

ir inner range

Intelligent Security Solutions



SkyTunnel Connectivity Guide

SkyTunnel is a free cloud-based connectivity service that helps simplify remote management and installation of Inner Range products.

The following document provides information that can assist system integrators and Site IT contractors to successfully connect compatible Inner Range devices and software the SkyTunnel service. This primarily includes best practices and recommendations around site firewall rules.

Overview

Inner Range's SkyTunnel service utilizes cloud-based infrastructure that connects Inner Range technologies together. SkyTunnel consists of multiple geolocated servers around the world that increase the capacity, redundancy, reliability and geographic responsiveness of the platform.

Inner Range products that connect to the SkyTunnel cloud service are:

- Integriti Controllers
- Integriti Software
- Inception Controllers
- T4000 / T4000 Pro

Inner Range products establish outbound TCP connections to SkyTunnel and utilize AES encryption to ensure secure communications. The features the Inner Range SkyTunnel cloud service provides include:

- Communication between Integriti software and Integriti controller for remote sites
- Inception controller secure web access from web browsers
- T4000 Pro secure web access from web browsers
- Alarm reporting from Integriti controllers and Inception controllers to MultipathIP systems
- A failover alarm reporting path for T4000s if the direct "T4000 to MultipathIP" path stops working
- SkyCommand control from web browsers and iOS & Android apps of Inception controllers, Integriti controllers and T4000s
- T4000 upload/download

Connectivity to SkyTunnel

Inner Range appreciates the need for IT administrators to provide a secure network infrastructure. The following describes the recommended approach to secure a network while still allowing Inner Range products to reliably connect and function.

SkyTunnel consists of multiple servers around the world and over time, Inner Range intends to add additional SkyTunnel instances as required. This means that the Inner Range devices may not always connect to the same SkyTunnel server.

With this in mind, Inner Range recommends that for Inner Range products, outbound firewall rules are not locked down to specific destination IP addresses. Otherwise, connectivity may work initially, but could break at any time in the future if the device shifts to a closer / different server cluster that the firewall is blocking.

SkyTunnel Device Ports

To ensure ongoing connectivity, the following port ranges should be allowed for outbound TCP connections by all Inner Range products:

- 40844
- 41000 to 41010

Web Browser Access

The web browser for several Inner Range products can be remotely accessed securely via SkyTunnel. The following port ranges should be opened for any devices (Phones, PCs, etc) accessing web interfaces via HTTPS.

- 443
- 8100 to 8110

SkyTunnel IP Addresses

As mentioned, due to the multi-server nature of SkyTunnel, Inner Range does not recommend locking down Inner Range device access to specific destination IP addresses. If this is done, while it may work initially, connectivity may break or be unnecessarily slow in future.

If still desired though, the latest list of SkyTunnel server addresses are available at www.skytunnel.com.au/info. The ports listed above should be opened for each of the addresses listed at that link. New server clusters may be added in future, and existing IP addresses are subject to change at any time.