Príloha P4 Návrh cieľového stavu z pohľadu obstarávateľa

1. Navrhovaný cieľový stav

Cieľom projektu je obnova časti bezpečnostnej infraštruktúry pozostávajúcej primárne z firewall riešenia, ktorého väčšia časť ku koncu roku 2025 dosiahne koniec životného cyklu EOL. Cieľom je vytvorenie moderného riešenia, ktoré bude efektívne mitigovať aktuálne a budúce bezpečnostné hrozby, je možné ho jednoducho spravovať a bude flexibilne reagovať na meniace sa požiadavky SSD.

V súčasnej prevádzke je používaných viacero firewallových systémov ktoré je potrebné nahradiť, či už z dôvodu nedostatočnej funkčnosti alebo ukončenia podpory výrobcom na dané zariadenia. Tieto sú uvedené nižšie:

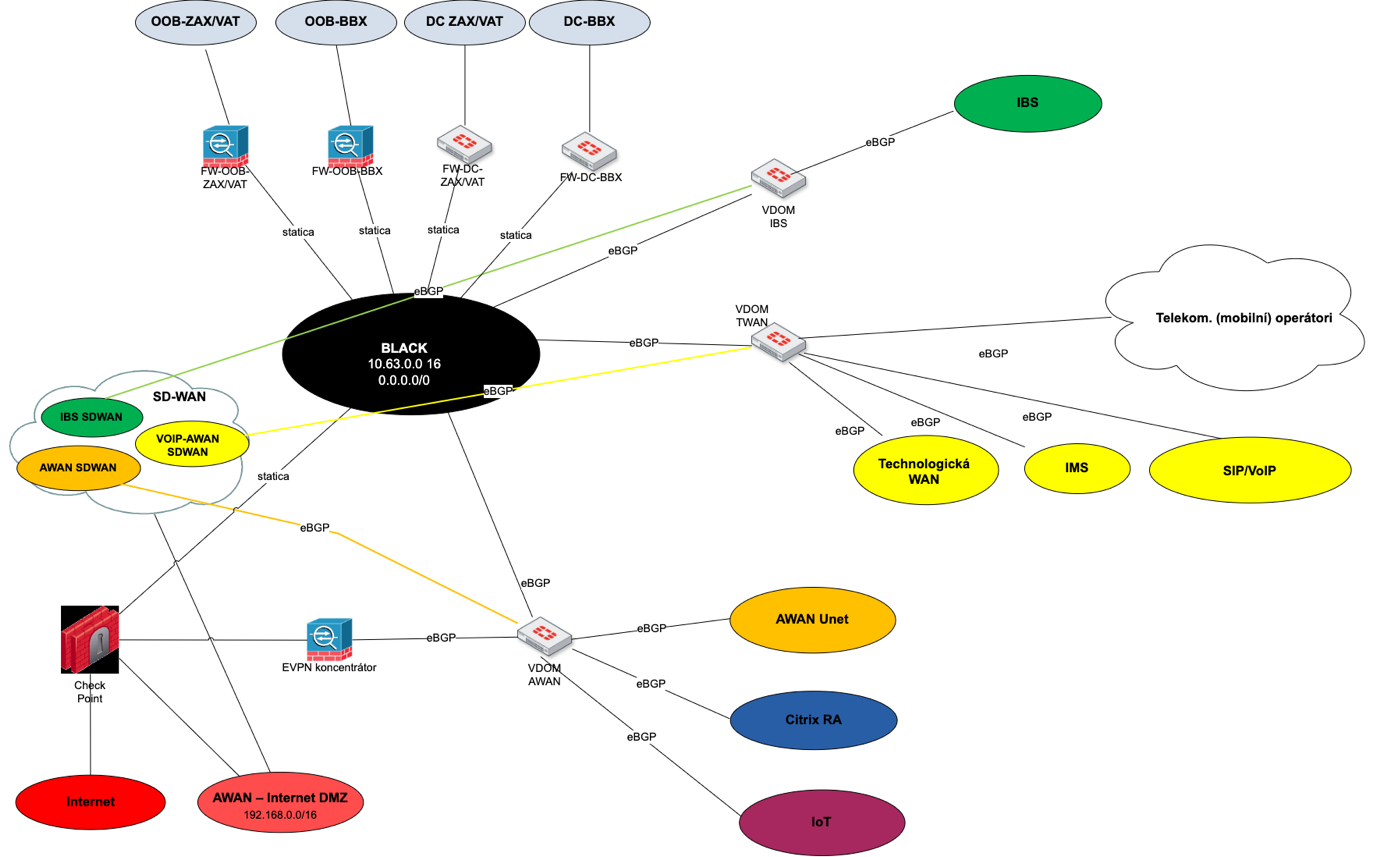
* Check Point firewall na perimetri => **zachovať**
* Fortinet zónovací FW => **nahradiť**
* Fortinet DataCenter FW => **nahradiť**
* Cisco Firepower 2100 VPN koncentrátor => **nahradiť**
* Cisco ASA OOB MGMT => **nahradiť**
* Fallback Console VPN **= doplniť**

1. Schémy zapojenia

A diagram of a computer network

Description automatically generated

Obr.1 Navrhovaná logická schéma zapojenia

Obr.2 Pôvodná logická schéma zapojenia

1. High-Level požiadavky na riešenie

Cieľom nižšie uvedených požiadaviek je modernizácia firewallového riešenia, tak aby bolo možné dané prostredie efektívne spravovať, získať viditeľnosť v sieťovom a bezpečnostnom prostredí a pružne s minimálnym úsilím reagovať na nové a existujúce hrozby.

* 1. Automatizácia konfigurácie
* Možnosť správy riešenia pomocou automatizačných nástrojov ako sú Terraform, Ansible, Script
* Možnosť integrácie s helpdeskovým systémom Jira, kedy ticket obsahujúci komunikačnú maticu automaticky aplikuje požadovanú bezpečnostnú politiku na FW a iné
* Vytváranie pravidiel cez viacero FW
* Automatizovaná optimalizácia pravidiel pomocou AI
* Možnosť napojenia sa na SOAR – toto by malo umožniť automaticky aplikovanie opatrení na bezpečnostné incidenty
  1. ZTNA 2.0
* Možnosť aplikovania Zero Trust Network Access (ZTNA) v sieti SSD, ktorá umožňuje konfiguráciu bezpečnostných politík na základe konkrétnych používateľov a ich členstva v AD skupinách, čo umožňuje konzistentné pravidlá prístupu, či už pri prístupe z internej siete alebo vzdialeného prístupu.
* Možnosť definovať pravidlá pomocou tzv. Device Posture Check, kde nespĺňajúce koncové body majú obmedzený sieťový prístup. Poskytuje kontinuálne vyhodnocovanie bezpečnostnej politiky na klientovi, umožňujúc tak real-time Zero Trust Network Access.
* Možnosť aplikovania transparentnej správy prístupu k privilegovaným aplikáciám a službám v sieti pomocou Multi-Factor Autentifikácie (MFA).
* Podporuje nasadenie na hlavných platformách vrátane Windows, macOS, Linux, Android a iOS.
* Identita používateľov bude redistribuovaná na všetky dotknuté FW v prostredí.

**User/Remote Access/ZTNA**

* Jednotný zdroj používateľských identít - možnosť používania viacerých súčasných zdrojov identít (AD, EntraID, RADIUS) a následne aplikovanie bezpečnostnej politiky
* Unifikovaná autentifikácia používateľov pre prístup z vnútra aj vonku siete
* Host based policy
* Redistribúcia identít
* Jednotný sieťový prístup VPN/onsite
  1. Zjednodušenie sieťovej infraštruktúry
* Plánovaná výmena OOB/TWAN firewallov by mala umožniť zjednodušenie prístupu pre privilegovaných používateľov bez potreby pripojenia sa do internej OOB alebo TWAN VPN, pričom je zachovaná 2FA autentizácia.
* Navrhované riešenie umožňuje konsolidáciu všetkých VPN prístupov do jedného riešenia, vrátane prístupu tretích strán, nahrádzajúc tak doterajšie Check Point VPN, okrem site-to-site VPN.
* Proxy server: Možnosť eliminovať nutnosť proxy servera v sieti, ktorý spôsoboval problémy pre rôzne moderné aplikácie. Odstránenie proxy z komunikácie zjednoduší sieťovú topológiu a odstráni potrebu konfigurovania výnimiek pre rôzne aplikácie. Moderné bezpečnostné riešenia dokážu plnohodnotne nahradiť proxy servery a prebrať ich kompletnú funkcionalitu bez nutnosti ďalších komponentov v sieti. Umožňujú tak získať vlastnosti Secure Web Gateway (SWG) bez nutnosti HTTP Proxy. Eliminácia proxy servera v sieti je možná, avšak nie nutná alternatíva, bude potrebné preveriť dopad na celkovú sieťovú a bezpečnostnú architektúru, špeciálne DMZ segment.
  1. Vyššia robustnosť a flexibilita

Nakoľko sa v návrhu počíta s rozdelením firewallov určených pre ochranu administratívnych a technologických sietí, táto zmena umožní väčšiu flexibilitu v prípade nutnosti odstávky a rovnako zníži riziko výpadku technologických sietí. V tomto prípade je nutné aby firewally umožňovali tzv. “session synchronization” medzi jednotlivými nodmi.

Riešenie voliteľne počíta s tým, že v prípade zásadnej potreby zvýšenia výkonu, napr. potreba SSL offloadingu na FW, bude možné rozšíriť FW o ďalší box, ktorý bude tvoriť jeden logický prvok. Pre dosiahnutie vlastnosti jediného logického prvku bude potrebné použiť externý load-balancer mechanizmus. Loadbalancer nie je súčasťou dodávky.

* 1. Zvýšenie celkového zabezpečenia siete

Aplikácia bezpečnostných mechanizmov ako Threat Prevention, DNS Security, URL filtering a Sandboxing na kritické NGFW komponenty umožní aplikovanie unifikovanej bezpečnostnej politiky bez nutnosti výnimiek. Moderný prístup k sieti, aplikáciám a koncovým staniciam na siedmej vrstve (L7) pomocou technológií identifikácie používateľa a nie IP, identifikácie aplikácie a nie TCP portu, identifikácia a viditeľnosť do prenášaného obsahu spolu s identifikáciou zariadení v sieti, či už Enterprise alebo IoT/OT umožnia definovanie bezpečnostnej politiky pre potreby moderných riešení.

**Bezpečnostné vlastnosti**

* IPS/Threat Prevention
* Vizibilita do šifrovanej komunikácie
* Identifikácia aplikácií na L7
* IoT Security
* DNS Security
* AV Sandbox
  1. Viditeľnosť a unifikácia v sieťovom prostredí
* Riešenie musí umožniť nastavenie prístupu pre systémy v DC na základe URL/Domén a dešifrovanie SSL/TLS komunikácie pre administratívne siete umožní lepšiu viditeľnosť do sieťovej komunikácie a jej obsahu.
* Prechod od definovania bezpečnostných pravidiel na L4 úrovni k povoľovaniu konkrétnych aplikácií a definovanie prístupu na základe skutočného autentifikovaného používateľa sprehľadní sieťovú a bezpečnostnú architektúru.
  1. Zabezpečenie Cloud Native workloadov
* Navrhované riešenie musí umožniť flexibilne aplikovať bezpečnostnú politiku v Cloud Native aplikáciách (bežiacich v Kubernetes) rovnako ako pre tradičné sieťové prostriedky, pomocou NGFW nasadených natívne ako kontajnery do kontajnerového prostredia (Kubernetes), ktoré budú riadené centrálne.
  1. IoT/OT Security

Pre systémy technologických sietí je by malo umožniť zabezpečiť a zvýšiť viditeľnosť do daných sietí pomocou dedikovaného riešenia IoT security. Toto riešenie by malo zabezpečiť kompletnú viditeľnosť na existujúcej NGFW platforme len za pomoci aktivácie IoT licencie. Primárne je navrhované zabezpečenie technologickej siete, avšak je možné ho bez akejkoľvek zmeny v sieťovej topológii rozšíriť aj do ostatných sieťových segmentov len pomocou aktivácie licencie.

* 1. Centrálny management

Centralizovaný management - musí mať možnosť spravovať a konfigurovať všetky firewally z jedného miesta, čo by malo množiť jednoducho distribuovať a uplatniť bezpečnostnú politiku napriek všetkým FW. Toto umožní, že bezpečnostná politika je konzistentná na všetkých miestach siete.

**Konsolidácia bezpečnostnej politiky**

* Centralizácia bezpečnosti pri prístupe do internetu pre používateľov a serverové systémy
* Možnosť odstránenia používania explicitných http proxy systémov
* Fyzické oddelenie systémov, ktoré chránia administratívnu a technologickú sieť