Kapitola 1 - Příloha 1 – Konfigurace sítě

Při provozu aplikací ATEAS Security je v případě potřeby nutné provést konfiguraci síťových prvků (to se může týkat například nastavení routerů, pokud je kamerový systém umístěn uvnitř lokální sítě), tak aby mohly být serverové aplikace kontaktovány na uvedených portech. Následující tabulka shrnuje základní síťové porty. Klient systému je vždy stranou, která spojení vytváří, na klientské straně není třeba provádět žádná speciální nastavení.

POZNÁMKA

Pro základní fungování systému postačí otevření portu 8501 pro administrační a portu 8502 pro kamerový server. Ostatní porty slouží pro pokročilejší či doplňkové funkce a integrace.

1.1. Administrační server

Port	Transportní protokol	Aplikační protokol	Komunikace
8501	TCP	ATEAS	Základní komunikační port
8503	TCP	ATEAS	Podpora cloudového připojení
8504	TCP	ATEAS	Příjem externích událostí z jiných systémů
9001 – N	TCP	WebSocket / TLS	Podpora cloudového připojení pro web klienta
80	TCP	HTTP	Domovská stránka systému, webový klient, automatické aktualizace
443	TCP	HTTPS / TLS	Domovská stránka systému, webový klient, automatické aktualizace
162	UDP	SNMP	Příjem trapů pro aktivaci událostí

1.2. Kamerový server

Port	Transportní protokol	Aplikační protokol	Komunikace
8502	TCP	ATEAS	Základní komunikační port
8505	TCP	ATEAS	Vlastní události kamer

8506	TCP	HTTP	Přístup k webovému rozhraní všech kamer
8507	TCP	WebSocket	Nezabezpečené vysílání pro web
8508	TCP	WebSocket / TLS	Zabezpečené vysílání pro web
8509	TCP	HTTP	Vysílání videa pomocí DLNA
3702	UDP	SOAP	Vyhledávání Onvif kamer (WS Discovery)
8080	TCP	HTTP	Body Worn System

POZOR

Pokud je použito schéma přenosu dat z kamer RTP/UDP, UDP porty jsou alokovány dynamicky a musí být nastavena výjimka pro celý kamerový server, nikoliv pro konkrétní porty. To platí i pro klienta, pokud má profil LOCAL a připojuje se tak na multicastové adresy a přijímá data pomocí protokolu UDP.