Príloha P3 Opis súčasného stavu

 Bezpečnostná sieťová infraštruktúra v prostredí SSD je pomerne komplexná, vznikla budovaním a integráciou rôznych infraštruktúr, služieb a aplikácií. Návrh nového riešenia musí do budúcna poskytovať moderné technológie pre zabezpečenie organizácie a zároveň zjednodušenie práce administrátorov. Zároveň nové riešenie musí poskytovať flexibilitu pre rast a potenciálnu zmenu architektúry do budúcna. Rovnako nové riešenie musí zabezpečiť oddelenie technologických a administratívnych sietí na fyzicky oddelených zariadeniach.

1. Základné členenie infraštruktúry obstarávateľa

Infraštruktúra obstarávateľa je z pohľadu tohto dokumentu možné členiť na nasledujúce logické funkčné bloky:

* DMZ – oddeľuje Internet od ostatných funkčných blokov
* AWAN – sieť pre administratívnych používateľov
* BLACK – backbone prepájajúci všetky funkčné bloky medzi sebou
* DataCentrum (DC) – poskytuje štandardné IT služby. Ďalej sa člení na oddelene zóny Frontend a Backend
* TWAN – sieť obsahujúca zariadenia typu IoT/OT
* IBS – sieť obsahujúca prvky poskytujúce objektovú bezpečnosť
* OOB – oddelenia sieť pre správu ostatných IT zariadení a sieťovej infraštruktúry
* EVPN – časť siete v ktorej sú ukončené Remote Access prístupy zamestnávateľov, dodávateľov a iných tretích strán

Predmetom obnovy zariadení v tomto obstarávaní sú technológie a systémy nachádzajúce sa v blokoch AWAN, DC, TWAN, IBS, OOB a EVPN. Infraštruktúra v zónach DMZ a BLACK ostáva v rámci implementácie riešenia tohto obstarávania nezmenená.

1. Zónovací FW (FW-WAN)

Centrálne zónovacie firewall-y FW-WAN (ZAX,VAT,BBX), ktoré sú geograficky inštalované v lokalitách Žilina, Varín, Banská Bystrica-Bánoš, poskytujú segmentáciu siete a bezpečnostné funkcie.

Pre lokality Žilina, Varín sa jedná sa o Fortigate 1500D a obsahuje 3 virtuálne systémy tzv. VDOMy:

* TWAN - Technologická sieť
* IBS - Integrovaný bezpečnostný systém
* AWAN - Administratívna WAN

Režim vysokej dostupnosti je riešený prostredníctvom dynamického routovacieho protokolu BGP pomocou ktorého je riešené preklápanie prevádzky medzi jednotlivými lokalitami Na zariadeniach v lokalite Žilina a Varín je zapnutá session synchronization, čo umožňuje online synchronizáciu aktívnych spojení.

Na zariadeniach FW-WAN je nakonfigurovaný dynamický smerovací protokol eBGP, ktorý zabezpečuje vzájomné prepojenie všetkých NET-zón ukončených na firewalle ako je znázornené na sieťovej topológii viď obr. 1.

Na základe analýzy aktuálneho zaťaženia tohto zariadenia bolo zistené nasledovné:

Tab1. FW-AWAN

|  |  |  |
| --- | --- | --- |
| **Utilizácia** | **priemer** | **peak** |
| CPU  | 20% | 40% |
| Sieťová priepustnosť | 5Gbps | 10Gbps |
| Počet spojení | 150k | 200k |
| Počet nových spojení | 300cps | 1300cps |
| log sprav za sekundu | 500 | n/a |

Pre lokalitu Banská Bystrica - Bánoš sa jedná sa o Fortigate 1000D a obsahuje 4 virtuálne systémy tzv. VDOMy:

* TWAN - Technologická sieť
* IBS - Integrovaný bezpečnostný systém
* AWAN - Administratívna WAN
* Frontend DC-BBX

Okrem WAN prostredia daný firewall riadi prístup k službám v DC3, v ktorom sa nachádzajú kritické služby ako AAA,AD,NTP, atď.

1. Datacentrum FW (FW-DC)

Firewally, ktoré oddeľujú komunikáciu Dátového Centra od zvyšku siete sú, rovnako ako Zónovacie FW, postavené na technológii Fortinet.

Dátové centrá lokalizované v Žiline a Varíne sú zabezpečené zariadením Fortigate 1500D. Tieto sú zapojené v režime vysokej dostupnosti v móde Active-Standby. Na FW-DC umiestnených v týchto lokalitách sú nakonfigurované dva virtuálne VDOMy (Frontend, Backend). Pri štandardnej prevádzke je každý VDOM aktívny v inom dátovom centre.

FW-DC VDOMy:

* Frontend DC – (Všetky služby DC užívateľ vs server, server vs server)
* Backend DC – (izolovaná VRF, slúži na komunikáciu server vs server – Tento koncept je platný len pre existujúce systémy ktoré nemôžu byť migrované iba na Frontend komunikáciu. Nové servery sa umiestňujú výhradne len do Frontend DC)

Na základe analýzy aktuálneho zaťaženia firewallov primárneho DC (FW-DC-ZAX) bolo zistené nasledovné:

Tab2. FW-DC-ZAX

|  |  |  |
| --- | --- | --- |
|  Utilizácia | priemer | peak |
| CPU  | 20% | 40% |
| Sieťová priepustnosť | 5Gbps | 15Gbps |
| Počet spojení | 100k | 150k |
| Počet nových spojení | 800cps | 1300cps |
| log sprav za sekundu | 600 | n/a |

Na základe analýzy aktuálneho zaťaženia firewallov primárneho DC (FW-DC-VAT) bolo zistené nasledovné:

Tab3. FW-DC-VAT

|  |  |  |
| --- | --- | --- |
| **Utilizácia** | **priemer** | **peak** |
| CPU  | 10% | 30% |
| Sieťová priepustnosť | 0,5Gbps | 3Gbps |
| Počet spojení | 10k | 16k |
| Počet nových spojení | 10cps | 100cps |
| log sprav za sekundu | 30 | n/a |

Záložné dátové centrum v Banskej Bystrici je pripojené prostredníctvom zariadenia Fortigate 1000D, ktoré je označené ako FW-WAN-BBX.

Na základe analýzy aktuálneho zaťaženia firewallov záložného DC (FW-WAN-BBX) bolo zistené nasledovné:

Tab4. FW-WAN-BBX

|  |  |  |
| --- | --- | --- |
| **Utilizácia** | **priemer** | **peak** |
| CPU  | 10% | 30% |
| Sieťová priepustnosť | 2Gbps | 3,6Gps |
| Počet spojení | 9k | 17k |
| Počet nových spojení | 60cps | 266cps |
| log sprav za sekundu | 10 | n/a |

1. VPN koncentrátor (EVPN)

VPN koncentrátor je prevádzkovaný na dvojici zariadení Cisco ASA FirePower 2110, ktoré sú zapojené v režime vysokej dostupnosti v móde Active-Standby, umiestnených v lokalitách Žilina a Varín. VPN slúži pre pripojenie interných zamestnancov pracujúcich mimo infraštruktúry SSEH, ktorí sa pripájajú pomocou VPN klienta Cisco Any Connect. Pripojenie do užívateľskej VPN je podmienené pozitívnym výsledkom kontroly compliance zariadenia (hostscan).

Externý interface EVPN koncentrátorov je pripojený voči pertimetrickému firewallu, smerovanie je zabezpečené statickou routou. Interný interface VPN koncentrátora je pripojený voči vnútorným zónovacím firewallom. Smerovanie je zabezpečené dynamickým routingom eBGP.

Na základe analýzy aktuálneho zaťaženia VPN koncentrátora boli zistené nasledujúce údaje:

Tab4. FW-EVPN

|  |  |  |
| --- | --- | --- |
| **Utilizácia** | **priemer** | **peak** |
| CPU  | 24% | 38% |
| Sieťová priepustnosť | 100Mbps | 275Mbps |
| Počet aktívnych spojení | 7k | 18k |
| Max počet súčasných VPN spojení | 350 | n/a |
| log sprav za sekundu | 5 | n/a |

1. Out-Of-Band FW (FW-OOB)

Firewally OOB sú prevádzkované na technológii od spoločnosti Cisco ASA 5516X. Jedná sa o FW, ktoré slúžia na oddelenie a riadenie prevádzky určenej pre Out-of-Band manažment zariadení a terminálov umiestnených v DC.

Zároveň slúžia ako VPN koncentrátor pre riadenie privilegovaných užívateľov pripájajúcich sa do OOB a DC net-zón.

* Net-oblasť OOB slúži na správu a monitorovanie IS. Je fyzicky a aj logicky oddelená od produkčnej komunikácie a prevádzkovaná na samostatnej sieťovej infraštruktúre.
* Prístup do OOB siete je riadený pomocou pravidiel definovaných na OOB bezpečnostnej infraštruktúre.
* OOB je vybudovaná v troch lokalitách, kde lokality ZAX a VAT sú vzájomne prepojené na L2 úrovni a lokalita BBX je úplne samostatná, t.j. L3 oddelená.
* Samostatnou súčasťou Net-oblasti OOB je Net-skupina Console-Net, do ktorej sú pripojené Console porty sieťových a bezpečnostných prvkov.

Na základe analýzy aktuálneho zaťaženia OOB firewallu boli zistené nasledujúce údaje:

|  |  |  |
| --- | --- | --- |
| **Utilizácia** | **priemer** | **peak** |
| CPU  | 7% | 30% |
| Sieťová priepustnosť | 15Mbps | 300Mbps |
| Počet aktívnych spojení | 6k | 8k |
| Max počet súčasných VPN spojení | 45 | n/a |
| log sprav za sekundu | 13 | n/a |

1. FW Management

Management zónovacích a datacentrových firewallov je centralizovaný, jedná sa o produkt Fortimanager, pričom obsahuje aj licenciu Fortianalyzer. Inštalácia je realizovaná ako jednonodová a beží na virtualizovanej platforme. Licencovaný diskový priestor je 200 GB a retencia logov je momentálne približne 30 dní.

Management OOB a VPN FW nie je centralizovaný a jedná sa o ASDM prípadne CLI. Všetky firewally sú prepojené na systém SIEM, kde formou syslog správ preposielajú všetky relevantné logy.

1. Net Oblasť BLACK (Core/Backbone)

Net-oblasť BLACK primárne slúži na prepojenie všetkých Net-oblastí v rámci IP siete Net-SSE. BLACK je komunikačné jadro, ktorého primárnou funkciou je poskytovanie optimalizovanej a spoľahlivej transportnej štruktúry.

Priamo do Net-oblasti BLACK sú pripojené len sieťové a bezpečnostné prvky.

Net-oblasť BLACK je dizajnovaná na zabezpečenie vysokej dostupnosť a spoľahlivosti komunikácie. Z hľadiska bezpečnostného členenia Net-SSE, net-oblasť BLACK ako jediná obsahuje informácie o všetkých smerovacích informáciách existujúcich v rámci Net-SSE.

Routovacie informácie sú zabezpečené prostredníctvom statického alebo dynamického routovacieho protokolu (BGP), v závislosti od preferovaného spôsobu prepojenia sieťových/bezpečnostných prvkov.

1. Súčasná schéma zapojenia:



Obr.1 Logická schéma zapojenia