KRAMER

USER MANUAL

VIA Multiple Network Installation Guide

P/N: 2900-300977 Rev 1

Contents

Introduction

This document describes communication methods used by VIA to obtain optimal performance, full integration into existing and new networks, and effective segmentation of users for security purposes.

VIA uses common network infrastructure and installation strategies to enable its wide range of features. These networks follow certain rules that are primarily defined in RFCs. In networks, computing devices pass data to each other and establish either wired or wireless connections. The VIA product family is based mainly on a wired connection of the gateway (VIA device) and a wireless connection for clients such as Windows, Mac, iOS, Android or Chrome devices. In addition, a connection can be made to a server known as VSM (VIA Site Management). The VSM node can operate in a different mode than a VIA gateway or a client and necessitates unique policies.

Policies define communication rules in networks. Most networks are segmented or separated into different parts, each belonging to a specific functionality. A segmentation can be done for many reasons. The most common segmentation is to separate internal users from guest users.

In some cases, segmentation cannot be performed for an existing network. In that case, VIA gateways enable a segmentation through the use of a second network – wired or wireless, depending on the VIA gateway you are using (see Available Connection Types by Device on page 6).

Communication Diagram

The communication diagram presented below can help you understand deployment of VIA gateways inside a network or as standalone devices. It further includes information about how the different components of a deployment communicate with each other to ensure a fully functional environment.

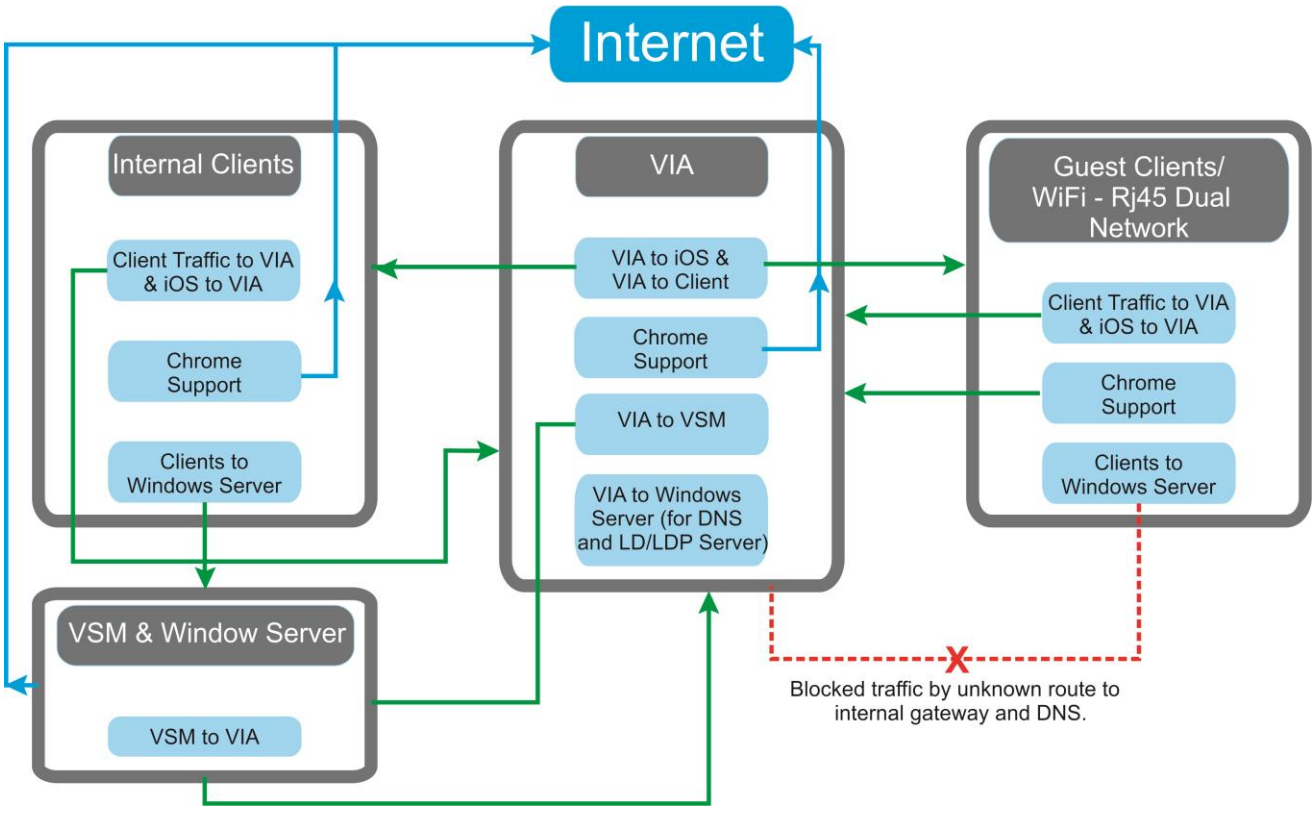
The components of a VIA deployment include:

- Internal and external clients,
- VIA gateways
- Servers (including VSM).

All services used by and provided by VIA should be clearly understood to facilitate the creation of a system that works as expected. The communication diagram reflects the origin and destination of each service.

Rule sets must be defined as services and policies for today's firewall or router systems. Using this information, scenarios from one to a dozen segments can be generated by applying the common rule sets required by VIA for each segment.

For a complete list and description of all communication ports, see the VIA IT Deployment Guide, at www.KramerAV.com.



How to Segment System Users

Segmentation of system users is accomplished by dividing users by trust level. In general, communication for internal users is treated with a higher trust level than external users. Trust levels are usually defined by the Chief Information Security Officer (CISO) or the IT department. It is also common practice to hire external companies that manage security segmentation and trust levels.

In recent years, a change in the behavior of IT administrators, CIOs, CISO and IT departments has occurred. It is now more likely to treat all users as untrusted rather than separating them into groups with different levels. This change was brought about by the BYOD culture, a more open and collaborative environment in companies and shared desk home office setups.

To deal with these challenges, Kramer designed all VIA communication to work through TCP and separated functions by ports that can be activated or deactivated. Kramer also implemented the Dual Network feature that enables using different IPs on the same device.

Dual Network segmentation separates users with a simple and reliable method. The VIA gateway does not provide any route between the networks that would enable the guest segment to interact directly with the internal segment. Each segment communicates to its ports on the VIA gateway and each port sits on a different subnet.

For a complete list and description of all communication ports, see the VIA IT Deployment Guide, at www.KramerAV.com.

Guests in a Dual Network

To ensure fast and direct communication that does not cross network segments, VIA functions are capable of communicating directly to multiple networks. However, to ensure separation of the user segments, guests communicating over the secondary LAN/WLAN of a VIA gateway are subject to the following limitations and parameters:

- No direct communication to the authentication server used by the default adapter is provided.
  - Communication to port 5224 is forwarded by a “Bridge APP” to port 5222 of the default adapter.
  - Port 5222 is used by the default adapter.
  - Port 5224 is used by the secondary adapter.
- There is no route provided from the second LAN to first LAN. The secondary adapter cannot communicate with the gateway, DNS or any other component of the default adapter.
- Chrome on the second LAN/WLAN goes first to VIA, then it is redirected to the default gateway on the first LAN, and, finally, it reaches cb.wowvision.com.
- Communication possibilities between the second LAN and first LAN are limited to specific, documented ports.
- Port 22/TCP is only open if activated.
- If the VIA installation site has its own secondary network, it can be used instead of the VIA second LAN/WIFI. In that case, VIA’s second LAN/WIFI acts as a client or access point. (For more information see Available Connection Types by Device on page 6.)

The following are things to consider when using a dual network:

- By default, direct communication between the networks connected to VIA is not possible.
- Opening the SSH port reveals it to all networks.
- Communication for Chrome support is forwarded through VIA to the default gateway. If you do not want to allow Chrome users on a secondary adapter, please block the responsible traffic on the first possible node of your default adapter’s network.
- VIA does not provide antivirus, IPS, IDS, web control, or similar technology.

Firewalls

Based on the information of the communication diagram we are now able to setup Firewall services and policies to ensure a working system.

If possible, communication should always be limited to the addresses used by VIA. This makes it easier to track unwanted communication and to maintain an IDS/IPS system that works quickly and effectively.

The following is a rule overview of VIA services:

VIA-Services (13)			
Client-to-VIA-SW	VIA-Services	TCP/5222 TCP/5224 TCP/7001-7024 TCP/7777 TCP/5555 TCP/9955 TCP/9954 TCP/9985 TCP/9982 TCP/9986 TCP/9994 TCP/9987 TCP/9989 TCP/9990 TCP/9993 TCP/9992	0.0.0.0
Client-to-VIA-WEB	VIA-Services	TCP/80 TCP/443 TCP/22	0.0.0.0
PC-to-mobile-VIA-clients	VIA-Services	TCP/12345 TCP/20000	0.0.0.0
VIA-Chrome-Support-1	VIA-Services	TCP/3478 UDP/3478	turn1.wowvision.com
VIA-Chrome-Support-2	VIA-Services	TCP/3478 UDP/3478	turn2.wowvision.com
VIA-Chrome-Support-3-cb	VIA-Services	TCP/446	cb.wowvision.com
VIA-to-Clients	VIA-Services	TCP/80 TCP/8080 TCP/12345	0.0.0.0
VIA-to-VSM	VIA-Services	TCP/9988 TCP/5555 TCP/5557 TCP/5558 TCP/80 TCP/443	0.0.0.0
VIA-to-iOS-mDNS	VIA-Services	UDP/5353	0.0.0.0
VIAPad-to-VIA-Download	VIA-Services	TCP/9983	0.0.0.0
VSM+VIA-Autodiscovery	VIA-Services	TCP/443	cb.wowvision.com
VSM-to-VIA	VIA-Services	TCP/80 TCP/443	0.0.0.0
iOS-to-VIA	VIA-Services	TCP/7000 TCP/7100-7300 TCP/29053 UDP/2001-2201 UDP/61875-62000	0.0.0.0

Additional Information

VIAapp Download over VIAPad

VIAapp Download over the VIAPad has changed dramatically in its behavior. This function now operates on a separate port (9983 TCP) so that guest users cannot see port 80 or 443 open on their subnet.

Isolating Communication per Client

In an integrated environment, potential vulnerabilities must always be considered. A key factor in dealing with vulnerabilities is to isolate communication per client as much as possible. Another helpful factor is blocking the user from viewing too much information about a system. A simple way to do that is to request the Web server versions running on those systems.

Available Connection Types by Device

Device	Wired LAN 1	Wired LAN 2	Wireless
VIA Collage	✓	✓	
VIA Campus	✓	✓*[1]	
VIA GO	✓		✓*[4]
VIA Connect PRO	✓		✓*[2/4]
VIA Connect PLUS	✓		✓*[2/4]
VIAware* [3]	✓	✓	✓

*1 USB to RJ-45

*2 USB to WLAN

*3 Available connection types depend on the hardware being used.

*4 Built-in access point possibility (works only with connected WLAN module).

KRAMER

P/N: 2900- 300977 Rev: 1

SAFETY WARNING

Disconnect the unit from the power supply before opening and servicing

For the latest information on our products and a list of Kramer distributors, visit our Web site where updates to this user manual may be found.

We welcome your questions, comments, and feedback.

www.KramerAV.com
info@KramerAV.com