FortigateDemo

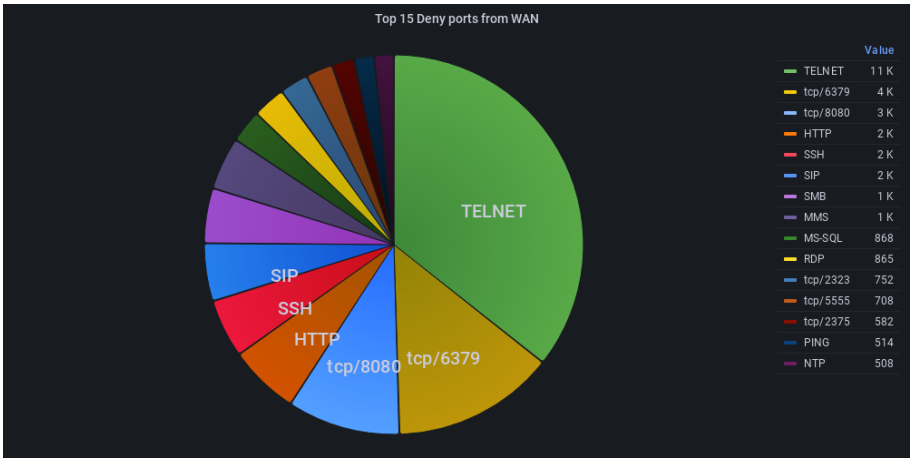
Reporting period 2022-10-19 - 2022-11-02

Report created 2022-11-03

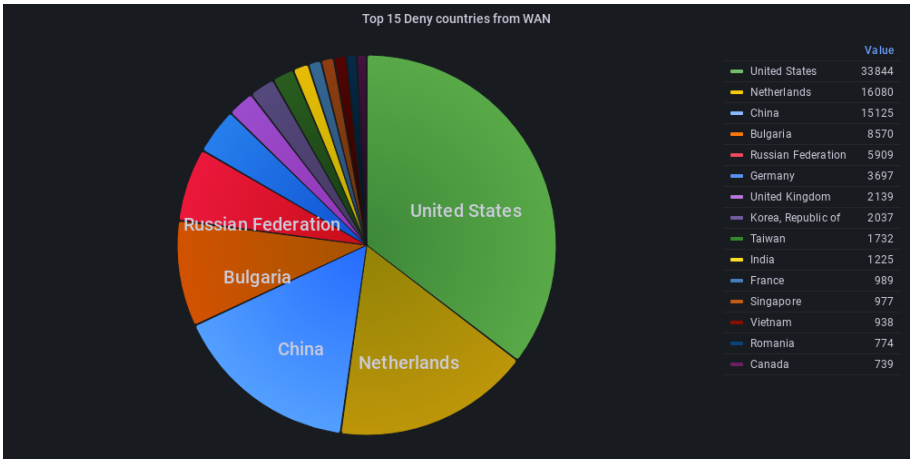
Fortigate statistical data

All the data from this section is collected from Elasticsearch using Fortigate syslog capabilities and Zabbix monitoring. Syslog dataformat is CEF, so it can be easilly parsed.

Fortigate ACL deny, based on settings.

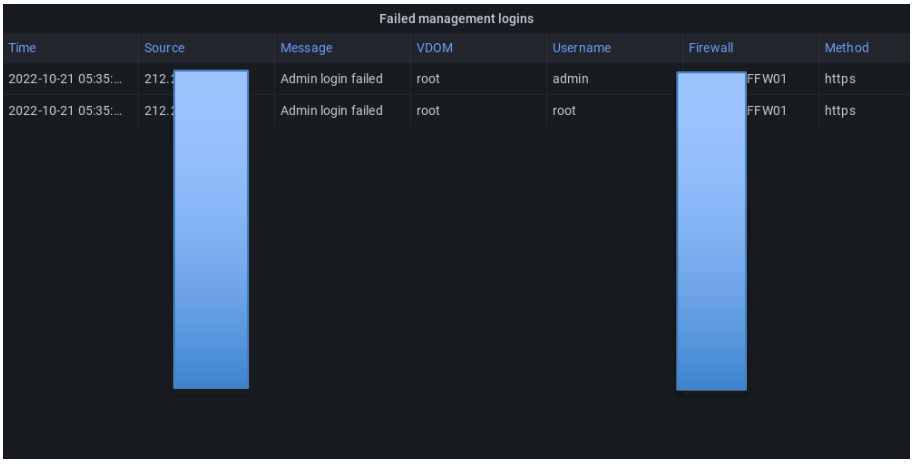


1. Top 15 Deny ports from WAN



2. Top 15 Deny countries from WAN

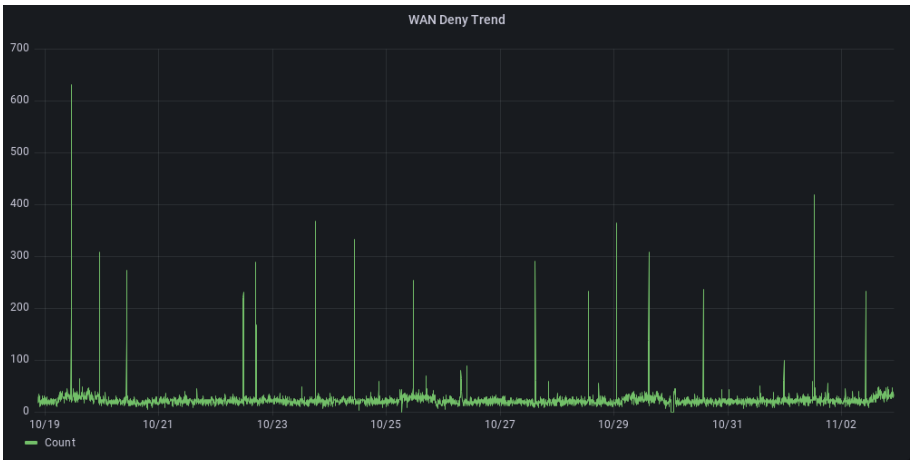
Fortigate failed management logins.



3. Failed management logins

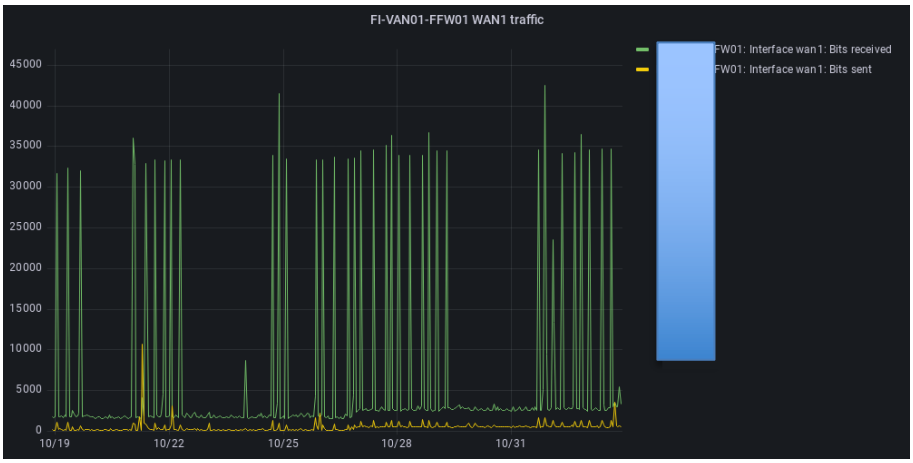
Fortigate monitoring data from Zabbix

Data from this section comes from Zabbix.



4. WAN Deny Trend

Peaks in graph can indicate some network scanner activity.



5. FI-VAN01-FFW01 WAN1 traffic