WatchGuard User Anonymization & the EU General Data Protection Regulation

Technical Brief
WatchGuard Technologies, Inc.
Published: May 2016

Introduction

As the Internet continues to grow, the issue of privacy surrounding user data has taken center stage. Many countries are engaged in developing regulations that set standards for how to move, store, view, and report on data containing users' personally identifiable information, or PII.

The European Union (EU) is setting precedents with the most stringent data and privacy protection regulations in the world. In April 2016, the EU Parliament officially adopted the **General Data Protection Regulation** framework, or **GDPR**, scheduled to be fully enforced in two years. The obligations coming as part of the GDPR are significant, and accountability – especially regarding a business's workforce – is an important component of compliancy. Insider threats continue to be a major source for data breaches and data abuse. "Encrypt everything" is a great start, there is much more that a business must do to be in compliance with the upcoming law.

EU businesses will be required to demonstrate compliance with GDPR measures that include:

- **Conducting a data protection impact assessment** for riskier processing before processing begins

- **Implementing "data protection by design and by default"** – in other words, organizations will need to design data protection into their service infrastructures and conduct assessments on those deployments from an accountability perspective

- **Carrying out technical and organizational measures on data processors**

  - Notify the controller of any breaches

  - Appoint a Data Protection Officer, or DPO*

- **Pseudonymization of personal data** – personally identifiable information is anonymized to the extent that it cannot be attributable to its owner during any stage of processing.

Though not all business may be required to fill such a position, the focus on accountability and strict user privacy is universal across all data processors.

WatchGuard User Anonymization

WatchGuard's Dimension™ visibility platform, which is included with purchase for all WatchGuard Firebox security appliances, delivers a new **User Anonymization** feature that takes an EU organization's capability to be in compliance with the GDPR regulation framework to the next level. The feature works very simply, is easily accessible and configurable, and was designed with GDPR compliance and the reality of insider threats in mind.

How does User Anonymization work?

User Anonymization works by replacing all personally identifiable information (PII) in Dimension's reports, dashboards, and summary pages with hashed placeholder text. When enabled, User Anonymization hashes user names, IP addresses, host names, and mobile device names with unique, randomly generated alphanumeric sequences. The anonymized sequences are not only unique within anonymized sessions, but across all anonymized sessions as well. So, the same anonymized PII data element will be hashed differently each session, disabling any ability to trend hashed PII data within and across sessions.
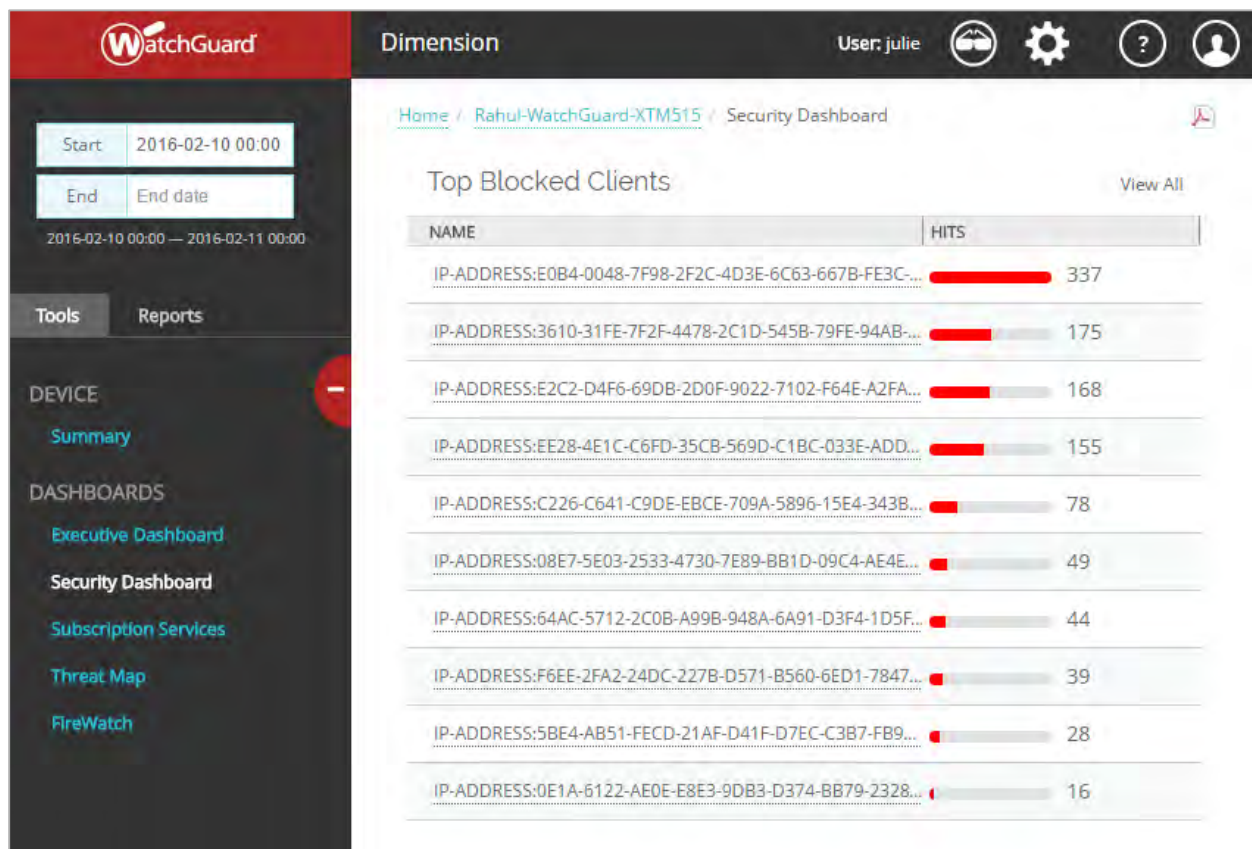

Figure 1. Anonymized mode encrypts only at the visibility platform level. It does not encrypt the database.
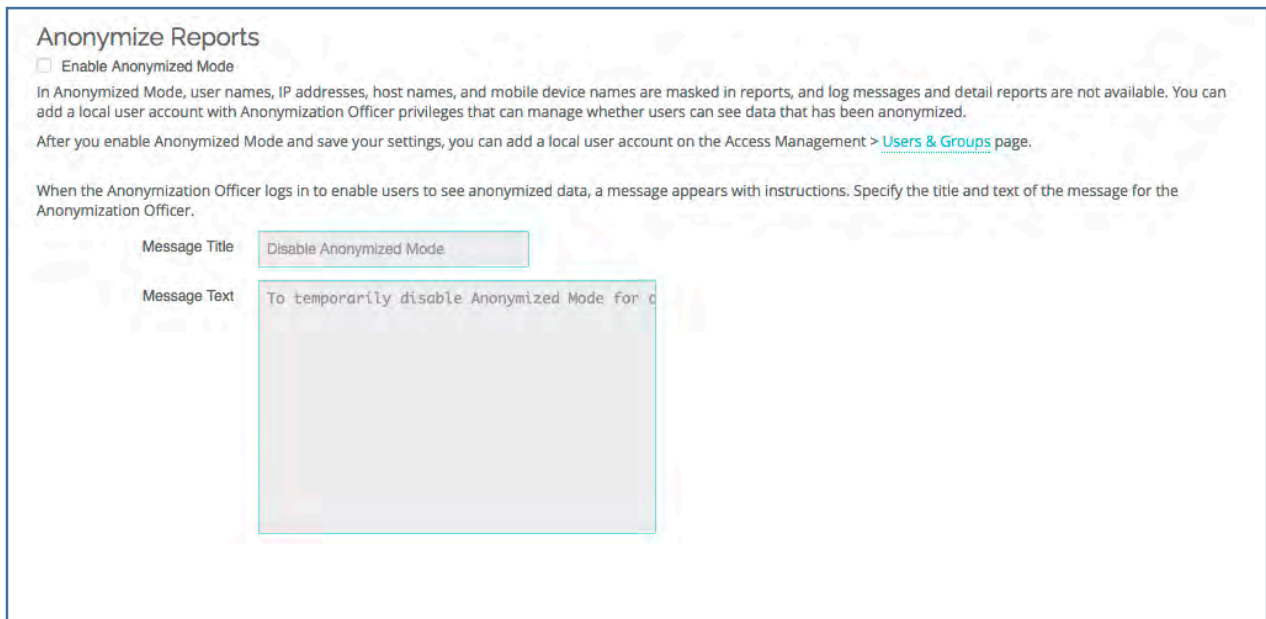
When users log into Dimension while Anonymized Mode is enabled, they will see a restricted view of the pages their user roles allow them to see. Additionally, when the feature is enabled, log messages and detail reports are not available. Dimension visibility dashboards available in Anonymized Mode are:

- Executive Dashboard
- Security Dashboard
- Subscription Services Dashboard
- Threat Map
- FireWatch

As for reporting, only Summary reports are available while in Anonymized mode. "View Details" drill-downs in the Summary reports, as well as Client reports and Detail reports are only available when Dimension is de-Anonymized mode.

How do I enable User Anonymization?

When initially configuring Dimension on a Firebox appliance, User Anonymization can be enabled via the Dimension Setup Wizard. If Dimension has already been deployed, User Anonymization can be enabled via the Server Management and Access Management pages.

Figure 2. Configuring User Anonymization after Dimension has been deployed on a Firebox.

What is the Anonymization Officer?

The **Anonymization Officer** is a new role available in Dimension to support GDPR compliance, mirroring the new Data Protection Officer (DPO) role introduced in the GDPR regulation framework. The Anonymization Officer role was created in such a way that a technical or non-technical person can hold it and it fulfills the "four-eyes" or two-logins approach to authentication. For example, when an IT admin needs to de-anonymize Dimension, the admin would need approval from the Anonymization Officer. This avoids situations in which a single person holds all the access to PII without any accountability or external verification.
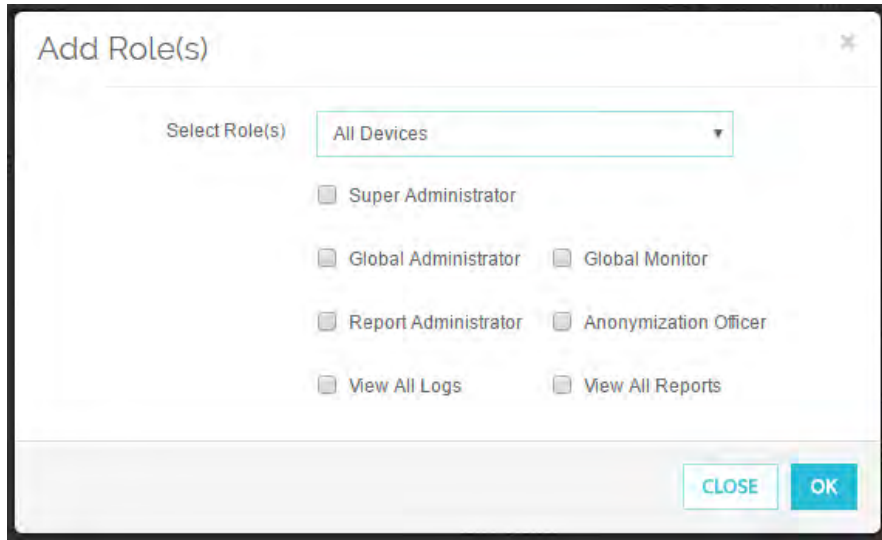

Figure 3. User Anonymization makes it easy designate someone as the Anonymization Officer.

Auditing

Auditing occurs when a Dimension session is de-anonymized. Dimension will log all activity that takes place within Dimension so that the user's actions can be tracked, enabling an organization to hold its IT staff accountable for times when they have permitted access to PII data. Auditing can occur throughout Dimension when anonymized or not, or can be limited to just de-anonymized sessions when Anonymized Mode is enabled.
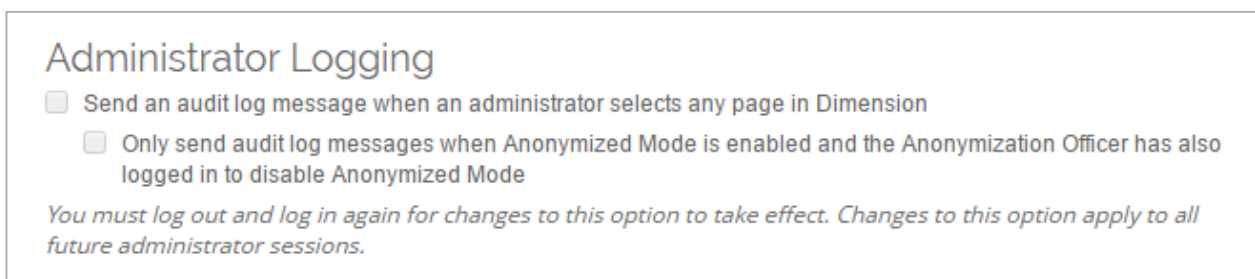

Figure 4. Easily configure whether you want to create an audit log of all actions taken in Dimension or limit that logging to only when Anonymized Mode is enabled but disengaged.

For more information on User Anonymization and WatchGuard's powerful Dimension visibility tools, visit http://www.watchguard.com/dimension

ABOUT WATCHGUARD
WatchGuard® Technologies, Inc. is a global leader of integrated, multi-function business security solutions that intelligently combine industry-standard hardware, best-in-class security features, and policy-based management tools. WatchGuard provides easy-to-use, but enterprise-powerful protection to hundreds of thousands of businesses worldwide. WatchGuard is headquartered in Seattle, Washington with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.