# DNS Firewall Data Visualization

Stanislav Špaček*†, Vít Rusňák* and Anna-Marie Dombajová†
*Masaryk University, Institute of Computer Science, Brno, Czech Republic
†Masaryk University, Faculty of Informatics, Brno, Czech Republic
Email: spaceks@ics.muni.cz, rusnak@ics.muni.cz, dombajova@mail.muni.cz

***Abstract*—Common security tools generate a lot of data suitable for further analysis. However, the raw form of the data is often too complex and useful information gets lost in a large volume of records. In this paper, we propose a system for visualization of the data generated by a DNS firewall and outline a process of visually emphasizing information important to incident handlers. Our prototype suggests that such visualization is possible, keeping the balance between the amount of displayed information and the level of detail.**

## I. Introduction

In our previous work, we have shown that the DNS firewall is a viable security tool that can prevent users from accessing known malicious domains [1]. The DNS firewall also generates a significant amount of data when it is operated on a large-scale internal network. Firewall operators can use this data to stay informed on the firewall status and to be aware of anomalies. However, the data in its raw form contain too many details and are generated too fast to be human-readable. The operators need to react as swiftly as possible in case of an incident. Therefore, the data must be aggregated and presented in a concise form.

In the rest of the paper, we first describe the data generated by the DNS firewall and their important attributes concerning two anomaly detection use cases. Next, we present the requirements on the visualizations followed by the description of the two prototype visualizations suitable for inspection of the two specified anomalies.

## II. DNS Firewall Data Types

We identified the following use cases for the visualizations: (a) DNS Firewall status overview, and (b) anomaly detection. Regarding the latter one, we discussed possible utilization of the firewall data with the CSIRT-MU (https://csirt.muni.cz) incident handlers. They suggested the two types:

- *Infected device* within the internal network may be indicated by a high number of blocked access attempts from a specific internal IP address.
- Ongoing *phishing campaign* may be indicated by a high number of blocked access attempts to a specific domain from a wide range of internal IP addresses.

For these two use cases, we distinguish between the *operational* and *management* data generated by the DNS firewall.

Management Data is created by the actions of firewall operators and provide information on the current firewall status. The DNS firewall manages two lists: blacklist and whitelist. Each operation (add, update or delete) with these lists produce management data record in an audit log.

The mandatory log attributes are: *Timestamp*, *Domain*, *List* to which the domain was added (blacklist or whitelist), *Reason* for listing the domain and *Originator* of the record. The *Reason* should be limited to a set of pre-defined values such as phishing, typosquatting or illegal content. These attributes can be used in the visualization of current and past firewall status.

Operational Data is created each time the firewall blocks a connection attempt on a blacklisted domain. Each connection attempt from an internal IP address to a blacklisted domain generates a record in the firewall log. We reduced each record to only four main attributes: target *Domain*, source *IP address*, and *Date* and *Time* of occurrence. This quadruple is sufficient input for detecting the two presented anomalies.

These attributes allow us to answer key questions related to the *infected device* and *phishing campaign* anomalies identification: WHO (*IP address*) was involved?; WHERE (*Domain*) they attempt to go? *WHEN* (*Date* and *Time*) it happened?

## III. Visualization Concept

Data types should be presented as individual views. The view is a combination of tabular and visual elements (charts) providing an interface for inspecting respective data. The aims are to increase situational awareness over the firewall operation and to enable detailed inspection of the logged data. Any view should not overwhelm the operators with information, as they typically must keep track of more tools than one firewall.

Management Data Visualization should provide a view on the black- and white-listed domains and allow monitoring of blocking actions within a selected time-frame. The view should also include an aggregated data about a number of blocked domains and their categorization based on the *Reason*.

Operational Data Visualization should provide a view allowing the operator to verify whether some anomaly indicates a security incident or not. The view should thus be interactive and support configurable filters and time-frames. Facing the three key questions:

- WHO? – the view should aggregate all blocked attempts originating from the same source, so an *IP address* with a large number of accesses within a specified time-frame can be easily singled out.
- WHERE TO? – the view should aggregate all blocked attempts directed towards the same *Domain*. A *Domain*

978-3-903176-15-7 

with a large number of access attempts within a specified time-frame is easy to reveal.
- WHEN? – the view should aggregate the access attempts with a predefined granularity (e.g., 24 hours).

## IV. Visualization Prototype

Our prototype visualization is a web-based front-end application implemented in the Angular framework (https://angular.io). It offers two main views with a similar layout of principal components. Our design goal was to craft a simple and intuitive user interface.

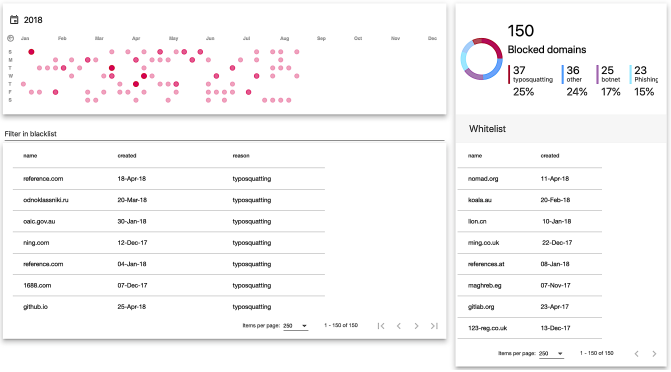


Fig. 1. Management data view. Components: heatmap calendar view showing a distribution of blocked domains based on the entry date (top-left), blacklist records with a search field (bottom-left), blacklisted domains summary (top-right), whitelist records (bottom-right).

The first view provides an interactive interface for showing management data of the DNS firewall (Fig. 1). There are four main components:

- *Heatmap calendar* showing the distribution of blocked domains based on the entry date; by clicking on the dot, blacklist table shows the records of a selected day; the intensity of color hints the number of records for that day (darker color = more records).
- *Blacklist table* with details on blacklisted domains; the table is accompanied with the search input which enables filtering based on the input string including date or category of blocking reasons. All columns are sortable.
- *Categorized summary of blacklisted domains* shows the global statistics on the number of blacklisted domains and their counts in different blocking reason categories.
- *Whitelist table* whitelisted domains table (bottom-right).

The tables, as well as chart visualization, are also scrollable and the components are interconnected (e.g., when a user clicks on the blocking reason category in the chart, the blacklist table filters only relevant records).

The second view provides users with the operational data from the DNS firewall log. There are three main components:

- *Heatmap calendar* showing the distribution of records based on their occurrence; by clicking on the dot, log details table shows the records of a selected day; the intensity of color hints the number of records for that day likewise the previous one.

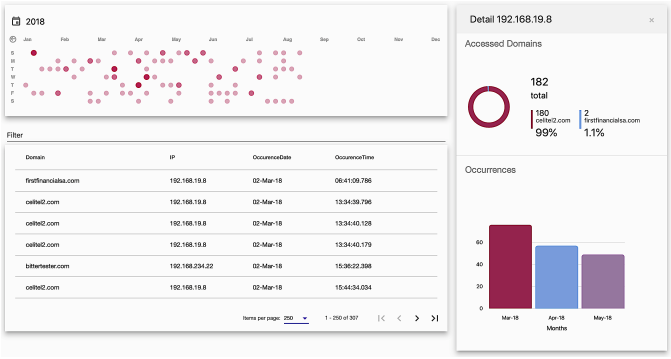


Fig. 2. Operational data view. Components: heatmap calendar view showing the distribution of records based on the domain occurrence (top-left), log details with a search field (bottom-left), IP address inspector (right side) – contains summary of accessed domains for selected IP address (top), occurrence of accessed domains from the selected IP address (bottom).

- *Log details table* with details on records in the firewall log; the table is accompanied with the search input having the same capabilities as in the DNS firewall view. By clicking on either domain name or IP address in the table, the related details are displayed.
- *Domain/IP address inspector* shows details from one of the two perspectives. When a user selects an IP address, it shows the number of blacklisted domains which the IP was trying to reach and their aggregated counts in time. When a user selects a domain name, the number of IP addresses trying to access it and their aggregated counts is shown instead.

## V. Demonstration Structure

We are going to present views on both the management and operational data of the DNS firewall. In the demonstration, we will use real anonymized data from our DNS firewall. We want to discuss other possible views on the data and the balance between the level of detail and the amount of the data displayed.

## VI. Conclusion

We introduced a system for visualization of the DNS firewall data. The system can transform the raw data into illustrative and human-readable form so that the incident handlers can distinguish anomalies in the firewall operation.


## Acknowledgement

This research was supported by the Security Research Programme of the Czech Republic 2015–2020 (BV III / 1 VS) granted by the Ministry of the Interior of the Czech Republic under No. VI20172020070 Research of Tools for Cyber Situation Awareness and Decision Support of CSIRT Teams in the Protection of Critical Infrastructure.


## References


[1] S. Spacek, M. Lastovicka, T. Plesnik, and M. Horak, "Current Issues of Malicious Domains Blocking," in *Proceedings of the 2019 IFIP/IEEE International Symposium on Integrated Network Management, IM 2019*, 2019, [To appear].