

# Multidisciplinárny pohľad na komplexnú správu heterogénneho sieťového prostredia

Automatizácia konfigurácie, monitorovanie, bezpečnosť a  
umelá inteligencia

# Obsah

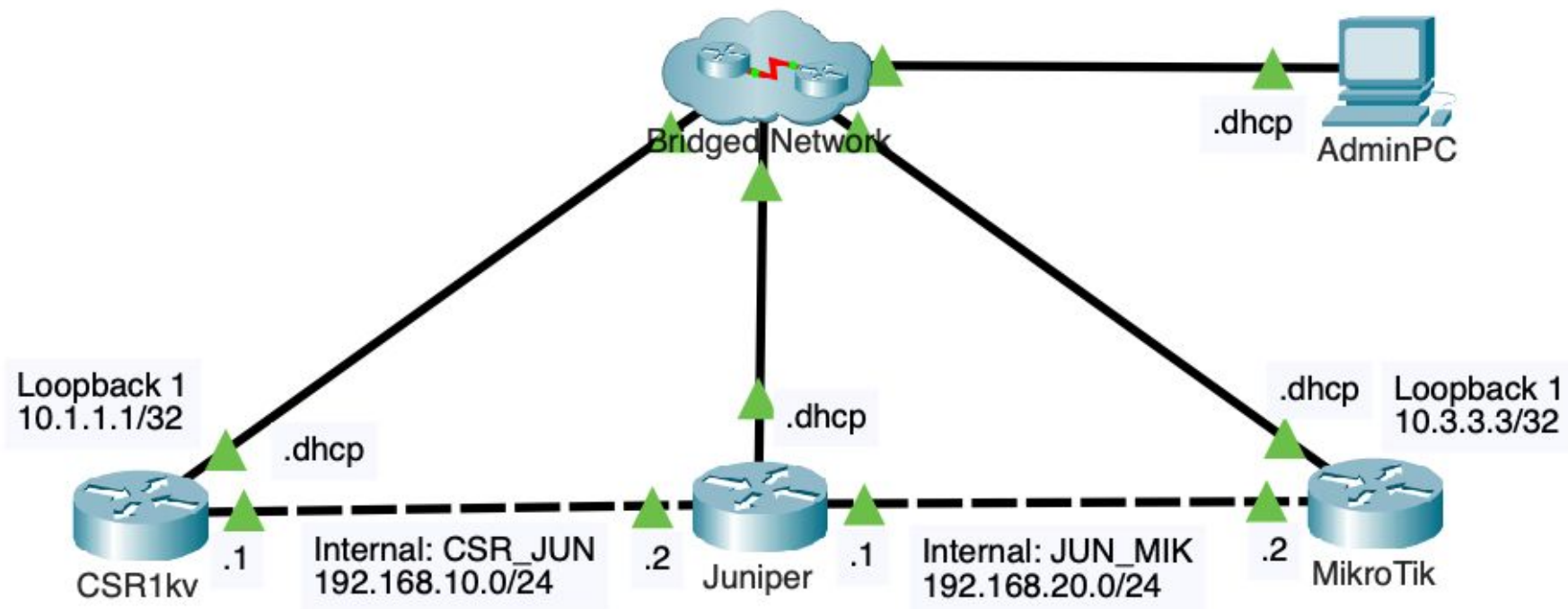
- Jednotná konfigurácia Cisco, Juniper a Mikrotik smerovača
  - CLI (to čo poznáme)
  - Grafické rozhranie (user friendly, no pomalé)
  - Programový prístup (RESTCONF, NETCONF)
  - Automatizácia nástrojmi Ansible a Terraform
- Nasadenie filtrovania sieťovej prevádzky - OPNsense Firewall
- Monitorovanie SIEM nástrojom Splunk
  - Inštalácia
  - Zber dát (Nginx log, Syslog, NetFlow, Snort)
  - Vyhľadávanie a analýza dát
- Testovanie bezpečnosti nástrojmi Nessus, ZAP, SonarQube a Locust
- Analýza zozbieraných dát metódami strojového učenia
  - Klasifikácia = identifikácia udalostí
  - Clustering = detekcia anomálií
  - Reinforcement Learning = automatizácia procesov

# CCNA Update

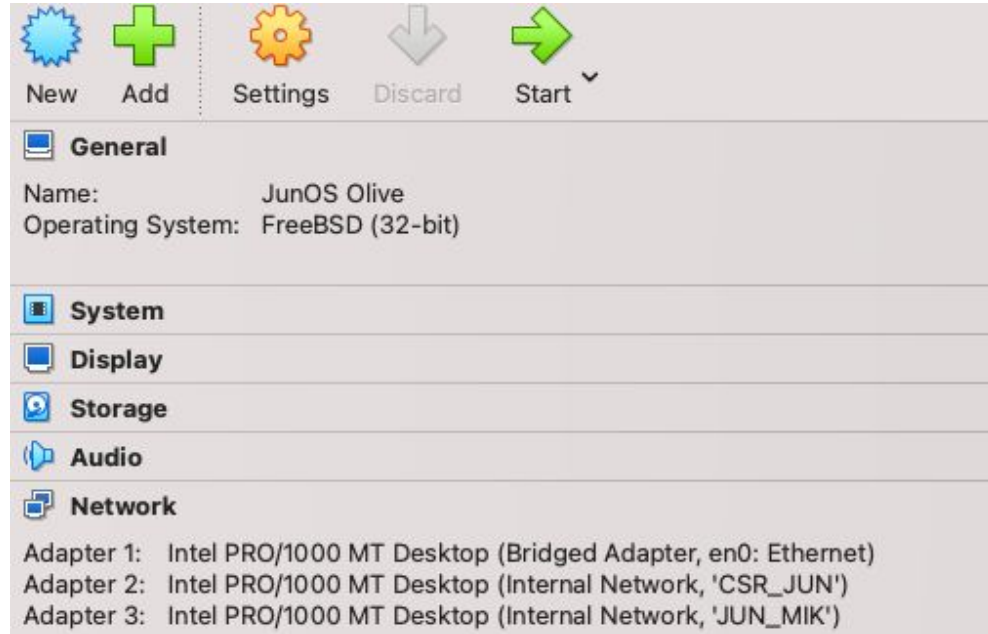
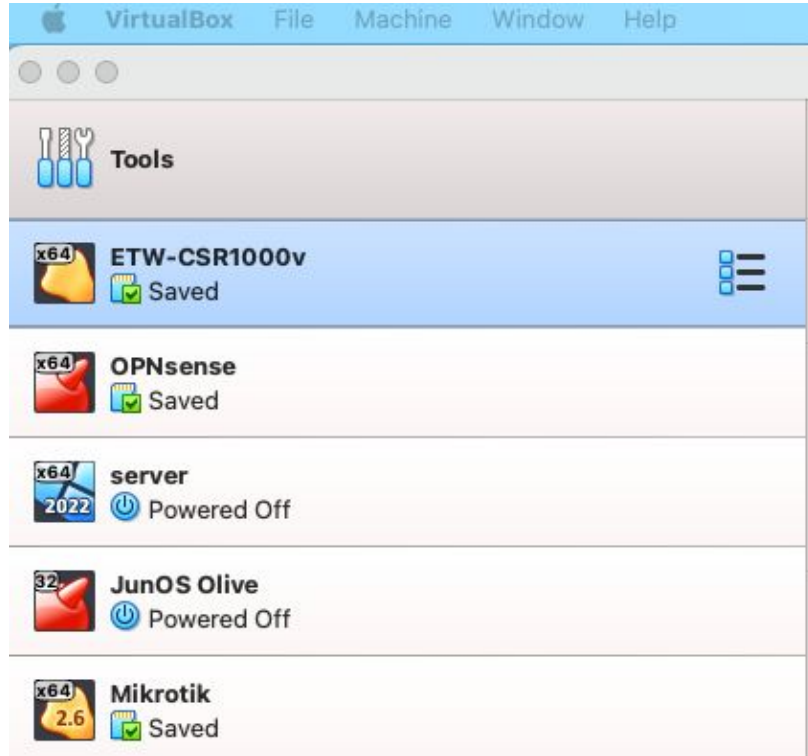
1. Rozšírenie STP obsahu o témy:
  - Root guard, BPDU guard, BPDU filter a Loop guard
2. Ukážka správy sieťového prostredia v cloude (napr. využitím AWS konzoly)
3. Vysvetlenie rozdielu medzi generatívnou a prediktívnou AI
4. Vysvetlenie a praktická ukážka práce so strojovým učením v kontexte počítačových sietí
  - Učenie s učiteľom, učenie bez učiteľa, učenie s posilňovaním a neurónové siete
  - Tvorba a predspracovanie dátovej sady
  - Tvorba, tréovanie a vyhodnotenie modelu strojového učenia
5. Bližší pohľad na REST API a ich možnosti využitia pri správe sieťových zariadení
6. Konfigurácia a správa sieťových zariadení a prostredí využitím nástrojov ANSIBLE a Terraform

Jednotná konfigurácia Cisco, Juniper a Mikrotik  
smerovača

# Topológia



# VBox



# CLI konfigurácia

## # CISCO

```
interface gi1
  ip address dhcp
  no shutdown
interface gi2
  ip add 192.168.10.1 255.255.255.0
  no shutdown
interface loopback 1
  ip add 10.1.1.1 255.255.255.255
```

## # JUNIPER

```
set interfaces em0 unit 0 family inet
address 192.168.2.200/24

set interfaces em1 unit 0 family inet
address 192.168.10.2/24

set interfaces em2 unit 0 family inet
address 192.168.20.1/24
```

## # Mikrotik

```
/ip/dhcp-client/add interface=ether1
disabled=no comment="Bridged Interface
- DHCP"

/ip/address/add
address=192.168.20.2/24
interface=ether2 comment=" JUN_MIK"
/interface/ethernet/set ether2
disable=no

/interface/bridge/add name=Loopback
/ip/address/add address=10.3.3.3/32
interface=Loopback comment="Router
Loopback"
```

# Konfigurácia grafickým rozhraním - Cisco

Cisco CSR1000V 16.6.6

Welcome cisco

Dashboard

Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Troubleshooting

### CPU & Memory Pressure Graph

Last Updated: 6/29/2025, 8:21:51 AM

Slot: RPO

#### CPU Utilization

CPU: 0

Process	CPU (%)
User	1.27
System	4.44
Idle	93.30

#### CPU (%) vs Device Time

Process	14:43	14:43
User	~1.27%	~1.27%
System	~4.44%	~4.44%
Idle	~93.30%	~93.30%

#### Memory Utilization

Memory Details	Size (KB)
Total	3984816
Used	3148280
Free	836536
Committed	4323064

#### Memory Used (%) vs Device Time

14:43 14:43

Healthy Critical (>95%)

### FlashMemory

Last Updated: 6/29/2025, 8:21:51 AM

Category	Percentage
Free	68.44%
Used	31.56%

Free : 5.03(GB)

### Top Applications

Last Updated: 6/29/2025, 8:21:22 AM

Application visibility is not enabled on interface [click here](#) to enable.

### System Information

Last Updated: 6/29/2025, 8:21:22 AM

- Hostname: CSR1kv
- Device Uptime: 4 hours, 16 minutes
- System Time: 14:43:22.221 UTC Thu Jun 26 2025
- Device Type: CSR1000V
- Boot Image: bootflash:packages.conf
- Last Reload Reason: reload
- Last Configuration Change: 14:18:03 UTC Thu Jun 26 2025

# Konfigurácia grafickým rozhraním - Mikrotik

The screenshot displays the Mikrotik WinBox interface for a device named 'mikrotik@192.168.2.9'. The interface is divided into a left sidebar with navigation icons and a main configuration area. The main area is currently showing the 'Bridge' configuration page, with a sub-tab for 'Interface List' selected under the 'Ethernet' category.

**Bridge Configuration Table:**

Name	Actual MTU	L2 MTU	MAC Address	IGMP Snooping	DHCP Snooping	Protocol Mode	Priority	Port Cost Mode	VLAN Filtering
Loopback	1500	65535	72:C0:56:44:68:79	no	no	RSTP	8000	long	no

**Interface List Configuration Table:**

Name	Type	MTU	Actual MTU	L2 MTU	Tx	Rx	Tx Packet	Rx Packet	FP Tx
ether1	Ethernet	1500	1500	0	27.9 kbps	3.7 kbps	3	4	
ether2	Ethernet	1500	1500	0	0 bps	0 bps	0	0	

**System Information:**

- Device: mikrotik\_device
- IP: 192.168.2.9
- Architecture: x86\_64
- OS: CHR innotek GmbH VirtualBox / 7.19.2 (stable)
- CPU: 0%
- Memory: Free/Used/Total: 812.3 MIB / 211.7 MIB / 1024.0 MIB
- Uptime: 00:04:09
- Date: 2025-06-29 06:25:40

# Programový prístup - NETCONF

```
<rpc message-id="103" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get>
    <filter>
      <native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native">
        <hostname>
        </hostname>
      </native>
    </filter>
  </get>
</rpc>
```

```
from ncclient import manager
```

```
netconf_filter= """
<filter> ... </filter>
"""
```

```
m = manager.connect(host="192.168.10.1", port=830, username="cisco",
password="cisco123!", hostkey_verify=False, device_params={"name": "csr"})
```

```
reply = m.get_config(source="running", filter = netconf_filter)
```

# Programový prístup - RESTCONF

The screenshot shows a REST client interface with the following details:

- Method: GET
- URL: https://192.168.2.100:443/restconf/data/native/hostname
- Response Status: 200 OK, 28 ms, 294 B
- Response Body (JSON):

```
{
  "Cisco-IOS-XE-native:hostname": "CSR1kv"
}
```

```
import requests
```

```
headers = {
    'Accept': 'application/yang-data+json', 'Content-Type': 'application/yang-data+json',
    'Authorization': 'Basic Y2lzY286Y2lzY28xMjMh '}
```

```
get_result = requests.request("GET", "https://192.168.2.100:443/restconf/data/native",
    headers=headers, data={}, verify=False)
json_data = get_result.json()
```

# Automatizácia nástrojmi **Ansible** a Terraform = IaaC

```
root@monit-VirtualBox:~/ansible# ansible-playbook -i inventory.ini config_csr.yml

PLAY [Configure CSR1000v device] *****

TASK [Configure interface Loopback11] *****
[WARNING]: To ensure idempotency and correct diff the input configuration lines should be similar to how they
appear if present in the running configuration on device
changed: [csr]

PLAY RECAP *****
csr                : ok=1    changed=1    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
```

inventory.ini

```
[servers]
csr ansible_host=192.168.13.8

[servers:vars]
ansible_become=yes
ansible_become_method=enable
#ansible_become_password=enpass123!
ansible_network_os=ios
ansible_connection=network_cli
ansible_user=nag25csr
ansible_password=Cis_co#123!
```

play.yml

```
---
- name: Configure CSR1000v device
  hosts: servers
  gather_facts: no
  tasks:
    - name: "Configure interface Loopback11"
      ios_config:
        lines:
          - "interface loopback 11"
          - "ip add 10.11.8.8
            255.255.255.255"
```

# Automatizácia nástrojmi Ansible a Terraform = IaaC

## terraform\_providers.tf

```
terraform {
  required_providers {
    iosxe = {
      version = "0.1.1"
      source  = "CiscoDevNet/iosxe"
    }
  }
}

provider "iosxe" {
  host          = "${var.host}"
  device_username =
"${var.username}"
  device_password =
"${var.password}"
  request_timeout = 30
  insecure       = true
}
```

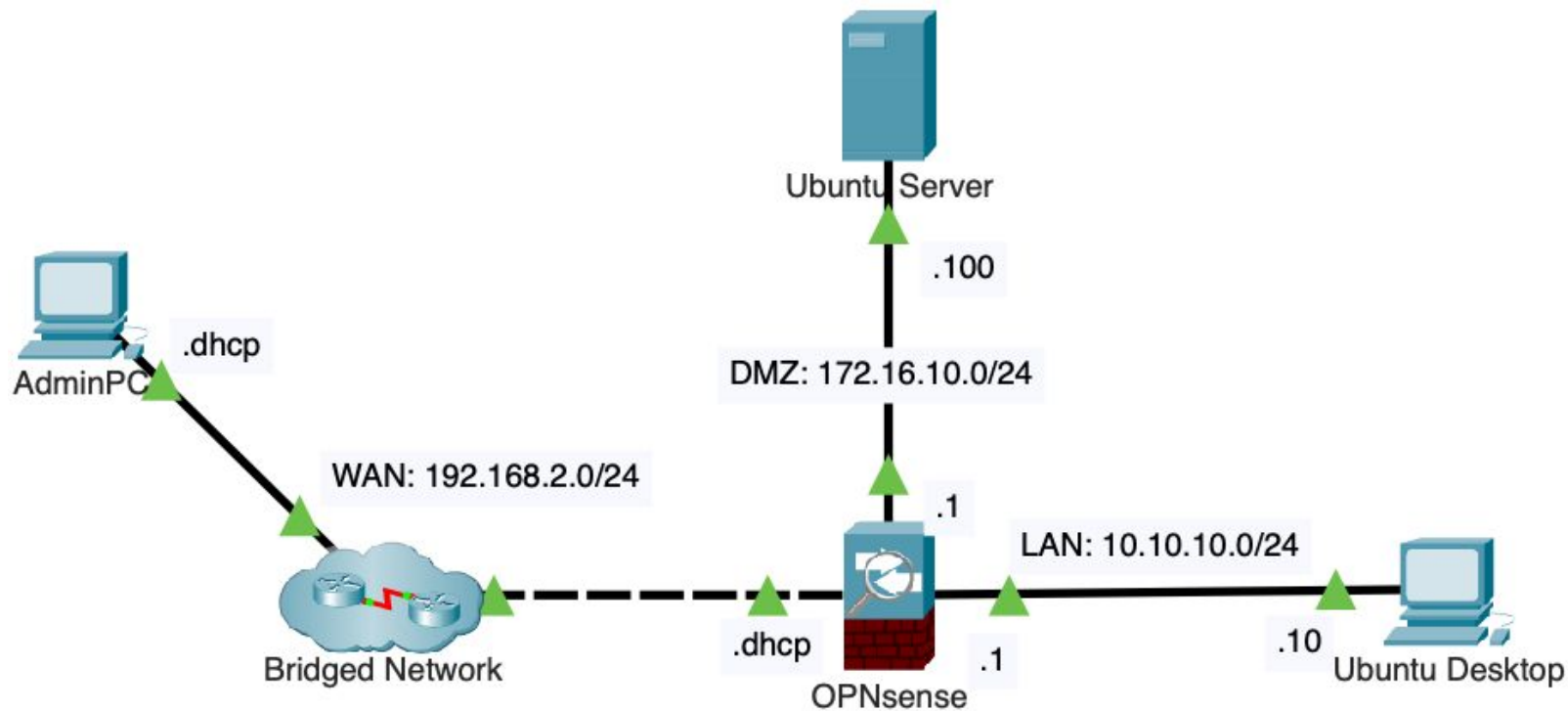
## change-file.tf

```
resource "iosxe_rest" "HOSTNAME_PUT" {
  method = "PUT"
  path   =
"/data/Cisco-IOS-XE-native:native/hostname"
  payload = jsonencode(
    {
      "Cisco-IOS-XE-native:hostname" :
"from_terraform"
    }
  )
}
```

```
terraform init
terraform plan
terraform apply
-auto-approve
```

# Nasadenie filtrovania sieťovej prevádzky - OPNsense Firewall

# Topológia



# Konfigurácia grafickým rozhraním

**OPNsense** Securing networks made easy

root@OPNsense.localdomain

## Lobby: Dashboard

You are currently running in live media mode. A reboot will reset the configuration. SSH remote login is enabled for the users "root" and "installer" using the same password.

### System Information

Name: OPNsense.localdomain

Versions:  
OPNsense 25.1-amd64  
FreeBSD 14.2-RELEASE  
OpenSSL 3.0.15

Updates  
[Click to check for updates.](#)

Uptime: 11:28:35

Load average: 1.24, 0.74, 0.61

Current date/time: Fri Jun 27 16:39:48 UTC 2025

Last configuration change: Fri Jun 27 16:08:16 UTC

### Memory

12.95% (180 / 1393.1 MB)

### Disk

100%

### Interface Statistics

### Firewall

let out anything from fire  
anti-lockout rule

### Services

System Configuration Daemon

Cron

DHCPv4 Server

Users and Groups

Network Time Daemon

### Gateways

- WAN\_DHCP6 (active) undefined
- WAN\_DHCP (active) 192.168.2.1

### Announcements

Re: OPNsense 25.1.9 released

### Traffic Graph

Traffic In

Traffic In (Kb)
100.00
90.00
80.00
70.00
60.00
50.00
40.00
30.00
20.00

# Konfigurovatel'né technológie

- Networking
  - WAN
  - LAN
  - DMZ
- NAT
- Filtrovane sieťovej prevádzky
- VPN
  - Site-to-Site
  - Remote-Access

# Monitorovanie SIEM nástrojom Splunk

# Inštalácia využitím technológie Docker

```
$ docker-compose up -d

# docker-compose.yml
version: "3.9"

services:
  splunk-server:
    image: splunk/splunk:latest container_name: splunk-free environment:
      - SPLUNK_START_ARGS=--accept-license - SPLUNK_PASSWORD=P4ssw0rd123!
      - SPLUNK_HOST=0.0.0.0
    ports:
      - 8000:8000 # GUI
      - 9997:9997/udp # UDP syslog port
      - 514:514/udp # Common UDP syslog port
      - 2055:2055/udp # NetFlow port
      - 8088:8088 #HTTP Event Collector
    volumes:
      - ./splunk_data:/opt/splunk/var/lib/splunk
      - /var/log/nginx/access.log:/opt/splunk/etc/system/local/inputs/nginx_access.log
      - /var/log/nginx/error.log:/opt/splunk/etc/system/local/inputs/nginx_error.log
      - /var/log/auth.log:/opt/splunk/etc/system/local/inputs/auth.log
      - /var/log/snort/snort.alert.fast:/opt/splunk/etc/system/local/inputs/snort.log
```

# Grafické rozhranie

← → ↻ <https://splunk.vnet2.at.cnl.sk/en-US/app/launcher/home> ☆

splunk>enterprise Apps Administrator 5 Messages Settings Activity Help Find

## Apps

Find more apps [Manage](#)

- Search & Reporting
- AT Audit Trail
- Splunk Secure Gateway
- Upgrade Readiness App

## Hello, Administrator

[Home page settings](#)







Bookmarks Dashboard Search history Recently viewed Created by you Shared with you

> My bookmarks (0) [Add bookmark](#)

> Shared with my organization (0) [Add bookmark](#)

▼ Splunk recommended (13)

Common tasks [Show for users](#)

 <b>Add data</b> Add data from a variety of common sources.	 <b>Search your data</b> Turn data into doing with Splunk search.	 <b>Visualize your data</b> Create dashboards that work for your data.
 <b>Manage alerts</b> Manage the alerts that monitor your data.	 <b>Add team members</b> Add your team members to Splunk platform.	 <b>Manage permissions</b> Control who has access with roles.

# Zber dát

- Nginx log
- Syslog
- NetFlow
- Snort

# Syslog dáta

## # Filter:

```
source="udp:514" index="csr_syslog" sourcetype="syslog_router_st" s_id="local_csr:514"
```

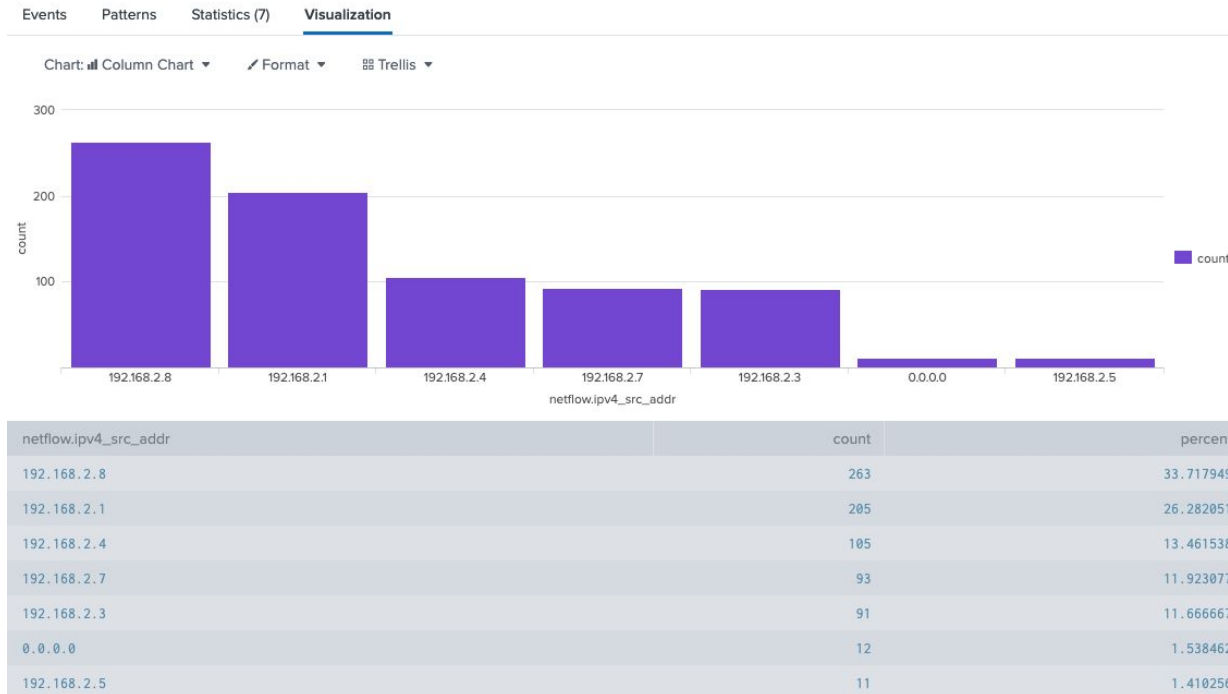
i	Time	Event
>	6/30/25 6:52:19.000 AM	Jun 30 06:52:19 192.168.2.100 158: [syslog@9 s_id="local_csr:514"]: *Jun 26 20:33:27.268: %DMI-5-SYNC_COMPLETE: F0: syncfd: The running configuration has been synchronized to the NETCONF running data store. host = CSR   source = udp:514   sourcetype = syslog_router_st
>	6/30/25 6:52:19.000 AM	Jun 30 06:52:19 192.168.2.100 157: [syslog@9 s_id="local_csr:514"]: *Jun 26 20:33:26.638: %DMI-5-SYNC_START: F0: syncfd: External change to running configuration detected. The running configuration will be synchronized to the NETCONF running data store. host = CSR   source = udp:514   sourcetype = syslog_router_st
>	6/30/25 6:52:17.000 AM	Jun 30 06:52:17 192.168.2.100 156: [syslog@9 s_id="local_csr:514"]: *Jun 26 20:33:25.451: %SYS-5-CONFIG_I: Configured from console by console host = CSR   source = udp:514   sourcetype = syslog_router_st
>	6/30/25 6:52:08.000 AM	Jun 30 06:52:08 192.168.2.100 155: [syslog@9 s_id="local_csr:514"]: *Jun 26 20:33:16.139: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.2.7 port 514 started - CLI initiated host = CSR   source = udp:514   sourcetype = syslog_router_st
>	6/30/25 6:52:07.000 AM	Jun 30 06:52:07 192.168.2.100 154: [syslog@9 s_id="local_csr:514"]: *Jun 26 20:33:15.141: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.2.7 port 0 CLI Request Triggered host = CSR   source = udp:514   sourcetype = syslog_router_st

# NetFlow dáta

i	Time	Event
>	6/30/25 9:11:47.000 AM	<pre>{ [-]   @timestamp: 2025-06-26T22:19:25.000Z   @version: 1   netflow: { [-]     flow_seq_num: 91     flowset_id: 256     in_bytes: 1008     in_pkts: 12     in_src_mac: 44:f0:9e:a8:b5:d1     ipv4_dst_addr: 192.168.2.100     ipv4_src_addr: 192.168.2.8     version: 9   }   netflow_host: 192.168.2.100   tags: [ [+] ] type: netflow }</pre> <p>Show as raw text</p> <p>host = 192.168.2.7:8088   source = http:netflow_collector   sourcetype = httpevent</p>

# Vyhľadávanie a analýza dát


```
index="netflow_index" | top limit=10 netflow.ipv4_src_addr
```




Testovanie bezpečnosti nástrojmi Nessus, ZAP,  
SonarQube a Locust

# Nessus - sken zraniteľnosti

## DISCOVERY




**Host Discovery**  
A simple scan to discover live hosts and open ports.




**Ping-Only Discovery**  
A simple scan to discover live hosts with minimal network traffic.


## VULNERABILITIES




**Basic Network Scan**  
A full system scan suitable for any host.




**Credential Validation**  
Verify that host credential pairs for Windows & Unix successfully authenticate to scan targets.




**Advanced Scan**  
Configure a scan without using any recommendations.




**Advanced Dynamic Scan**  
Configure a dynamic plugin scan without recommendations.




**Malware Scan**  
Scan for malware on Windows and Unix systems.




**Nessus 10.8.0 / 10.8.1 Agent Reset**  
Scan to find, reset, and update Nessus 10.8.0 / 10.8.1 Agents.




**Mobile Device Scan**  
Assess mobile devices via Microsoft Exchange or an MDM.




**Web Application Tests**  
Scan for published and unknown web vulnerabilities using Nessus Scanner.



**Credentialed Patch Audit**  
Authenticate to hosts and enumerate missing updates.



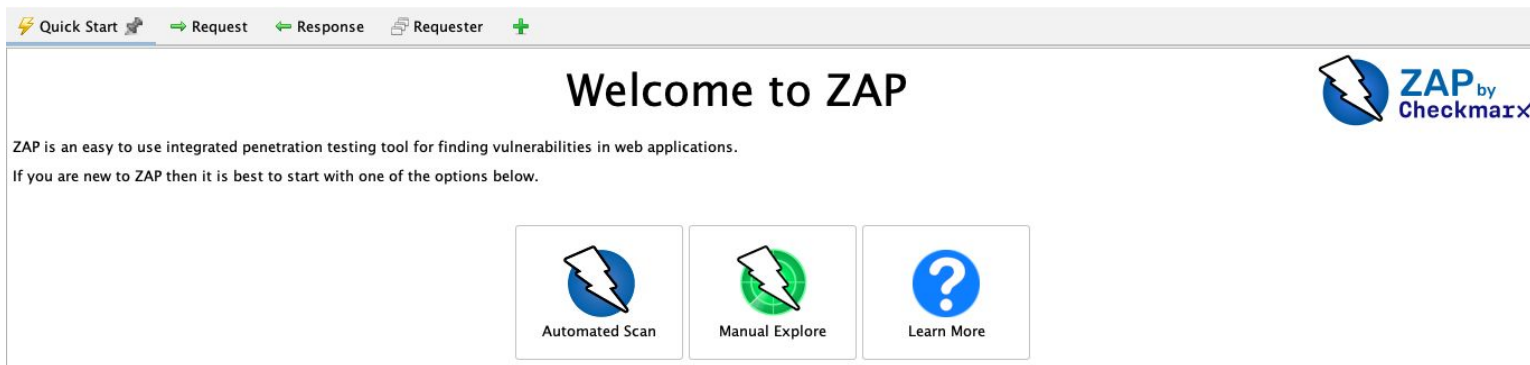
**Active Directory Starter Scan**  
Look for misconfigurations in Active Directory.



**Find AI**  
AI, LLM, ML related detections and vulnerabilities.

<input type="checkbox"/>	Sev	CVSS	VPR	EPSS	Name
<input type="checkbox"/>	MEDIUM	4.3 *			Web Application Potentially Vulnerable to Clickjacking
<input type="checkbox"/>	MIXED	...	...	...	5 HTTP (Multiple Issues)
<input type="checkbox"/>	LOW				Web Server Allows Password Auto-Completion
<input type="checkbox"/>	INFO	...	...	...	2 HTTP (Multiple Issues)

# ZAP - DAST = dynamická analýza aplikácií



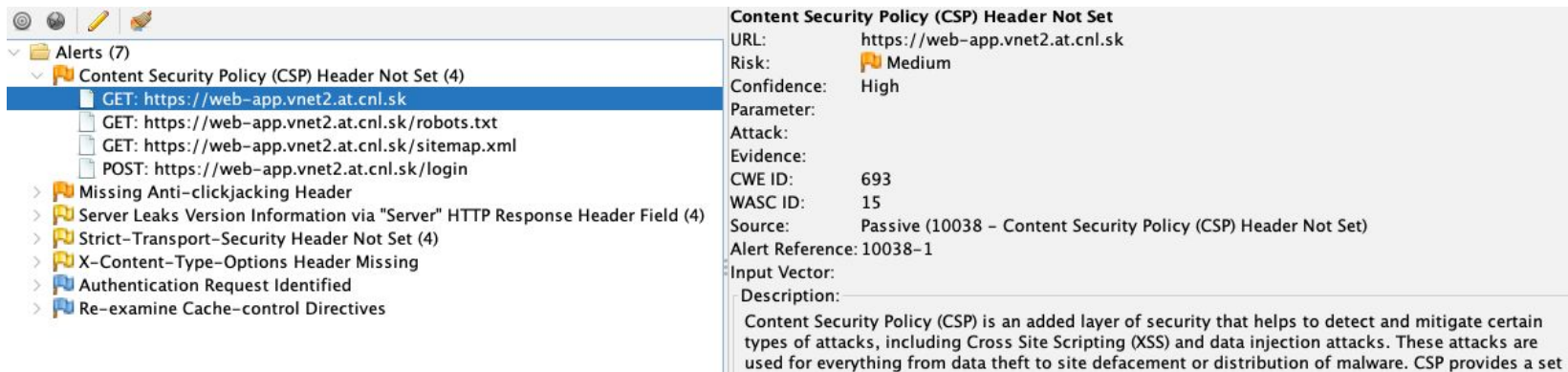
Quick Start → Request ← Response Requester +

## Welcome to ZAP

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.  
If you are new to ZAP then it is best to start with one of the options below.

- Automated Scan
- Manual Explore
- Learn More

**ZAP** by Checkmarx



Alerts (7)

- Content Security Policy (CSP) Header Not Set (4)
  - GET: <https://web-app.vnet2.at.cnl.sk>
  - GET: <https://web-app.vnet2.at.cnl.sk/robots.txt>
  - GET: <https://web-app.vnet2.at.cnl.sk/sitemap.xml>
  - POST: <https://web-app.vnet2.at.cnl.sk/login>
- Missing Anti-clickjacking Header
- Server Leaks Version Information via "Server" HTTP Response Header Field (4)
- Strict-Transport-Security Header Not Set (4)
- X-Content-Type-Options Header Missing
- Authentication Request Identified
- Re-examine Cache-control Directives

### Content Security Policy (CSP) Header Not Set

URL: <https://web-app.vnet2.at.cnl.sk>  
Risk: Medium  
Confidence: High  
Parameter:  
Attack:  
Evidence:  
CWE ID: 693  
WASC ID: 15  
Source: Passive (10038 - Content Security Policy (CSP) Header Not Set)  
Alert Reference: 10038-1  
Input Vector:  
Description:  
Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set

# SonarQube = SAST = statická analýza kódu

```
nano docker-compose.yml
version: "3.8"
```

```
services:
```

```
  sonarqube:
```

```
    image: sonarqube:latest
```

```
    volumes:
```

```
      - ./sonarqube_conf:/opt/sonarqube/conf
```

```
      - ./sonarqube_data:/opt/sonarqube/data
```

```
      - ./sonarqube_extensions:/opt/sonarqube/extensions
```

```
      - ./sonarqube_logs:/opt/sonarqube/logs
```

```
    ports:
```

```
      - "9000:9000"
```

Spustenie skenovania pre daný projekt:

```
docker run --rm -e SONAR_HOST_URL="<ip_add>:9000" -e
SONAR_SCANNER_OPTS="-Dsonar.projectKey=Test-Project" -e
SONAR_TOKEN="sqp_f24ab6a9347f449c727b93480df15c0b07e0b3d9" -v
"/opt/python_project:/usr/src" sonarsource/sonar-scanner-cli
```

# SonarQube

☆ Test-Project PUBLIC

Last analysis: 2 minutes ago • 28 Lines of Code • Python

**D** 2 Security    **A** 0 Reliability    **A** 3 Maintainability    **E** 0.0% Hotspots Reviewed    **0** 0.0% Coverage    **0** 0.0% Duplications

Where is the risk?

What's the risk?

Assess the risk

How can I fix it?

Activity

/main.py



Open in IDE

⌵

36

37

38

39

40

41

42

43

44

45

46

```
put_request = requests.request("PUT", url, headers=headers, data=json.dumps(payload), verify=False)
```


```
print(put_request.status_code)
```

```
if __name__ == '__main__':  
    get_hostname("192.168.2.5")  
    # username = "cisco"  
    # password = "cisco123!"  
    password = "test123!"
```

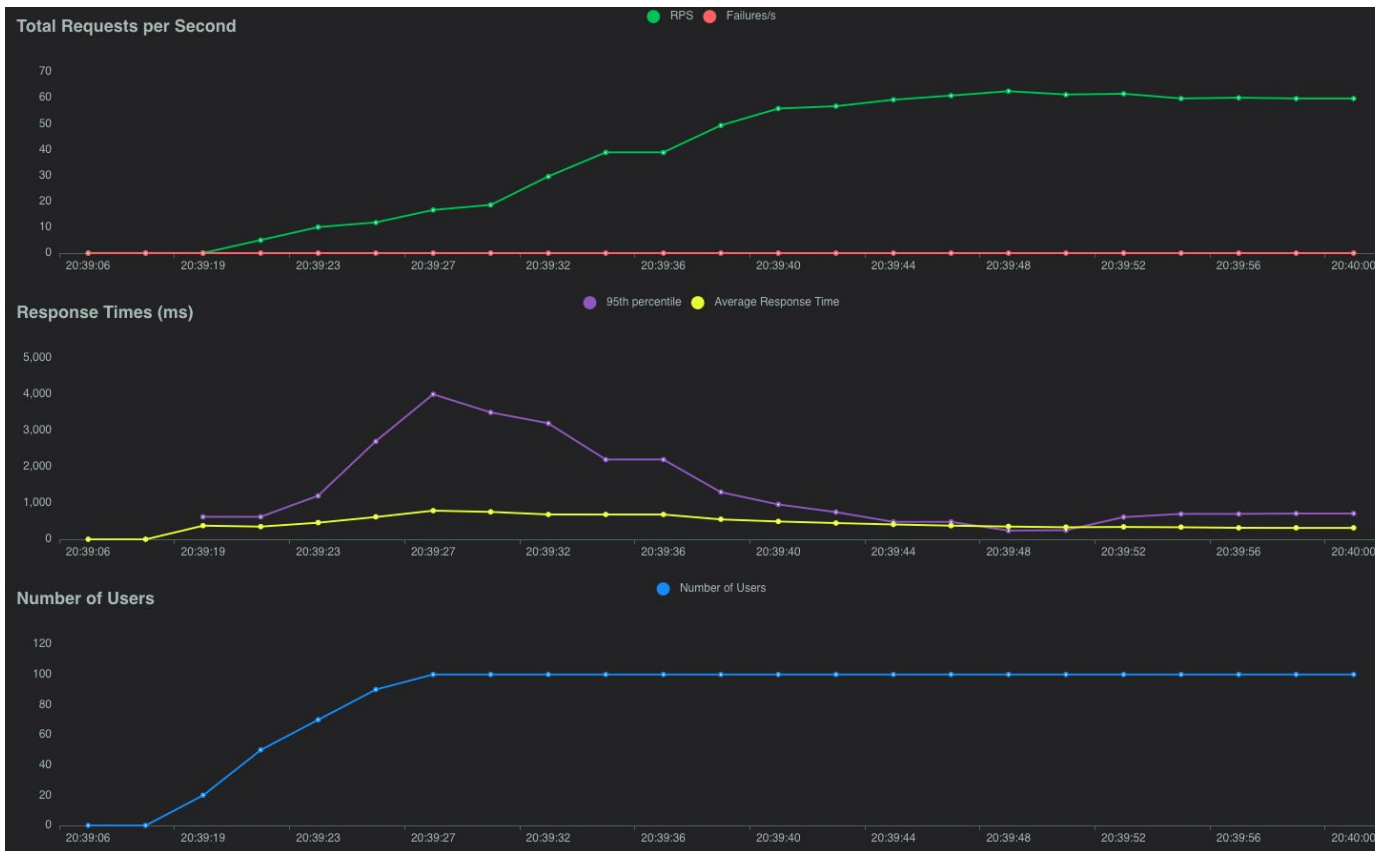
"password" detected here, review this potentially hard-coded credential.

# Locust - výkonnostné testovanie = test dostupnosti

```
locust -f test_app.py
```

 <b>Locust</b>		HOST	STATUS	RPS	FAILURES					
		https://web-app.vnet2.at.cnl.sk	STOPPED	57.3	0%					
<a href="#">STATISTICS</a>		<a href="#">CHARTS</a>	<a href="#">FAILURES</a>	<a href="#">EXCEPTIONS</a>	<a href="#">CURRENT RATIO</a>	<a href="#">DOWNLOAD DATA</a>	<a href="#">LOGS</a>			
Type	Name	# Requests	# Fails	Median (ms)	95%ile (ms)	99%ile (ms)	Average (ms)	Min (ms)	Max (ms)	Average size (bytes)
GET	/	4479	0	160	1200	3000	349.38	16	8606	1542
	Aggregated	4479	0	160	1200	3000	349.38	16	8606	1542

# Locust



Analýza zozbieraných dát metódami strojového učenia

# Dátová sada

```
Source, Destination, Protocol, Length
10.22.22.22, 224.0.0.9, RIPv2, 66
10.22.22.2, 224.0.0.5, OSPF, 94
10.22.22.22, 224.0.0.10, EIGRP, 74
1.1.1.1, 22.22.22.22, ICMP, 114
```

```
# PREDSPRACOVANIE DÁT
```

```
import pandas as pd
data = pd.read_csv('cls.csv')
```

```
X = data.drop('Protocol', axis=1)
y = data['Protocol']
```

```
X_train, X_test, y_train, y_test = train_test_split(X, y,
test_size=0.3, random_state=1)
```

# Klasifikácia = identifikácia udalostí

```
from sklearn.tree import DecisionTreeClassifier
```

```
clf = DecisionTreeClassifier()  
clf.fit(X_train, y_train)
```

```
from sklearn.metrics import accuracy_score  
y_pred = clf.predict(X_test)  
accuracy = accuracy_score(y_test, y_pred)
```

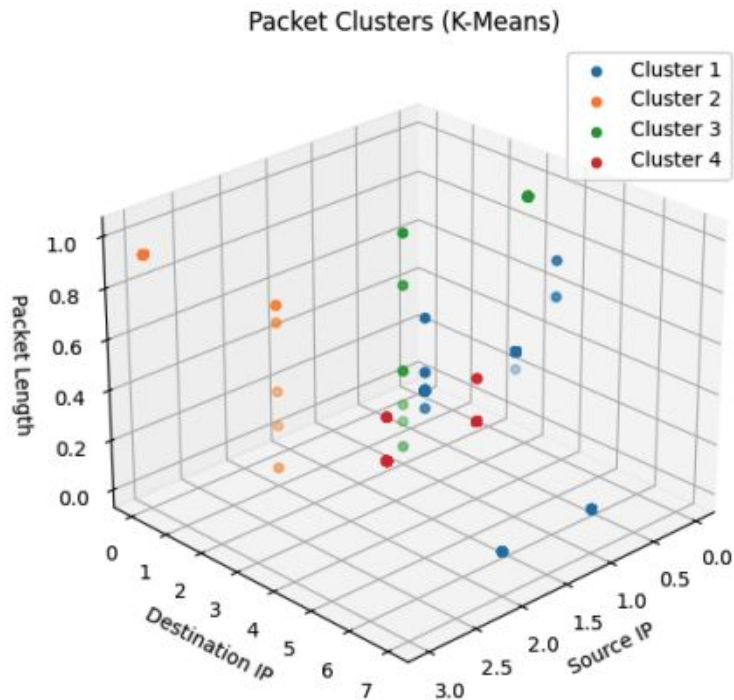
```
new_predict = clf.predict(new_data)
```

# Klastrovanie = detekcia anomálií

```
from sklearn.cluster import KMeans  
kmeans = KMeans(n_clusters = 4)  
kmeans.fit(X)
```

```
X["Cluster"] = kmeans.labels_
```

	Source	Destination	Protocol	...	dst_encode	length_encode	cluster
0	10.22.22.22	224.0.0.9	RIPV2	...	7	0.103448	0
1	10.22.22.2	224.0.0.5	OSPF	...	5	0.586207	0
2	10.22.22.22	224.0.0.10	EIGRP	...	4	0.241379	3
3	10.22.22.2	224.0.0.5	OSPF	...	5	0.517241	0
4	10.22.22.22	224.0.0.5	OSPF	...	5	0.517241	0
..	...	...	...	...	...	...	...
825	10.22.22.2	224.0.0.5	OSPF	...	5	0.586207	0
826	10.22.22.22	224.0.0.9	RIPV2	...	7	0.103448	0
827	10.22.22.22	224.0.0.5	OSPF	...	5	0.586207	0
828	10.22.22.2	224.0.0.10	EIGRP	...	4	0.241379	3
829	10.22.22.22	224.0.0.10	EIGRP	...	4	0.241379	3



# Reinforcement Learning = automatizácia procesov

- Agentové systémy
- Agent vykonáva akcie, na základe ktorých získava odmenu
- Na základe odmeny prispôsobuje svoje správanie tak, aby maximalizoval odmenu v nasledujúcej iterácii

# Knihy a vzdelávacie materiály = netacad.sk

VZDELÁVACIE MATERIÁLY: <https://netacad.sk/category/vzdelavacie-materialy/>

**Správa rozsiahlych sieťových prostredí**

<https://netacad.sk/sprava-rozsiahlych-sietovych-prostredi/>

**IoT – ESP32**

<https://netacad.sk/iot-esp32/>

**Riešenie problémov rozsiahlych infraštruktúr**

<https://netacad.sk/riesenie-problemov-rozsiahlych-infrastruktur/>

**Doplnkový vzdelávací materiál pre vybrané témy z počítačových sietí a kyberbezpečnosti**

<https://netacad.sk/doplnkovy-vzdelavaci-material-pre-vybrane-temy-z-pocitacovych-sieti-a-kyberbezpecnosti/>

**Sieťová programovateľnosť**

<https://netacad.sk/sietova-programovatelnost/>

Ďakujem za pozornosť

[rastislav.petija@cni.sk](mailto:rastislav.petija@cni.sk)