Príloha P5 Požiadavky na firewall zariadenia

Na základe parametrov uvedených v dokumente v dokumente „Priloha-P3-Popis súčasného stavu.docx“ a „Priloha-P4-Navrh cielového stavu z pohladu obstaravatela.docx“ je navrhované použiť nižšie uvedené zariadenia z portfólia spoločnosti Palo Alto Networks, prípadne iného výrobcu ktorý spĺňa požiadavky definované v uvedených dokumentoch.

*Informácia : Vymenované parametre v tomto článku sa tiež nachádzajú v dokumente “Príloha-P11-Detailne poziadavky.xlsx. V prípade, ak náhodou je hodnota rozdielna (ľubovoľného údaju tu uvedeného), voči “zhodnému” údaju v “Príloha-P11-Detailne poziadavky.xlsx”, tak platí údaj uvedený v “Príloha-P11-Detailne poziadavky.xlsx”. Teda príloha Príloha-P11-Detailne poziadavky.xlsx je* ***mandatórna****.*

* 1. Zónovací FW (FW-AWAN)

Ako zónovací firewall pre administratívne siete sa požaduje naceniť:

Tab1. FW-AWAN

|  |  |
| --- | --- |
| počet | položka |
| 2 | Palo Alto Networks PA-3430 with redundant AC power supplies |
| 2 | Palo Alto Networks PA-3400 Series 4 post rack mount kit |
| 2 | PA-3430, Core Security Subscription Bundle (Advanced Threat Prevention, Advanced URL Filtering, Advanced Wildfire, DNS Security and SD-WAN) |
| 2 | PA-3430, GlobalProtect subscription |

Alternatívne je možné pre tento firewall ponúknuť iné ekvivalenté zariadenie spĺňajúce nasledovné technické parametre:

* Priepustnosť FW (appmix) App-ID: 29Gbps
* Priepustnosť FW Threat Prevention: 15Gbps
* Počet súčasných spojení: 3M
* Počet nových spojení za sekundu (CPS): 268k
* Podpora bezpečnostných mechanizmov:
  + ekvivalent Advanced Threat Prevention
  + ekvivalent Advanced WildFire
  + ekvivalent Advanced URL Filtering
  + ekvivalent DNS Security
  + ekvivalent GlobalProtect
* Sieťové rozhrania:
* 12x 1G/2.5G/5G/10G
* 10x 1G/10G SFP/SFP+
* 4x 25G SFP28
* 2x 40G/100G QSFP/QSFP28
  1. Technologický FW (FW-TWAN)

Ako technologický firewall pre technologické WAN siete sa požaduje naceniť:

Tab.2: FW TWAN

|  |  |
| --- | --- |
| počet | položka |
| 3 | Palo Alto Networks PA-1420 with redundant AC power supplies |
| 3 | Palo Alto Networks 4-Post rack mount kit for 1U PA-1400 |
| 3 | PA-1420, Advanced Threat Prevention |
| 3 | PA-1420, DNS security subscription |
| 3 | PA-1420, IoT subscription - optional |
| 3 | Virtual systems upgrade - Additional 5 virtual systems for PA-1410 |

Alternatívne je možné pre tento firewall ponúknuť iné ekvivalenté zariadenie spĺňajúce nasledovné technické parametre:

* Priepustnosť FW (appmix) App-ID: 9,5Gbps
* Priepustnosť FW Threat Prevention: 5,8Gbps
* Počet súčasných spojení: 1,4M
* Počet nových spojení za sekundu (CPS): 140k
* podpora bezpečnostných mechanizmov:
  + ekvivalent Advanced Threat Prevention
  + ekvivalent DNS Security
  + voliteľné ekvivalent IoT Security
* Sieťové rozhrania:

## 4x 10/100/1000

## 4x 1G/2.5G/5G

## 4x 1G/2.5G/5G (4)/PoE

## 2x 1G SFP

## 8x 1G/10G SFP/SFP+

* 1. Primárne Datacentrum FW (FW-DC-ZAX/VAT)

Pre primárné DC v Žiline a Varíne sa požaduje naceniť:

Tab.3: FW DC ZAX/VAT

|  |  |
| --- | --- |
| počet | položka |
| 2 | Palo Alto Networks PA-3430 with redundant AC power supplies |
| 2 | Palo Alto Networks PA-3400 Series 4 post rack mount kit |
| 2 | PA-3430, Advanced Threat Prevention |
| 2 | PA-3430, DNS security subscription |
| 2 | Virtual systems upgrade - Additional 10 virtual systems (1 to 11) for PA-3430 |

Alternatívne je možné pre tento firewall ponúknuť iné ekvivalenté zariadenie spĺňajúce nasledovné technické parametre:

* Priepustnosť FW (appmix) App-ID: 29Gbps
* Priepustnosť FW Threat Prevention: 15Gbps
* Počet súčasných spojení: 3M
* Počet nových spojení za sekundu (CPS): 268k
* podpora bezpečnostných mechanizmov:
  + ekvivalent Advanced Threat Prevention
  + ekvivalent DNS Security
* Sieťové rozhrania:

## 12x 1G/2.5G/5G/10G

## 10x 1G/10G SFP/SFP+

## 4x 25G SFP28

## 2x 40G/100G QSFP/QSFP28

* 1. Sekundárne Datacentrum FW (FW -DC-BBX)

Alternatíva 1

Záložné DC v Banskej Bystrici je z dôvodu menšieho vyťaženia navrhované pokryť virtuálnou edíciou firewallov vo vysokej dostupnosti. Každý virtuálny firewall bude obsahovať 4 vCPU, pričom približná priepustnosť je 1GBps na 1vCPU v závislosti od použitých CPU. Rovnako ako v DC v Žiline a Varíne je navrhované použiť Advanced Threat Prevention a DNS Security.

Pre sekundárne DC v Banskej Bystrici sa požaduje naceniť:

Tab.4.1: FW DC BBX virtual

|  |  |
| --- | --- |
| počet | položka |
| 49 | Software NGFW Credit (2x FW, 4vCPU, DNS, ATP) |

Alternatívne je možné pre tento firewall ponúknuť iné ekvivalenté zariadenie spĺňajúce nasledovné technické parametre:

* Virtualizovaný firewall v HA móde
* 4vCPU
* sieťová priepustnosť 1GBps na 1vCPU
* podpora bezpečnostných mechanizmov:
  + ekvivalent Advanced Threat Prevention
  + ekvivalent DNS Security

Alternatíva 2

Tab.4.2: FW DC BBX fyz appliance

|  |  |
| --- | --- |
| počet | položka |
| 2 | Palo Alto Networks PA-1420 with redundant AC power supplies |
| 2 | Palo Alto Networks 4-Post rack mount kit for 1U PA-1400 |
| 2 | PA-1420, Advanced Threat Prevention |
| 2 | PA-1420, DNS security subscription |

Alternatívne je možné pre tento firewall ponúknuť iné ekvivalenté zariadenie spĺňajúce nasledovné technické parametre:

* Priepustnosť FW (appmix) App-ID: 9,5Gbps
* Priepustnosť FW Threat Prevention: 5,8Gbps
* Počet súčasných spojení: 1,4M
* Počet nových spojení za sekundu (CPS): 140k
* podpora bezpečnostných mechanizmov:
  + ekvivalent Advanced Threat Prevention
  + ekvivalent DNS Security
* Sieťové rozhrania:
* 4x 10/100/1000
* 4x 1G/2.5G/5G
* 4x 1G/2.5G/5G (4)/PoE
* 2x 1G SFP
* 8x 1G/10G SFP/SFP+
  1. OutOfBand FW (FW-OOB)

Pre OutOfBand firewall OOB FW sa požaduje naceniť:

Tab.5: FW OOB

|  |  |
| --- | --- |
| počet | položka |
| 3 | Palo Alto Networks PA-415 |
| 3 | Rack mountable tray for up to two PA-400s and 4 power adapters for a 4 post rack mount (PA-440/450/460 models only) |
| 3 | 50W AC power adapter for PA-440, PA-450 and PA-460 |
| 3 | PA-415, Advanced Threat |
| 3 | PA-415, DNS security subscription |

Alternatívne je možné pre tento firewall ponúknuť iné ekvivalenté zariadenie spĺňajúce nasledovné technické parametre:

* Priepustnosť FW (appmix) App-ID: 1,2Gbps
* Priepustnosť FW Threat Prevention: 0,6Gbps
* VPN spojení: 250
* podpora bezpečnostných mechanizmov:
  + ekvivalent Advanced Threat Prevention
  + ekvivalent DNS Security
* Sieťové rozhrania:

## 1x 1G SFP/RJ45 combo

## 4x 1G RJ45 (4)

## 4x 1G RJ45/PoE (4)

* 1. Console FW (FW-CON)

Pre Console firewall FW-CON sa požaduje naceniť:

Tab.6: FW CON

|  |  |
| --- | --- |
| počet | položka |
| 3 | Palo Alto Networks PA-415-5G |
| 3 | Rack mountable tray for up to two PA-400s and 4 power adapters for a 4 post rack mount (PA-440/450/460 models only) |
| 3 | 50W AC power adapter for PA-440, PA-450 and PA-460 |
| 3 | PA-415, GlobalProtect subscription |

Rovnako ako pre OOB FW je pre Console FW je navrhované použiť menšie zariadenia v tomto prípade ale tieto navyše disponujú 5G/LTE pripojením. 5G/LTE pripojenie je plnánované použiť ako záložné pripojenie ku konzole v prípade zlyhania pripojenia cez primárnu linku. Navrhované zariadenie PA-415-5G má nasledovné parametre:

Alternatívne je možné pre tento firewall ponúknuť iné ekvivalenté zariadenie spĺňajúce nasledovné technické parametre:

* Priepustnosť FW (appmix) App-ID: 1,2Gbps
* Priepustnosť FW Threat Prevention: 0,6Gbps
* VPN spojení: 250
* integrovaný 5G modem
* podpora bezpečnostných mechanizmov:
  + ekvivalent Global Protect
* Sieťové rozhrania:

## 1x 1G SFP/RJ45 combo

## 4x 1G RJ45

## 4x 1G RJ45/PoE

* 1. VPN koncentrátor (FW-EVPN)

Pre vpn koncentrátor FW-EVPN sa požaduje naceniť:

Tab.7: FW-EVPN

|  |  |
| --- | --- |
| počet | položka |
| 2 | Palo Alto Networks PA-1420 with redundant AC power supplies |
| 2 | Palo Alto Networks 4-Post rack mount kit for 1U PA-1400 |
| 2 | PA-1420, GlobalProtect subscription |

Alternatívne je možné pre tento firewall ponúknuť iné ekvivalenté zariadenie spĺňajúce nasledovné technické parametre:

* Priepustnosť FW (appmix) App-ID: 9,5Gbps
* Priepustnosť FW Threat Prevention: 5,8Gbps
* Počet súčasných spojení: 1,4M
* Počet nových spojení za sekundu (CPS): 140k
* VPN client spojení: 1500
* VPN clientless spojení: 200
* podpora bezpečnostných mechanizmov:
  + ekvivalent Global Protect
* Sieťové rozhrania:

## 4x 10/100/1000

## 4x 1G/2.5G/5G

## 4x 1G/2.5G/5G (4)/PoE

## 2x 1G SFP

## 8x 1G/10G SFP/SFP+

* 1. FW Cloud Native Workload (FW-Cloud-Native)

Pre Cloud Native Workload sa požaduje naceniť:

Tab.8: FW Cloud Native

|  |  |
| --- | --- |
| počet | Položka |
| 22 | Software CNFW Credit (1x FW, 2vCPU, TP, DNS) - optional |

Alternatívne je možné pre tento firewall ponúknuť iné ekvivalenté zariadenie spĺňajúce nasledovné technické parametre:

* Virtualizovaný firewall pre Cloud Native workload (Kubernetes)
* 2vCPU
* sieťová priepustnosť 1GBps na 1vCPU
* podpora bezpečnostných mechanizmov:
  + ekvivalent Advanced Threat Prevention
  + ekvivalent DNS Security

*Poznámka: 1x CNFW (22 kreditov) je potrebné pre každý Node v Kubernetes clusteri. Pre 3 nodový cluster je potrebné 3x 22 kreditov.*

* 1. Management FW

Pre Management FW sa požaduje naceniť:

Tab.9: FW Management

|  |  |
| --- | --- |
| počet | Položka |
| 2 | Panorama pre virtualizované prostredie VMware ESXi |

Alternatívne je možné pre tento management ponúknuť iné ekvivalenté zariadenie spĺňajúce nasledovné technické parametre:

* Virtualizovaný management v HA móde
* Log management v HA móde – uvedený produkt môže byt kombináciou management a zároveň log kolektor
* Diskový priestor 2TB pre uchovávanie log súborov
  1. Sieťové moduly SFP, QSFP

Pre sieťové moduly sa požaduje naceniť:

Tab.10: Sieťové moduly

|  |  |
| --- | --- |
| počet | Položka |
| 60 | SFP+ form factor, SR 10Gb optical transceiver, short reach 300m, OM3 MMF, duplex LC, IEEE 802.3ae 10GBASE-SR compliant |
| 6 | QSFP+ form factor, 40Gb Bidirectional optical transceiver, 100m reach over OM3 MMF, 150m over OM4 MMF, duplex LC |
| 6 | Fiber optic breakout cable for QSFP+ and QSFP28 applications, 2m, OM4, single MPO to 4 x LC pairs |

1. Sumarizácia

Uvedené zariadenia a prislúchajúce vlastnosti v podobe subskripcií a licencií je požadované dodať na základe zistení v rozdieloch medzi aktuálnym a požadovaným stavom FW bezpečnostného riešenia v SSD. Popis jednotlivých cieľových vlastnosti pre jednotlivé FW je definovaný v kapitolách vyššie.

1. Podpora pre FW riešenie

Pre zadané FW riešenie je požadované dodať podporu na dodané riešenie zo strany výrobcu na 5 rokov. Požadovaná verzia je Premium support 24/7. Pre dosiahnutie maximálnej dostupnosti poskytovaných služieb v sieti SSD je požadované dodanie cold stand-by zariadení tak aby z každého typu použitého zriadenia v sieti SSD bol k dispozícii jeden cold stand-by kus. V prípade použitia RMA procesu je požadované aby bolo možné ponechať cold stand-by zariadenie v produkcii a RMA zariadenie sa stalo novým cold stand-by kusom.