



Seznámení studentů s projektem

B0B32KTI- Komunikační technologie pro IoT

Ing. Bc. Marek Neruda, Ph.D., Ing. Tomáš Straka

Datum: 9 / 2022



1. Seznámení s bezpečnostní sondou SonIoT	3
1.1 Etické hackování	3
2. IDS/IPS a DPI	4
2.1 Další SW nástroje	4
3. Potřebné komponenty	5
4. Způsoby připojení	6
4.1 IDS režim	6
4.2 IPS režim	7
5. Bloky sondy	8
5.1 Lokální řešení	8
5.2 Remote řešení	8
5. Ovládání	9
5.1 Přihlášení k sondě SonIoT	9
5.1.1 Připojení k ssh koncentrátoru a sondě	10
5.1.2 Přístup ke GUI pomocí SSH tunelování webového rozhraní	10
5.2 Změna režimu IDS/IPS	12
5.3 Výstup ze zachycených hrozeb / útoků z logů	12
5.4 Přístup k DPI GUI	13
5.5 Sběr, ukládání a vizualizace IDS/IPS zachycených hrozeb	14
5.6 Přístup k Kibana GUI	14
5.7 Ověření statusu důležitých SonIoT služeb	15
6. Ukázky	16
6.1 Ukázka zachyceného SSH Bruteforce útoku	16
6.1.1 Výstup z příkazu tail -f /var/log/suricata/fast.log	16
6.1.2 Výstup z příkazu tail -f /var/log/suricata/eve.json jq 'select(.event_type=="alert")'	17
6.1.3 Výstup z grafického prostředí Kibana, přesněji z dashboardu "[Filebeat Suricata] Alert Overview"	17
6.1.4 Výstup z grafického prostředí Kibana, přesněji ze sekce "Discover", která obsahuje veškeré logy	18

1. Seznámení s bezpečnostní sondou SonIoT

Bezpečnostní sonda SonIoT obsahuje funkce IPS/IDS zachytávající bezpečnostní hrozby a DPI (Deep Packet Inspection) pro detailní pohled síťové komunikace v LAN. Informační logy jsou uchovávány lokálně, nebo odesílány šifrovaným spojením do vzdáleného serveru umístěného na půdě ČVUT. V rámci sondy je implementováno grafické rozhraní pro monitoring sítě. Sondu lze provozovat v případě potřeby (tj. např. zvýšená citlivost dat) zcela lokálně.

V této laboratorní úloze obdrží studenti vzdálený přístup k sondě SonIoT umístěné v předem připravené univerzitní architektuře v provozním stavu tak, že:

- budou schopni číst logy zachycených hrozeb na sondě
- budou moci využít webové GUI DPI a analyzovat síťový provoz na aplikační vrstvě
- budou schopni přepínat mezi režimy IPS a IDS
- budou schopni využít GUI Kibana pro vizualizaci zachycených hrozeb

Studenti budou mít přístup jako “user” v rámci celé sondy. Uživatel “root” bude zpřístupněn na vyžádání dle předchozí dohody, protože zde vzniká riziko možné změny v konfiguraci, která může způsobit částečnou či úplnou nefunkčnost sondy. Je třeba zvážit každý vlastní konfigurační krok, v opačném případě bude potřeba sondu vrátit do továrního nastavení.

Veškeré zachycené nesrovnalosti, bugy a chybové stavy zjištěné během jednotlivých výukových modulů studenti zaznamenají do předem domluvené tabulky, případně informuje vedoucího cvičení během pravidelných konzultací.

1.1 Etické hackování

Cílem je zlepšení obrany založené na vcítení se do role útočníka při objevování zranitelností.

Studenti mají zakázáno využívat sondu SonIoT a s tím spojené penetrační testování proti vojenských organizacích, tajných službách nebo pro nelegální účely. Veškeré testy by měly probíhat v uzavřeném prostředí a v případě potřeby testování z externích zdrojů jsou testy aplikovány po dohodě s vyučujícím. Studenti berou na vědomí, že síť ČVUT má detekční systémy proti útokům vycházejícím ze školní sítě a svými nedbalými činy by studenti mohli poškodit univerzitu samotnou. Některé testy jsou zakázány mimo LAN síť a lze je povolit pouze po předchozí domluvě se správcí sítě ČVUT.

2. IDS/IPS a DPI

Se systémy pro detekci (Intrusion Detection Systems, zkratka IDS) a systémy pro prevenci (Intrusion Prevention Systems, zkratka IPS) průniku, dále jen IDS a IPS systémy, se často setkáváme ve spojitosti se síťovou bezpečností telekomunikačních sítí a v dnešní době tvoří nedílnou součást komplexní ochrany sítě.

Princip fungování IDS/IPS systémů je založen na monitorování síťového provozu z venkovní sítě, ale také uvnitř LAN sítě a identifikování podezřelých a škodlivých aktivit a jejich záznamu, tj. logování, pro následné vyhodnocení správcem systému. Specifické vlastnosti IDS systémů jsou:

- detekce útoků pocházejících od osob a programů,
- zaznamenávat vzorce útoků pro následné zlepšení detekce,
- generování a zaznamenávání upozornění na incident,
- uchovávání záznamů incidentů pro případné budoucí vyhodnocování.

IPS pak navíc oproti IDS disponuje funkcí částečného, nebo úplného potlačení podezřelé aktivity, např. zahazováním paketů od/pro určité IP adresy. **V našem řešení je využit IDS/IPS open-source nástroj Suricata¹.**

Hlubková kontrola paketů (DPI) je pokročilá metoda zkoumání a správy síťového provozu. Jedná se o formu filtrování paketů, která vyhledává, identifikuje, klasifikuje síťový provoz a na základě získaných dat je možné vyhodnotit např. velikost datového provozu mezi uzly (IP), geolokalizovat zdroje IP adres a do určité míry DPI poskytne i přehled o aplikacích, které komunikují, např. Netflix, Spotify apod. **V našem řešení je využit DPI open-source nástroj ntopng².**

2.1 Další SW nástroje

- Filebeat³ - sběr logů ze souborů a jejich směrování do databáze
- Elasticsearch⁴ - dokumentově orientovaná databáze
- Kibana⁵ - uživatelské rozhraní, které umožňuje vizualizovat data

Filebeat je nástroj z rodiny tzv. Beatů. Jednotlivé druhy beatů představují mechanismy pro sběr různých druhů dat, např. pro sběr logů ze souborů nebo sběr systémových metrik jako je vytížení HW. Dohromady tyto nástroje na sondě tvoří systém, který se stará o čtení logů, jejich směrování do DB a následnou vizualizaci v grafickém prostředí.

¹ <https://suricata.io/>

² <https://www.ntop.org/products/traffic-analysis/ntop/>

³ <https://www.elastic.co/beats/filebeat>

⁴ <https://www.elastic.co/elasticsearch/>





⁵ <https://www.elastic.co/kibana/>

3. Potřebné komponenty

Soubory:

- Excel "nazev.csv" uvedený na Moodle.

Komponenty sondy:

Komponenta	Označení	Počet kusů
UP Squared 	UPS-APLC2F-A20-0432 (2core x 4GB RAM) ⁶	1
Kryt 	EP-CHUPSABSVESA	1
Zdroj 5V@6A 	EP-PS5V6A65WUPS	1
Kabel ke zdroji 	EP-CBPC250V3PEU	1

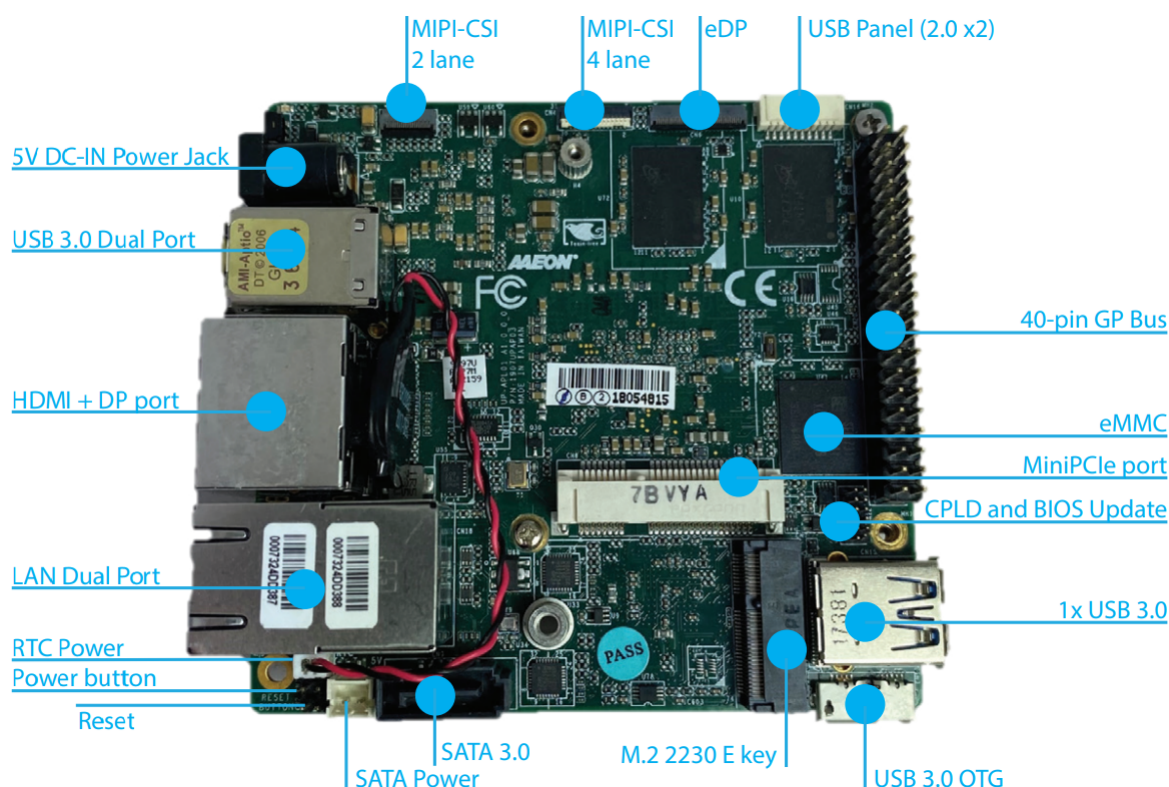
⁶ https://cz.mouser.com/datasheet/2/826/UP_Squared-1889627.pdf

4. Způsoby připojení

Sonda je defaultně v IPS režimu.

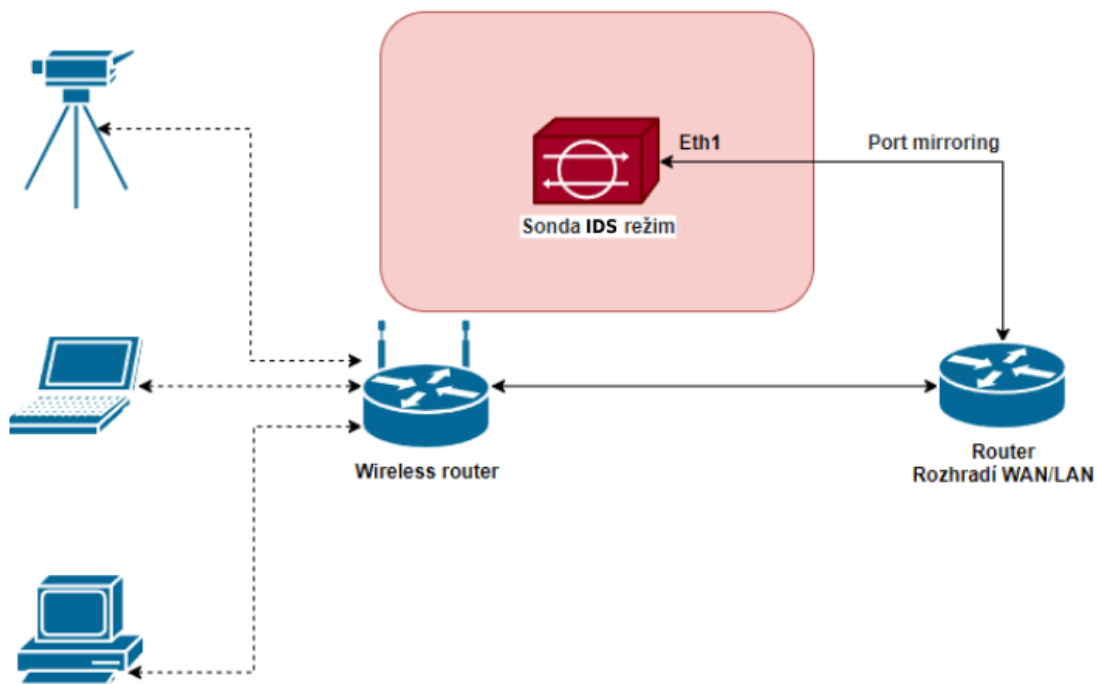
Sondu lze ovládat dvěma způsoby:

1. Lokálně s pomocí připojených periférií:
 - a. Monitor (HDMI nebo DP port)
 - b. Klávesnice a myš (2x USB 3.0)
2. Pomocí SSH přístupu z jiného PC, pokud je připojeno alespoň jedno Eth. připojení do libovolného Eth. portu a sonda obdrží IP z DHCP poolu. Zároveň musí být sonda i PC ve stejném LAN.



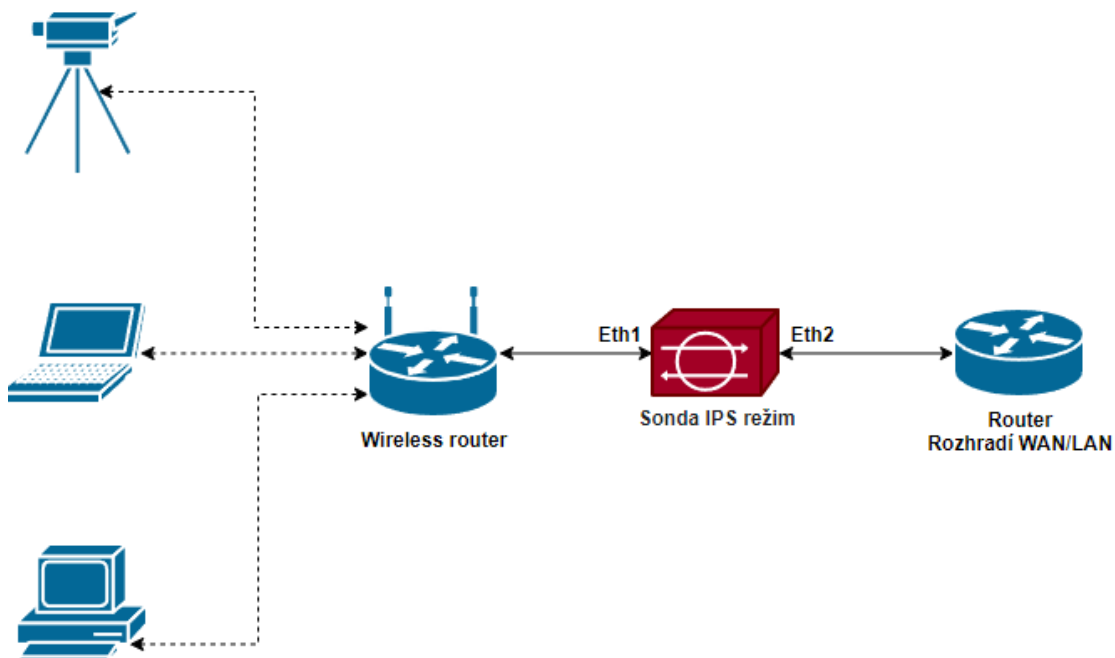
4.1 IDS režim

1. Připojit sondu do LAN sítě podle blokového schématu - zapojit ethernetový kabel do ethernet portu příslušného síťového prvku a do horního ethernet portu sondy.
2. Zapojit sondu do napájecího zdroje.
3. Nutnou podmínkou IDS režimu je možnost zrcadlení portu (Port mirroring) na routeru v dané síti, tj. duplikování síťové komunikace z jednoho portu na port s připojenou sondou. V opačném případě lze na sondě provádět měření přímou komunikací vůči sondě.



4.2 IPS režim

1. Připojit sondu do LAN sítě podle blokového schématu - zapojit 2 ethernetové kabely do ethernet portů příslušných síťových prvků.
2. Zapojit UP Squared do napájecího zdroje.

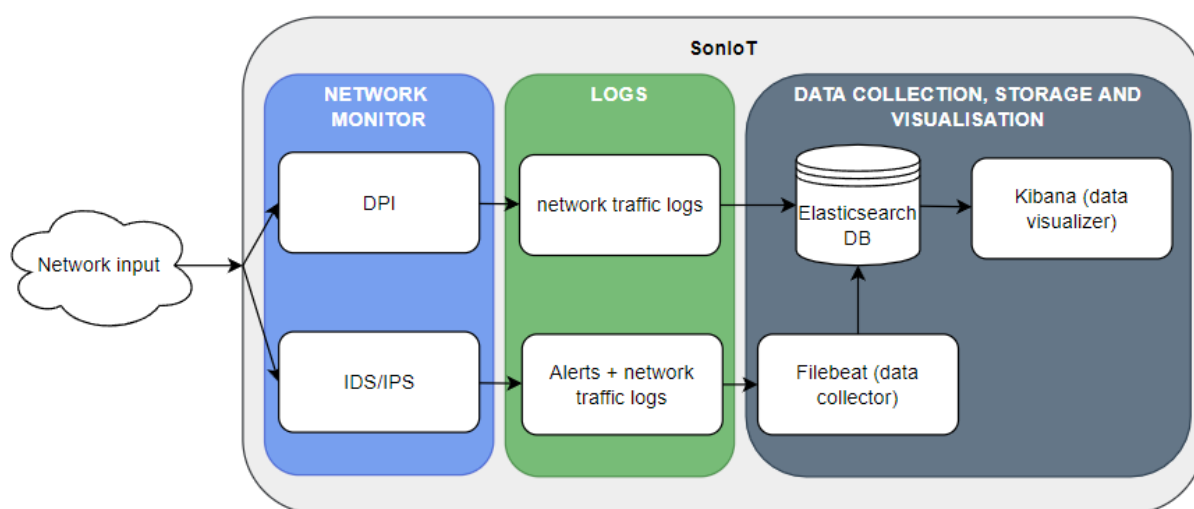


5. Bloky sondy

Sondu SonIoT lze rozdělit na 3 bloky se kterými by se měli studenti seznámit a naučit se s nimi pracovat v průběhu jednotlivých projektů:

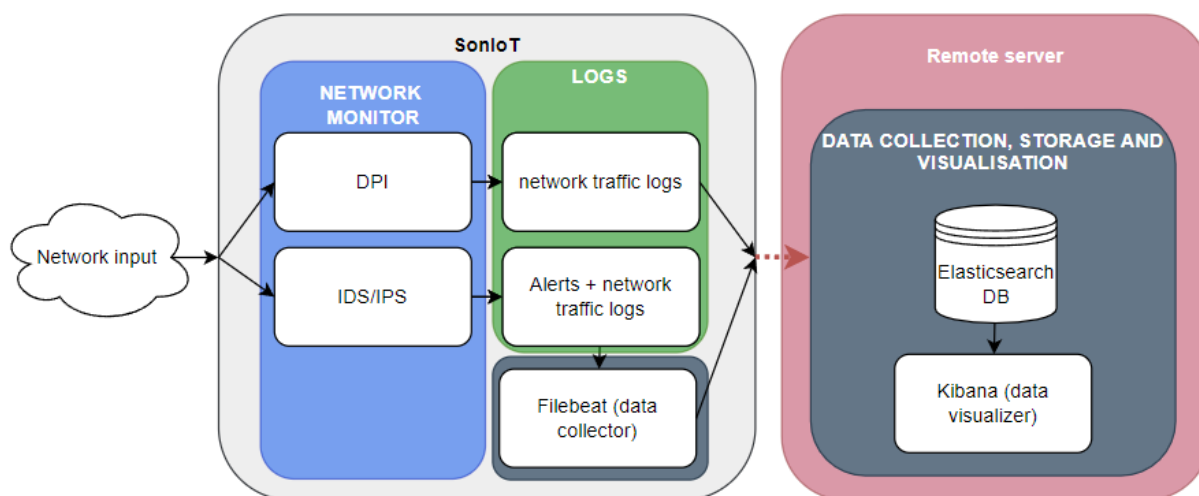
- Network Monitor - zajišťuje logiku, tj. detekce a prevence hrozeb (IDS/IPS) a sběr dalších statistik o síťovém provozu (DPI)
- Logs - ukládání logů z Network Monitoru
- Data Collection, Storage and Visualisation - čtení logů, jejich směrování do DB a vizualizace v grafickém prostředí

5.1 Lokální řešení



5.2 Remote řešení

- Červená šipka - šifrované spojení mezi sondou a vzdáleným serverem pro bezpečnost dat.



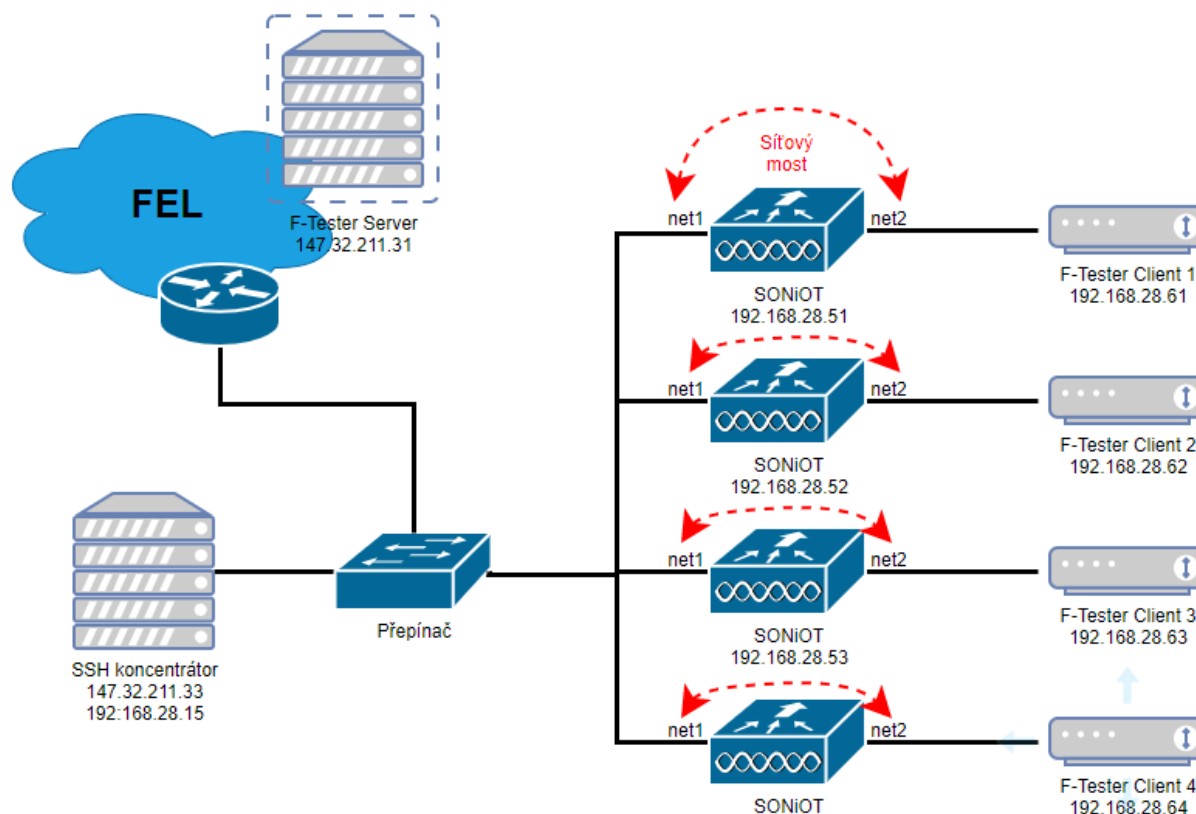
5. Ovládání

Sonda běží na OS Ubuntu, přesněji verzi ubuntu-20.04.5-live-server-amd64 bez značných úprav, proto se lze v rámci sondy pohybovat stejně jako ve standardní distribuci Ubuntu. Studenti mohou využít pro lepší osvojení navigace v OS např. tento Linux Commands Cheat Sheet⁷. **Veškeré přihlašovací údaje studenti obdrží na prvním společném cvičení. Pokud je v příkazech níže uvedeno např. “SonIoT_username”, tak si studenti vyhledají tento parametr v poskytnutých přihlašovacích údajích.**

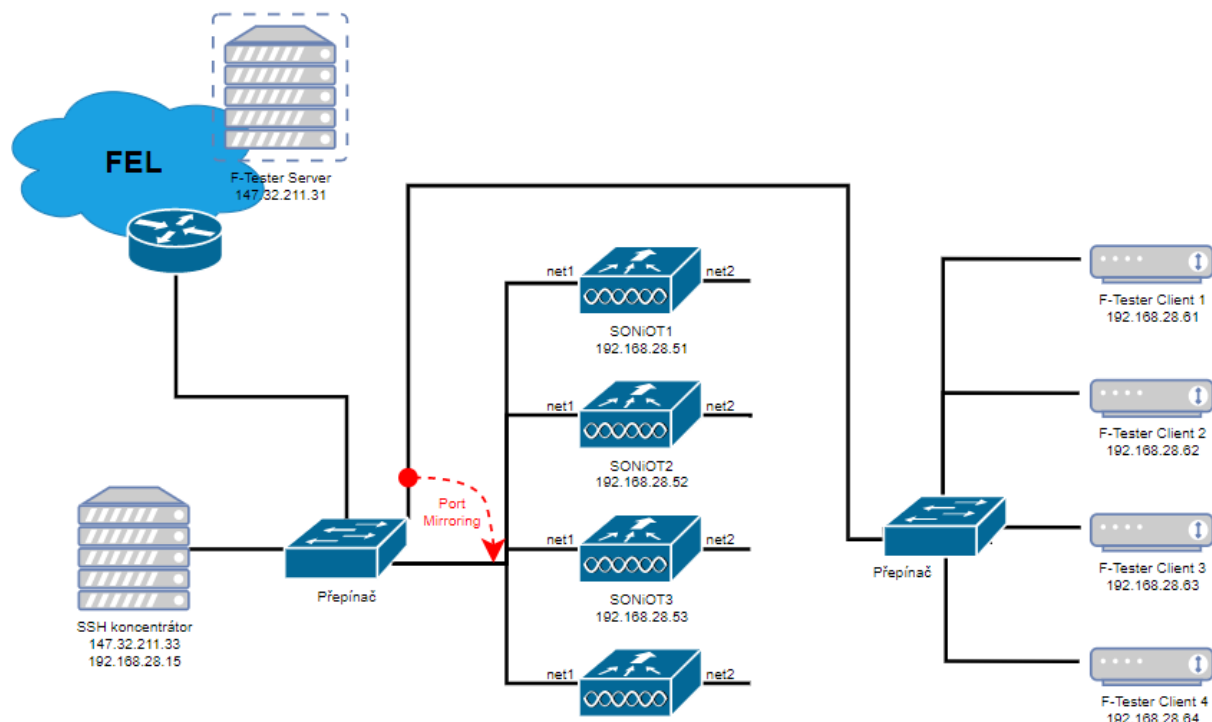
5.1 Přihlášení k sondě SonIoT

Přihlášení k sondě probíhá skrze centralizovaný bod, tzv. ssh koncentrátor dle schématu, viz níže. V rámci zapojení je zajištěna propustnost řešení až 1Gbit/s. Reálné zapojení projektu viz Schémata pro IPS a IDS níže.

IPS



⁷ <https://phoenixnap.com/kb/wp-content/uploads/2022/03/linux-commands-cheat-sheet-pnap.pdf>



5.1.1 Připojení k ssh koncentrátoru a sondě

Aby mohli studenti přistoupit k sondě, musí se nejprve připojit na ssh koncentrátor s přihlašovacími údaji dle týmu

```
ssh -p 6666 team1@147.32.211.28
```

```
ssh -p 6666 team2@147.32.211.28
```

```
ssh -p 6666 team3@147.32.211.28
```

```
ssh -p 6666 team4@147.32.211.28
```

“Heslo je uvedeno v obdržených přihlašovacích údajích”

1. Ve windows spustit příkazovou řádku
2. Zadat ssh příkaz dle vaše týmu, viz výše
`ssh -p 6666 team<cislo_teamu>@147.32.211.28`
3. Zadat heslo <heslo_koncentrátoru>
4. Následně je třeba se připojit k sondě
`ssh user@<soniot_ip>`
5. Zadat heslo <SonIoT_passwd>

5.1.2 Přístup ke GUI pomocí SSH tunelování webového rozhraní

Jelikož není skrze koncentrátor přístup ke grafickému prostředí sondy, lze využít SSH tunelování webového rozhraní, tj. studenti si připojí ke svému lokálnímu portu port ze sondy tak, aby mohli ke GUI přistupovat

1. Ve windows spustit příkazovou řádku
2. Zadat ssh příkaz dle vaše týmu
`ssh -p 6666 -L 8051:<soniot_ip>:<port> team<vasecislo>@147.32.211.28`
3. Zadat heslo koncentrátoru <heslo_koncentrátoru>
4. Nechat ssh session otevřenou

Nyní student ve svém PC může zobrazit danou stránku (port 3000 pro DPI a 5601 pro Kibanu) na lokálním portu 8051, tj. Do prohlížeče zadá 127.0.0.1:8051 a zobrazí se mu GUI dané služby. Toto lze opakovat otevřením dalšího ssh tunelu s možností jiného portu.

Ukázka pro GUI Kibany sondy teamu1 pro localhost na portu 8051:

```
ssh -p 6666 -L 8051:192.168.28.51:5601 team1@147.32.211.28
```

5.1.3 Přístup k F-Tester GUI

Pro měření maximální propustnosti sondy je v řešení implementován nástroj F-Tester⁸ jako fyzický HW mimo sondu, IP = <FlowTester IP>. Defaultně jsou všechny sondy v režimu IPS, tzn. je možné měřit maximální síťovou propustnost sondy. Pro měření IDS je třeba udělat fyzické přepojení na sondě po dohodě s vyučujícím.

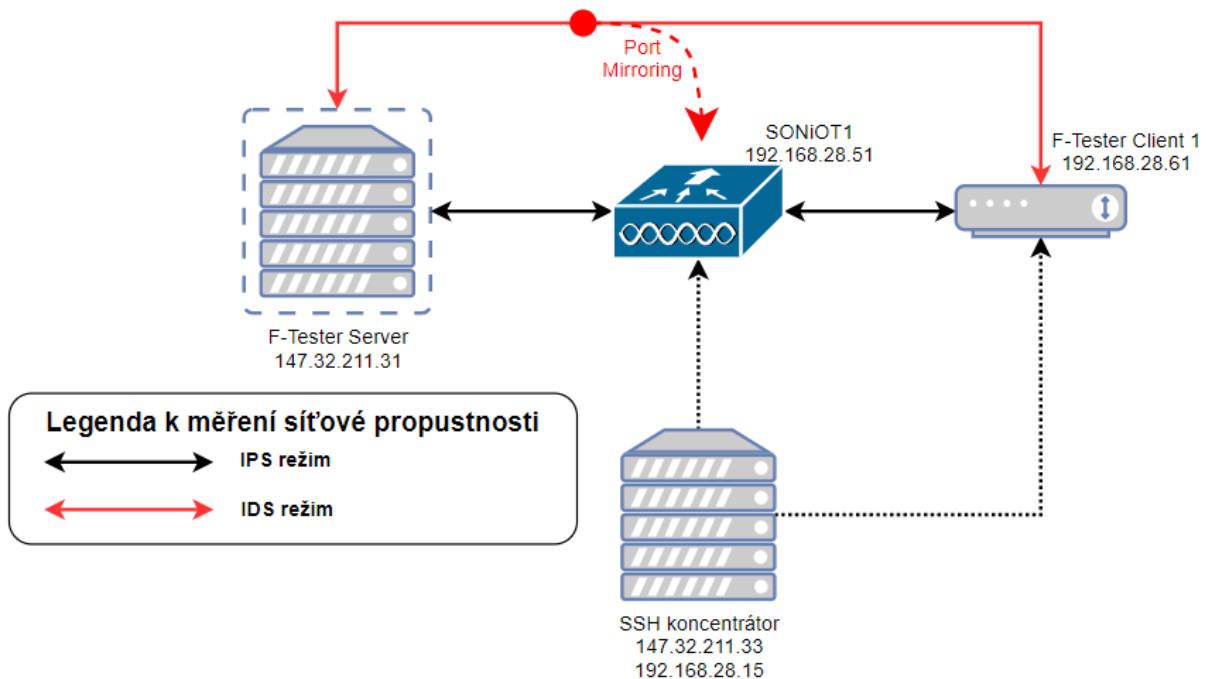
1. Ve windows spustit příkazovou řádku
2. Zadat ssh příkaz dle vaše týmu
`ssh -p 6666 -L 8555:<FlowTester IP>:80 team<vasecislo>@147.32.211.28`
3. Zadat heslo koncentrátoru <heslo_koncentrátoru>
4. Nechat ssh session otevřenou

Nyní student ve svém PC může zobrazit danou stránku F-Testeru na lokálním portu 8555, tj. do prohlížeče zadá 127.0.0.1:8555 a zobrazí se mu GUI dané služby.

Ukázka pro GUI F-Testeru sondy teamu1 pro localhost na portu 8555:

```
ssh -p 6666 -L 8555:192.168.28.61:80 team1@147.32.211.28
```

⁸ <https://f-tester.fel.cvut.cz/>



5.2 Změna režimu IDS/IPS

Po provedení změn je proveden automatický restart.

1. Přepnout se do adresáře `/home/<SonIoT_username>/scripts`
`cd /home/user/scripts`
2. Spustit `mode_of_operation.sh`
`sudo ./mode_of_operation.sh`
3. Uživatel bude vyzván, aby si zvolil IDS (objeví se hláška “Installing IDS mode for enp3s0 and rebooting...”) nebo IPS (objeví se hláška “Installing IPS mode and rebooting...”) režim, poté nastane restart sondy (dojde k odpojení SSH)

```
user@soniot:~/scripts$ sudo ./mode_of_operation.sh
Would you like to change to IDS (1) or IPS (2)? 2
```

Pozn. pokud příkaz požaduje heslo, zadává se heslo přidělené k sondě, tj. `<SonIoT_passwd>`

Boot může trvat až 2 minuty.

5.3 Výstup ze zachycených hrozeb / útoků z logů

1. Zobrazit celý výpis všech zachycených hrozeb, resp. vygenerovaných alertů
`cat /var/log/suricata/fast.log`
2. Čtení pouze aktuálně přibývajících zachycených hrozeb
`tail -f /var/log/suricata/fast.log`
3. Smazání aktuálně zachycených hrozeb
`> /var/log/suricata/fast.log`

4. Pokročilejší zobrazení zachycených hrozeb lze získat také ze souboru eve.json, který obsahuje kromě alertů i další logy, proto je třeba výstup filtrovat
`tail -f /var/log/suricata/eve.json | jq 'select(.event_type=="alert")'`

Detailní podobu alertů lze najít v dokumentaci⁹

5.4 Přístup k DPI GUI

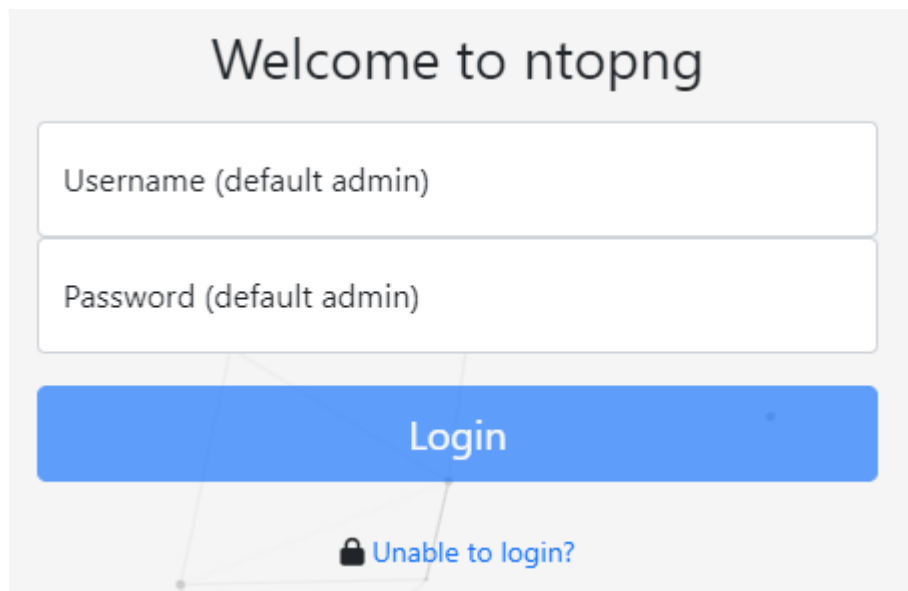
Jelikož sonda nemá žádné grafické prostředí, je třeba k zobrazení DPI GUI prostředí ve webovém prohlížeči třeba využít ssh tunel, viz 5.1.2. Nástroj pro DPI má své grafické prostředí, které je přizpůsobené k vizualizaci zachycených informací a tedy jsou v něm uchovávány stejné informace jako ty, které se následně posílají do DB a lze je následně vizualizovat v prostředí Kibana.

1. Ověření, zda je proces služby DPI aktivní - zadáváme na sondě

`sudo systemctl start ntopng`

```
user@soniot10:~$ systemctl status ntopng
● ntopng.service - ntopng high-speed web-based traffic monitoring and analysis tool
   Loaded: loaded (/etc/systemd/system/ntopng.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2022-09-18 15:09:34 UTC; 2min 7s ago
```

2. V případě potřeby lze proces vypnout/zapnout zadáním příkazů
`sudo systemctl stop/start ntopng`
3. Přístup ke grafickému prostředí DPI je možný po zadání IP v lokálním prohlížeči a portu, který byl zvolen pro SSH tunel.
4. Přihlášení do DPI pomocí jména <DPI_user> a hesla <DPI_passwd>



Detailní popis nástroje lze nalézt v dokumentaci¹⁰.

⁹<https://suricata.readthedocs.io/en/latest/quickstart.html#alerting>

¹⁰ <https://www.ntop.org/guides/ntopng/index.html>

5.5 Sběr, ukládání a vizualizace IDS/IPS zachycených hrozeb

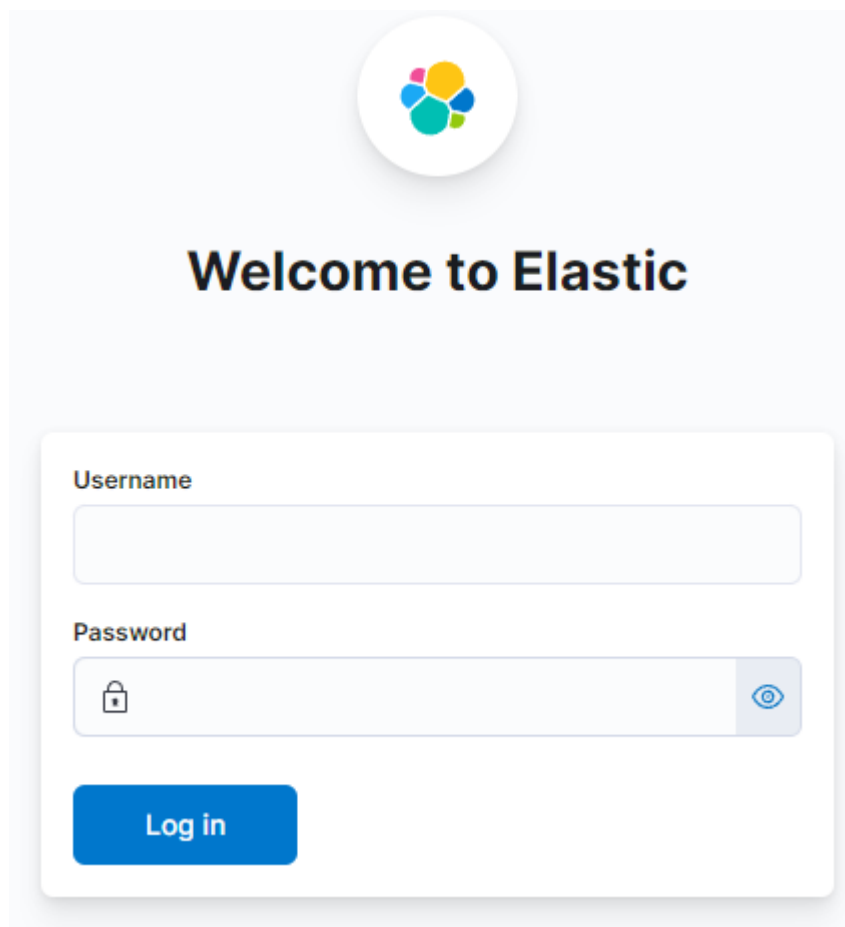
Jelikož nástroj Suricata nemá grafické prostředí pro vizualizaci zachycených hrozeb, tak má sonda svůj vlastní systém pro sběr, ukládání do DB a následnou vizualizaci dat. Postup pro aktivaci/deaktivaci sběru, ukládání a vizualizace zachycených hrozeb v GUI Kibana

1. Přepnout se do adresáře `/home/<SonIoT_username>/scripts`
`cd /home/user/scripts`
2. Spustit `CSV_system.sh`
`sudo ./csv_system.sh`
3. Objeví se informace, zda je sběr, ukládání a vizualizace aktivní či nikoliv. Následně bude uživatel vyzván, aby si zvolil zapnout (1), vypnout (2) či opustit skript (3). Pokud je zvoleno vypnout či zapnout, tak se po několika vteřinách objeví informace, zda byla akce úspěšná či nikoliv.

5.6 Přístup k Kibana GUI

Pokud je sběr, ukládání a vizualizace z kapitoly 5.5 aktivní, tak lze k prostředí Kibana přistoupit z PC dle bodu 5.1.2.

1. zadat IP a port zvolený pro SSH tunel do webového prohlížeče
2. Přihlíšení do Kibany pomocí jména `<Kibana_user>` a hesla `<Kibana_passwd>`



Detailní popis nástroje lze nalézt v dokumentaci¹¹.

5.7 Ověření statusu důležitých SonIoT služeb

Tento skript ověří a ukáže, zda jsou aktivní nejdůležitější procesy sondy v případě, že má uživatel podezření na částečnou či úplnou nefunkčnost.

1. Přepnout se do adresáře /home/<SonIoT_username>/scripts
cd /home/user/scripts
2. Spustit healthcheck.sh
sudo ./healthcheck.sh
3. Výstupem je výpis služeb a jejich status, tj. ON/OFF a případně dodatečné info.

¹¹ <https://www.elastic.co/guide/en/kibana/current/get-started.html>

6. Ukázky

6.1 Ukázka zachyceného SSH Bruteforce útoku

Příkaz z OS Kali Linux připraveného v nástroji VirtualBox

```
hydra -l user -P /usr/share/wordlists/rockyou.txt.gz 10.0.1.47 -t 4 ssh
```


6.1.1 Výstup z příkazu tail -f /var/log/suricata/fast.log

```
09/19/2022-16:51:36.569303  [**] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [**]  
[Classification: Attempted Information Leak] [Priority: 2] {TCP} 10.0.1.22:51376 -> 10.0.1.47:22  
09/19/2022-16:53:52.879787  [**] [1:2001219:20] ET SCAN Potential SSH Scan [**]  
[Classification: Attempted Information Leak] [Priority: 2] {TCP} 10.0.1.22:51406 -> 10.0.1.47:22  
09/19/2022-16:53:52.879787  [**] [1:2003068:7] ET SCAN Potential SSH Scan OUTBOUND [**]  
[Classification: Attempted Information Leak] [Priority: 2] {TCP} 10.0.1.22:51406 -> 10.0.1.47:22
```















6.1.2 Výstup z příkazu `tail -f /var/log/suricata/eve.json | jq 'select(.event_type=="alert")'`

```
{
  "timestamp": "2022-09-19T16:59:14.881551+0000",
  "flow_id": 1767570703283087,
  "in_iface": "enp0s3",
  "event_type": "alert",
  "src_ip": "10.0.1.22",
  "src_port": 51468,
  "dest_ip": "10.0.1.47",
  "dest_port": 22,
  "proto": "TCP",
  "community_id": "1:0Q47k+nSO/vVW9gBYKGufkCKvH0=",
  "alert": {
    "action": "allowed",
    "gid": 1,
    "signature_id": 2003068,
    "rev": 7,
    "signature": "ET SCAN Potential SSH Scan OUTBOUND",
    "category": "Attempted Information Leak",
    "severity": 2,
    "metadata": {
      "created_at": [
        "2010_07_30"
      ],
      "updated_at": [
        "2010_07_30"
      ]
    }
  },
  "flow": {
    "pkts_toserver": 1,
    "pkts_toclient": 0,
    "bytes_toserver": 74,
    "bytes_toclient": 0,
    "start": "2022-09-19T16:59:14.881551+0000"
  }
}
```

6.1.3 Výstup z grafického prostředí Kibana, přesněji z dashboardu “[Filebeat Suricata] Alert Overview”

Top Alert Signatures [Filebeat Suricata]			
 Export			
Alert Signature	Alert Category	Count	
ET SCAN Potential SSH Scan	Attempted Information Leak	8	

6.1.4 Výstup z grafického prostředí Kibana, přesněji ze sekce “Discover”, která obsahuje veškeré logy

 suricata.eve.alert.category	Attempted Information Leak
 suricata.eve.alert.created_at	Jul 30, 2010 @ 02:00:00.000
 suricata.eve.alert.gid	1
 suricata.eve.alert.metadata	{}
 suricata.eve.alert.rev	7
 suricata.eve.alert.signature	ET SCAN Potential SSH Scan OUTBOUND
 suricata.eve.alert.signature_id	2,003,068
 suricata.eve.alert.updated_at	Jul 30, 2010 @ 02:00:00.000
 suricata.eve.community_id	1:F8/v12BCIEAcISoNbcPJHh+UL+c=
 suricata.eve.event_type	alert
 suricata.eve.flow_id	1268401060915122
 suricata.eve.in_iface	enp0s3
 tags	suricata