Vilniaus Gedimino technikos universitetas

Elektronikos fakultetas

Kompiuterijos ir ryšių technologijų katedra

Duomenų centrų ugniasienės

Modulis ELKRM17303

Laboratorinio darbo nr. 6 ataskaita

Atliko: TETfm-20 grupės magistrantas
Saulius Krasuckas
Tikrino: lekt. dr. Liudas Duoba

VILNIUS, 2022

Laboratorinis darbas nr. 6

Duomenų centrų ugniasienės

Darbo tikslas

Susipažinti su duomenų centrų (DC) ugniasienėmis.

Užduotis

1. Parinkti ir apžvelgti ugniasienes.
   - Internete raskite bent dviejų skirtingų gamintojų naujos kartos DC ugniasienes (NGFW, angl. *Next-Generation Firewall*) ir jų specifikaciją (angl. *Data sheet*) pagal savo reikalavimus:

Studentas	**Threat Protections, Gbps**	**SSL/TLS Inspections, Gbps**	**New Session rate (per second)**
Saulius Krasuckas	≥ 3	≥ 4	≥ 250.000

   - Atlikite tyrimą ir atsakykite, kas yra mikrosegmentavimas.
2. Parenkite trumpą ataskaitą, kurioje:
   - Bus pateikta medžiaga (ir specifikacijos) ne mažiau nei apie dvi ugniasienes.
   - Laikysitės principo: *Less is more*; svarbu kokybė.
   - Išlaikykite vienodą stilių.
3. Parengtą ataskaitą .pdf formatu įkelkite į *Moodle* sistemą.

Darbo eiga

Pasirenku ugniasienes.

- Pirmoji ugniasienė, atitinkanti duotus LD reikalavimus: **Juniper vSRX Virtual Firewall (https://www.juniper.net/content/dam/www/assets/datasheets/us/en/security/vsrx-virtual-firewall-datasheet.pdf)**

  Pasirinkau virtualią šio gamintojo NGFW implementaciją, t.y. *Virtual Appliance*:

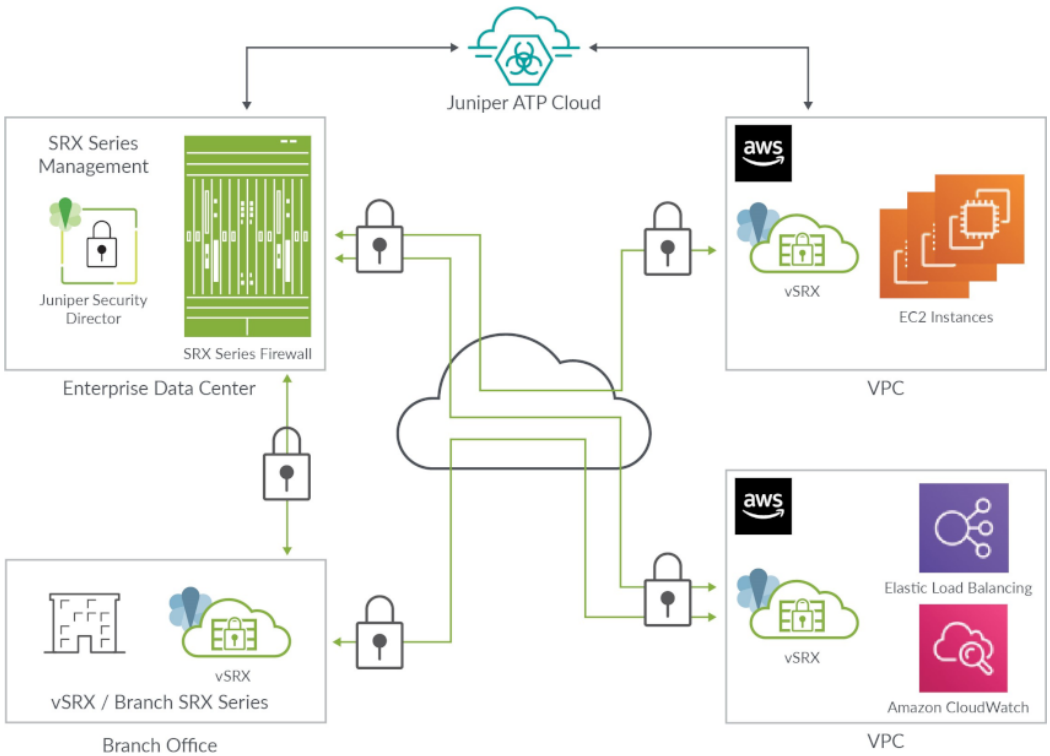


Table 1. vSRX Virtual Firewall sparta

Spartos / pajėgumo rodiklis	**VMware hipervizorius**	**KVM hipervizorius**
vCPU skaičius	9	9
Atminties kiekis	16 GiB	16 GiB
Ugniasienės pralaidumas (dideliems paketams, 1514 B)	73 Gbps	79 Gbps
Ugniasienės pralaidumas (IMIX * srautui)	**17 Gbps**	**22 Gbps**
Aplikacijų matomumas ir valdymas**	**21 Gbps**	**20.7 Gbps**
IPS sparta su rekomenduotinomis signatūromis	**18 Gbps**	**20.8 Gbps**
Naujų TCP sesijų augimo sparta (vnt. / s)	**351.250**	**360.000**

Spartos / pajėgumo rodiklis	VMware hipervizorius	KVM hipervizorius
Didžiausias vienu metu palaikomų sesijų sk.	4M	4M

* IMIX — "Internet MIX traffic": tai įprastinis internetinis srautas, keliaujantis per tinklo įrenginius.

** Matuota naudojant HTTP srautą ir 44 kiB dydžio tranzakcijas.

- Antroji ugniasienė, atitinkanti duotus LD reikalavimus: **Palo Alto PA-5250 (https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-5200-series-specsheet)**

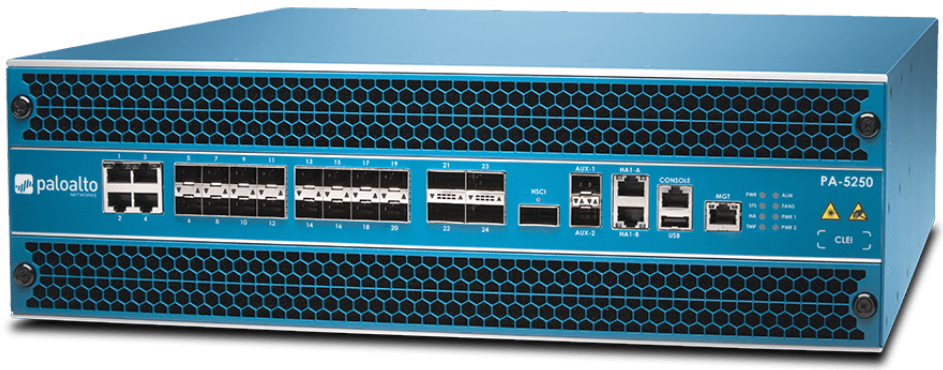


Table 2. PA-5250 sparta

Rodiklis	PA-5250
Ugniasienės pralaidumas (HTTP srautui)	**35.7 Gbps**
Ugniasienės pralaidumas (*appmix* srautui)	37.3 Gbps
***Threat Prevention* sparta** (HTTP srautui)	**18.3 Gbps**
Threat Prevention sparta (*appmix* srautui)	23.0 Gbps
Naujų TCP sesijų augimo sparta (vnt. / s)	**392.000**
Didžiausias vienu metu palaikomų sesijų sk.	8M

Mikrosegmentavimo apžvalga

Remiuosi šia apžvalga:
https://www.paloaltonetworks.com/cyberpedia/what-is-microsegmentation

Mikrosegmentacija — būdas atskirti darbinius duomenų srautus vieną nuo kito ir kiekvieną iš jų apsaugoti atskirai.

Šis būdas padeda įgyvendinti taip vadinamą (angl.) *Zero Trust* strategiją.

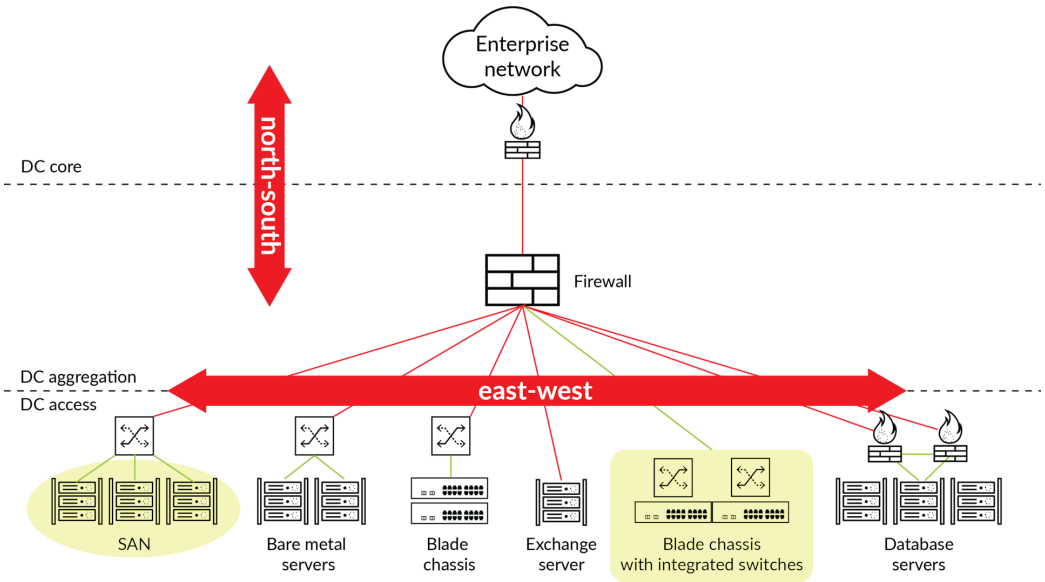
Būdas įgalina:

- sumažinti tinklinių atakų perimetrą,
- padidinti įsilaužimų suvaldymą,
- sustiprinti reglamentinės politikos atitiktį
- ir lengvesnį filtravimo politikų valdymą.

Žiūrint techniškiau, veikia trys pagrindiniai principai:

1. Matomumas

   Mikrosegmentuojant stebimas ne tik srautas Šiaurės-Pietų kryptimi, bet ir srautas Rytų-Vakarų kryptimis. Efektyviam mikrosegmentavimui reikalingas viso tinklo srauto stebėjimas:



2. Kvantuotas saugumas

   Kvantuotas saugumas atsiranda, kai tinklo administratoriai įgalinami identifikuoti itin jautrius duomenų srautus (laike ir tarp sistemų) ir sukurti jiems specifines saugos politikas. Būtent taip, naudojant preciziškumą yra sustabdomas netiesioginiai, slapti kenkėjiški srautai.

3. Dinaminė adaptacija

   Gi dinaminė adaptacija užtikrina, kad minimi principai veikia net itin sparčiai besikeičiančiose šiuolaikinėse skaitmeninėse aplinkose. Mikrosegmentavimo atveju saugumo politikos aprašomos gana abstrakčiomis sąvokomis (pvz. aplikacijų pakopomis, angl. *Tiers*) vietoj žemo lygmens konstruktų (pvz. IP adresų ar transportinių porto numerių). Aplikacijos ar infrastruktūros pokyčiai taikant mikrosegmentavimą įjungia automatinį saugumo politikų revizavimą realiu laiku, ir (tariamai) nebereikalauja žmogiško įsikišimo.