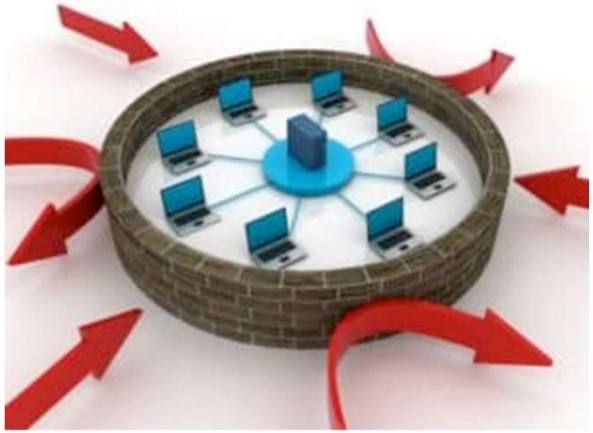
F5 - Implementácia ochrany perimetra

Juraj Nemeček, Alanata a.s.

Alanata
Technology Meets Business

Perimeter



- Čo je dnes možné považovať za perimeter?
  - ? Rozhranie medzi internetom a Vašou sieťou
  - ? Miesto sústredenia Vašich aplikácií
  - ? Prvý bod nasadenia ADC

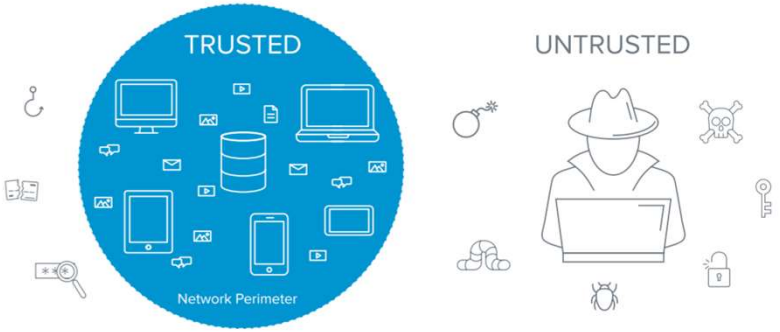
Alanata
Technology Meets Business

Perimeter

- Tradičný perimeter
  - „v nútri“ vs “vonku“
- „Polopriepustný“ perimeter, hybridný perimeter
  - Cloud vs On-prem
  - Work-from-home

Alanata
Technology Meets Business

Perimeter



- Zero-Trust perimeter
  - „kto“, „kam“, “prečo“
- Perimeter mikrosegmentovanej infraštruktúry
  - Tradičný perimeter v novom šate?

Alanata
Technology Meets Business

Nástroje na ochranu perimetra

- Výber správneho nástroja je polovica roboty

- Hľadáme nástroj ktorý:
  - ✓ Rozumie aplikácií
  - ✓ Pozná čo je správne
  - ✓ Pozná čo je zaručene nesprávne
  - ✓ Vie tieto dva extrémy porovnať

Alanata
Technology Meets Business

Nástroje na ochranu perimetra

- ? Firewall
- ? Cloud-native riešenie
- ? Schovám aplikáciu za ZTNA

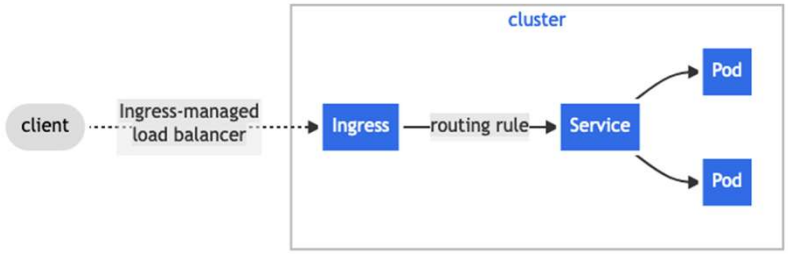
Alanata
Technology Meets Business

Nástroje na ochranu perimetra

- Tradičný, zero-trust a hybridný perimeter
  - WAF - Web application firewall
  - WAAP - Web application and API protection
  - Autonómna bezpečnostná politika
    - Strojové učenie
  - Multicloud

Nástroje na ochranu perimetra

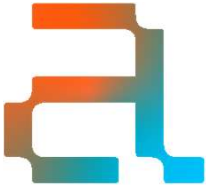
- Mikrosegmentačný perimeter
  - WAF nasadený ako tradičný sieťový perimeter
  - Integrácia WAF cez ingress controller



Alanata
Technology Meets Business

F5

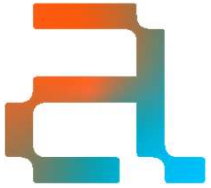
- Nástroje na ochranu perimetra od F5
  - ✓ WAF
    - ✓ BIG-IP
  - ✓ WAAP
    - ✓ F5 XC
    - ✓ NGINX App Protect



Alanata
Technology Meets Business

F5

- Funkcionalita
  - ✓ OWASP TOP 10
  - ✓ Pravidelné aktualizované signatúry, threat intelligence
  - ✓ Možnosť definovať manuálnu a granulárnu bezpečnostnú politiku
  - ✓ Možnosť definovať rámce pre autonómnu bezpečnostnú politiku
  - ✓ Multicloud



Alanata
Technology Meets Business

Case-study nr. 1

- Zákazník z oblasti governmentu
- Výzva
  - Veľké množstvo drobných perimetrov
  - Problém skĺbiť podporu pre väčšie množstvo systémov
  - Rastúci množstvo poskytovaných e-gov služieb
- Riešenie
  - Multidatacentrová konsolidácia na platformu F5 Velos

Alanata
Technology Meets Business

Case-study nr. 1

- Lessons learned
  - ! F5OS umožňuje aj iný pohľad na architektúru siete
  - ! Chassis riešenie vie mať lepší pomer cena/výkon ako appliance
  - ! Pozor na alokáciu RAM podľa počtu CPU
  - ! Pozor na správnu verziu F5OS firmware
  - ! Automatizácia cez AS3 má svoje limity (AWAF, APM)

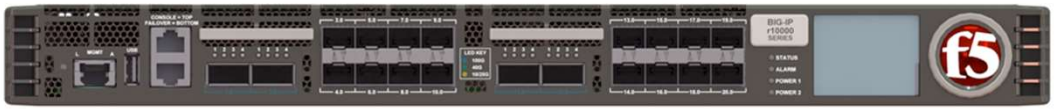
Alanata
Technology Meets Business

Case-study nr. 2

- Komerčný zákazník
- Výzva
  - Výmena perimetrového aj datacentrového WAF
  - Neskoršie uvedenie r-series na trh spôsobilo že bolo stávajúce ADC nutné udržiavať pri živote dlhšie ako bolo pôvodne projektované
  - Zákazník zvažoval úplný prechod na SDN-based datacentrum
- Riešenie
  - Zákazník sa rozhodol zmigrovať riešenie na F5 r-series hardvér

Alanata
Technology Meets Business

Case-study nr. 1



- Lessons learned
  - ! F5OS ma striktnejšie pravidlá na pridelovanie VLAN konkrétnym portom
  - ! Journeys je užitočný, vie za Vás spraviť cca 90% roboty
  - ! S výnimkou zariadení série 2000 majú všetky F5 licenciu na aspoň 2och tenantov
  - ! SFP+ i-series transcievery sú plne podporované aj na r-series
    - ! Požičať SFP+ pre potreby migrácie
  - ! Už najnižšia séria 2000 má na sebe SFP28 porty

Alanata

Technology Meets Business

Alanata a.s.
Einsteinova Business Center
Krasovského 14
851 01 Bratislava 5
Slovenská republika

www.alanata.sk