



Teldat IP Alarm System

Traffic patterns and network integration highlights

APPLICATION DOCUMENT

Product : VisorALARM & IPDACT Summary: System IP traffic patterns & network integration highlights Date : August 2008	Product version : ---- Document version : 2.0
--	--



INDEX

INDEX	1
SYSTEM IP TRAFFIC FLOWS	2
SCENARIO 1: IPDACT AND VISORALARM BEHIND A NAPT ROUTER	3
SCENARIO 2: IPDACT AND VISORALARM IN A VPN	4
ANNEX: ARC BANDWIDTH DIMENSIONING	6

System IP traffic flows

All the IP traffic exchanged between the IPDACT and the VisorALARM is of type UDP. This traffic runs on a single UDP connection (i.e. a single UDP port).

Although the Teldat UDP frame payload is encrypted, the frame header is sent without any encryption, so all network equipments can process and forward them without any restriction at all, just as they do with any other application traffic based on UDP (IP telephony audio streams, video streams, etc).

As such, the UDP header of all frames transmitted from the IPDACT to the VisorALARM:

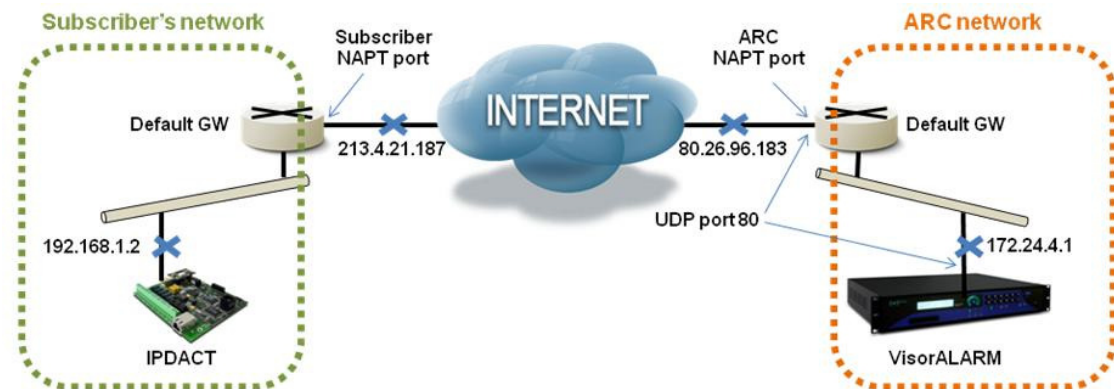
- Have both the UDP source and destination ports set to the VisorALARM serving port value (UDP port 80, by default). This port is manually configured.
- Have the source IP address set to the IPDACT local IP address. This address is manually configured or obtained from DHCP.
- Have the destination IP address set to either the VisorALARM IP address. This IP address is also manually configured in the IPDACT.
- Are transmitted through the IPDACT default gateway IP address.

In analogy, all UDP frames sent from the VisorALARM to the IPDACT:

- Have the UDP source port value set to the VisorALARM serving port (UDP port 80, by default).
- Have the destination UDP port set to the IPDACT port, that was learnt in the VisorALARM from the last IPDACT keep-alive frame received.
- Have the source IP address set to the VisorALARM LAN port IP address.
- Have the destination IP address set to the IPDACT address, that was learnt in the VisorALARM from the last keep-alive received.
- Are transmitted through the VisorALARM default gateway IP address.

Scenario 1: IPDACT and VisorALARM behind a NAPT router

In a typical scenario, the IPDACT and VisorALARM default gateways are connected to the Internet. The UDP frames transmitted to the Internet through these gateways are hence modified according to NAPT (Network Address Port Translation). The following diagram illustrates a network diagram for this scenario as well as the UDP frame header parameters in each network segment (subscriber network, the Internet and the ARC network):



		UDP frame header parameters			
Transmission flow	Network	Source IP address	Destination IP address	Source Port	Destination port
IPDACT → VisorALARM	Subscriber	192.168.1.2	80.26.96.183	80	80
	Internet	213.4.21.187	80.26.96.183	Subscriber NAPT port	80
	ARC	213.4.21.187	172.24.4.1	Subscriber NAPT port	80
VisorALARM ← IPDACT	ARC	172.24.4.1	213.4.21.187	80	Subscriber NAPT port
	Internet	80.26.96.183	213.4.21.187	ARC NAPT port	Subscriber NAPT port
	Subscriber	80.26.96.183	192.168.1.2	ARC NAPT port	80

Figure 1. NAPT scenario and UDP frame header conversions

As we can observe in Figure 1, both routers need to do NAPT so the transmitted UDP frame travels along the Internet with the system public IP addresses (213.4.21.187 and 80.26.96.183 in the Figure). For the correct system operation, the subscriber's network firewall should allow:

- UDP traffic sent from the IPDACT (IP address: 192.168.1.2 in the example) to the ARC public IP address (80.26.96.183 in the example). On transmission, the subscriber's default gateway sets a NAPT conversion entry in its cache memory, so the received UDP traffic from the Internet can be forwarded back to the IPDACT.
- UDP traffic received from the ARC (80.26.96.183). The subscriber's default gateway will forward this traffic to the IPDACT (192.168.1.2) according to its cached NAPT entry.

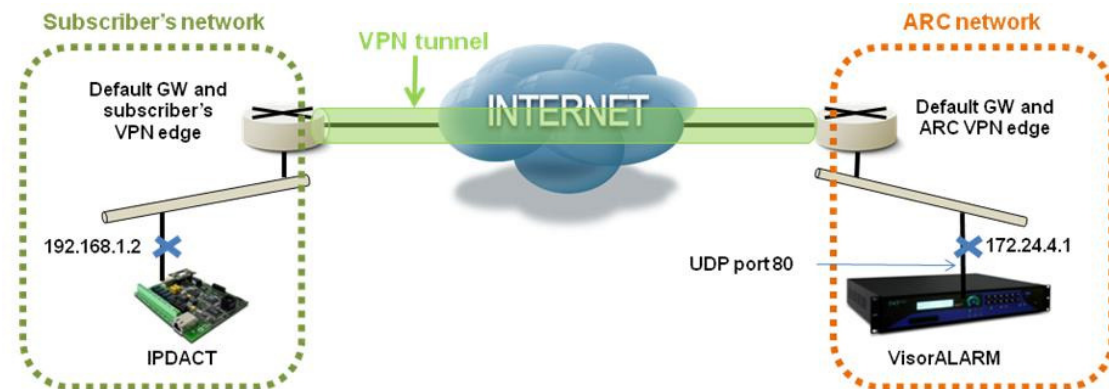
In analogy, the ARC network firewall should allow:

- UDP traffic received from the Internet to its serving port (port 80 in the example). Traffic to this port should be triggered to the VisorALARM (IP address: 172.24.4.1, serving port 80).
- UDP traffic sent from the VisorALARM to the Internet.

Scenario 2: IPDACT and VisorALARM in a VPN

The Teldat IP alarm system already offers high protection and secured data transmission. The payload of the UDP traffic exchanged between the IPDACT and the VisorALARM is encrypted in AES-512, but also the system offers its own protection mechanism for device substitution and man-in-the-middle attacks. As such, the implementation of a VPN network for this system is not necessary. However, if a VPN network is already available, the user can seamlessly integrate his IPDACT's and VisorALARM's, just as he integrates other third party or generic hosts, with no additional precautions.

Typical VPN implementations consist on establishing a tunnel between the subscriber's and the ARC gateways along the Internet. Figure 2 depicts a simple scenario where the subscriber's and ARC default gateways are also terminating the VPN tunnel at their respective sides:



Transmission flow	Network	UDP frame header parameters			
		Source IP address	Destination IP address	Source Port	Destination port
IPDACT → VisorALARM	Subscriber	192.168.1.2	172.24.4.1	80	80
	Internet (*)	Subscriber VPN edge	ARC VPN edge	----	----
	ARC	192.168.1.2	172.24.4.1	80	80
VisorALARM ← IPDACT	ARC	172.24.4.1	192.168.1.2	80	80
	Internet (*)	ARC VPN edge	Subscriber VPN edge	----	----
	Subscriber	172.24.4.1	192.168.1.2	80	80

(*) The UDP header parameters of frames transmitted through the Internet tunnel depends on the VPN implementation

Figure 2. VPN scenario and UDP frame header parameters.

VPN implementation based on IP tunnels provides the user with LAN-to-LAN “transparency”: Some hosts in the subscriber's LAN network (those ones defined in the Security Policy) will have direct IP connectivity to hosts and servers in the ARC LAN network. For the host (IPDACT) “sees” its remote peer (VisorALARM) as if it was connected to the same IP network.

In the Figure 2 example, the subscriber's VPN edge gateway should be capable of route the IP traffic destined to host 172.24.4.1 through the VPN tunnel. The ARC VPN gateway should include a route to the host at 192.168.1.2 through the VPN tunnel.



The VPN network edge (i.e. the subscriber's gateway or ARC gateway) adapts the UDP traffic flow so it can be transmitted through the tunnel. This adaptation may imply modifications on the UDP frame header formats specified in the Figure Chart. Nevertheless, the VPN peer (the ARC gateway or subscriber's gateway, respectively) will undo these modifications to convert the tunnelled IP traffic to LAN IP traffic so it can be transmitted all the way to its destination.

In this case, the subscriber and ARC network firewalls should also include the security rules that allow the traffic flows specified in Figure 2 Chart.

ANNEX: ARC BANDWIDTH DIMENSIONING

In this section we are going to analyze the mIP/IPDACT-VisorALARM system traffic. This analysis should be used as a basis in order to size the IP communications in the alarms reception center.

The incoming and outgoing IP traffic in the VisorALARM depends on:

- The number of mIP/IPDACT devices being served. Each VisorALARM is capable of managing up to 3000 mIP/IPDACTs. In High-availability ARC setups, a Backup VisorALARM is added, but the limit of 3000 mIP/IPDACT accounts is kept.
- The poll time (i.e. the *keep-alive* time interval) configured in the mIP/IPDACT. The minimum configurable poll time is 10 seconds. More traffic is generated with a shorter poll time.
- Alarms sent by the mIP/IPDACT modules.
- Traffic generated by the configuration synchronizations between the VisorALARM devices.

If we fix the poll time to the minimum configurable value of 10 seconds, we can estimate the maximum throughput required for the ARC IP service:

Number of mIP/IPDACT	Incoming traffic in the VisorALARM	Outgoing traffic from the VisorALARM
500	600 Kbps	550 Kbps
100	950 Kbps	900 Kbps
1500	1300 Kbps	1250 Kbps
2000	1700 Kbps	1650 Kbps
2500	2100 Kbps	2050 Kbps
3000	2500 Kbps	2450 Kbps

Chart 1. Maximum ARC throughput as a function of the amount of served mIP/IPDACT's

The poll time in UL-listed mIP and IPDACT devices is limited to a minimum of 90 seconds, complying with UL specifications.

The values in Chart 1 were measured assuming a traffic pattern of a typical ARC, where 55% of the IP traffic corresponds to user alarms, 35% corresponds to account supervision and the rest is used for the Main and Backup VisorALARM Data Base synchronization in High Availability scenarios. The traffic breakdown is illustrated in Chart 2.

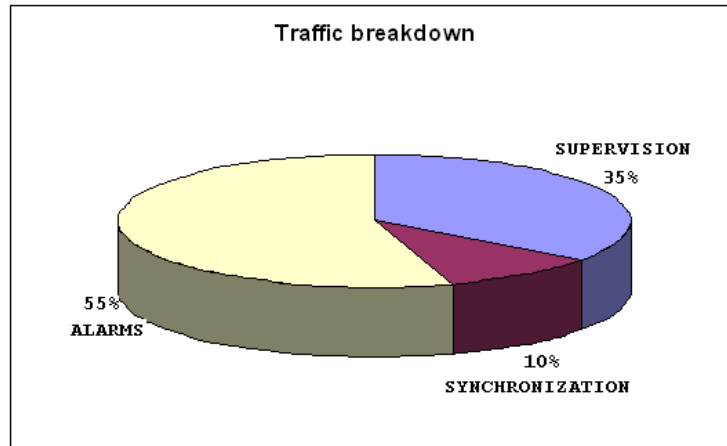


Chart 2. The typical ARC traffic breakdown

Teldat recommends that the network infrastructure in the alarms reception center is sized bearing in mind the values in the above table.

Through a linear interpolation, we can obtain the bandwidth capacity estimation for a keep-alive of 90 seconds (minimum poll time interval for UL-listed mIP/IPDACT's):

Number of mIP/IPDACT	Incoming traffic in the VisorALARM	Outgoing traffic from the VisorALARM
500	67 Kbps	61 Kbps
100	106 Kbps	100 Kbps
1500	144 Kbps	139 Kbps
2000	189 Kbps	183 Kbps
2500	233 Kbps	228 Kbps
3000	278 Kbps	272 Kbps

Chart 3. ARC throughput with a poll time of 90 seconds.

If the user wants to adjust the keep-alive timer to receive a *Communication loss trouble* within 5 minutes, the keep-alive time interval should be set to 140 seconds, which yields the following estimation:

Number of mIP/IPDACT	Incoming traffic in the VisorALARM	Outgoing traffic from the VisorALARM
500	21 Kbps	19 Kbps
100	32 Kbps	31 Kbps
1500	45 Kbps	43 Kbps
2000	59 Kbps	57 Kbps
2500	72 Kbps	71 Kbps
3000	86 Kbps	84 Kbps

Chart 4. ARC throughput with a poll time of 140 seconds.