3xLOGIC

# Tech Tip 170011

## VIGIL Server – Configuring Direct Connection for VIGIL Connect

| | |
|---|---|
| **Tech Tip #:** | 170011-1 |
| **Date:** | March 1st, 2016 |
| **Product Affected:** | VIGIL Server 7 Series and newer. |
| **Purpose:** | This document is intended to instruct a user on the process of configuring a network to facilitate a direct connection for VIGIL Connect on an applicable VIGIL Server system |



## 1 Introduction

VIGIL Connect allows VIGIL VMS users to remotely connect to a VIGIL Server using the system serial number or user defined alias without the need for extensive changes to an existing network's settings.

Two separate connection methods exist for VIGIL Connect; *Direct Connection* or *TCP Tunnel Relay*. This guide is intended to instruct a user on the process of setting up their network and VIGIL Server to utilize a ***Direct Connection***.

A VIGIL Connect Direct Connection operates as follows:

- **Direct Connection**:
  1. Check if VIGIL Server is connected directly to the internet
  2. Use UPnP to automatically forward ports if the router supports UPnP. This will allow VIGIL Client (or other VIGIL VMS Utilities utilizing the VIGIL Connect system) to directly connect to a VIGIL Server with TCP. If UPnP is not supported, port forwarding must be completed manually.

**Note:** Only Server Location Info, IP and Port and VIGIL Connect alias info is passed through the VIGIL Connect system. All other data is passed directly between the VIGIL VMS and other VIGIL utilities utilizing Connect.

Proceed through the remaining sections of this guide for instruction on configuring a network and a VIGIL Server to utilize a direct connection for VIGIL Connect.

## 2 VIGIL Server - Configuring Network for Direct Connection

To ensure your VIGIL Server system is able to utilize VIGIL Connect via direct connection, two requirements must be met. Both the All TCP/UDP ports related to VIGIL Connect must be opened and the required VIGIL Connect IP whitelist must be in place on your VIGIL Server's host network.

### 2.1 Required TCP/UDP Ports

The following inbound and outbound TCP/UDP Ports must be open in order for VIGIL Connect to function successfully across a direct connection. On most existing networks, outbound ports are not blocked and opening the listed ports is not required, however, some restricted networks may require that specific outbound ports are opened to traffic by a network administrator.

**Required Inbound Ports (for VIGIL Server):**

- Ports 22801-22811 (these are VIGIL Server defaults, may vary based on custom VIGIL Server port numbers).

**Required Outbound Ports (for VIGIL Connect):**

- 80
- 443
- 22700

### 2.2 Required IP Whitelist

Network / firewall rules must also be in place for all associated VIGIL Connect IP addresses. Manually create a network IP whitelist for all VIGIL Connect addresses listed below.

**Server IP List:**

- 184.71.22.230
- 52.10.75.167
- 138.91.90.99
- 23.102.157.13

## 3 Contact Information

If you require more information, or if you have any questions or concerns, please contact 3xLOGIC Support:
Email: helpdesk@3xlogic.com
Online: www.3xlogic.com