

● Zabbix Conference Poland 2026

# From Metrics to Meaning

Extending Zabbix with Flow Data and External Pipelines  
for Real-Time Network Intelligence

Prezentuje

**Marcin Kaźmierczak**

—  
Czy ICMP i SNMP  
wystarczą do pełnej  
widoczności?

—  
Gdzie szukasz  
przyczyny, gdy  
metryki są OK?

—  
Czy widzisz ruch, który  
nie generuje alertów?

—  
Co naprawdę  
wydarzyło się między  
dwoma pomiarami?

—  
W jaki sposób Sycopa  
może uzupełnić  
brakujące dane?



# Jakie możliwości monitorowania daje NetFlow?

# Jakie możliwości monitorowania daje NetFlow

- Monitorowanie całej sieci. Switche, routery, firewalle różnych producentów wysyłają NetFlow
- NetFlow to metadane o ruchu sieciowym – zbierane są tylko najważniejsze dane dla naszej analizy

Section	Variable	Value
<b>Basic Fields</b>		
1	Time	2022-11-29 17:02:00
2	Client IP	172.16.20.198
3	Server IP	216.58.215.110
4	IP Protocol	6
5	Protocol Name	TCP (6)
6	Client Port	55250
7	Server Port	443
8	Application	443
9	Application Name	https (443)
10	Exporter IPs	172.16.100.1
11	Interfaces	172.16.100.1[4],172.16.100.1[5]
12	Client Function	Workstations

Client IP	172.16.20.198
Server IP	216.58.215.110

Kto?

IP Protocol	6
Protocol Name	TCP (6)
Client Port	55250
Server Port	443
Application	443
Application Name	https (443)

Co?

Exporter IPs	172.16.100.1
Interfaces	172.16.100.1[4],172.16.100.1[5]

Gdzie?

# Jakie możliwości monitorowania daje NetFlow

- Nawet 80–90% problemów w sieci można zauważyć wcześniej, analizując sam przepływ ruchu

- Nie trzeba znać treści pakietów, wystarczy wiedzieć:

- Kto wysyła
- Dokąd wysyła
- Jak dużo
- Jak często

To właśnie  
pokazuje NetFlow.

Section	Variable	Value
<b>Measures</b>		
30	Active Time	30296
31	First Timestamp	2022-11-29 16:56:58
32	Last Timestamp	2022-11-29 16:57:53
33	Bytes	33.70KB
34	Client Bytes	22.57KB
35	Server Bytes	11.13KB
36	Bits	269,576
37	Client Bits	180,560
38	Server Bits	89,016
39	Bits/s	4.49kb/s
40	Clients Bits/s	3.01kb/s
41	Server Bits/s	1.48kb/s
42	Packets	124
43	Client Packets	54
44	Server Packets	70
45	Packets/s	16.53pkt/s
46	Client Packets/s	0.90pkt/s
47	Server Packets/s	1.17pkt/s
48	Flows	12

30	Active Time	30296
31	First Timestamp	2022-11-29 16:56:58
32	Last Timestamp	2022-11-29 16:57:53

Kiedy?

36	Bits	269,576
37	Client Bits	180,560
38	Server Bits	89,016
39	Bits/s	4.49kb/s
40	Clients Bits/s	3.01kb/s
41	Server Bits/s	1.48kb/s
42	Packets	124
43	Client Packets	54
44	Server Packets	70
45	Packets/s	16.53pkt/s
46	Client Packets/s	0.90pkt/s
47	Server Packets/s	1.17pkt/s
48	Flows	12

Jak dużo?

# Syclope + Zabbix

Pasywne monitorowanie NetFlow uzupełnia luki aktywnego monitoringu ICMP/SNMP

**AKTYWNE MONITOROWANIE ICMP / SNMP w ZABBIX**

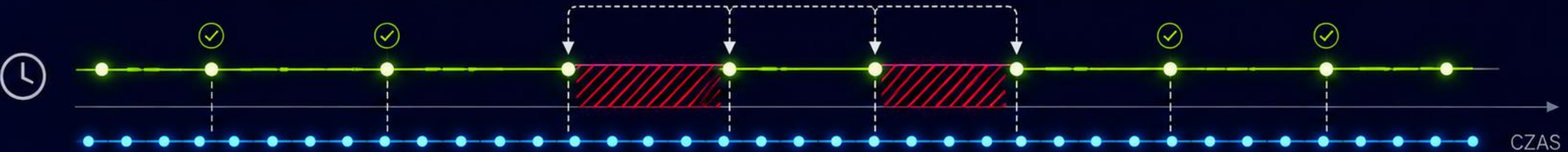
● Widoczność tylko w momentach sondowania

**LUKI W AKTYWNYM MONITORINGU**

Problemy mogą wystąpić między sondowaniami i pozostać niewykryte

**PASYWNE MONITOROWANIE NETFLOW w SYCOPE**

● Ciągła widoczność – 24/7/365



RAZEM = PEŁNY OBRAZ SIECI

**AKTYWNE + PASYWNE**



**ZABBIX**

Dane o urządzeniach, alertach, dostępności

**API**

Integracja przez API

**SYCOPE**

Dane o ruchu, rozmowach, aplikacjach, top talkers

**PEŁNA WIDOCZNOŚĆ SIECI**

- Więcej kontekstu
- Szybsza identyfikacja problemów
- Lepsze decyzje
- Optymalizacja sieci
- Oszczędność czasu i zasobów

# Monitoruj swoją sieć w czasie rzeczywistym – za darmo!

- Bez konieczności podawania karty płatniczej
- Gotowe do użycia od razu po instalacji
- Wykrywanie zagrożeń i anomalii
- Do 5 000 flows/s
- Retencja danych ograniczona do 14 dni

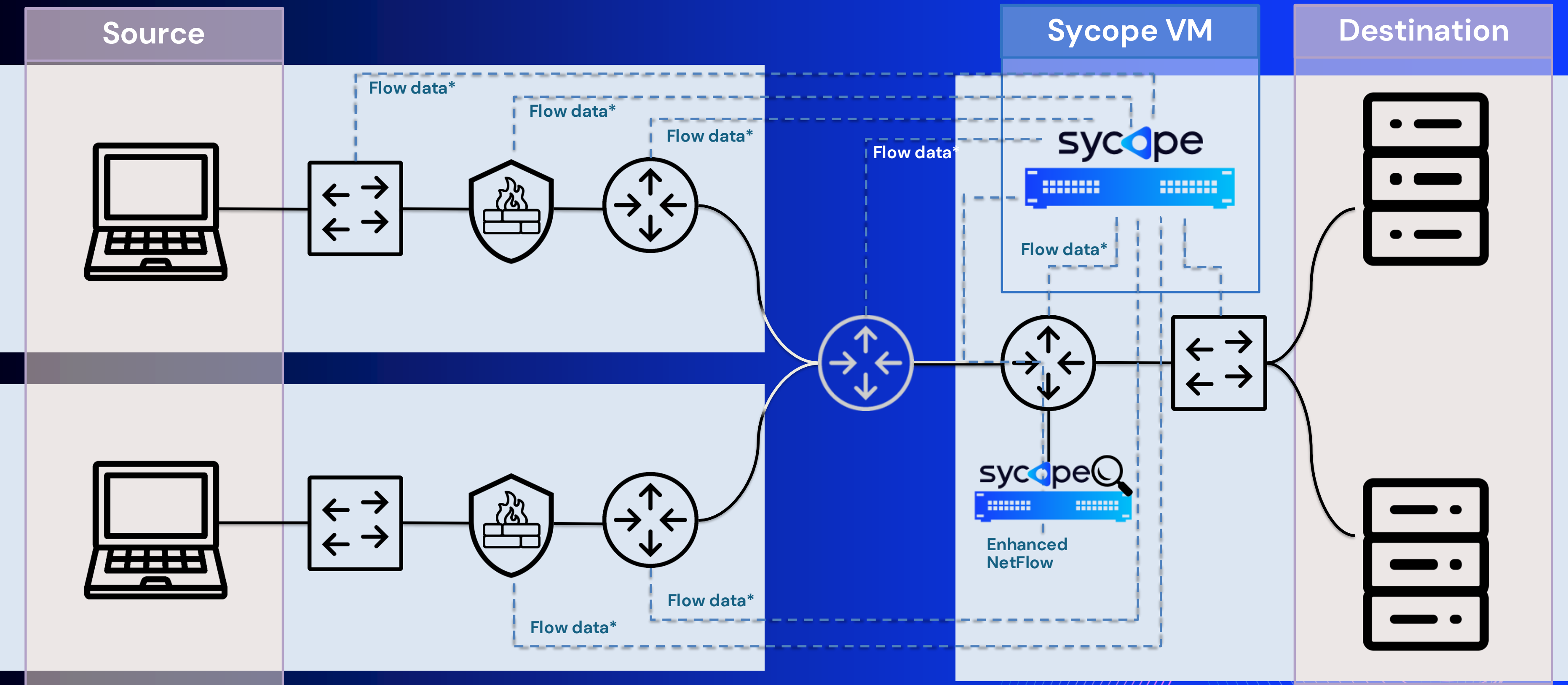


<https://free.syclope.com>



# Jak działa Syclope?

# Wiele źródeł ruchu – jedno centrum dowodzenia

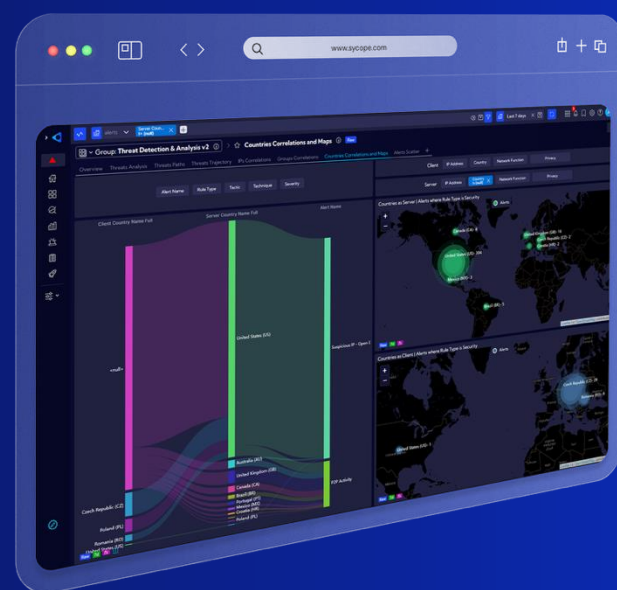


# Platforma Network Observability

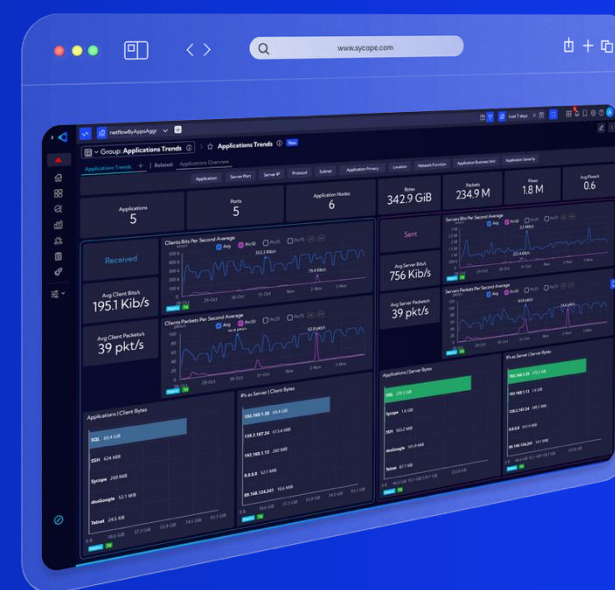
Podstawą systemu jest Visibility, zasilany danymi NetFlow, dostarczający informacje o ruchu sieciowym. Kolejne moduły wzbogacają informacje o ruchu sieciowym, o wskaźniki wydajnościowe, analizę L7, wykrywanie anomalii i inwentaryzację urządzeń.



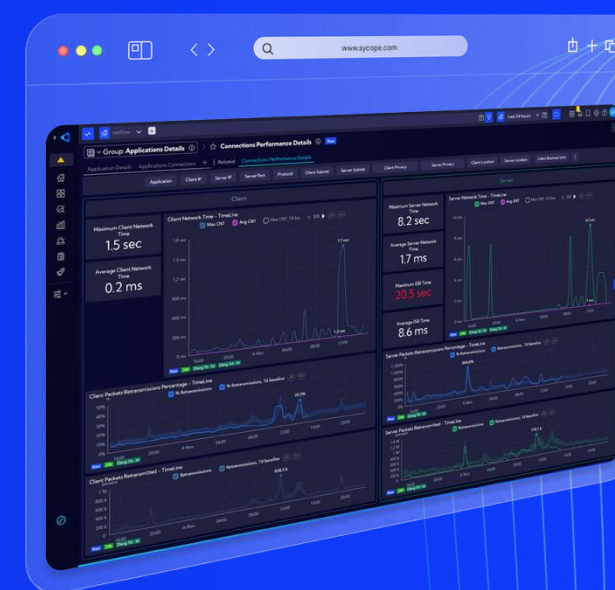
**VISIBILITY**  
Analiza ruchu



**PERFORMANCE**  
Wydajność sieci (NPM)



**SECURITY**  
Wykrywanie zagrożeń



**ASSET DISCOVERY**  
Inwentaryzacja zasobów

# Mądrzejsze decyzje z Sycope

● NETWORK INTELLIGENCE

● ZESPÓŁ NOC

● ZESPÓŁ SOC

## NTA

Network Traffic Analysis

- Inteligentne trendy & Baselines
- Pasywna analiza ruchu flowego

## NPM

Network Performance Monitor

- Automatyczna inwentaryzacja zasobów
- Wykrywanie aplikacji
- Bez dodatkowych uprawnień

**sycope**

UNIFIED PLATFORM

NOC + SOC  
w jednym widoku

SHARED CONTEXT

## NDR

Network Detection and Response

- Ponad 70 reguł i alertów
- Repozytorium online – CTI
- IDS oraz analiza pakietów

# Integracje



# SycopeSolutions – Otwarte Repozytorium GitHub

• <https://github.com/SycopeSolutions/>



A screenshot of a web browser showing the GitHub repository page for 'Integrations/zabbix'. The browser's address bar shows 'github.com/SycopeSolutions/Integrations/tree/main/zabbix'. The page is divided into a left sidebar and a main content area. The sidebar, titled 'Files', shows a file tree with folders like 'examples', 'phpipam', 'suricata', 'sycope', 'webhooks', 'jira', 'jira\_with\_power\_automate', 'slack', 'teams', and 'zabbix'. The 'zabbix' folder is expanded, showing subfolders like 'dashboards', 'drilldowns', and 'fields', along with files like 'README.md', '\_\_init\_\_.py', 'config.json', 'install.py', 'requirements.txt', 'uninstall.py', 'zabbix\_lookup\_sync.py', and 'zabbix\_statistics.py'. The main content area is titled 'Integrations / zabbix /' and contains a section 'How the Integrations works'. This section describes two scripts: 'zabbix\_statistics\_sync.py' and 'zabbix\_lookup\_sync.py'. The 'zabbix\_statistics\_sync.py' script is described as logging into the Zabbix API, collecting metrics for defined IP addresses, aligning timestamps for different metrics (CPU Load, ICMP Reponse Time, Memory Usage and Packet Loss), comparing gathered metrics with already available metrics in Sycope's custom index to avoid duplicate samples, and saving the difference in Sycope. The 'zabbix\_lookup\_sync.py' script is described as logging into the Zabbix API and collecting inventory data such as Hostname, OS version, Serial number, Notes and URLs, comparing gathered inventory data with already available custom Lookup to avoid duplicate records, and saving the difference in Sycope. Below this is a 'Repository Content' section showing a tree view of the repository structure with comments for each folder and file. The 'Requirements' section is partially visible at the bottom.





# Łączenie danych – wspólne GUI

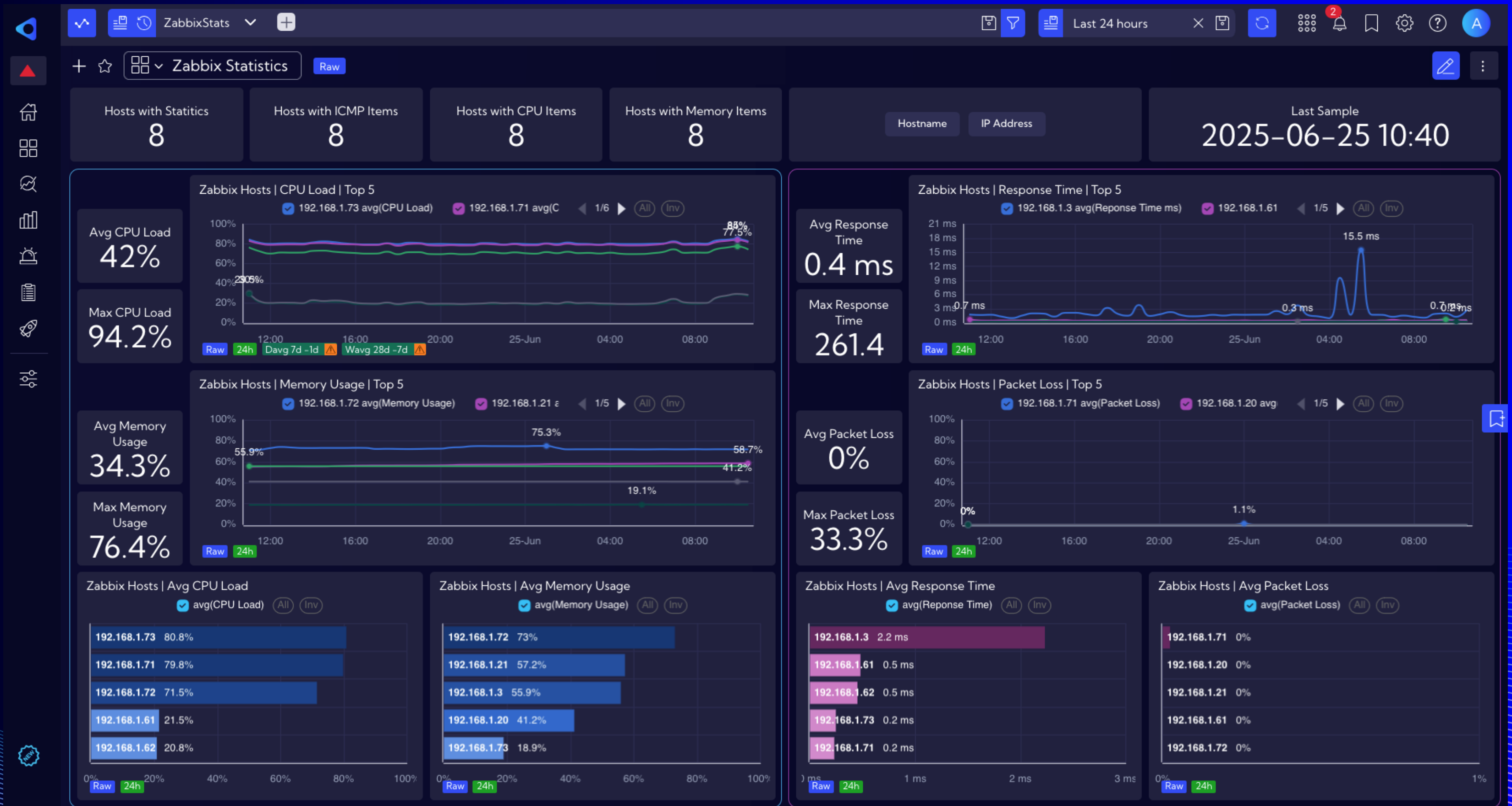
# Synchronizacja Inwentaryzacji

- Zidentyfikuj, które Hosty są Włączone i jakie Elementy Zabbix są dostępne
- Używaj filtrów w Sycope na podstawie Inwentarza Zabbix (dane z SNMP, WMI, SSH)

The screenshot displays the Zabbix Asset Management interface. At the top, it shows 'Total IPs: 168' and 'Private IPs: 168'. Below this, there are filter buttons for 'Privacy', 'Subnet', 'IP Address', 'Domain name', 'Profile Names', 'Country', 'Location', 'Severity', 'Network Function', and 'Service'. The main table has 14 columns and 18 rows of data. The 'Privacy' column contains 'PRIVATE' for all entries. The 'Zabbix Status' column shows 'Enabled' for all entries.

Action	Privacy	IP address	Zabbix Name	Subnet	Profile Names	Zabbix Type	Zabbix Notes	Zabbix Group	Zabbix ICMP URL	Zabbix Graph URL	Zabbix Status
<input type="checkbox"/>	PRIVATE	192.168.175	CentOS-5	LAN	<blank list>	SNMP	Test VM5 (CentOS)	Linux servers	http://192.168.1.46:808...	http://192.168.1.46:808...	Enabled
<input type="checkbox"/>	PRIVATE	192.168.174	CentOS-4	LAN	<blank list>	SNMP	Test VM4 (CentOS)	Linux servers	http://192.168.1.46:808...	http://192.168.1.46:808...	Enabled
<input type="checkbox"/>	PRIVATE	192.168.173	CentOS-3	LAN	<blank list>	SNMP	Test VM3 (CentOS)	Linux servers	http://192.168.1.46:808...	http://192.168.1.46:808...	Enabled
<input type="checkbox"/>	PRIVATE	192.168.172	CentOS-2	LAN	<blank list>	SNMP	Test VM2 (CentOS)	Linux servers	http://192.168.1.46:808...	http://192.168.1.46:808...	Enabled
<input type="checkbox"/>	PRIVATE	192.168.171	CentOS-1	LAN	<blank list>	SNMP	Test VM1 (CentOS)	Linux servers	http://192.168.1.46:808...	http://192.168.1.46:808...	Enabled
<input type="checkbox"/>	PRIVATE	192.168.138	192.168.138	SQL Server	[SQL]	ICMP	SQL Server	Databases	http://192.168.1.46:808...	No Other Items	Enabled
<input type="checkbox"/>	PRIVATE	192.168.123	pve4	LAN	<blank list>	SNMP	Proxmox VE pve4	Hypervisors	http://192.168.1.46:808...	http://192.168.1.46:808...	Enabled
<input type="checkbox"/>	PRIVATE	192.168.122	192.168.122	LAN	<blank list>	ICMP	Proxmox VE pve3	Hypervisors	http://192.168.1.46:808...	No Other Items	Enabled
<input type="checkbox"/>	PRIVATE	192.168.121	pve2	LAN	<blank list>	SNMP	Proxmox VE pve2	Hypervisors	http://192.168.1.46:808...	http://192.168.1.46:808...	Enabled
<input type="checkbox"/>	PRIVATE	192.168.120	pve1	LAN	<blank list>	SNMP	Proxmox VE pve1	Hypervisors	http://192.168.1.46:808...	http://192.168.1.46:808...	Enabled
<input type="checkbox"/>	PRIVATE	192.168.137	192.168.137	CRM Website	[SQL, Web Application]	ICMP	Network Performanc...	Discovered hosts	http://192.168.1.46:808...	No Other Items	Enabled
<input type="checkbox"/>	PRIVATE	192.168.13	Switch	LAN	<blank list>	SNMP	Core Switch A	Discovered hosts	http://192.168.1.46:808...	http://192.168.1.46:808...	Enabled
<input type="checkbox"/>	PRIVATE	192.168.162	Router2.localdomain	LAN	<blank list>	SNMP	Cisco Cloud Services ...	Discovered hosts	http://192.168.1.46:808...	http://192.168.1.46:808...	Enabled
<input type="checkbox"/>	PRIVATE	192.168.161	Router1.localdomain	LAN	<blank list>	SNMP	Cisco Cloud Services ...	Discovered hosts	http://192.168.1.46:808...	http://192.168.1.46:808...	Enabled
<input type="checkbox"/>	PRIVATE	192.168.153	BRW7440BB6BC2271...	LAN	<blank list>	SNMP	<blank string>	Discovered hosts	No ICMP Items	No Other Items	Enabled
<input type="checkbox"/>	PRIVATE	192.168.1201	wso2apm.localdomain	LAN	<blank list>	ICMP	<blank string>	Discovered hosts	No ICMP Items	No Other Items	Enabled
<input type="checkbox"/>	PRIVATE	192.168.131	192.168.131	LAN	<blank list>	ICMP	<blank string>	Discovered hosts	http://192.168.1.46:808...	No Other Items	Enabled

# Zabbix Statistics Dashboard



# Zabbix Inventory Dashboard

assetDevices [ + ] Last 24 hours [ 2 ] [ ? ] [ A ]

+ ☆ Zabbix Inventory [ Raw ] [ ✎ ] [ ⋮ ]

### Zabbix Inventory

IP address	Zabbix Name	Zabbix Type	Zabbix Status	Zabbix Group	Zabbix Notes	Zabbix OS	Zabbix Serial No	Zabbix ICMP URL	Zabbix Graph URL
192.168.1.75	CentOS-5	SNMP	Enabled	Linux servers	Test VM5 (CentOS)	<blank string>	<blank string>	http://192.168.1.46.808	http://192.168.1.46.808
192.168.1.74	CentOS-4	SNMP	Enabled	Linux servers	Test VM4 (CentOS)	<blank string>	<blank string>	http://192.168.1.46.808	http://192.168.1.46.808
192.168.1.73	CentOS-3	SNMP	Enabled	Linux servers	Test VM3 (CentOS)	<blank string>	<blank string>	http://192.168.1.46.808	http://192.168.1.46.808
192.168.1.72	CentOS-2	SNMP	Enabled	Linux servers	Test VM2 (CentOS)	<blank string>	<blank string>	http://192.168.1.46.808	http://192.168.1.46.808
192.168.1.71	CentOS-1	SNMP	Enabled	Linux servers	Test VM1 (CentOS)	<blank string>	<blank string>	http://192.168.1.46.808	http://192.168.1.46.808
192.168.1.38	192.168.1.38	SNMP	Enabled	Databases	SQL Server	<blank string>	<blank string>	http://192.168.1.46.808	No Other Items
192.168.1.23	pve4	SNMP	Enabled	Hypervisors	Proxmox VE pve4	<blank string>	<blank string>	http://192.168.1.46.808	http://192.168.1.46.808
192.168.1.22	192.168.1.22	SNMP	Enabled	Hypervisors	Proxmox VE pve3	<blank string>	<blank string>	http://192.168.1.46.808	No Other Items
192.168.1.21	pve2	SNMP	Enabled	Hypervisors	Proxmox VE pve2	<blank string>	<blank string>	http://192.168.1.46.808	http://192.168.1.46.808
192.168.1.20	pve1	SNMP	Enabled	Hypervisors	Proxmox VE pve1	<blank string>	<blank string>	http://192.168.1.46.808	http://192.168.1.46.808
192.168.1.37	192.168.1.37	SNMP	Enabled	Discovered hosts	Network Performance Monitor	<blank string>	<blank string>	http://192.168.1.46.808	No Other Items
192.168.1.3	Switch	SNMP	Enabled	Discovered hosts	Core Switch A	15.0(2)SE11	<blank string>	http://192.168.1.46.808	http://192.168.1.46.808
192.168.1.61	Router1.localdomain	SNMP	Enabled	Discovered hosts	Cisco Cloud Services Router 1000v	17.3.3	9E1ACJ3VXDX	http://192.168.1.46.808	http://192.168.1.46.808
192.168.1.62	Router2.localdomain	SNMP	Enabled	Discovered hosts	Cisco Cloud Services Router 1000v	17.3.3	964R4WIWQY2	http://192.168.1.46.808	http://192.168.1.46.808
192.168.1.1	unifi.localdomain	SNMP	Enabled	Discovered hosts	<blank string>	<blank string>	<blank string>	No ICMP Items	No Other Items
192.168.1.10	192.168.1.10	SNMP	Enabled	Discovered hosts	<blank string>	<blank string>	<blank string>	No ICMP Items	No Other Items
192.168.1.11	192.168.1.11	ICMP	Enabled	Discovered hosts	<blank string>	<blank string>	<blank string>	No ICMP Items	No Other Items
192.168.1.13	192.168.1.13	SNMP	Enabled	Discovered hosts	<blank string>	<blank string>	<blank string>	http://192.168.1.46.808	No Other Items
192.168.1.14	192.168.1.14	SNMP	Enabled	Discovered hosts	<blank string>	<blank string>	<blank string>	http://192.168.1.46.808	No Other Items
192.168.1.15	192.168.1.15	SNMP	Enabled	Discovered hosts	<blank string>	<blank string>	<blank string>	http://192.168.1.46.808	No Other Items
192.168.1.16	192.168.1.16	ICMP	Enabled	Discovered hosts	<blank string>	<blank string>	<blank string>	http://192.168.1.46.808	No Other Items
192.168.1.19	192.168.1.19	SNMP	Enabled	Discovered hosts	<blank string>	<blank string>	<blank string>	http://192.168.1.46.808	No Other Items
192.168.1.27	192.168.1.27	ICMP	Enabled	Discovered hosts	<blank string>	<blank string>	<blank string>	No ICMP Items	No Other Items
192.168.1.28	192.168.1.28	ICMP	Enabled	Discovered hosts	<blank string>	<blank string>	<blank string>	No ICMP Items	No Other Items

[ Raw ] [ 24h ] [ fx ]

# Filtruj dowolny widok używając Fields i Inventory z Zabbix

The screenshot displays the Syclope interface with a Zabbix Group (ServerIP) filter dialog open. The dialog shows a search bar with the placeholder "eg. \*abc\* or >value" and a list of categories with their respective percentages:

- Linux servers 4.2%
- <null> 51.1%
- Discovered hosts 32.5%
- Databases 9.1%
- Hypervisors 3.1%

Buttons for "Clear filters" and "Apply" are visible at the bottom of the dialog. The main interface shows a network flow visualization on the left and a table of network flows on the right. The table has columns for Client IP, IP Address, Port, Subnet, Private, Location, Country, Network Function, Bytes, Server Bytes, Client Bytes, Packets, Flows, and Client requests. The table shows data for various IP addresses and ports, including snmp (161), ssh (22), and www (80).

Server IP	Client IP	Port Name	Protocol Name	Application	Bytes	Server Bytes	Client Bytes	Packets	Flows	Client requests
192.168.1.46	192.168.1.46	snmp (161)	UDP (17)	<null>	1.4 MiB	1 MiB	379.3 KiB	10.2 k	1.9 k	0
192.168.1.37	192.168.1.37	ssh (22)	TCP (6)	<null>	223.3 KiB	133.8 KiB	89.5 KiB	1.2 k	24	12
192.168.1.37	192.168.1.37	snmp (161)	UDP (17)	<null>	136.9 KiB	79.2 KiB	57.7 KiB	1 k	148	0
192.168.1.50	192.168.1.50	ssh (22)	TCP (6)	<null>	74.9 KiB	57.4 KiB	17.5 KiB	626	4	0
192.168.1.50	192.168.1.50	snmp (161)	UDP (17)	<null>	53.4 KiB	28.6 KiB	24.9 KiB	564	412	0
192.168.1.71	78.10.161.3	(0)	ICMP (1)	<null>	3.7 KiB	0 B	3.7 KiB	31	1	0
192.168.1.71	192.168.1.46	ssh (22)	TCP (6)	<null>	1.5 KiB	1.2 KiB	290 B	9	4	0
192.168.1.71	192.168.1.46	telnet (23)	TCP (6)	<null>	106 B	46 B	60 B	2	4	0
192.168.1.71	192.168.1.46	www (80)	TCP (6)	<null>	106 B	46 B	60 B	2	4	0
192.168.1.71	192.168.1.46	zabbix-agent (10000)	TCP (6)	<null>	106 B	46 B	60 B	2	4	0
192.168.1.71	192.168.1.46	https (443)	TCP (6)	<null>	106 B	46 B	60 B	2	4	0
192.168.1.71	192.168.1.131	ndmp (10000)	TCP (6)	<null>	15.2 MiB	11.5 MiB	3.7 MiB	93 k	18	5

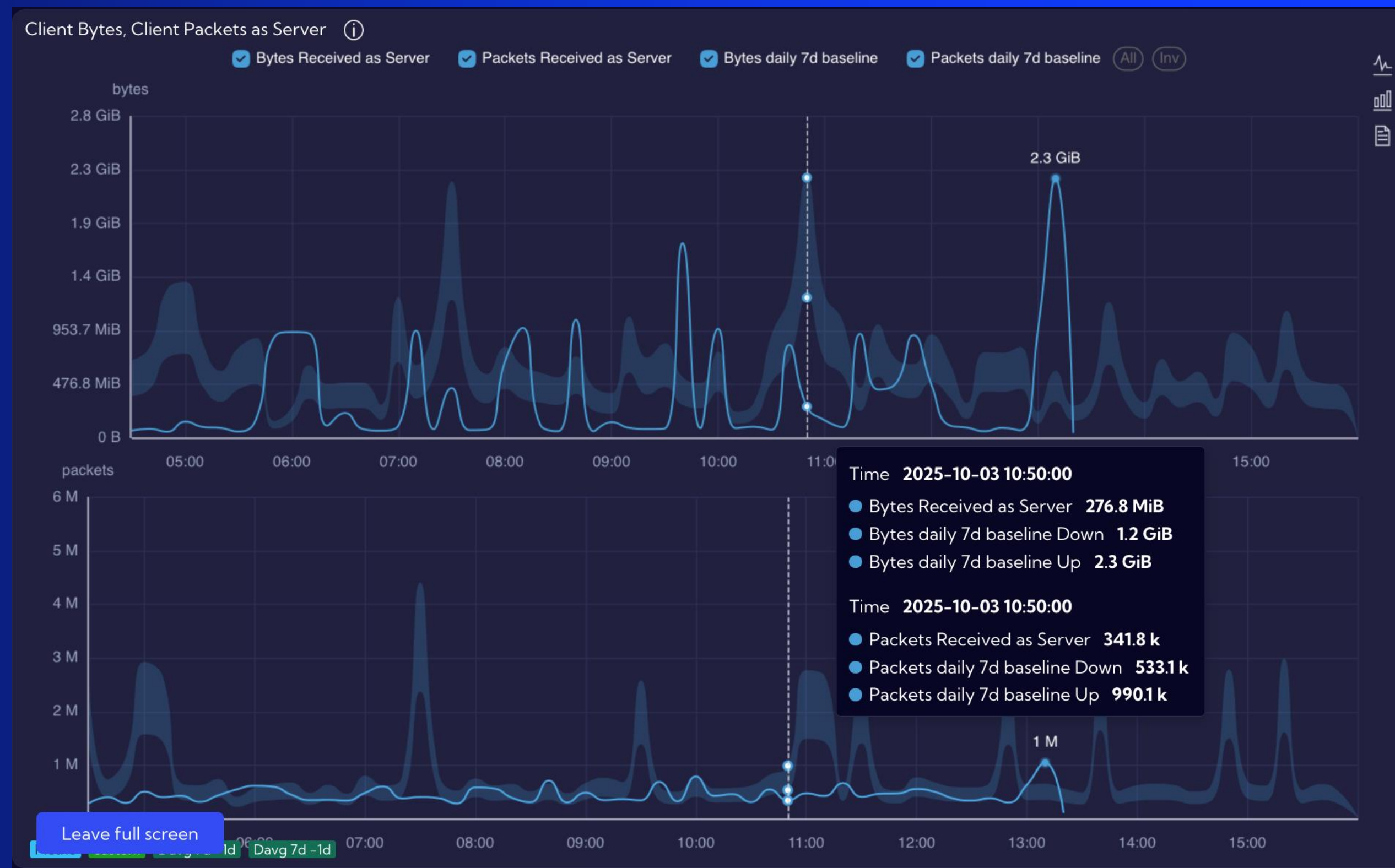
# Automatyczne Trendy i Baseline

Efekt wstążki dla bieżącego i przyszłego ruchu

Zakres dla baseline – wartości Górna i Dolna

Twórz trendy na dowolnym wykresie używając wszystkich dostępnych metryk

Wsparcie dla punktów końcowych, aplikacji, podsięci, lokalizacji, krajów, AS





**Przejdźmy do Zabbixa...**

# Akcje Drilldown, aby wyświetlić dowolne dane z Zabbix i..

Copy

- Exclude (Add to filter with negation)
- Open filter modal
- Drilldown >
- Actions >
- Resolve >
- Net Mask Search >

Servers >

- Zabbix Inventory
- Asset Device First/Last Seen
- Asset Device Info
- Basic Conversation Metrics
- Host Info (Server)
- Session Details

Add drilldown action


Manage drilldowns


Zabbix Inventory Filtering: Global Local

assetDevices IP address =192.168.1.38

IP address	Zabbix Status	Zabbix Group	Zabbix Notes	Zabbix ICMP URL	Zabbix Graph URL
192.168.1.38	Enabled	Databases	SQL Server	http://192.168.1.46:8080/history.php?acti...	No Other Items

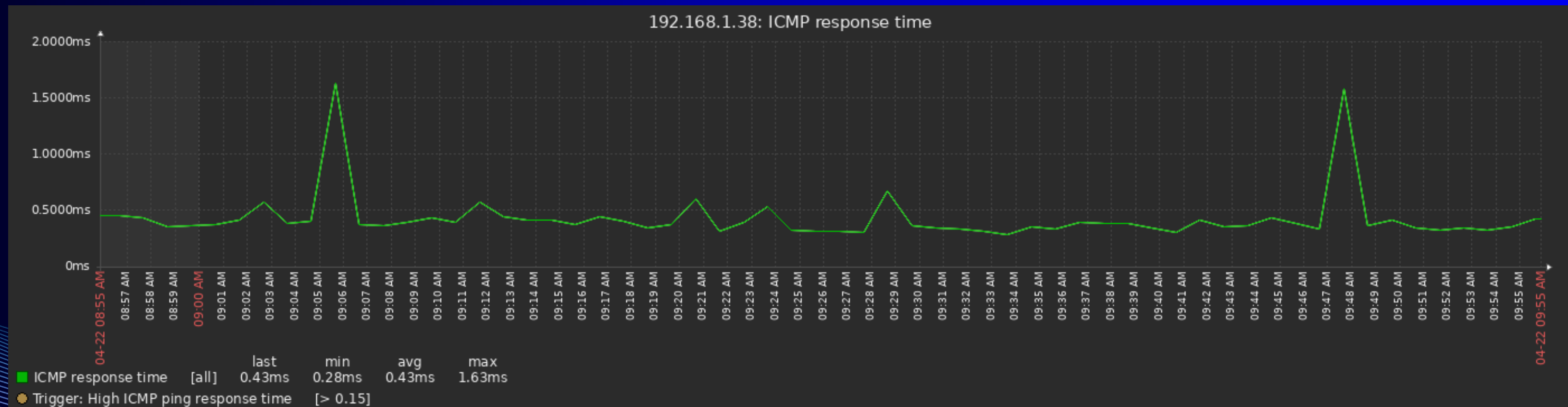
# ...przejdź bezpośrednio do dashboardów Zabbix

Zabbix Inventory  Filtering: Global Local

 assetDevices IP address = 192.168.1.38 + × ⌂ 🔍

📊 6/6 🔍

IP address	Zabbix Status	Zabbix Group	Zabbix Notes	Zabbix ICMP URL	Zabbix Graph URL
192.168.1.38	Enabled	Databases	SQL Server	http://192.168.1.46:8080/history.php?acti...	No Other Items



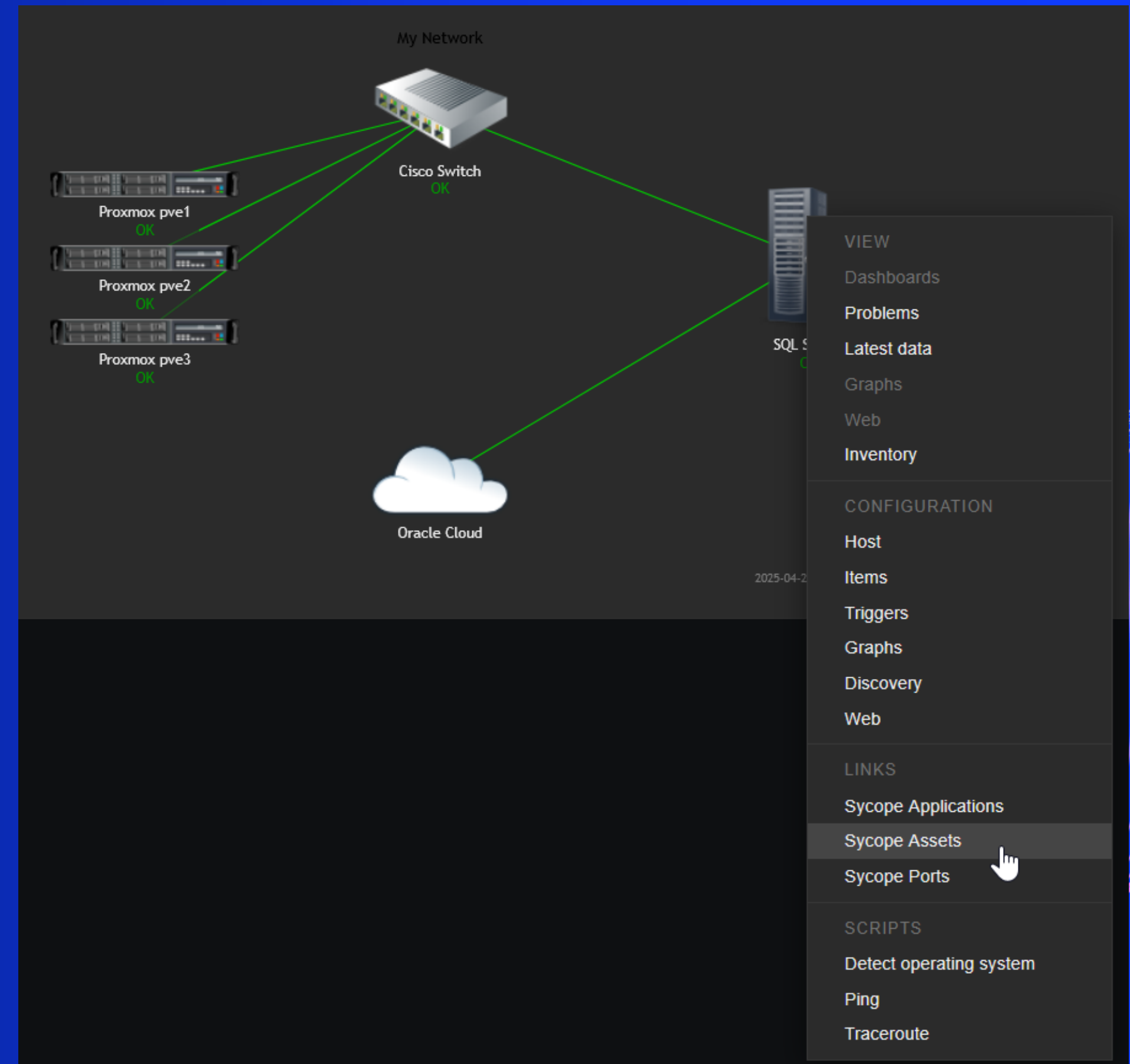
# Możliwość umieszczenia czegokolwiek na Mapie

Dodaj adresy URL Sycopu do dowolnych wbudowanych lub niestandardowych dashboardów (+definiuj automatyczny filtr dla adresu IP lub innej wartości)

- Wiele hiperłączy do każdego modułu Sycopu

Używaj Szablonów Zabbix do prezentacji (etykiety z makrami):

- Licznik alertów
- Serwery z dostępem do Internetu
  - Publiczne połączenia „od” i „do” Hosta
- Liczba połączeń, sesji
- Otwarte porty





Host	Name ▲	Last check	Last value	Change	Tags	Info
192.168.1.50	Asset Discovery - Active Services (count)	4m 58s	7		component: asset_di...	Graph
192.168.1.50	Asset Discovery - Active Services (port list)	4m 57s	22 (not defined), 23 (...)		component: asset_di...	History
192.168.1.50	Asset Discovery - Matched Client Private IPs	4m 39s	1		22 (not defined), 23 (not defined), 80 (not defined), 443 (not defined), 2055 (NETFLOW), 2055 (not defined), 10050 (not defined)	
192.168.1.50	Asset Discovery - Matched Client Public IPs	4m 38s	0		component: asset_di...	Graph
192.168.1.50	Asset Discovery - Matched Server Private IPs	4m 37s	1		component: asset_di...	Graph
192.168.1.50	Asset Discovery - Matched Server Public IPs	4m 36s	0		component: asset_di...	Graph
192.168.1.50	Asset Discovery - Private Connections From Node	4m 43s	12		component: asset_di...	Graph
192.168.1.50	Asset Discovery - Private Connections To Node	4m 43s	5	-1	component: asset_di...	Graph
192.168.1.50	Asset Discovery - Public Connections From Node	4m 41s	102	-1	component: asset_di...	Graph
192.168.1.50	Asset Discovery - Public Connections To Node	4m 41s	0		component: asset_di...	Graph
192.168.1.50	Asset Discovery - Unmatched Client Private IPs	4m 34s	5		component: asset_di...	Graph
192.168.1.50	Asset Discovery - Unmatched Client Public IPs	4m 33s	0		component: asset_di...	Graph
192.168.1.50	Asset Discovery - Unmatched Server Private IPs	4m 33s	1		component: asset_di...	Graph
192.168.1.50	Asset Discovery - Unmatched Server Public IPs	4m 32s	0		component: asset_di...	Graph
192.168.1.50	Performance - High Client Network Latency	4m 56s	0		component: performa...	Graph
192.168.1.50	Performance - High Client Network Latency (detail)	4m 50s	Total: 0, Acknowledge...		component: performa...	History
192.168.1.50	Performance - High Server Network Latency	4m 55s	0		component: performa...	Graph
192.168.1.50	Performance - High Server Network Latency (detail)	4m 48s	Total: 0, Acknowledge...		component: performa...	History
192.168.1.50	Security - Horizontal Scan	4m 53s	0		component: security	Graph
192.168.1.50	Security - Horizontal Scan (detail)	4m 48s	Total: 0, Acknowledge...		component: security	History
192.168.1.50	Security - Vertical Scan	4m 51s	0		component: security	Graph
192.168.1.50	Security - Vertical Scan (detail)	4m 45s	Total: 0, Acknowledge...		component: security	History
192.168.1.50	Visibility - Initial connections from Public IPs	4m 53s	0		component: visibility	Graph
192.168.1.50	Visibility - Initial connections from Public IPs (detail)	4m 47s	Total: 0, Acknowledge...		component: visibility	History
192.168.1.50	Visibility - Only SYN Client TCP Flag	4m 51s	8	+2	component: visibility	Graph
192.168.1.50	Visibility - Only SYN Client TCP Flag (detail)	4m 45s	Total: 8, Acknowledge...		component: visibility	History



### SYN TCP Flag

8.00

Visibility - Only SYN Client ...

### Public Init Conns

0.00

Visibility - Initial connections from Publi...

### Horizontal Scan

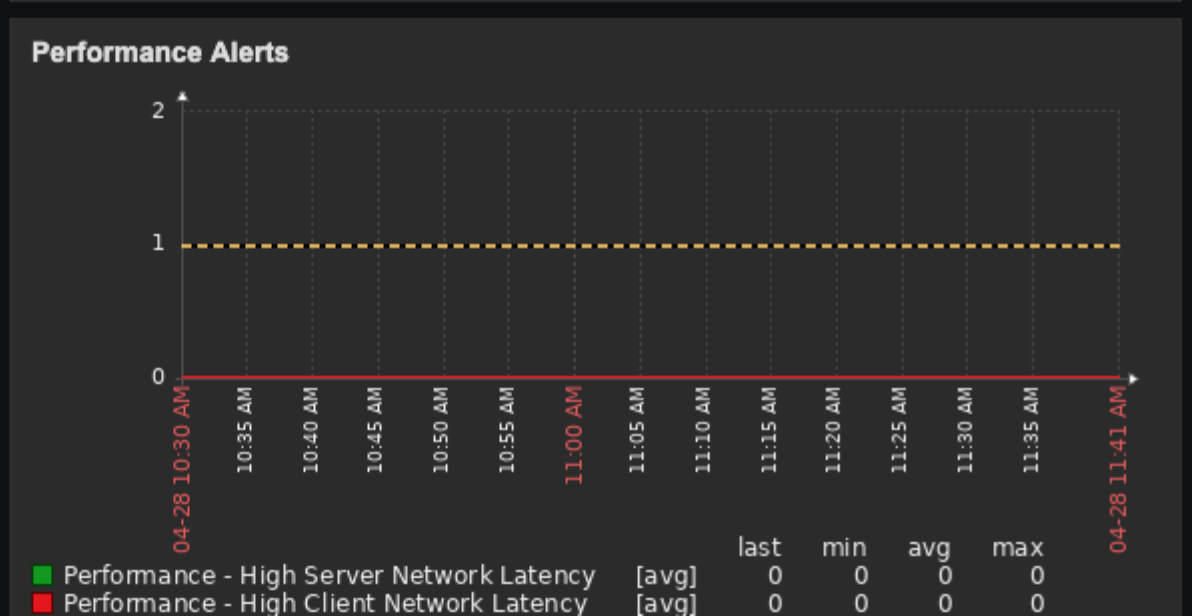
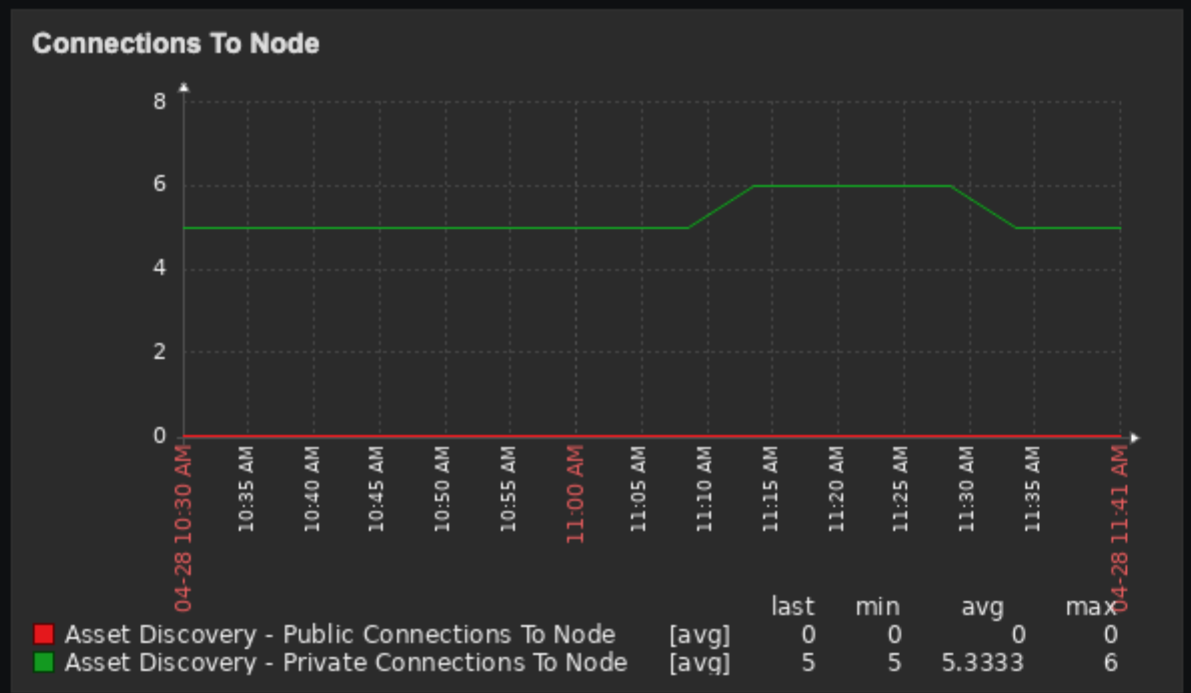
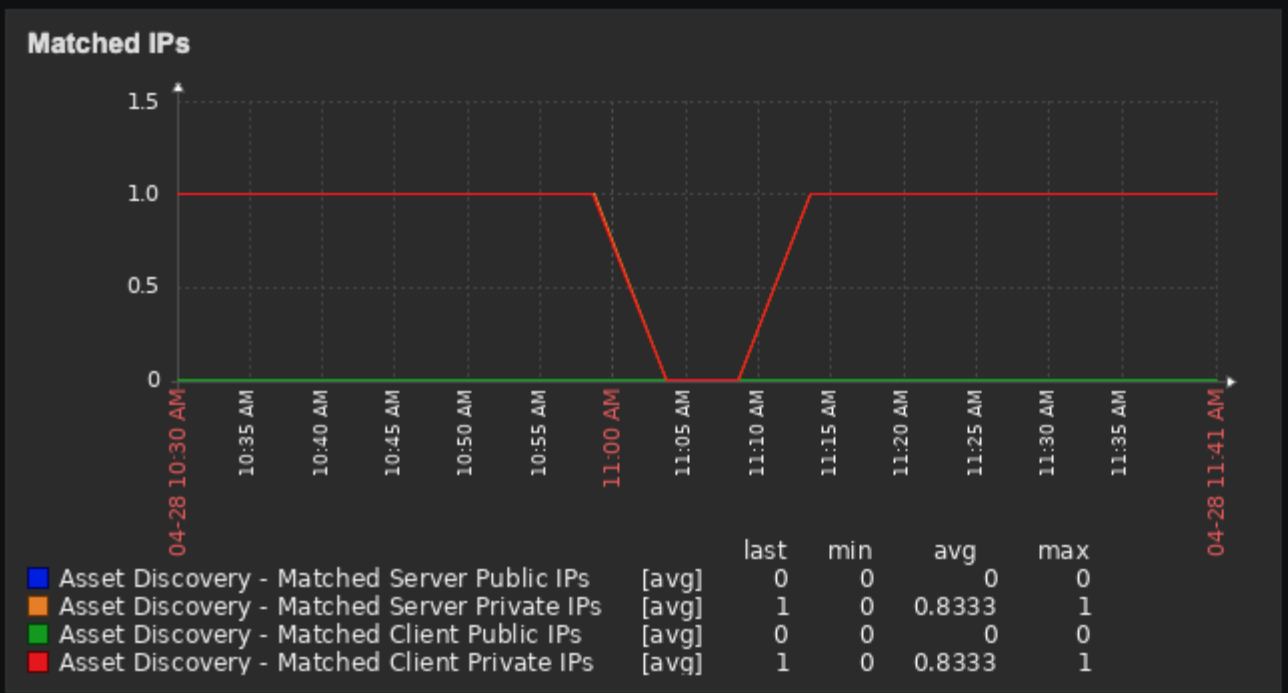
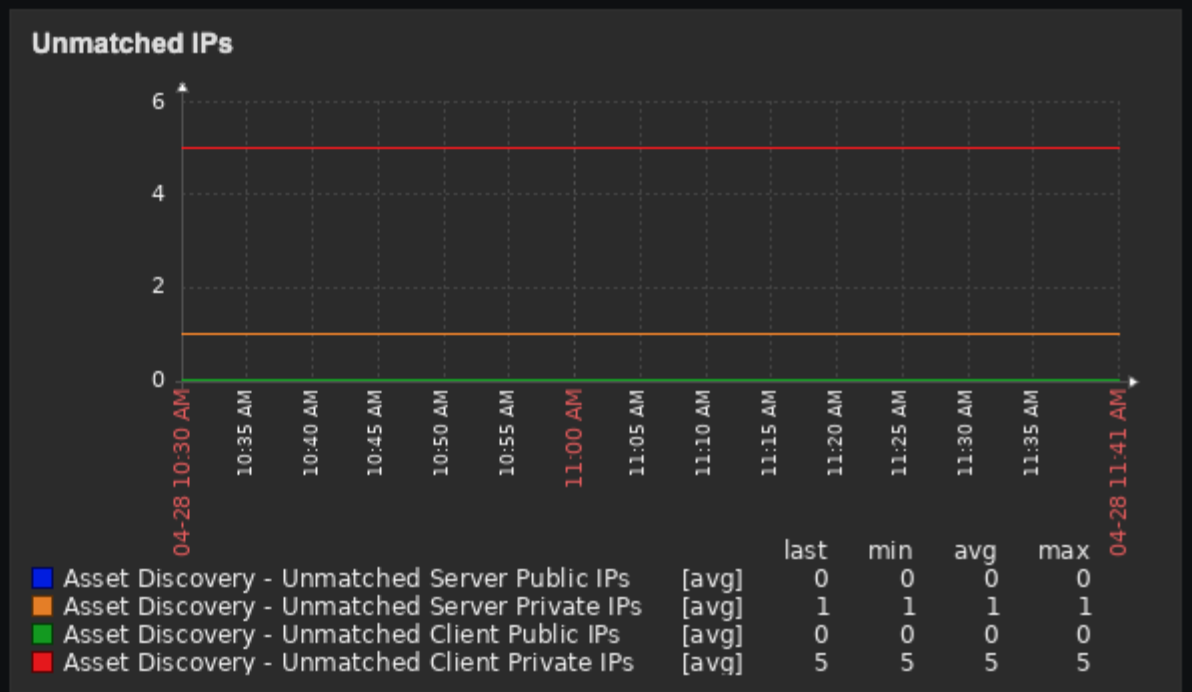
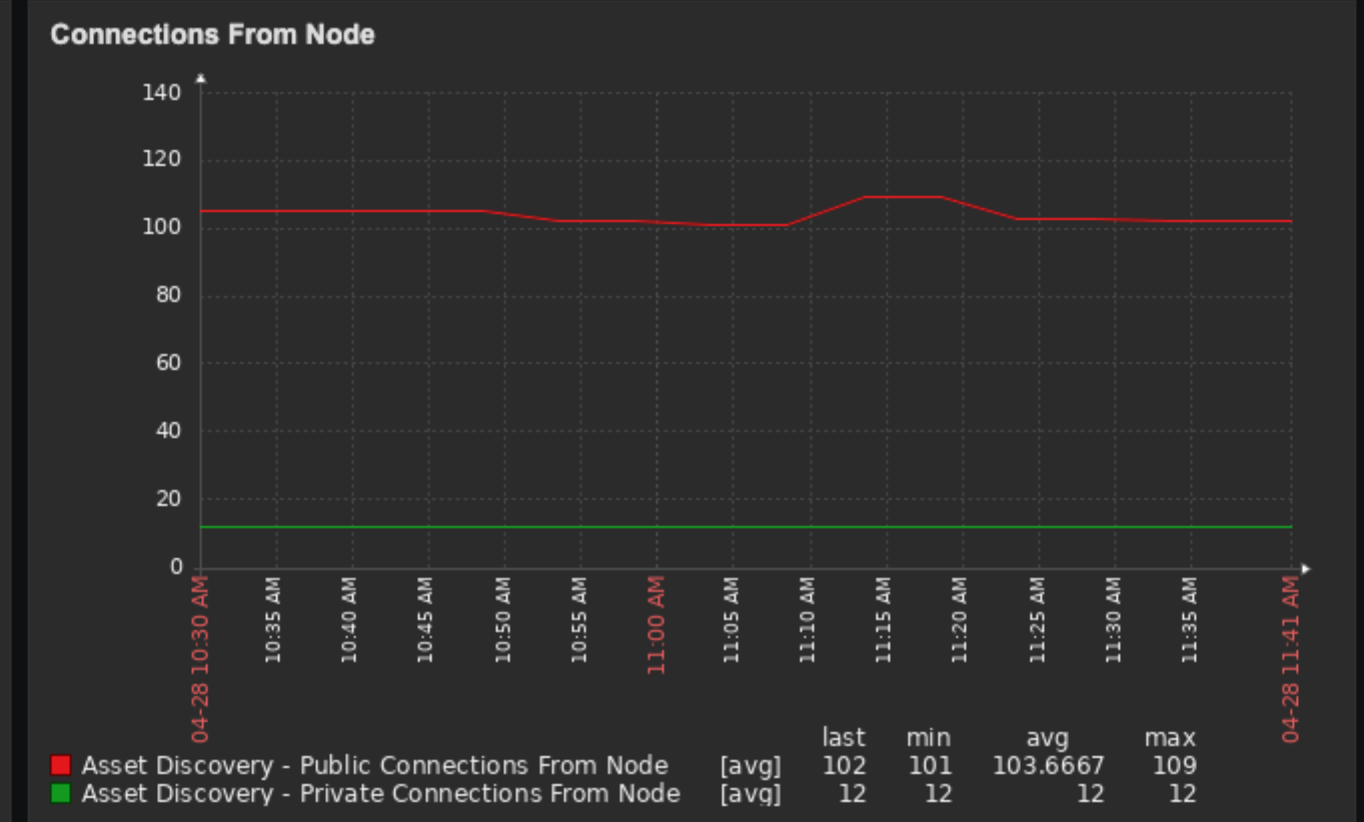
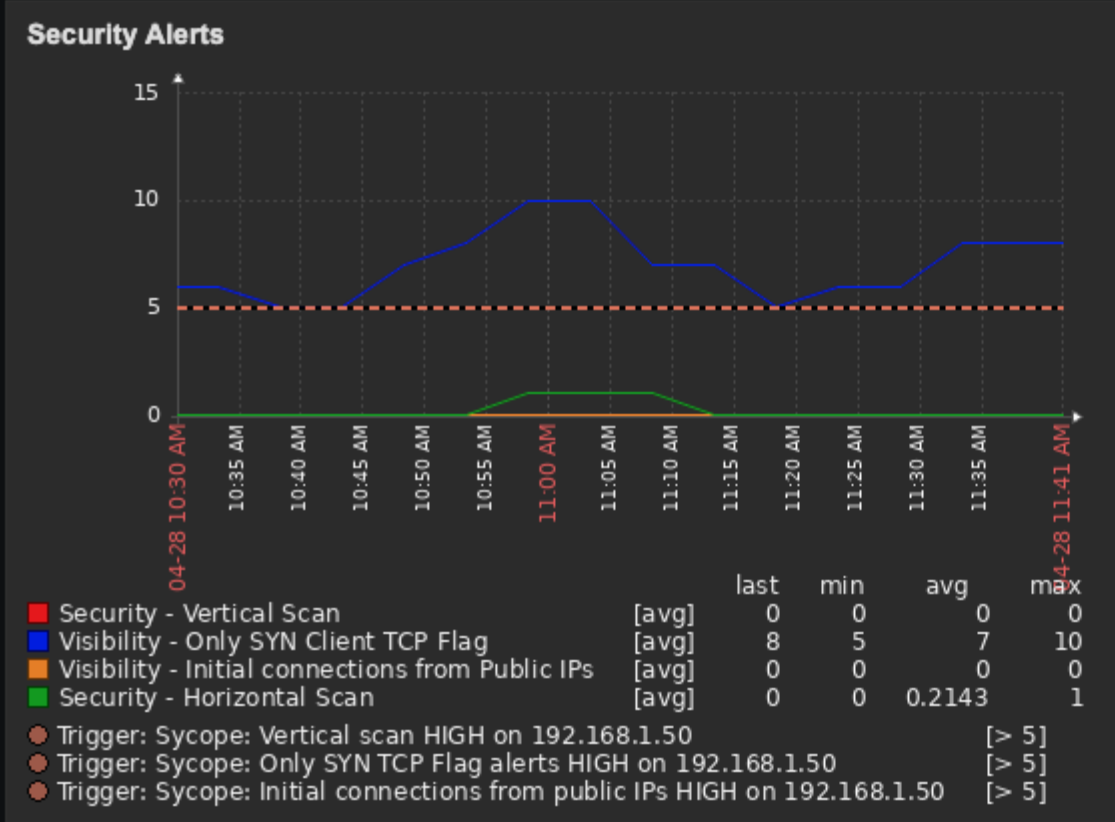
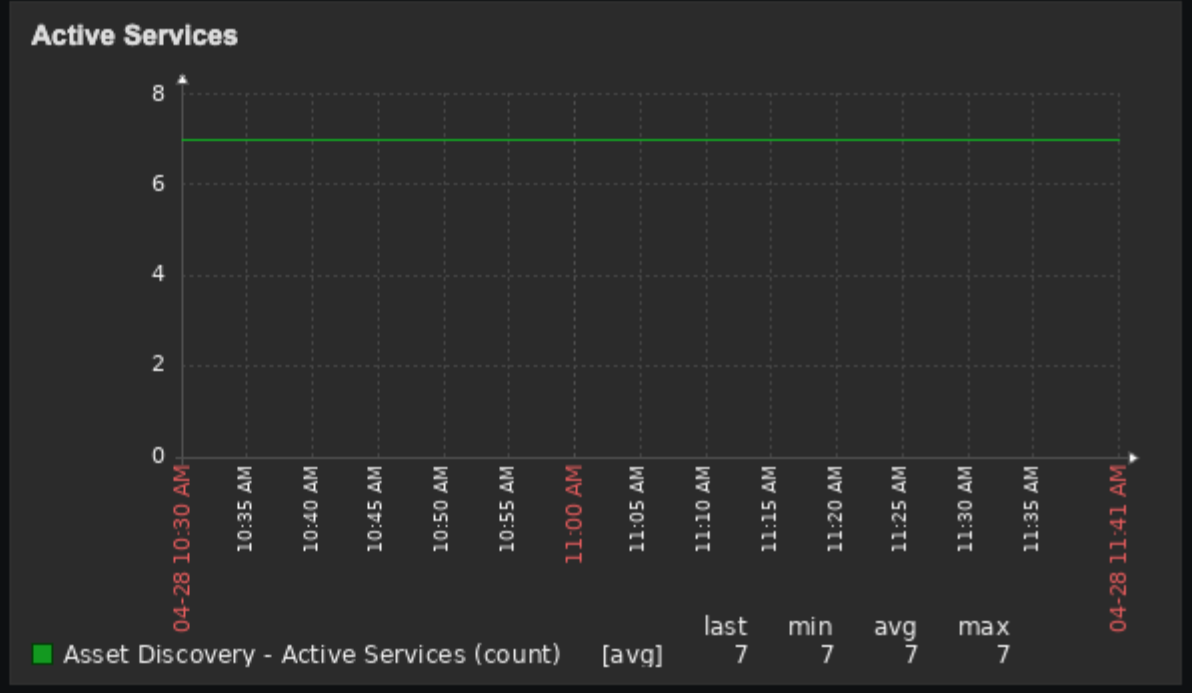
0.00

Security - Horizontal Scan

### Vertical Scan

0.00

Security - Vertical Scan



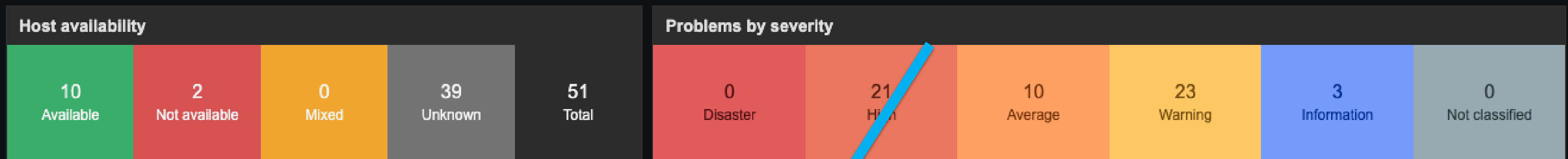


**Co zrobić, gdy coś się  
wydarzy?**

# Co zrobić, gdy coś się wydarzy? (szablon dla Zabbix)

<input type="checkbox"/>	Time ▾	Severity	Recovery time	Status	Info	Host	Problem	Duration	Update	Actions	Tags
<input type="checkbox"/>	11:18:22 AM	Warning		PROBLEM		192.168.1.50	Sycop: Only SYN TCP Flag alerts detected on 192.168.1.50	1m 11s	<a href="#">Update</a>		component: visibility
	11:00										
<input type="checkbox"/>	10:48:22 AM	High	11:18:22 AM	RESOLVED		192.168.1.50	Sycop: Only SYN TCP Flag alerts HIGH on 192.168.1.50	30m	<a href="#">Update</a>		component: visibility

Displaying 2 of 2 found



Time ▾	Info	Host	Problem · Severity	Duration	Update	Actions	Tags
11:23:41 AM		<a href="#">Samsung.localdomain</a>	<a href="#">Sycop: Only SYN TCP Flag alerts detected on Samsung.localdomain</a>	3m 53s	<a href="#">Update</a>		component: visibility
11:23:23 AM		<a href="#">192.168.1.50</a>	<a href="#">Sycop: Only SYN TCP Flag alerts HIGH on 192.168.1.50</a>	4m 11s	<a href="#">Update</a>		component: visibility
11:23:14 AM		<a href="#">192.168.1.29</a>	<a href="#">Sycop: Horizontal scan HIGH on 192.168.1.29</a>	4m 20s	<a href="#">Update</a>		component: security
11:00							

# Co zrobić, gdy coś się wydarzy? (przykład Slack)

The screenshot shows a Slack interface with a channel named '# alerts'. A message from 'Sycop Webhook' is displayed, titled 'Visibility Alert: Only SYN Client TCP Flag'. The message includes the following details:

- Time: 29.08.25 01:45:00
- Client IP: 192.168.1.80
- Threshold: Major
- Server IP: 142.251.9.27

The message also states: 'This alert was automatically generated by the Sycop monitoring solution.' Below the message, there is a 'View in Sycop' link and a reply from 'marcin.kazmierczak' at 14:36: 'replied to a thread You can assign it to my name, I can handle it today 😊'. The Slack interface includes a sidebar with channel navigation and a bottom message input area.

The screenshot shows the Sycop web interface. At the top, there is a navigation bar with 'Stats', 'alerts', and a search filter for 'Alert Name = Only SYN ...'. Below this is a bar chart showing the count of alerts over time, with the x-axis labeled '28-Aug', '29-Aug', '30-Aug', and '31-Aug'. The y-axis is labeled 'Count' and ranges from 0 to 120. Below the chart is a table with columns for 'Action', 'Time timestamp', 'Alert Name alertName', 'shold Level flagThreshol...', 'Alert Severity alertSeverity', and 'Server IP serverIp'. The table contains several rows of alert data, with the first row highlighted in blue. A blue arrow points from the 'View in Sycop' link in the Slack screenshot to the first row of the table.

Action	Time timestamp	Alert Name alertName	shold Level flagThreshol...	Alert Severity alertSeverity	Server IP serverIp
<input checked="" type="checkbox"/>	2025-08-29 01:45:00	Only SYN Client TCP ...	🔥	MEDIUM	142.251.9.27
<input type="checkbox"/>	2025-08-29 01:45:00	Only SYN Client TCP ...	🔥	MEDIUM	142.250.4.27
<input type="checkbox"/>	2025-08-29 01:45:00	Only SYN Client TCP ...	🔥	MEDIUM	108.177.125.26
<input type="checkbox"/>	2025-08-29 01:40:00	Only SYN Client TCP ...	🔥	MEDIUM	142.250.4.26
<input type="checkbox"/>	2025-08-29 01:40:00	Only SYN Client TCP ...	🔥	MEDIUM	142.251.9.27
<input type="checkbox"/>	2025-08-29 01:40:00	Only SYN Client TCP ...	🔥	MEDIUM	142.251.9.26

On the right side of the Sycop interface, there is a 'Details' panel for the selected alert. It includes a 'Classification' dropdown set to 'True Positive', a 'Status' dropdown set to 'ASSIGNED', and a 'Threshold Level' indicator (🔥). Below these are various fields for the alert, including 'Time', 'Rule Type', 'Alert Name', 'Alert Definition Id', 'Alert Severity', 'Threshold Level', 'Client Service', and 'Server Country Name Full'. An 'Incident Handling' section is also visible at the bottom of the details panel.

# Więcej sposobów integracji

Wysyłanie Syslog lub SNMP Trapów przy użyciu Reguł i wyzwolonych Alertów (Wydajność, Widoczność, Odkrywanie Zasobów, Bezpieczeństwo)

Automatyczne Akcje REST API w Alertach lub ad hoc Drilldown

- Zmiana statusu Hosta między Wyłączony a Włączony
- Tworzenie Okresów Konserwacji dla hostów

Pytaj Sycopę o cokolwiek przez REST API (użyj widgetów jako przykładu)

Niestandardowy Szablon Zabbix – przykład wyniku dla jednego Hosta:

- Bezpieczeństwo – Skanowanie Horyzontalne (alert):
  - Łącznie 10 (wyzwolonych alertów)
  - Potwierdzonych: 1, Fałszywie Pozytywnych: 0
- Aktywne Usługi:
  - 137 (NETBIOS), 445 (SMB), 1433 (SQL), 3389 (RDP)
- Niedopasowane Prywatne IP Klientów: 1
- Publiczne Połączenia Od Węzła: 73
- Publiczne Połączenia Do Węzła: 0

Modyfikuj dowolną zdefiniowaną Podsieć lub pojedyncze IP przez API (Zabbix, DHCP itp.)

Dodawaj odkryte adresy IP przez Sycopę do Zabbix

# Monitoruj swoją sieć w czasie rzeczywistym – za darmo!

- Bez konieczności podawania karty płatniczej
- Gotowe do użycia od razu po instalacji
- Wykrywanie zagrożeń i anomalii
- Do 5 000 flows/s
- Retencja danych ograniczona do 14 dni



<https://free.syclope.com>



**Dziękuję!**