DOM REG [.lt]

DNS ir saugumas

KTU Interneto paslaugų centras

Kaunas, 2021-11-24

Interneto DNS sistemos struktūra

Rekursiniai DNS serveriai

Autoritetingi DNS serveriai

Interneto naudotojų įrenginiai

Vietiniai

Išoriniai

Šakniniai DNS serveriai

ALD DNS serveriai

ALD DNS serveriai

ALD DNS serveriai

ALD DNS serveriai

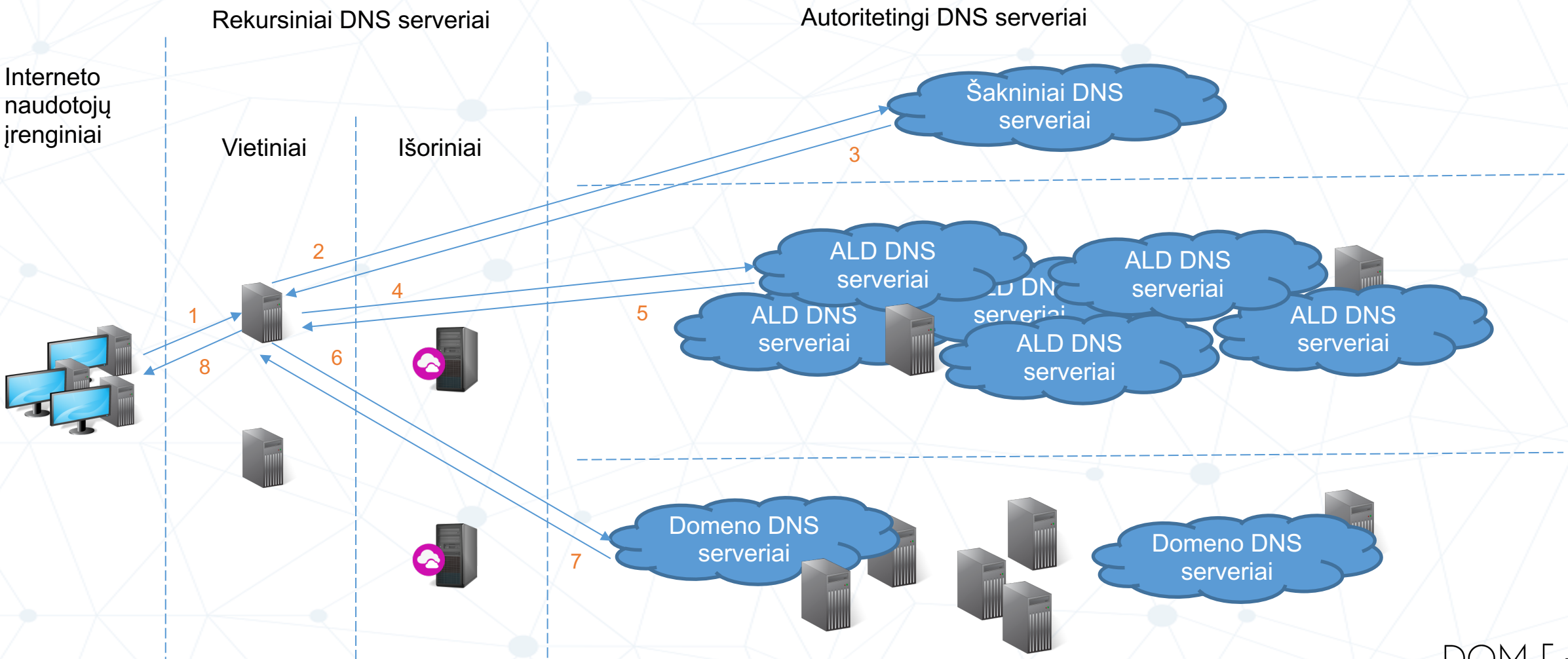
ALD DNS serveriai

Domeno DNS serveriai

Domeno DNS serveriai

DOM REG [.lt]

Interneto adreso pavadinimo įrašų radimas



DOM REG [.lt]

Grėsmingi DNS sistemos ypatumai

DNS naudoja UDP, ir tam tikrais atvejais TCP protokolą.

- UDP - galimas tinklo paketo siuntėjo adreso padirbinėjimas.

Turi būti pasiekiamas DNS serverių 53 prievadas.

- Užkardos praleidžia tinklo paketus į 53 prievadą.
- Galimas “DNS tuneliavimo” naudojimas.

DNS tinklo paketai yra nešifruoti.

- Galimas siunčiamos DNS informacijos stebėjimas tinkle.
- Galimas DNS pranešimų padirbinėjimas.

DOM REG [.lt]

DNS naudojimas žvalgybai

Registruoto domeno vieša informacija WHOIS duomenų bazėje.

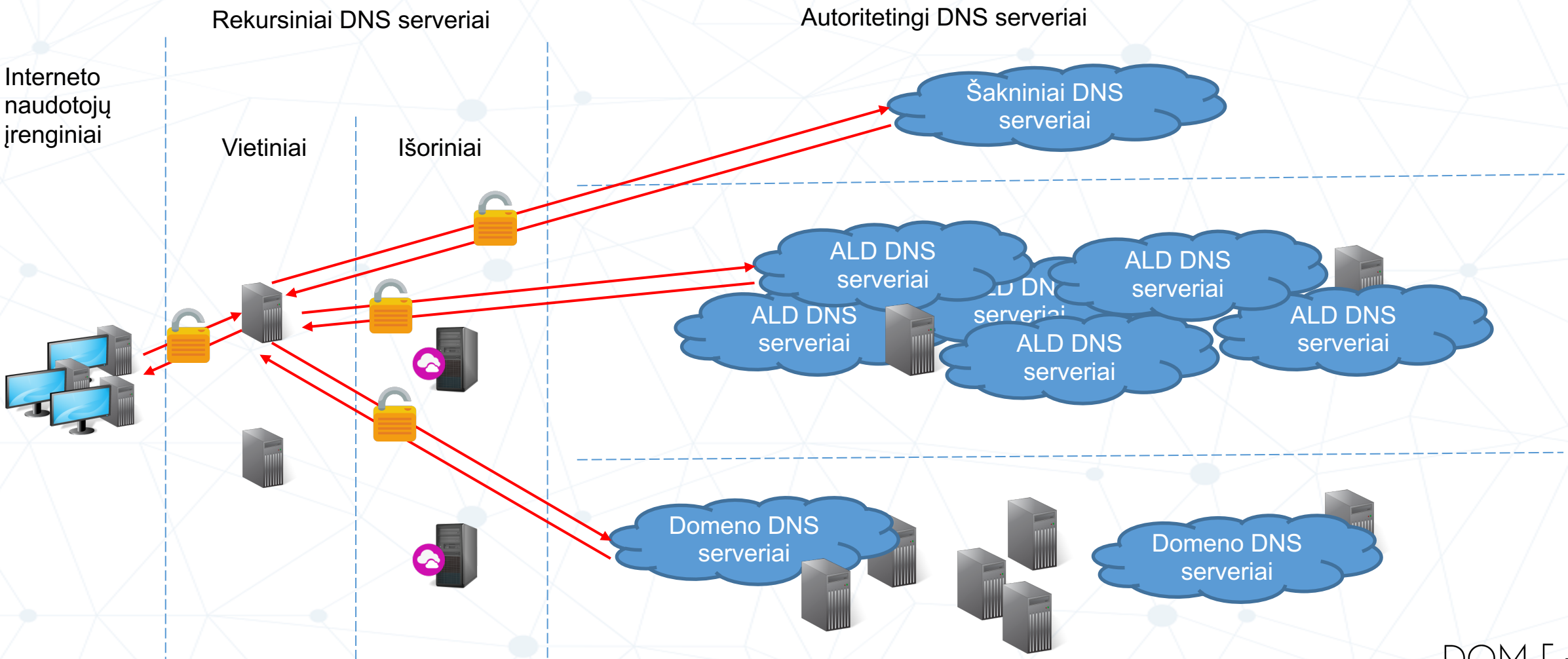
Domeno DNS įrašai atskleidžia turimų tarnybinių ir darbo stočių adresus, paslaugas ir paslaugų teikėjus.

DNS užklausų informacija parodo prie kokių interneto resursų yra jungiamasi.

Užklausa į rekursinį DNS serverį gali parodyti, ar kažkas jau klausė tokio adreso.

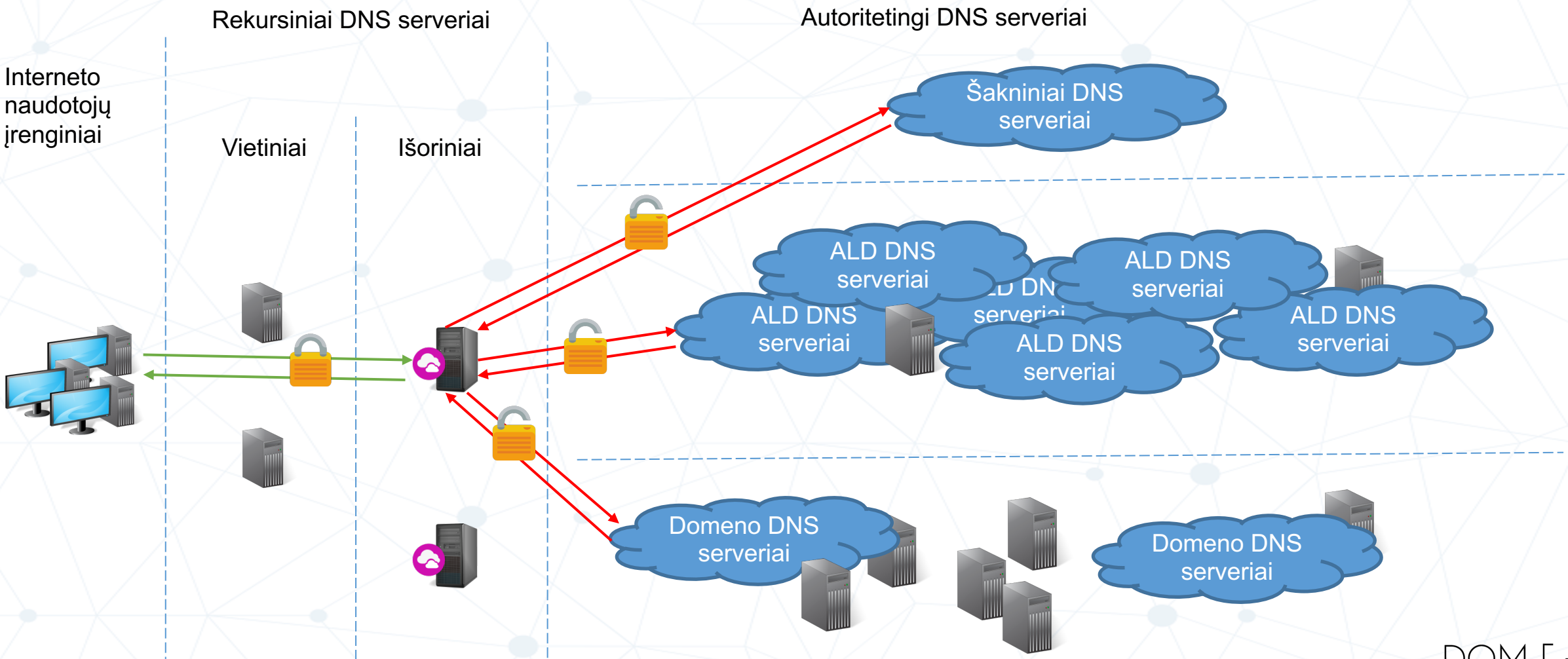
DOM REG [.lt]

DNS ir privatumas



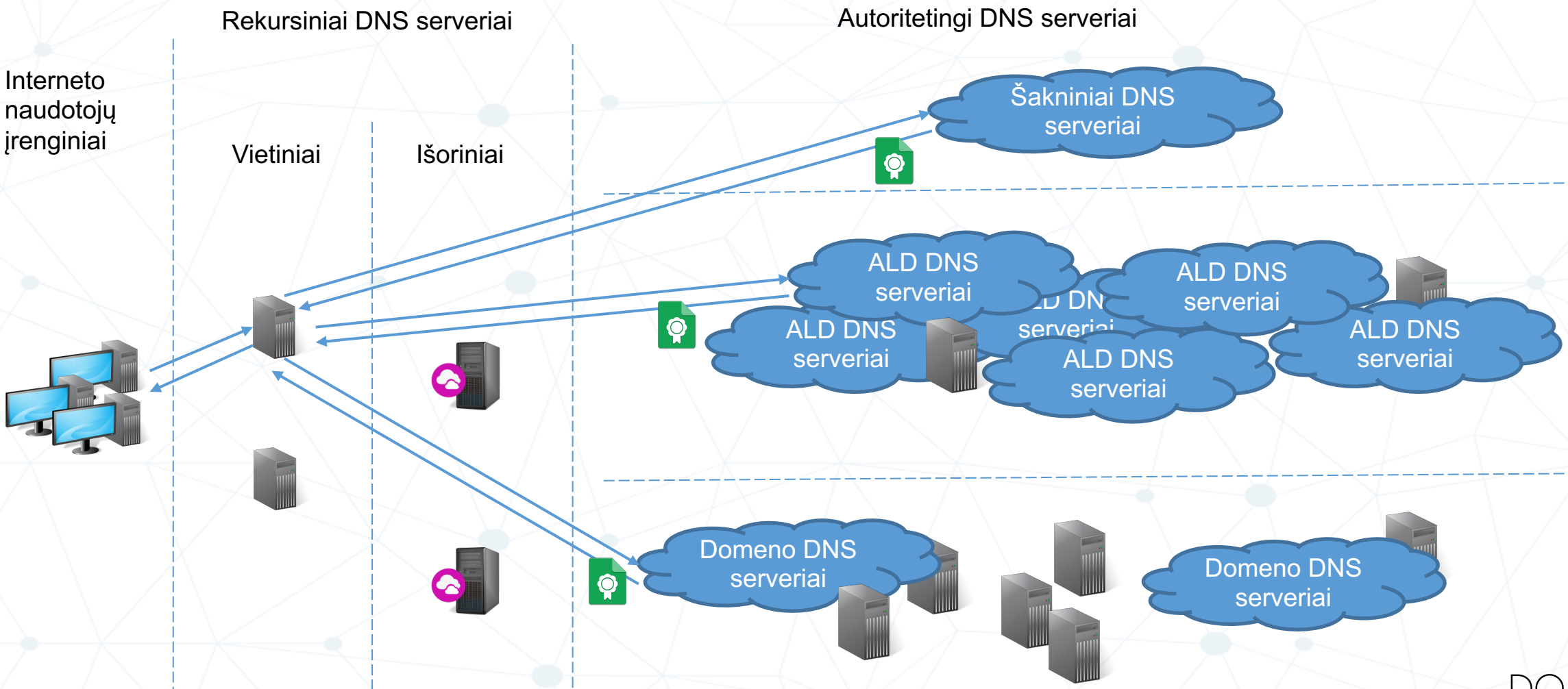
DOM REG [.lt]

DoH, DoT



DOM REG [.lt]

DNSSEC



DOM REG [.lt]

Pagrindiniai atakų tipai panaudojant DNS

DNS įrašų padirbimas (DNS Poisoning):

Atsakymo į DNS užklausą padirbimas (DNS Spoofing);

Padirbto DNS įrašo įrašymas į rekursinio DNS serverio laikinąją atmintį (DNS cache poisoning).

Atkirtimas nuo paslaugos (DoS, DDoS):

DNS serverių išnaudojimas nukreipiant atsakymų į DNS užklausas siuntimą užklausų nesiuntusiam adresatui (DNS reflection);

Mažų užklausų siuntimas į DNS serverius, suaktyvinant didelių atsakymų siuntimą nurodydam adresatui (DNS amplification).

DOM REG [.lt]

Administracinės priemonės DNS saugumui

Saugumu besirūpinančio domeno paslaugų teikėjo pasirinkimas.

Domeno valdymo paskyros duomenų saugumas.

Kontaktinės ir techninės informacijos aktualumas.

Viešos kontaktinės informacijos nuasmeninimas.

Keičiant seną domeną naujai registruotu – seną domeną išlaikyti tol, kol visos paslaugos ir nuorodos bus pilnai migravusios į naują domeną.

Klaidinamai panašių domenų įkūrimas (apsaugai nuo “phishing” atakų).

DOM REG [.lt]

Techninės priemonės DNS saugumui (I)

DNS serverių skaičiaus/pajėgumų didinimas.

Anycast DNS debesų naudojimas.

Rekursinių ir autoritatyvių DNS serverių atskyrimas.

Vidinio tinklo DNS įrašų/serverių atskyrimas nuo išoriniam tinklui skirtų.

Tinkama DNS serverių PI priežiūra.

Leidimo atsisiųsti DNS įrašų failą (zone) ribojimas.

DNSSEC įgalinimas naudojant NSEC3 (ne NSEC).

Neegzistuojančių DNS įrašų (NXDOMAIN) užklausų skaičiaus ribojimas.

DOM REG [.lt]

Techninės priemonės DNS saugumui (II)

Vietinių DNS serverių naudojimas rekursinėms užklausoms.

DNS užklausų siuntimo į išorinius serverius blokavimas.

Išorinių DNS užklausų į rekursinį DNS serverį užkardymas.

Rekursinių DNS serverių naudojimo leidimas tik vidiniams naudotojams.

Atsitiktinių imčių šaltinio prievadų ir užklausų ID naudojimo kiekvienai siunčiamai DNS užklausai nustatymas.

Automatizuotos DNS serverių ir įrašų stebėjimo priemonės.

Šifruoto ryšių kanalo naudojimas DNS įrašų failo persiuntimui į autoritatyvius DNS serverius.

DOM REG [.lt]

Ačiū!

[Klausimai?]

DOM REG [.lt]