Guide 180017

VIGIL VMS –VIGIL Services – Network Deployment Guide

Tech Tip #:	180017-1
Date:	May 30th, 2018
Product Affected:	VIGIL Server, VIGIL Connect, VIGIL VMS, VIGIL Trends, VIGL CPNS
Purpose:	The purpose of this document is to outline the baseline connectivity requirements for several VIGIL VMS components that are frequently used in conjunction with client networks.

1 Introduction

Several requirements exist for deployment of different VIGIL VMS components. Multiple cloud and hosted services exist to support several features and utilities across the suite, each with different connectivity requirements. Follow the connectivity requirements outlined in this guide for all VIGIL VMS components featured in your network design. This document is intended for network administrators and assumes the reader holds intermediate to advanced networking knowledge.

2 Network Deployment Requirements

VIGIL Connect Domain Name – Using Dig Command to Create VIGIL VMS Services Firewall White List (Recommended):
Use a dig command (Example: https://toolbox.googleapps.com/apps/dig/#A/vigilconnect.3xlogicip.com) with the below domain name to create and maintain a white list for your network firewall(s). All addresses associated with VIGIL VMS services will be included.

Domain Name:
VIGILConnect.3xlogicip.com

After creating the whitelist, your network can maintain connectivity with all VIGIL VMS services.

If you are unable to use the dig command or prefer to create network rules and permissions manually for only the VIGIL services your network design requires, see the remaining sections of this guide to obtain the required information for manual network rule creation. Each sub-section of this guide will pertain to a different VIGIL VMS component.

2.1 VIGIL Connect

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. If your network design requires the use of VIGIL Connect, read through the proceeding information and follow all connectivity requirements to successfully deploy VIGIL Connect.

Two separate connection methods exist for VIGIL Connect:

1. **Direct Connection**:
   - Check if VIGIL Server is connected directly to the internet
   - Use UPNP to automatically forward ports if the router supports UPNP. This will allow VIGIL Client to directly connect to a VIGIL Server with TCP.
   - If UPNP is not supported, a user can set up port forwarding manually.
   - 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.
2. **TCP Relay:**
   - If port forwarding is not available, a TCP Tunnel/Relay may be used. In this case, both VIGIL Server and Client will connect to a central server, and exchange data through it. Any network can support this feature.
   - All data (Video, POS, Camera Control, Login info, etc…) passed between the VIGIL VMS via VIGIL Client and other VIGIL utilities utilizing Connect will be passed through the relay server.

2.1.1 VIGIL Connect - Required TCP/UDP Outbound Ports

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

Required Outbound Ports:

- 80
- 81
- 443
- 444
- 22700
- 22703
- 22704

⚠ **Warning:** If network port restrictions are in place, at a minimum, port 80 **OR** 443 must be open.

2.1.2 VIGIL Connect – Creating Network/Firewall Rules

Network rules must also be in place for all associated VIGIL Connect and VIGIL Connect Relay Server IP addresses. If you have opted to forego creating a whitelist using a dig command (See Section 2), rules must be created manually. Manually create network firewall rules for all VIGIL Connect and VIGIL Connect Relay Server addresses listed below.

IP:

- 184.71.22.230
- 52.10.75.167
- 138.91.90.99
- 23.102.157.13
- 23.101.126.214
- 137.135.60.74
- 52.32.6.164
- 104.41.132.78
- 104.40.0.24
- 40.83.187.44
- 54.69.36.176
- 52.27.223.35
- 52.88.147.83
- 52.21.190.150
- 52.201.188.103
- 34.198.166.209
- 34.197.23.187
- 13.66.225.144

2.2 VIGIL Encoding Server:

If your network design requires the use of the VIGIL Encoding Server, create firewall rules for the following addresses:

Inbound:
N/A

Outbound:
40.78.18.232:80, 40.78.18.232:443 webcloudvigilapi.azurewebsites.net
23.99.65.65:80, 23.99.65.65:443 vigil-decode.azurewebsites.net

2.3 VIGIL Update Server:

If your network design requires the use of the VIGIL Update Server, create firewall rules for the following addresses:

Inbound:
N/A

Outbound:
23.99.65.65:80, 23.99.65.65:443 vigilupdate.azurewebsites.net

2.4 VIGIL Archive Server:

If your network design requires the use of the VIGIL Archive Server, create firewall rules for the following addresses:

Inbound:
N/A

Outbound:
23.99.65.65:80, 23.99.65.65:443 vigilarchive.azurewebsites.net

2.5 VISIX Setup Server:

If your network design requires the use of the VISIX Setup Server, create firewall rules for the following addresses:

Inbound:
N/A

Outbound:
104.45.231.79:80, 104.45.231.79:443 3xlogiccam.azurewebsites.net

2.6 VIGIL Cloud Push Notification Server (CPNS):

If your network design requires the use of the VIGIL CPNS, create firewall rules for the following addresses:

Inbound:
N/A

Outbound:
23.96.112.53:80, 23.96.112.53:443 pushnotificationservice.azurewebsites.net

2.7 VIGIL Media Server

If your network design requires the use of the VIGIL Media Server, create firewall rules for the following addresses:

Inbound:
N/A

Outbound:

1. 168.62.16.247:443 media.windows.net
2. 168.63.132.35:443 media.windows.net
3. 70.37.92.127:443 wamsprodglobal001acs.accesscontrol.windows.net
4. 168.62.52.104:443 wamsbluclus001rest-hs.cloudapp.net
5. 40.71.240.16: 443 3xstore.blob.core.windows.net ****NEW****
6. 13.66.226.80: 80 cloudapi.3xlogicip.com ****NEW****

Note: These ports must be opened to enable the VIGIL Media Server to upload video for use with VIGIL Trends. Opening the ports will only be necessary on highly-restrictive networks which limit outbound port traffic.

3 FAQ

1. **Q:** What (outbound) port(s) does the VIGIL Server use to contact the VIGIL Connect relay server (number, TCP/UDP etc)?
   A: VIGIL Server communicates with VIGIL Connect over port 22700. VIGIL Connect communicates with the Relay Server over port 22703. If either component is unable to communicate across their preferred port, they revert to port 80. If port 80 is also unavailable, then the system will use port 443.

2. **Q:** Are the outbound ports configurable?
   A: No. These ports are used universally by the VIGIL Connect system.

3. **Q:** Do we need to configure port forwarding in our router?
   A: No. In-bound ports are not required for VIGIL Connect, however, on systems utilizing a direct connection, forwarding the VIGIL VMS (DVR) ports can increase performance.

4. **Q:** When a client connects to an NVR via the relay server, are there any ports which need to be opened?
   A: No. In-bound ports are not required for the VIGIL Connect Relay Server.

5. **Q:** Does the relay server use a set of known URLs?
   A: Yes, please see the Outbound Port and IP lists in Section 2, above. If more ports or IPS are added in the future, this document will be revised accordingly.

6. **Q:** Why does 3xLOGIC recommend using a dig command with the VIGIL Connect domain name to create and maintain a firewall/network white list (Section 2.2)?
   A: Using an automated process is more efficient than manually updating network rules individually. So long as the process runs on a schedule, new IPs associated with VIGIL Connect will be automatically added to your network/firewall white list. An automated process also removes the risk introduced by human error when manually inputting network/firewall rules.

7. **Q:** Using the relay server seems to introduce a slight delay. Why?
   A: A slight delay may occur as using the Relay Server introduces an intermediary step between the end user and the Server. However, it should be noted that VIGIL Server and VIGIL Client have been engineered to use the most efficient connection available, such that if they are on the same network, they will immediately switch to direct connection if available. In this instance, having your VIGIL VMS (DVR) ports forwarded can increase performance.

8. **Q:** Does the relay server feature any other drawbacks or feature reductions as opposed to a direct peer-to -peer connection?
   A: No. Aside from the slight delay in sending and receiving information, there are no other technological drawbacks.

4 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