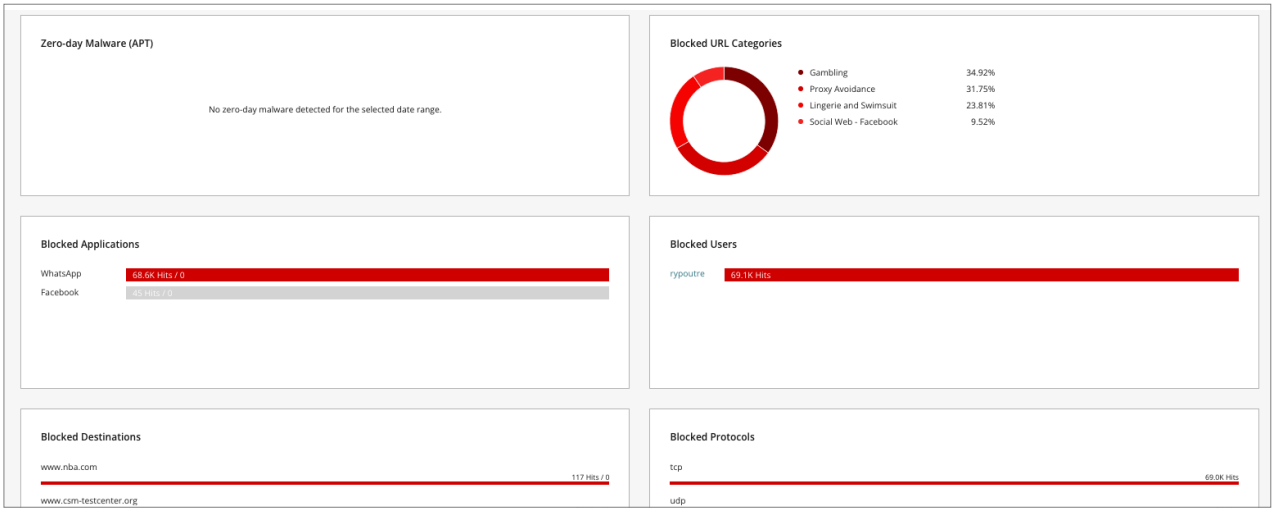


Figure 3. FireCloud security report view showing blocked traffic and user details

- **Traffic Insights Views:** The Traffic tab provides an overview of permitted network activity, offering insights into user behavior and application usage. It details the most accessed application categories and individual applications, and frequently visited websites and domains. Information on the most active FireCloud users is presented alongside data on commonly accessed locations and communication protocols. A geographic view of approved connections is available, showing the extent of network activity across different regions.

- **User Activity & Device Monitoring Views:** The Users tab tracks user-specific data, including authenticated user details, device information, and user group membership. Administrators can see the devices users connect from, the security policies applied to each user based on their group, and the client and operating system versions running on connected devices. Filters can be applied to refine the user list, making it easier to identify inactive users or users with specific client versions installed.

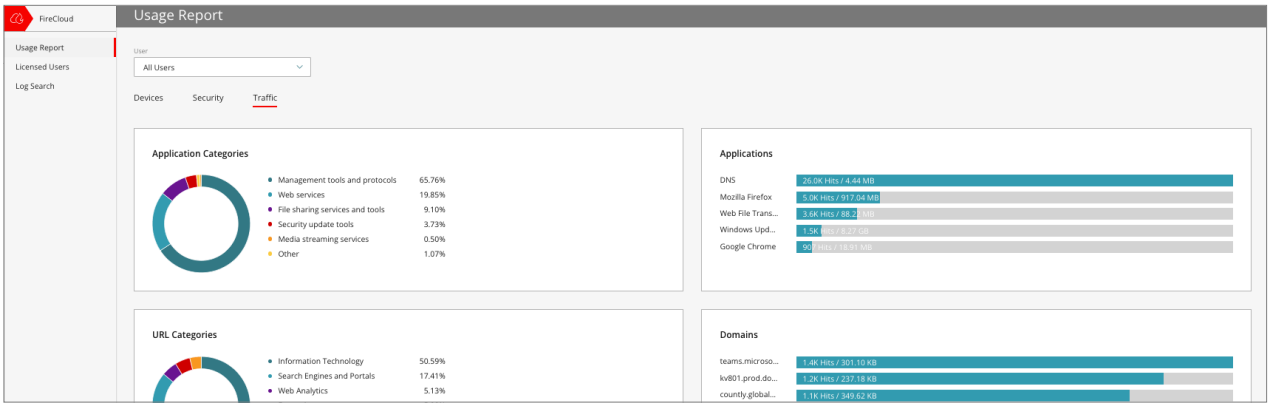


Figure 4. FireCloud usage reports detail top user activities by applications and destinations

Use Cases Covered

Securing Remote Workforces

Organizations embracing remote work require a security solution that ensures employees remain protected without relying on traditional VPNs. FireCloud Internet Access enables direct and secure connections to Cloud applications, eliminating performance bottlenecks and ensuring uniform security enforcement, regardless of where employees are working.

Protecting Against Advanced Threats

Modern cyber threats, including ransomware, phishing, and malware, necessitate proactive security measures. FireCloud Internet Access inspects network traffic in real time, blocking malicious activity before it reaches users. By leveraging Cloud-based threat intelligence, the solution continuously evolves to counter emerging cyber threats, minimizing the risk of data breaches and cyberattacks.

Enforcing Uniform Security Policies

Maintaining consistent security policies across a distributed workforce can be challenging. FireCloud Internet Access simplifies policy enforcement by allowing organizations to configure and apply security rules across all users and devices. Centralized management through WatchGuard Cloud ensures seamless policy deployment and uniform security standards for the entire organization.

FireCloud Differentiators

- **Hybrid:** FireCloud Internet Access differentiates itself by offering a hybrid security approach that integrates seamlessly with existing WatchGuard Firebox deployments. Its ease of deployment and centralized management simplify IT administration, while its cost-effective pricing model makes it an attractive alternative to competitors such as Zscaler and Fortinet.
- **Comprehensive:** The combination of firewall-as-a-service, secure web gateway, and DNS filtering provides a comprehensive security solution tailored to modern work environments.
- **Manageable:** FireCloud's integration with Firebox and WatchGuard Cloud means that a single set of security policies can be defined both on-premises and for Cloud/SaaS applications across in-office and remote workers. For lean IT teams or MSPs, this approach ensures easier management, consistent security controls, and lower costs compared to other SASE offerings.
- **Easy:** Ease of deployment is a key advantage – FireCloud utilizes the same universal agent as WatchGuard EPDR, ensuring a lightweight and stable SASE client. Combined with WatchGuard's global PoP infrastructure and WatchGuard Cloud's central management, FireCloud is more straightforward and easier to deploy.
- **Integrated:** Integration into WatchGuard's threat detection and response stack further strengthens security. FireCloud logs are ingested into ThreatSync, providing unified and correlated threat detection and response for remote worker use cases. This allows MSPs to offer a superior SASE solution while continuously monitoring the environment for risks and threats.

Conclusion

As businesses continue to embrace remote work and Cloud-based applications, securing distributed workforces has become a priority. WatchGuard FireCloud Internet Access delivers comprehensive, Cloud-native security that enhances protection, simplifies IT management, and improves network performance. By consolidating key security functions into a single, easy-to-manage platform, FireCloud empowers managed service providers to deliver a superior remote-worker security service and organizations to navigate today's cybersecurity challenges with confidence.

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in unified cybersecurity. Our Unified Security Platform® approach is uniquely designed for managed service providers to deliver world-class security that increases their business scale and velocity while also improving operational efficiency. Trusted by more than 17,000 security resellers and service providers to protect more than 250,000 customers, the company's award-winning products and services span network security and intelligence, advanced endpoint protection, multi-factor authentication, and secure Wi-Fi. Together, they offer five critical elements of a security platform: comprehensive security, shared knowledge, clarity & control, operational alignment, and automation. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. **To learn more, visit** WatchGuard.com.

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 WEB www.watchguard.com WatchGuard Technologies, Inc.

Part No. WGCE67814_022625