

**Klasifikace: Veřejný dokument**



Technická specifikace

Příloha č. 1 zadávací dokumentace „Ochrana perimetru a DMZ – Anti-DDoS řešení a internetová konektivita“

[1 Seznam zkratek 2](#_Toc124869454)

[2 Úvod 3](#_Toc124869455)

[2.1 Předmět plnění veřejné zakázky 3](#_Toc124869456)

[3 Požadavky na plnění 3](#_Toc124869457)

[3.1 Zavedení internetové konektivity do dvou lokalit 3](#_Toc124869458)

[3.2 Ochrany proti DDoS útokům 4](#_Toc124869459)

[3.3 Předání dokumentace obsahující všechny konfigurační parametry 5](#_Toc124869460)

[3.3.1 Internetová konektivita 5](#_Toc124869461)

[3.3.2 Ochrana proti DDoS útokům 5](#_Toc124869462)

# Seznam zkratek

Níže uvedená tabulka obsahuje seznam zkratek a pojmů použitých v rámci této Technické specifikace.

Přehled zkratek a pojmů:

|  |  |
| --- | --- |
| Zkratka | Popis |
| Dodavatel | Subjekt, který se uchází o realizaci veřejné zakázky s názvem „Ochrana perimetru a DMZ – AntiDDoS řešení a internetová konektivita“. |
| SŽ | Správa železnic |
| DDoS | Distributed Denial of Service |
| Gbps | Gigabits per second |
| HW | Hardware |
| BGP | Border Gateway Protocol |
| SFP+ | Small Form-factor Pluggable Plus |
| IP | Internet Protocol |
| WebUI | Web User Interface |
| DMZ | Demilitarizovaná zóna |
| SPoF | Single Point of Failure |

# Úvod

Tento dokument je přílohou a nedílnou součástí zadávací dokumentace týkající se veřejné zakázky s názvem „Ochrana perimetru a DMZ – Anti-DDoS řešení a internetová konektivita“ (dále jen „veřejná zakázka“), pro organizaci Správa železnic, státní organizace (dále jen „SŽ“ nebo “Zadavatel”). Dokument popisuje technické a jiné požadavky na veřejnou zakázku.

Technická specifikace je závazná a její nedodržení je důvodem k vyloučení Dodavatele ze zadávacího řízení.

## Předmět plnění veřejné zakázky

Předmětem plnění veřejné zakázky je zavedení a poskytování duální geograficky oddělené internetové konektivity pro SŽ včetně ochrany proti DDoS útokům, a to po dobu 60 měsíců.

Zahájení plnění veřejné zakázky je závislé na dodání HW vybavení pro DMZ a perimetr sítě. Konkrétně se jedná o projekt SŽ, který je označován jako Next-Generation firewally a aktivní prvky. Okamžik zahájení plnění veřejné zakázky je tedy závislý na součinnosti třetích osob, přičemž předpokládaný termín zahájení plnění je ve čtvrtém kvartálu roku 2023.

Tato veřejná zakázka obsahuje následující poptávané oblasti:

* Internetová konektivita pro lokalitu Pod Táborem 369/8a, Praha 9
* Internetová konektivita pro lokalitu Purkyňova 22, Plzeň
* Anti-DDoS technologie pro ochranu obou výše uvedených internetových konektivit

# Požadavky na plnění

Plnění veřejné zakázky se musí skládat alespoň z níže uvedených částí:

1. Zavedení internetové konektivity do dvou lokalit
2. Ochrany proti DDoS útokům
3. Předání dokumentace obsahující všechny konfigurační parametry

## Zavedení internetové konektivity do dvou lokalit

V oblasti zavedení internetové konektivity stanovuje Zadavatel následující technické požadavky:

|  |  |
| --- | --- |
| **Požadavek** | **Hodnota** |
| Zavedení internetové konektivity na adrese č. 1 | Pod Táborem 369/8a, Praha 9 |
| Zavedení internetové konektivity na adrese č. 2 | Purkyňova 22, Plzeň |
| Možnost přestěhování internetové konektivity z adresy č. 2 na adresu | Tovární 3137, Přerov |
| Propustnost internetové konektivity – symetricky | Minimálně 2,5 Gbps |
| Možnost navýšení propustnosti internetové konektivity na | Minimálně 10 Gbps |
| Zajištění vysoké dostupnosti | Redundantní HW na straně Dodavatele pro každou lokalitu |
| Architektura sítě poskytovatele | Síť poskytovatele je ve všech svých bodech redundantní bez tzv. SPoF v takové míře, aby výpadek jakéhokoliv hardwaru nebo celého datacentra nemohl způsobit výpadek lokalit Plzeň a Praha zároveň. |
| Technologie spojení hraničních směrovačů SŽ se směrovači Dodavatele | Linková agregace |
| Garantovaná dostupnost internetové konektivity | Minimálně 99,95 % pro každou lokalitu zvlášť |
| Počet veřejných IP adres IPv4 | Minimálně 254 |
| Počet veřejných IP adres IPv6 | Minimálně 254 |
| Propagace veřejných IP adres do obou lokalit pomocí směrovacího protokolu | BGP |
| Technologie fyzického připojení internetové konektivity | Opticky (SFP+) |

## Ochrany proti DDoS útokům

V oblasti zavedení internetové konektivity stanovuje Zadavatel následující technické požadavky:

|  |  |
| --- | --- |
| **Požadavek** | **Hodnota** |
| Režim čištění provozu | Trvalý |
| Varianty ochrany č. 1: Maximální kapacita DDoS útoku, proti kterému je poskytnuta ochrana | Minimálně 50 Gbps |
| Varianta ochrany č. 2: Šířka pásma chráněného cíle, tedy množství garantovaného doručení legitimního provozu (rozsah poskytovaných IP adres internetové konektivity) | Minimálně 2,5 Gbps |
| Podpora IP protokolů | IPv4 a IPv6 |
| Ochrana proti | známým botnetům |
| Ochrana proti | známým DDoS nástrojům |
| Ochrana proti FLOOD útokům typu | SYN  TCP ACK + FIN ACK  TCP RST  TCP SYN + ACK TCP fragmentation UDP FLOOD  ICMP FLOOD  IGMP FLOOD |
| Časový režim ochrany | 24x7 |
| Způsob notifikace o probíhajícím DDoS útoku | Email a telefon |
| Možnost sledování činnosti scrubbing centra | WebUI |

## Předání dokumentace obsahující všechny konfigurační parametry

Dodavatel předá Zadavateli dokumentaci obsahující minimálně následující informace.

### Internetová konektivita

* IPv4 a IPv6 IP adresace
* Výchozí brána
* Konfigurace linkové agregace
* Fyzická lokace routerů Dodavatele
* Telefonický a e-mailový kontakt na technickou podporu

### Ochrana proti DDoS útokům

* Parametry konfigurace DDoS ochrany
* Adresace a přístupové údaje k WebUI
* Telefonický a e-mailový kontakt na technickou podporu