# 12 Implementace Webového aplikačního firewallu a Loadbalanceru

## Technická a implementační specifikace Loadbalancer (Reverzní proxy)

### Popis požadovaného řešení

Požadujeme HW zařízení pro roli Reverzní proxy server a loadbalancer (Application Delivery Controller – ADC). Dvojice HW zařízení ADC bude publikovat definované služby a oddělovat reálné servery od přistupujících uživatelů. Zařízení ADC bude realizovat funkci řízení aplikačního provozu a požadujeme, aby splňovalo požadavky uvedené v kapitole Technická specifikace zařízení a funkcí ADC.

Řešení bude koncipované jako redundantní a vysoce dostupný cluster ADC a bude fungovat v režimu Active-Active nebo Active-Standby. ADC řešení bude odpovědné za monitoring dostupných aplikací služeb, řízení distribuce a zátěže aplikačního provozu mezi servery, které budou jednotlivé aplikace a služby poskytovat. Řešení bude také zodpovědné za optimalizaci a modifikaci aplikačního provozu s cílem efektivně využívat zdroje aplikace nebo zamezit nežádoucí distribuci dat k uživatelům (např. manipulace s HTTP záhlavím, HTML kódem apod. šifrování cookies apod.). Řešení bude také zodpovědné za optimalizaci TCP provozu, HTTP kompresi a související optimalizaci aplikačního provozu.

Implementaci politik a pravidel pro řízení aplikačního předpokládáme minimálně v rozsahu:

* Zapojení a integrace v prostředí Zákazníka
* Vytvoření HA clusteru
* Monitoring zdraví aplikací a služeb
* SSL terminace, management SSL certifikátů
* Napojení na monitorovací a logovací nástroje
* Reverzní proxy s funkcí NAT44, případně NAT 46, NAT 64
* Optimalizace HTTP provozu (HTTP komprese)
* Zabezpečení HTTP provozu (cookies, manipulace s HTTP záhlavím apod.)

### Technická specifikace zařízení a funkcí ADC

| *Požadavek na funkcionalitu* | *Způsob prokázání splnění:* | *Splněno: [ANO / NE / hodnota]* |
| --- | --- | --- |
| 2 ks HW zařízení s montáží do technologické 19" skříně (RACK), max. 2U |  |  |
| Plně redundantní napájecí zdroje AC vyměnitelné za provozu |  |  |
| Požadujeme min. 6x 1Gbps slotů pro Ethernet rozhraní typu SFP a zároveň min. 4 x 10 Gbps slotů pro Ethernet rozhraní typu SFP+. Případné transceivery SFP či SFP+ či další kabeláž pro obě strany připojení jsou součástí dodávky. |  |  |
| Lights-out management - nezávislý servisní procesor pro vzdálenou správu zařízení (vypnutí/zapnutí zařízení, konzolový přístup) |  |  |
| L4 propustnost minimálně 18 Gbps |  |  |
| L7 propustnost minimálně 18 Gbps |  |  |
| Podpora minimálně 225 000 L4 spojení za sekundu |  |  |
| Podpora minimálně 20 milionů současných TCP/UDP spojení |  |  |
| Podpora minimálně 9000 SSL transakcí za vteřinu pro RSA klíče s délkou 2048-bitů |  |  |
| Podpora minimálně 6000 SSL transakcí za vteřinu pro klíče ECDSA s P-256 |  |  |
| Podpora SSL certifikátů podepsaných SHA-2 metodou |  |  |
| Podpora TLS 1.2 |  |  |
| Podpora AES-GCM a ECC pro TLS 1.2 |  |  |
| Podpora STARTTLS pro SMTP provoz |  |  |
| Podpora šifrování pomocí Suite B, ECDSA, AES-GCM |  |  |
| Popdora symetrického šifrování včetně šifer Camellia |  |  |
| Podpora HTTP Strict Transport Security (HSTS) |  |  |
| Možnost pracovat až s 4096-bitovými klíči |  |  |
| Podpora hardwarové SSL akcelerace |  |  |
| Možnost zvýšit výkonnostní parametry SSL dokoupením licence |  |  |
| Balancing aplikačního provozu na základě vrstev L3 – L7 s podporou balancingu obsáhlého setu protokolů až do 7. vrstvy OSI (ftp, dns, https/http, sip, …) |  |  |
| Klient/Server NAT/PAT |  |  |
| Podpora různých typů load-balancingu: |  |  |
| ·         Kruhová metoda s vážením |  |  |
| ·         Podle počtu navázaných spojení |  |  |
| ·         Podle otisku zdrojové a cílové adresy |  |  |
| ·         Podle URL a cookie |  |  |
| ·         Na základě SNMP (např. zátěže procesorů) |  |  |
| ·         Podle vah pro skupiny |  |  |
| ·         Na základě počtu odezev od serverů |  |  |
| Podpora zajištění konektivity uživatelů k serveru (persistence) na základě IP adresy, L4 payloadu, HTTP cookie, HTTP obsahu, HTTP hlavičky, RADIUS atributů, RTSP hlavičky, SIP hlavičky, SSL Session ID |  |  |
| Podpora různých typů dostupnosti a zdraví aplikace (monitoring) - ICMP, DNS, HTTP, TCP/UDP port, SSL Hello, SMTP, RADIUS, LDAP, WMI… |  |  |
| Možnost kombinace více metod monitoringu (AND/OR) |  |  |
| Podpora modifikace HTTP provozu: |  |  |
| ·         Vložení/přepsání cookie |  |  |
| ·         Modifikace URL |  |  |
| ·         Možnost vložit zdrojovou IP do L7 hlavičky |  |  |
| ·         Modifikace HTTP obsahu |  |  |
| Podpora šablon pro konfiguraci balancingu aplikací – např. Microsoft Exchange Server 2016 Client Access Servers |  |  |
| Možnost tyto šablony upravovat dle potřeb zákazníka |  |  |
| Podpora TCP multiplexingu |  |  |
| Podpora multipath TCP (MPTCP) |  |  |
| Podpora symetrické akcelerace Citrix ICA |  |  |
| Podpora ICAP protokolu |  |  |
| Podpora http komprese |  |  |
| Podpora http mezipaměti (cache) |  |  |
| Podpora filtrování paketů |  |  |
| Podpora QoS – markování, rate-limiting |  |  |
| Podpora TCP SYN cookie ochrany |  |  |
| Podpora SDN služeb – VXLAN virtualizace sítě |  |  |
| Podpora NVGRE a Transparent Ethernet Bridging tunelu |  |  |
| TDS/ MSSQL DB Proxy |  |  |
| Podpora Financial Information eXchange (FIX) protokolu |  |  |
| Podpora pro monitoring, manipulaci a modifikaci dat procházejícího datového provozu na základě skriptovacího jazyka nebo obdobné technologie |  |  |
| Podpora protokolu HTTP/2 |  |  |
| Podpora IPv4/IPv6 brány |  |  |
| Plná podpora IPv6 |  |  |
| Podpora 802.1Q |  |  |
| Podpora sFlow |  |  |
| Podpora IPFIX |  |  |
| Správa přes GUI, CLI |  |  |
| Podpora SNMP (1, 2c a 3) |  |  |
| Podpora SSH |  |  |
| Podpora vysokorychlostního logování pro každou aplikaci zvlášť |  |  |
| Podpora režimu redundance se synchronizací stavových tabulek (state failover) |  |  |
| Podpora redundantních clusterů Active-Standby i Active-Active |  |  |
| Možnost zapojit do redundantniho clusteru různé typy HW nebo virtualizovaných platforem |  |  |
| Dostupnost jak hardwarového tak i virtuálního řešení |  |  |
| Podpora otevřeného API pro nástroje třetích stran pro konfiguraci a monitoring zařízení |  |  |
| Podpora virtualizace – separací IP adresního prostoru (obdoba VRF) nebo plnohodnotné virtualizace |  |  |
| Možnost rozšíření o funkci Web Aplikačního Firewalu dodatečnou licencí |  |  |
| Možnost rozšíření o funkci podpory externích šifrovacích karet (HSM) dodatečnou licencí |  |  |

### Specifikace implementačního procesu a požadovaných produktů a výstupů

* Dodavatel vytvoří na základě analytických schůzek tzv. Analýzu nasazení technologie ADC, jejíž obsah bude následující:
  + Popis terminologie, použité v dokumentu
  + Informace o stávajícím prostředí Zákazníka
  + Seznam aplikací, které budou ADC využívat
  + High-level popis řešení
  + Popis změny v infrastruktuře
  + Podpora autentizace administrátorů ADC protokolem TACACS+, který je součástí projektu
* Dodavatel vytvoří na základě analytických schůzek tzv. Funkční specifikaci, jejíž obsah bude následující:
  + Vymezení scope řešení
  + Popis funkčních vlastností požadovaného zabezpečení aplikací technologií ADC
  + Popis úprav existujícího IT prostředí Zákazníka
  + Schéma řešení včetně integrace do prostředí zákazníka
  + Popis cílové úpravy vnitřních procesů
* Dodavatel vytvoří Low Level Design s následujícím obsahem:
  + Celkový návrh řešení ADC
  + Typizované konfigurační šablony (soubor pravidel) pro řízení aplikačního provozu
  + Jmennou konvenci pro ADC řešení
  + Konfigurace ADC clusteru
  + Konfigurace politik řízení aplikačního provozu pro aplikace
  + Vytvoření a implementace standardů (soubor pravidel) pro SSL terminaci
  + Vytvoření a implementace standardů (soubor pravidel) pro monitoring aplikací
  + Vytvoření a implementace standardů (soubor pravidel) pro manipulaci s HTTP provozem (vkládání odebíraní HTTP záhlaví apod.)
  + Vytvoření a implementace standardů pro optimalizaci TCP a HTTP provozu
  + Konfigurace ochrany proti DoS a DDoS aplikačním útokům
  + Konfigurace ostatních aspektů bezpečnostní politiky dle funkční specifikace
  + Konfigurace spolupracujících systémů (MDM, Active Directory a další)
* Dodavatel ve spolupráci se Zákazníkem vytvoří plán scénářů vysoké dostupnosti aplikací
* Dodavatel připraví podrobné akceptační testy ADC
* Dodavatel provede pod dohledem Zákazníka akceptační testy ADC
* Dodavatel provede analýzu stávajících procesů zákazníka a připraví:
  + Soupis procesů, dotčených implementací ADC
  + Soupis rolí v rámci dotčených procesů
  + Návrh úpravy procesů tak, aby byly po implementaci systému funkční
  + Návrh dalších procesů, které jsou pro provoz systému technologie nezbytné
  + Přiřazení rolí k jednotlivým procesním krokům
* Dodavatel proškolí zástupce Zákazníka v:
  + Řešení a základní operativě
  + Upravených procesech
* Dodavatel připraví tzv. Dokumentace skutečného provedení, která bude obsahovat popis finálního nastavení jednotlivých komponent řešení a procesů

## Technická a implementační specifikace WAF

### Popis požadovaného řešení

Webové aplikace publikované do vnějších sítí, zejména veřejné sítě Internet, mohou být náchylné na zranitelnosti vůči kybernetickým útokům a aplikačním DoS a DDoS útokům. Nasazením webového aplikačního firewallu je možné zajistit inspekci webové komunikace a ochranu před kybernetickými útoky.

Požadujeme dvojici webových aplikačních firewallů ve formě HW zařízení nebo jako licenční rozšíření k požadovanému loadbalanceru. Webový Aplikační Firewall (WAF) bude poskytovat ochranu webových aplikací před kybernetickými útoky s využitím pozitivní i negativní bezpečnostní logiky v bezpečnostních politikách (detekci a ochranu před známými útoky a povolení explicitního legitimního provozu). K těmto základním bezpečnostním politikám předpokládáme implementaci dalších dodatečných bezpečnostních vlastností, jako je ochrana před útoky prolomením logovacích URL hrubou silou (Brute Force útoky) s možností eskalace a potlačení technologií CAPTCHA v případě podezření, že je aplikace pod útokem. Dále požadujeme, aby WAF obsahoval technologie pro detekci a potlačení robotických (nelidských) uživatelů s možností výjimek (např. pro legitimní vyhledávače Googlebot, Seznambot apod.). WAF také zajistí ochranu před únosy HTTP relací. WAF musí podporovat SSL terminaci, jelikož HTTP protokol bude šifrován.

Řešení musí být realizováno ve vysoké dostupnosti v režimu minimálně “active-standby”.

Implementace bezpečnostních politik bude minimálně v rozsahu:

* Ochrana proti aplikačním DoS a DDoS útokům (SlowLoris, R.U.D.Y, ApacheKiller, SSL útoky, SYN flood, HTTP flood aj.)
* Ochrana proti "forcefull browsing", XSS, SQL-INJ, CSRF, remote command execution a ostatním útokům podle OWASP Top 10 nejaktuálnějšího znění
* Ochrana proti manipulaci s cookies
* Ochrana parametrů webové aplikace
* Session Management – ochrana proti únosům relací
* Brute Force Ochrana – ochrana před prolomení hrubou silou
* Detekce robotických uživatelů aplikace u vybraných aplikací

V případě integrace WAF s funkcí loadblanceru (v roli reverzní proxy), je přípustné, aby požadavky byly splněny v loadbalancerem (např. fyzické porty aj.).

### Technická specifikace zařízení a funkcí WAF

| *Požadavek na funkcionalitu* | *Způsob prokázání splnění:* | *Splněno: [ANO / NE / hodnota]* |
| --- | --- | --- |
| 2 ks samostatného HW zařízení s montáží do technologické 19" skříně (RACK), max. 2U nebo jako rozšiřující licence k loadbalanceru |  |  |
| V případě samostatného HW zařízení WAF plně redundantní napájecí zdroj AC vyměnitelný za provozu |  |  |
| V případě samostatného HW zařízení WAF požadujeme min. 6x 1Gbps slotů pro Ethernet rozhraní typu SFP a zároveň min. 4 x 10 Gbps slotů pro Ethernet rozhraní typu SFP+.  Případné transceivery SFP či SFP+ či další kabeláž pro obě strany připojení jsou součástí dodávky. |  |  |
| V případě samostatného HW zařízení Lights-out management - nezávislý servisní procesor pro vzdálenou správu zařízení (vypnutí/zapnutí zařízení, konzolový přístup) |  |  |
| Vestavěná ochrana proti HTTP DoS a DDoS útokům |  |  |
| Detekce a blokování širokého spektra útoků na aplikační vrstvě, minimálně podle OWASP 2017 top10 |  |  |
| Možnost doprogramovat si filtrovaci pravidla pro aplikace |  |  |
| Ochrana AJAX a JSON aplikací |  |  |
| Detekce a ochrana před web scraping útoky |  |  |
| Detekce a ochrana před pokusy o prolomení logovacích stránek pomocí hrubé síly (brute force) |  |  |
| Blokování požadavků z podezřelých prohlížečů (proaktivní ochrana proti botnetům) |  |  |
| Rozšířená podpora pro detekci aktivity klávesnice a myši, detekce změn URL od klienta za krátkou dobu, detekce robotických klientů |  |  |
| Podpora odlišení lidských uživatelů od robotů pomocí Captcha |  |  |
| Zabezpečení XML komunikace |  |  |
| Podpora maskování/odstranění citlivých informací – např. rodné čísla, čísla kreditních karet apod. |  |  |
| Automatické nahrávání a aplikování nových signatur aplikačních útoků |  |  |
| Podpora pro vytváření vlastních signatur pro detekci HTTP útoků |  |  |
| Podpora pozitivního a negativního bezpečnostního modelu (pozitivní a negativní bezpečnostní logika) |  |  |
| Blokování útočníků na základě geolokace |  |  |
| Podpora ICAP pro antivirovou kontrolu – pro SOAP a SMTP |  |  |
| Ochrana protokolů SMTP a FTP |  |  |
| Podpora SSL (šifrování a dešifrování) |  |  |
| Podpora ECDSA a podpora hybridních certifikátů (DSA/ECDSA/RSA) |  |  |
| Podpora symetrického šifrování včetně šifer Camellia |  |  |
| Podpora HTTP Strict Transport Security (HSTS) |  |  |
| Podpora HTTP/2 |  |  |
| Podpora akcelerace |  |  |
| -          Konsolidace TCP spojení od klienta směrem k serveru tj. Z několika spojení od uživatele udělat jedno spojení na server |  |  |
| -          Caching |  |  |
| -          Komprese |  |  |
| -          Možnost optimalizace TCP stacku zvlášť směrem k uživateli a směrem k serveru |  |  |
| Podpora různých typů reportů – PCI, geolokační reporty |  |  |
| Podpora standardů PCI DSS, HIPAA, Basel II a SOX |  |  |
| Integrované bezpečnostní politiky pro Microsoft Outlook Web Access, Lotus Domino Mail Server, Oracle E-Business Financials a Microsoft SharePoint aj. |  |  |
| Integrace s nástrojem na detekci zranitelností webových aplikací |  |  |
| Podpora pro monitoring a měření výkonu HTTP aplikací |  |  |
| Možnost importu zranitelnosti aplikací z alespoň některých z následujících skenerů: |  |  |
| ·         Cenzic Hailstorm |  |  |
| ·         WhiteHat Sentinel |  |  |
| ·         IBM Rational AppScan |  |  |
| ·         QualysGuard Web Application Scanning |  |  |
| Podpora REST API pro správu zařízení |  |  |
| Autentikace klientů přes LDAP/Radius |  |  |
| Certifikace ICSA webového aplikačního firewallu |  |  |
| Možnost připojení k monitorovacích nástrojů třetích stran prostřednictvím otevřeného API |  |  |
| Možnost přidávat zákaznické požadavky na základě skriptovacího jazyka nebo obdobné technologie |  |  |
| Podpora Active-Active, Active-Passive módů |  |  |
| Granulární logování / logování per aplikace |  |  |
| K dispozici jako autonomní box nebo ve formě šasi |  |  |
| Management: sériový port, GUI, příkazový řádek, iLO |  |  |
| Podpora login a logout stránek pomocí AJAX/JSON |  |  |
| Mitigace DDoS útoků založená na behaviorální analýze |  |  |
| Povoleni jednotlivych HTTP metod pro jednotliva URL |  |  |
| Podpora více logovacích profilů pro danou aplikaci |  |  |
| Podpora WebSocketu |  |  |
| Prevence před únosy klientských HTTP relací „Session Hijacking“ |  |  |
| Detekce anomalií sledovanim ID koncove stanice uzivatele |  |  |
| Blokování požadavků z podezřelých prohlížečů (proaktivní ochrana proti botnetům) |  |  |
| Podpora virtualizace – separací IP adresního prostoru (obdoba VRF) nebo plnohodnotné virtualizace |  |  |
| Možnost rozšíření o funkci Web Aplikačního Firewalu dodatečnou licencí |  |  |
| Možnost rozšíření o funkci podpory externích šifrovacích karet (HSM) dodatečnou licencí |  |  |
| Možnost definice výjimek z pravidel na úrovni jednotlivých serverů nebo publikovaných služeb |  |  |
| Přístup do logování operací, vyhledávání v nich |  |  |
| Šablony WAF (základní typy), možnost vytvoření kopie stávající šablony |  |  |
| Podpora režimu bezpečnostní politiky v blokujícím nebo transparentním (neblokujícím) režimu pro každou jednotlivou chráněnou službu |  |  |
| Možnost správy bezpečnostních politik s oddělenými přístupovými rolemi |  |  |

### Specifikace implementačního procesu a požadovaných produktů a výstupů

* Dodavatel vytvoří na základě analytických schůzek tzv. Analýzu nasazení technologie webového aplikačního firewallu, jejíž obsah bude následující:
  + Popis terminologie, použité v dokumentu
  + Informace o stávajícím prostředí Zákazníka
  + Seznam aplikací, které budou WAF zabezpečeny
  + High-level popis řešení
  + Popis změny v infrastruktuře
  + High-level popis úpravy ovlivněných procesů např. řešení bezpečnostních incidentů
  + Podpora autentizace administrátorů WAF protokolem TACACS+
* Dodavatel vytvoří na základě analytických schůzek tzv. Funkční specifikaci, jejíž obsah bude následující:
  + Vymezení scope řešení
  + Popis funkčních vlastností požadovaného zabezpečení aplikací technologií WAF
  + Popis úprav existujícího IT prostředí Zákazníka
  + Schéma řešení včetně začlenění do prostředí zákazníka
  + Popis cílové úpravy vnitřních procesů
* Dodavatel vytvoří Low Level Design s následujícím obsahem:
  + Celkový návrh řešení
  + Typizované konfigurační šablony bezpečnostních politik WAF
  + Konfigurace WAF clusteru (zajištění konzistence bezpečnostních politik napříč clusterem WAF)
  + Konfigurace bezpečnostních politik
  + Ladění bezpečnostních politiky proti výskytu tzv. falešných poplachů
  + Konfigurace ochrany proti DoS a DDoS aplikačním útokům
  + Konfigurace ostatních aspektů bezpečnostní politiky dle funkční specifikace
  + Konfigurace spolupracujících systémů (MDM, Active Directory a další)
* Dodavatel připraví podrobné akceptační testy WAF
* Dodavatel provede pod dohledem Zákazníka akceptační testy WAF
* Dodavatel provede analýzu stávajících procesů zákazníka a připraví:
  + Soupis procesů, dotčených implementací WAF
  + Soupis rolí v rámci dotčených procesů
  + Návrh úpravy procesů tak, aby byly po implementaci systému funkční
  + Návrh dalších procesů, které jsou pro provoz systému technologie nezbytné
  + Přiřazení rolí k jednotlivým procesním krokům
* Dodavatel proškolí zástupce Zákazníka v:
  + Řešení a základní operativě
  + Upravených procesech
* Dodavatel připraví tzv. Předávací dokumentaci, která bude obsahovat popis finálního nastavení jednotlivých komponent řešení a procesů