Bezpečnost sítě CESNET2

Andrea Kropáčová, andrea@cesnet.cz
CESNET, z. s. p. o.

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI
2007–13
OP Výzkum a vývoj pro inovace

Bezpečnost CESNET2

- **Máme nástroje a technologie, které**
  - podají obraz o dění v síti
  - detekují anomálie (podezřelé chování) v provozu sítí a služeb
  - dovolí zaměřit se na podezřelý provoz
  - umožní sdílení zajímavých dat
  - informace o anomáliích (události, BI) dostanou do rukou správců

    ==> aktivní obrana

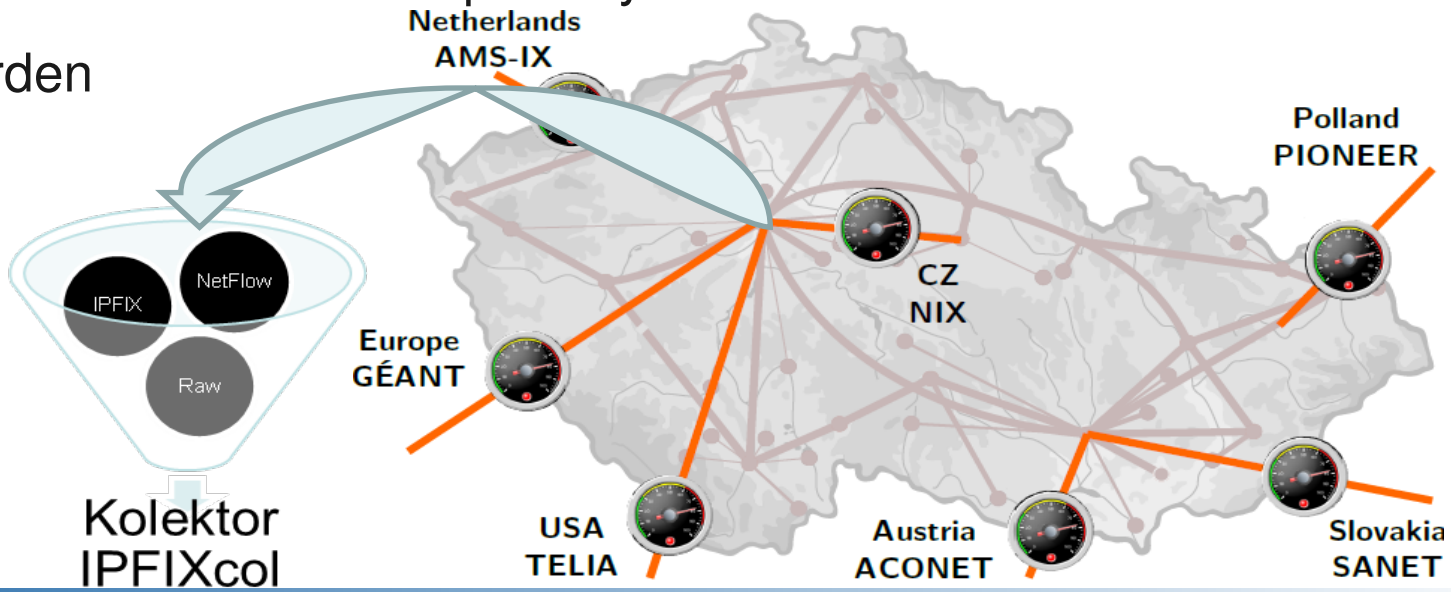
    ==> „zdravotní aspekt“, prevence
  - **umožní detekci, sběr, analýzu a vytěžení těchto dat**

Bezpečnostní infrastruktura

- **Síťové sondy** na perimetru sítě CESNET2
- **FTAS:**
  - plošné souvislé sledování IP provozu rozsáhlých síťových infrastruktur
  - plošně přes celou infrastrukturu
- **G3:**
  - plošné souvislé sledování stavu a chování rozsáhlých výkonných infrastruktur
  - plošně přes celou infrastrukturu
- **IDS systémy, Honeypoty**
- **Systémy pro sdílení a korelaci dat**
  - **Warden**
  - Mentat

Měřící infrastruktura

- Bezeztrátové a detailní měření síťových dat **na perimetru sítě CESNET2** na volitelné úrovni detailu
  - NetFlow v9, IPFIX, pakety
    - měření tunelovaného provozu
    - měření aplikací HTTP, DNS, SIP
- Sběr a uchování dat
  - IPFIXcol – uchování libovolné položky
  - FTAS, Warden
  - NfSen

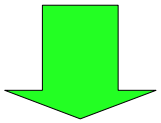


G3

- Plošné souvislé sledování stavu a chování rozsáhlých výkonných infrastruktur, primárně pro sledování provozu CESNET2
- Detekce on-the-fly anomálií a jejich notifikace
- Event notifier
  - automatický visualisér anomálních stavů, aktuální události z infrastruktury, možno konfigurovat per device
- Interaktivní UI
  - agregovaná vizualizace aktuálních anomálních stavů (včetně historie)
  - provázání na detailní reporting příslušných objektů
- G3 system reporter
  - využití sítě CESNET2
  - mapy chybovosti
  - „zdraví“ sítě CESNET2

FTAS

- Plošné souvislé sledování IP provozu rozsáhlých síťových infrastruktur
- Zpracování provozních informací o IP tocích (NetFlow)
- Vlastnosti a využitelnost
  - cílené sledování a dlouhodobé uchování informací o provozu
    - komplexní klasifikační a filtrační aparát pro vyčlenění provozu
    - statistické zpracování
  - informace o již uskutečněné komunikaci, včetně trajektorie
  - odhalení podvržení adres
  - umožňuje zaměřit se na provoz mající anomální charakter



  - **verifikace a analýza bezpečnostních incidentů**
  - **automatická detekce anomálií**
  - **systematické sledování provozu sítě (instituce)**

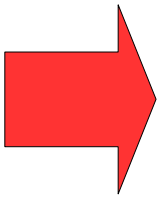
G3, FTAS

- G3
  - 2 instance systému
  - sběr dat ze 150 zařízení
  - 600000 údajů / 600s
- FTAS
  - distribuovaná architektura
  - instance na páteřní síti
    - cca 14 uzlů
    - sběr dat ze 22 prim. zdrojů
  - 21 instancí “FTAS jako služba”
    - 6 instancí na vlastním železe

Akademie Věd ČR
Fakultní nemocnice Motol
Jihočeská Univerzita v Českých Budějovicích
Masarykova Nemocnice v Ústí n. L.
Masarykova Univerzita v Brně
Ostravská Univerzita v Ostravě
PASNET metropolitní síť
Slezská Univerzita Opava
SOUE Plzeň
SŠEAS Ustí nad Labem
Technická univerzita Ostrava - VŠB
Technická Univerzita v Liberci
Univerzita Hradec Králové
Univerzita J. E. Purkyně v Ústí n. L.
Univerzita Karlova v Praze
Univerzita Obrany
Univerzita Palackého v Olomouci
Univerzita J. A. Komenského Praha
Všeobecná fakultní nemocnice
Vysoká škola ekonomická
Západočeská Univerzita v Plzni

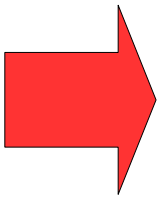
Pro koho je FTAS a G3

- Bezpečnostní týmy
- Dohledová pracoviště
- Výzkumné týmy



- konkrétní informace o provozu
- řešení bezpečnostních incidentů
- automatická detekce anomálií
- vzorky dat, ladění sítě
- obrana

- Manažery
- Ředitele IT
- Správce



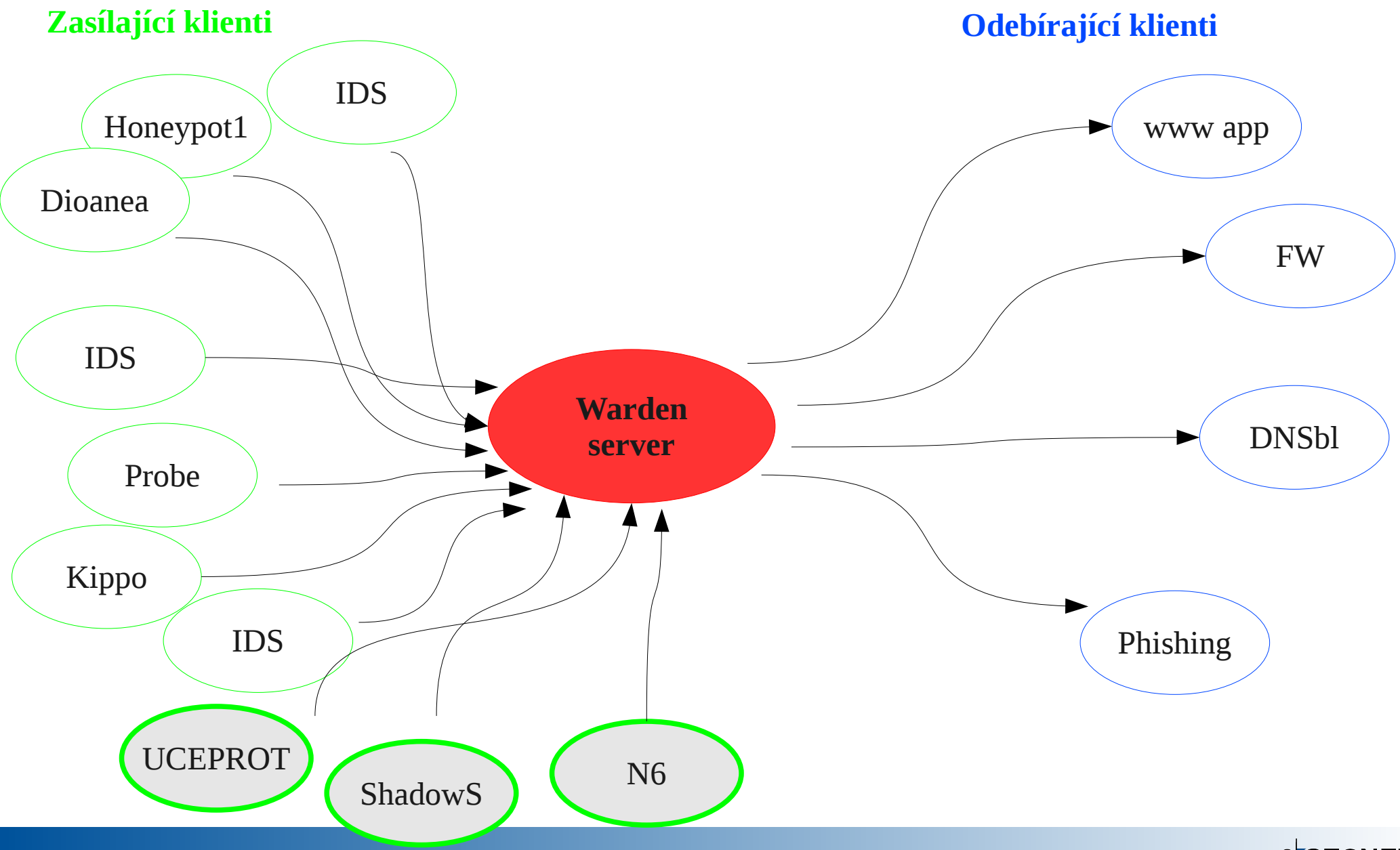
- náhled na provoz sítě
- zdraví
- vytížení
- architektura
- statistiky provozu

Warden

- Systém pro efektivní sdílení informací o bezpečnostních událostech
- Motivace
  - mám data, ale kam s nimi?
  - chci data, ale kde je vzít?
- Hlavní cíle
  - platforma pro sdílení dat (dej, odeber)
  - sledování zdraví sítě a služeb
  - aktivní obrana
- Architektura
  - client-server, jednoduchý protokol a klienti
  - zasílají se ***události***
  - zabezpečení připojení

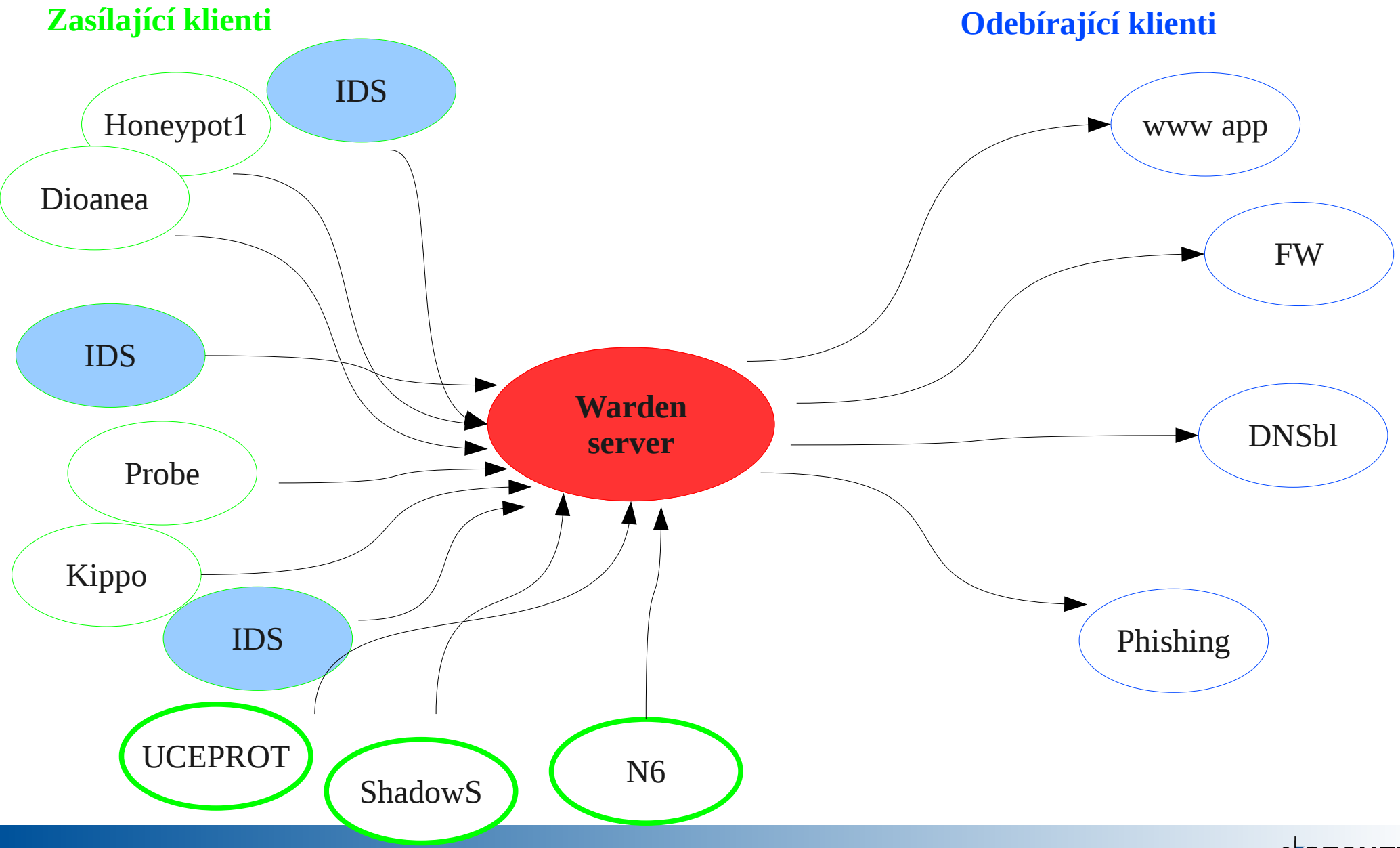
```
Hostname,Service: CESNET_IDS

Detection time, arrival
time:

Event type: Portscan,
            bruteforce,
            spam,
            phishing,
            ...
Source: IP/URL/Reply-To

Aim: protocol TCP, port 22

Scale: scan 666 ports,
       sweep 66 machines

Note: Free text note

Client tags: Network,
             Connection,
             Honeypot,
             LaBrea
```

Architektura



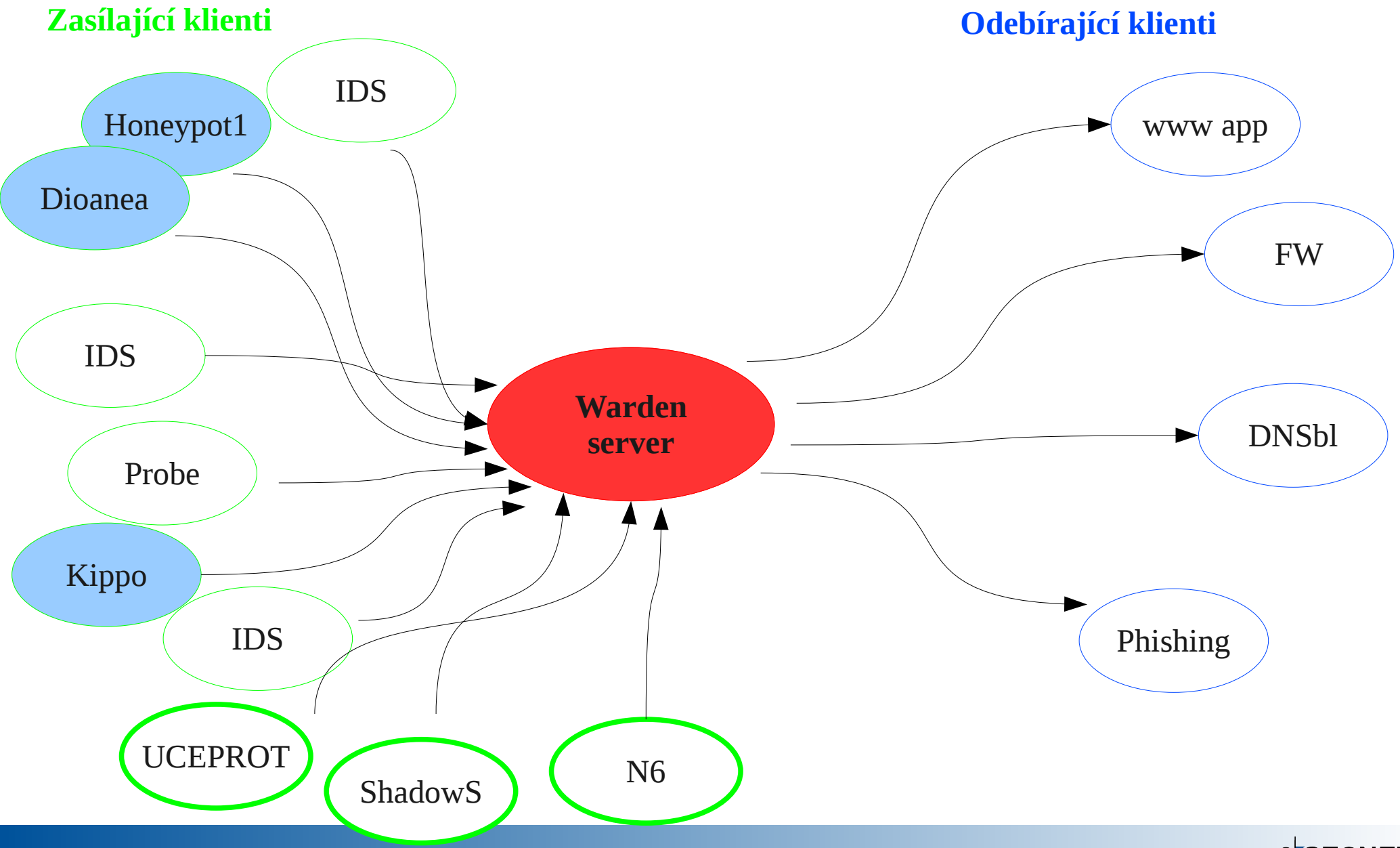
Use-case 1

Odebírání dat generovaných IDS systémy



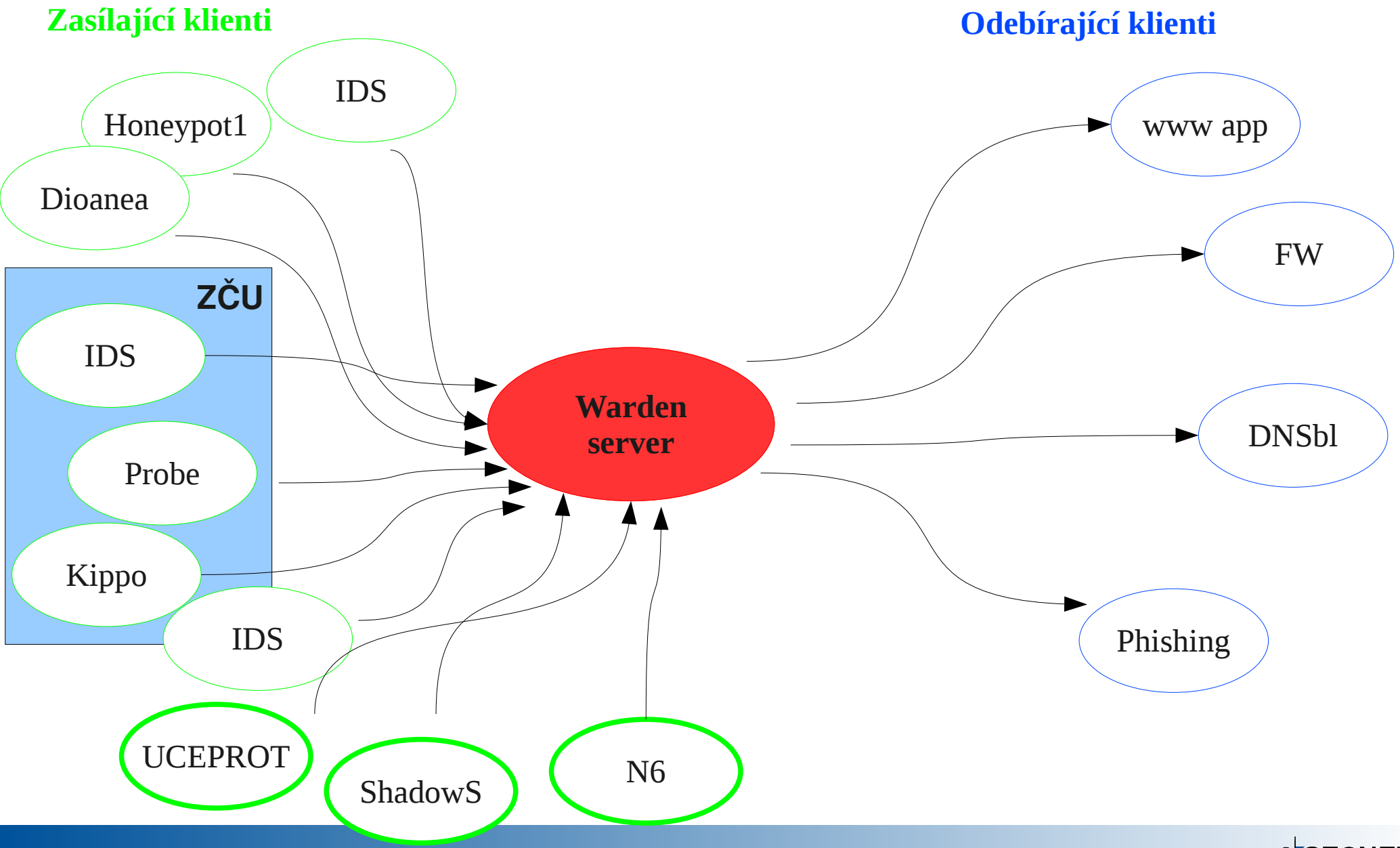
Use-case 2

Odebírání dat generovaných honeypoty



Use-case 3

Odebírání dat generovaných z jedné konkrétní sítě



Warden: kdy, proč a jak se zapojit

- **Aktuálně jsou zapojeni**
  - CESNET, VŠB, TUL, MUNI, ZČU, SLU, CUNI, VUT
- **Kdy**
  - když máte zajímavé zdroje dat (IDS, sondy, honeypots)
  - když máte zájem o data pro správu své sítě
- **Proč**
  - zisk zajímavých dat (aktivní obrana, „zdraví“ sítě)
  - rozvoj komunity
- **Jak**
  - warden-info@cesnet.cz

Bezpečnost: Shrnutí

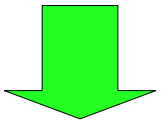
- Asistence při problému (útok, nefunkčnost)
  - máme připraveny mechanismy
    - kam problém nahlásit (PSS, NOC, CESNET-CERTS)
    - jak problém detekovat, zmírnit, vyřešit (RTBH, IG, filtry ...)
    - jak problém analyzovat – FLAB
- Služby na bázi detekce (FTAS, G3)
  - můžete využít instanci běžící na páteři
  - můžete mít vlastní instanci ve vlastní síti
- Služby na bázi sdílení a rozvoje komunity (dáš, dostaneš)
  - Warden
- Služby pro otestování sítě a služeb
  - *penetrační testy sítě*, penetrační testy služeb (server, SIP)
  - testy odolnosti

Bezpečnost: Shrnutí

Budujeme komunitu:

FTAS, G3, Warden

? Kam dál ?



Posunujeme se k „Security as a Service“

- *Byl by zájem o síťovou sondu do koncové sítě?*
- *Integrovaný Warden client?*

Děkuji za pozornost.