LITNET paslauga – Duomenų srautų užkarda

LITNET konferencija 2018

Arvydas Žiliukas, KTU-ITSG/LITNET CERT

Esama situacija

- IT Saugos politikos, apimančios duomenų tinklo užtvaras ir jų roles nebuvimas
- Duomenų srautų segmentavimo nepakankamumas
- Tinklo užtvarų funkcijų persidengimas su kitomis IT saugą užtikrinančiomis priemonėmis ir technologijomis ir konsensuso nebuvimas
- Nėra proaktyvaus IT saugos įvykių koreliavimo ir stebėjimo

Kasdieniniai CERT incidentai

- Autorinių teisių pažeidimai (a.k.a torrent)
- Aplikacijų pažeidžiamumas
  - SSL (poodle)
  - Portmapper
  - Telnet
  - SNMP
  - MSSQL
- Virusai ir Malware IN/OUT
- SPAM OUT (abuse content)
- Išoriniai skenavimai, DDoS
- Nesankcionuota prieiga (atviri portai, prisijungimai)

Nuo ko pradėti?

- Kokiems srautams reikia užkardos ir kodėl?
- Srautų profiliavimas apsaugos prasme.
- Tinklo segmentų ir architektūros perdarymo galimybės – (ne)galime, (ne)norime?
- Užkardos(-ų) darbo režimo(-ų) parinkimas
- Užkardos inspektavimo režimo parinkimas atsižvelgiant į srautų profilius.

Galimi užkardų režimai*

- Tinkliniai darbo režimai – Maršrutizavimo (*Route/NAT*) arba Skaidrus (*Transparent*)
  - Skaidriame režime „stateful firewall“ palaikomas !!!
- Abu darbo režimai gali veikti dviem Inspektavimo režimais – Flow-based ir Proxy
- Flow-based inspektavimas (NGFW/UTM) gali veikti dviem režimais – Profile-based ir Policy-based

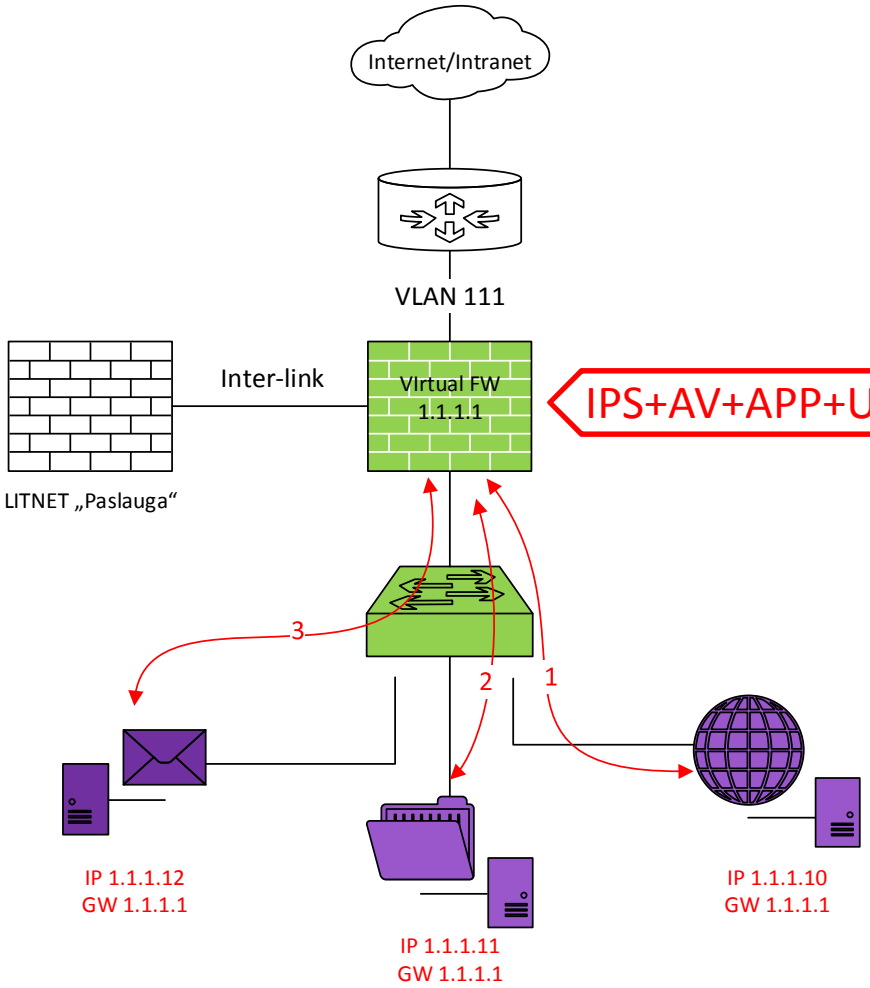
* - gali kažkiek skirtis priklausomai nuo gamintojo

Inspektavimo funkcionalumas

Funkcija	Flow-based inspekcija	Proxy-based inspekcija
Anti-virus	✓	✓
Web filtravimas	✓	✓
DNS/Botnet filtravimas	✓	✓
Aplikacijų kontrolė	✓	✓
IPS	✓	✓
Anti-Spam	×	✓
DLP	×	✓
VoIP	×	✓
ICAP	×	✓
WAF	×	✓
Proxy opcijos	✓	✓
SSL inspekcija	✓	✓
SSH inspekcija	×	✓
IPSec GW	✓ tik Policy-based	✓
SSL GW	✓ tik Route/NAT	✓ tik Route/ANT

Galimi diegimo scenarijai

Užkarda – srautų šliuzas ir maršrutizatorius



Route režimas
Inspekcija – Proxy
Policy-based
AntiBotnet/DNSBL

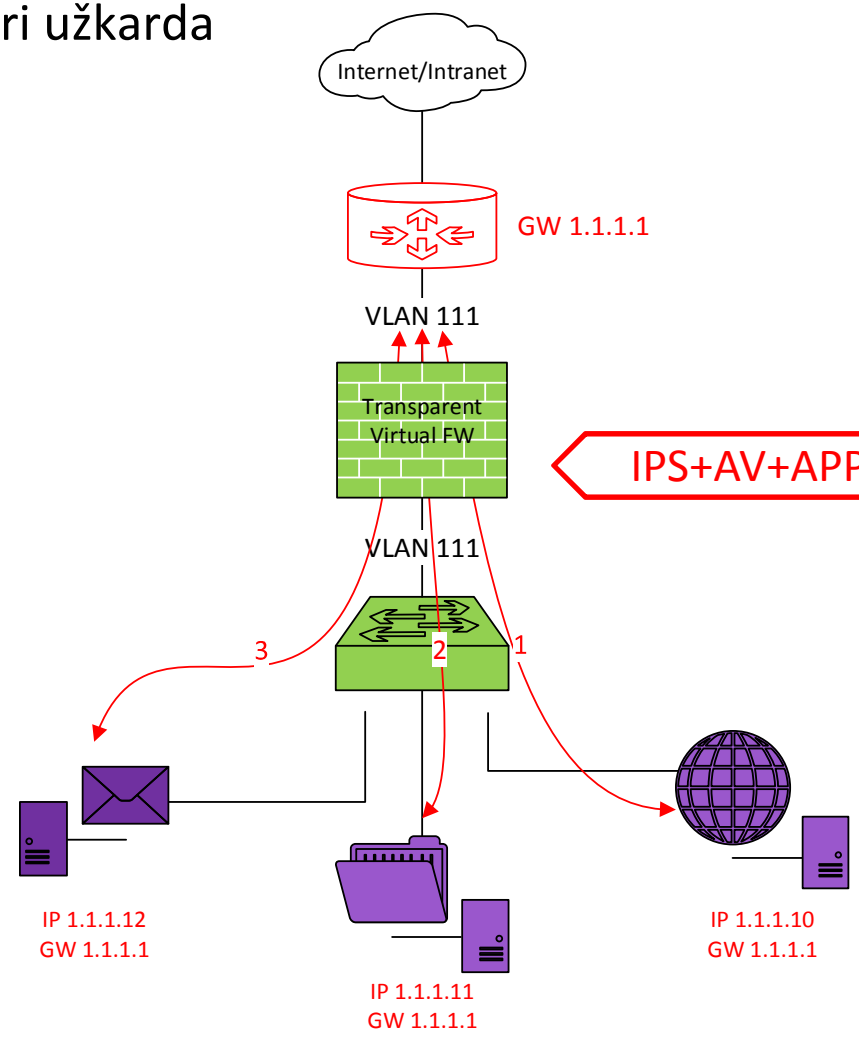
1. All OUT allow (stateful)
2. WWW IN allow
3. SMTP IN allow

IPS+AV+APP+URL+SSL+VPN(IPSec/SSL)

Lokali saugos taisyklių politika

Galimi diegimo scenarijai

Skaidri užkarda



Skaidrus režimas
Inspekcija – Proxy
Policy-based
AntiBotnet/DNSBL

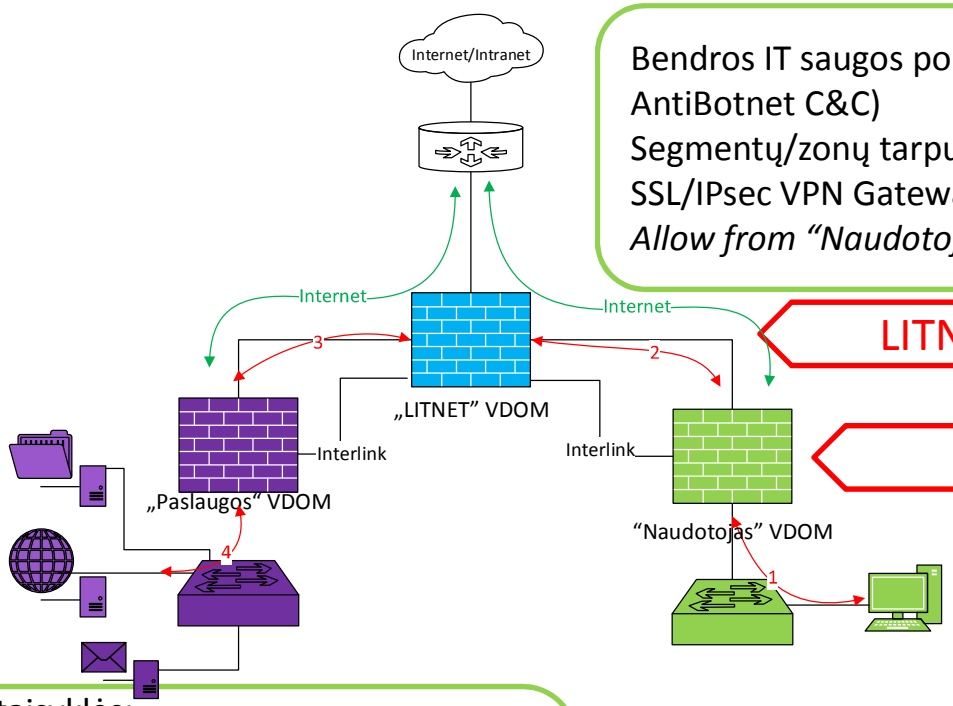
1. All OUT allow (stateful)
2. WWW IN allow
3. SMTP IN allow

IPS+AV+APP+URL+SSL+VPN(IPSec)

Lokali saugos taisyklių politika

Galimi diegimo scenarijai

Sunkus diegimas - maksimalus rezultatas



Bendros IT saugos politikos taisyklės (AntiDDoS L2/L3 AntiBotnet C&C)
Segmentų/zonų tarpusavio sąveikos taisyklės
SSL/IPsec VPN Gateway
Allow from "Naudotojas" to "Paslaugos" All

LITNET (globalios) taisyklės

Lokalios taisyklės

Lokalios taisyklės:
IPS/AV/App/URL IN/OUT
SSL/SSH controll/offload
WAF/WCCP/Proxy
AntiDDoS L3/L4
Allow IN from Any Src. IP-port to Dst. IP „Paslaugos" port

Lokalios taisyklės:
Policy-based FW
IPS + AV + APP control (?)
SSL/IPSec VPN
All OUT allow
All IN deny
Allow Any from/to „Paslaugos"

Duomenų srautų užkarda kaip paslauga

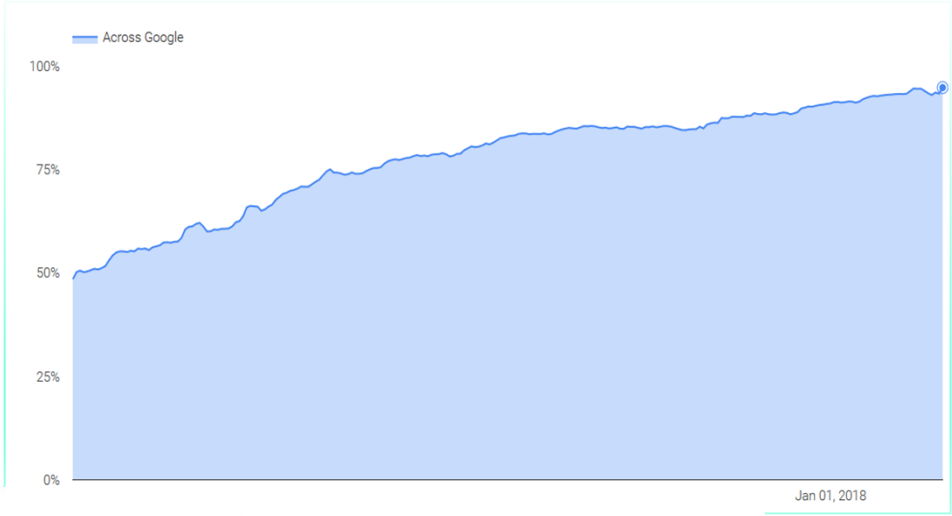
- Reikalavimai (žinios) paslaugai įsidiegti:
  - Duomenų srautai aptarnaujami (tiekiami) LITNET
  - Duomenų srauto paslaugai identifikavimas ir tikslingumo nustatymas
  - Užkardos darbo režimo pagal srauto aptarnavimo ar nukreipimo galimybes pasirinkimas
  - Užkardos inspektavimo režimo pasirinkimas
  - Atsakingo asmens (koordinatoriaus ar/ir administratoriaus pasiskyrimas)
  - Užkardos valdymo (paslaugos) modelio pasirinkimas – administruoja pats paslaugos užsakovas, ar administruoja LITNET CERT?

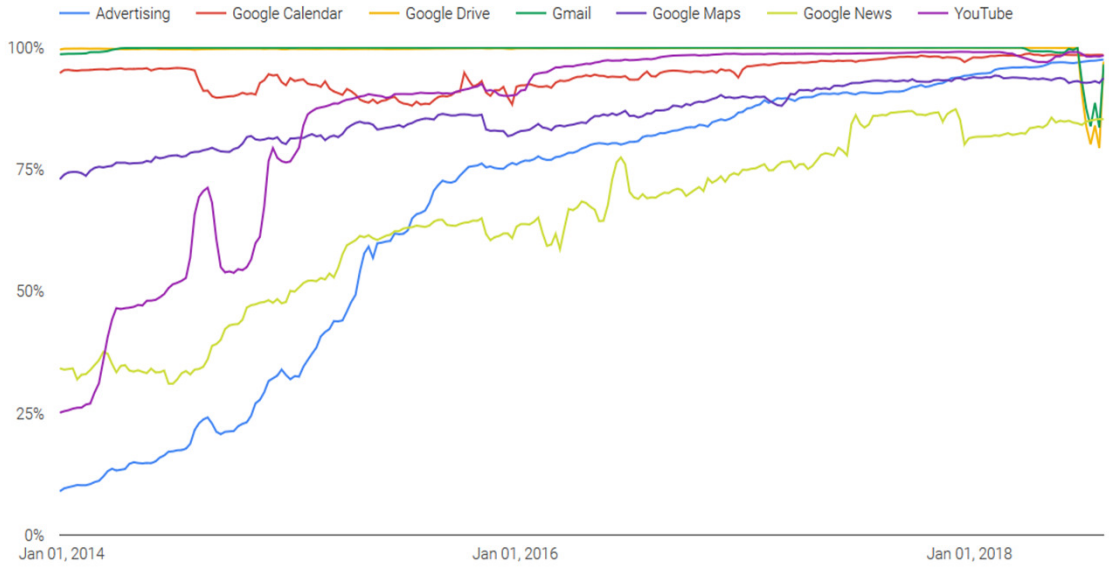
Duomenų srautų užkarda kaip paslauga

- Užkardos paslaugos įdiegimas (numatoma 2018 pabaiga)
  - Užkardos paraiškos-formos užpildymas
  - Paraiškos įvertinimas ir priėmimas vykdymui
  - Tiesioginis bendravimas tarp užsakovo koordinatoriaus (administratoriaus) ir LITNET CERT, techninės užduoties ir darbo eigos pasirengimas.
  - Pirminis užkardos parengimas ir sukonfigūravimas iš LITNET CERT pusės
  - (a) Prisijungimo duomenų prie užsakovui parengtos užkardos perdavimas. Užsakovas diegiasi ir tvarkosi su užkardos taisyklėmis savarankiškai.
  - (b) Užkardos taisyklių suderinimas su užsakovu ir taisyklių detalus įdiegimas. Taisyklių diegimo, keitimo procedūrų nustatymas ir vykdymas iš LITNET CERT pusės, ataskaitų teikimas užsakovui.

Ateities (rytdienos) iššūkiai

HTTPS srautas





... iššūkiai

- Duomenų nutekėjimo prevencija – DLP
  - Palengvinimas ir atitikimas BDAR-o reikalavimams
- Aplikacijų užtvara
  - Profiliai pagal aplikacijas, jų grupes ir naudotojus
  - Web aplikacijų užtvara
- Debesija
  - IT politika (DLP)
  - Debesijos paslaugų naudojimo stebėsena
- Proaktyvus įvykių koreliavimas ir stebėjimas
  - Grėsmės duomenų tinkle/sraute
  - Kompiuterio, aplikacijos pažeidžiamumas
  - Srautų elgsena

... iššūkiai

- QUIC
  - Šiuo metu naudojamas tik Google paslaugose, eksperimentuojama su Opera.
  - Sudaro iki 9% viso Internet srauto ir iki 50% Google srauto.
  - Įtrauktas į IETF svarstymus, standartizavimą.
- DNS užklausos per (DNS over)
  - DNS per HTTPS proxy – DOH
    - API, Agent, JSON ir pan.
  - DNS over TLS – DOT
    - Egzistuoja RFC 7858
    - RFC rekomenduoja konkretaus TCP porto – 853 naudojimą
- Autentikavimas
  - AD/LDAP
  - RADIUS
  - SSO

Klausimai? ...(ar spausti mygtuką?)

... jei jų nėra, reiškia viskas buvo labai aišku

... arba viskas buvo visiškai nesuprantama