Technical Advice Note 312 Ed6

Central Station connection to UTC UltraSync Network

24 Oct 2016

Intended Audience for this Document

This document describes the network and equipment setup required to connect a central station to the UTC UltraSync network, specifically:

- Internet access
- Routers
- Firewalls, and,
- Central station Automation Software
- Central Station Automation System Host computer

This document is targeted at central station staff and their IT support staff familiar with the configuration of these systems and the connection of central station receivers.

Overview

The UltraSync network supports permanent connectivity to fourth generation alarm panels such as the UltraSync Self-Contained Hub, NX595E and UltraSync Modular Hub. This connectivity is used to:

- Deliver alarms from panels to central monitoring stations
- Supervise the communications links to the alarm panels and report disconnections
- Carry out remote configuration of the alarm panels using remote programming software such as the DLX-900
- Provide end customers with remote access to their alarm panel via a smart phone App to: check the state of the panel, arm or disarm the panel, view video and control home automation devices
- Facilitate remote access to diagnostic information from the alarm panel
- Allow new firmware versions to be downloaded into the alarm panel

The UltraSync network appears to the central station automation system as two dialer receivers, main and backup (for redundancy) both supporting the typical receiver functionality of:

- Alarm delivery to the Automation System using either the Surgard or the Ademco685 protocol
- Receiving the event Ack message from the Automation System. The Ack message from the Automation System is used to 'kiss-off' to the alarm panels.
- Poll the Automation System and monitor the responses – UltraSync will raise an indication on the UltraSync portal if Automation System responses are not received

The connection between the UltraSync network and the central station Automation System is carried out over secure IPsec tunnels terminated in two SonicWall SoHo IPsec routers located at the central station (main and backup). The physical connection into the Automation System can be via:

- IP – This uses the decrypted IP stream directly from the SonicWall router into the Automation System. In this mode the Automation System operates as a client and establishes an IP connection to the UltraSync network (via the SonicWall router) which acts as a server.
- Serial – This mode uses a serial connection into the Automation System. It uses a LANtronix EDS2100 (or UDS1100) Ethernet to Serial converter to convert the IP traffic from the SonicWall router.

  *** This LANtronix device is not part of the SonicWall kit and needs to be purchased separately by the Central Station

The following sections detail:

1. The setup of the connection with the UltraSync network using the SonicWall security router
2. The configuration of IP connectivity between the Automation System and the UltraSync network
3. The configuration of serial connectivity between the Automation System and the UltraSync network

Setting Up the SonicWall SoHo

As both the IP and serial connection options into the Automation System use the SonicWall SoHo security router, it is essential to cover the setup of the SonicWall security routers.

The SonicWall SoHo is used to provide a secure connection between the UltraSync network and the alarm monitoring center. This is achieved by transporting the data traffic between the Automation System and the UltraSync network through an encrypted IPsec tunnel.

The SonicWall SoHo may be installed at the central station as follows:

1. Using a direct internet connection with a dynamic public IP address (not preferred)
2. Using a direct internet connection with a static public IP address (not preferred)
3. Behind a NAT firewall with a dynamic (private) IP address
4. Behind a NAT firewall with a static (private) IP address

Option 3. and 4. are preferred as they provide the highest level of security by using the central station's existing firewall to block unwanted IP traffic. In addition, as the SonicWall only makes outgoing IP connections there is no need to setup port forwarding to the SonicWall WAN address.

The ideal location for the SonicWall router is in the central station's network DMZ is as shown in Figure 1. The SonicWall router's WAN/X1 port is wired to the central station's DMZ or router.

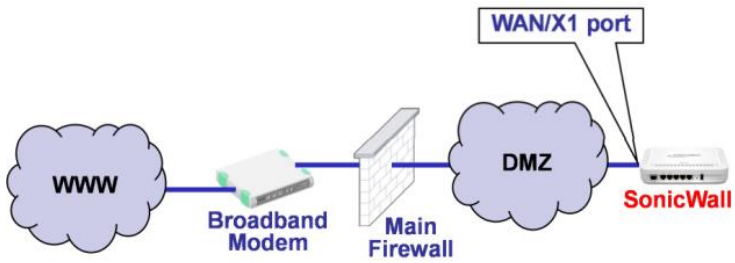

Figure 1: SonicWall Network Connections

While not shown above, the setup is duplicated to increase the reliability of the connection. Thus the SonicWall router designated as A-Side is used as the main connection for alarm delivery to the Automation System and the one designated as B-Side provides the backup alarm delivery path. For path redundancy each SonicWall router (A-Side and B-Side) is connected to the internet via a different internet service provider.

Generally firewalls do not restrict outgoing IP traffic. However if the existing central station firewall is configured to restrict outgoing traffic, in order to support connectivity to UltraSync the firewall needs to be setup to allow the connections detailed in Table 1. Note that the connections listed support redundant connectivity to UltraSync under both normal and disaster recovery situations.

Firewall Configuration	A-Side SonicWall	B-Side SonicWall	Comment
Outgoing connection from the SonicWall to:	54.165.85.1	54.173.40.41	Main
Outgoing IP Port	UDP 500 (ISAKMP)	UDP 500 (ISAKMP)	
Outgoing IP Port	UDP 4500 (IPSEC NAT-T)	UDP 4500 (IPSEC NAT-T)	
Outgoing connection from the SonicWall to:	52.4.36.36 52.8.34.159	52.4.36.36 52.8.31.34	Disaster Recovery
Outgoing IP Port	UDP 500 (ISAKMP)	UDP 500 (ISAKMP)	
Outgoing IP Port	UDP 4500 (IPSEC NAT-T)	UDP 4500 (IPSEC NAT-T)	

Table 1

Configuring the Network settings of the SonicWall WAN port

The SonicWall router is delivered with its private tunnel IP address labeled on the unit. This address is unique and is used only by the UltraSync network to identify the particular unit and associate it with the specific central monitoring station. This address has to be provided to the UTC personnel to support its activation and is displayed on the UltraSync web portal.

The SonicWall unit's WAN port (also designated as X1) is connected to the central monitoring station's network – preferably on the DMZ as shown in Figure 2. The SonicWall unit's WAN/X1 port requires an IP address on the DMZ. This port is configured as a DHCP client by default allowing the IP address to be set automatically, or it can be set manually with a static IP address as detailed below.

The following procedure is only required if the SonicWall router port X1 is to be configured with a static IP address:

- Connect a laptop configured as a DHCP client directly to the SonicWall router's X0 port, also called "LAN" port (note that for security reasons configuration of the WAN port is only available via the LAN port)
- Launch a web browser on the laptop and enter the URL https://192.168.168.168 on the address bar
- Log in to the SonicWall router using the following credentials:

  Username: installer

  Password: 9713
- Select the "Network Interfaces" menu. For the X1 (WAN) interface, click the configure icon. Enter the following information in the box that pops up:

Field	User Entry
IP assignment	Static
IP address	as required for network
Subnet Mask	as required for network
Default Gateway	as required for network
DNS Server 1	as required for network
DNS Server 2	as required for network, use 0.0.0.0 if not required
DNS Server 3	as required for network, use 0.0.0.0 if not required

Table 2

It is necessary to have at least one DNS server configured as the IPsec VPN setup uses a hostname.

Press OK to save the settings and dismiss the popup.

Please note that the SonicWall login should only be used to:
1. Configure the static IP address on port X1 as detailed above
2. Carry out network diagnostics as detailed below
3. Optionally configure port X2 under the guidance of the UTC Network Engineer

No other settings on the SonicWall router are to be changed via the web page.

IP Connections to Automation System

As noted above the SonicWall router can deliver alarms directly to the Automation System over IP. The Alarm Receiving Software which is acting as a client establishes a TCP/IP connection via Port 4000 to each of the SonicWall routers acting as a server (through port X1 of the SonicWall router).

Figure 2 below illustrates the central station network setting for IP connectivity to the Automation System.

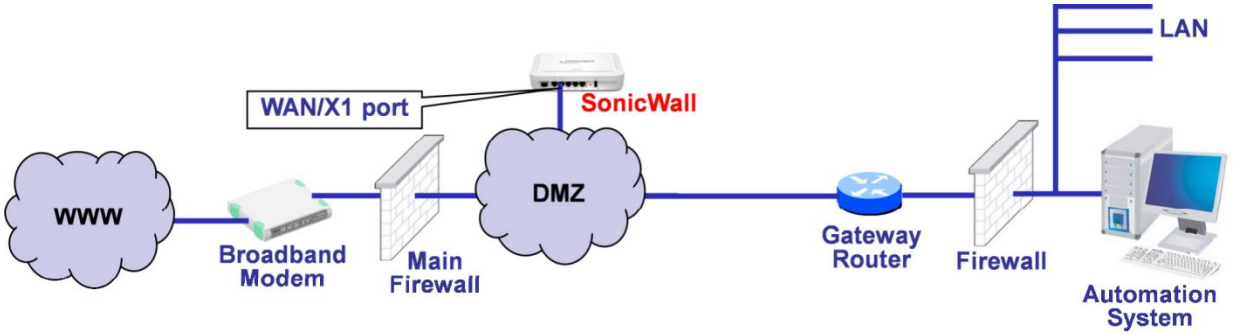

Figure 2: IP Connection to Automation System

In order to maximize security, the LAN firewall on the right-hand side of Figure 2 is configured to ensure that only Automation System traffic is able to reach the SonicWall router from the LAN side.

The Gateway Router is optional. It is used only when the LAN is on a different subnet to the SonicWall. If a Gateway Router is deployed, it is recommended that Source NAT is performed on TCP connections initiated from the Automation System to the SonicWall so that the data packets appears to come from the same WAN/X1 subnet as the SonicWall. This eliminates the need to modify the standard configuration in the SonicWall.

Please contact the UTC Network Engineer if a more complex network setup is required.

As the Automation System connects out to the SonicWall routers, each SonicWall router must have a known IP address. This is achieved by either:

- Allocating each SonicWall router a static IP address, or,
- In the LAN router allocating to each SonicWall router a fixed DHCP address assignment

Summary of data required to setup the connection:

Information Required	Value
Automation System Protocol	Select one: • Surgard (default), or, • Ademco685 • SIA-DC09
IP Address of SonicWall (A-Side)	To be provided by the central station as part of the setup
SonicWall (A-Side) TCP Port	4000
IP Address of SonicWall (B-Side)	To be provided by the central station as part of the setup
SonicWall (B-Side) TCP Port	4000
Gateway address(es) Required where the Automation System is on a different subnet to the SonicWall.	To be provided to UTC Network Engineer by central station. The UTC Network Engineer will remotely setup the required Gateway in the SonicWall routers.

Table 3

As part of a final check please ensure that:

- The firewall allows traffic flow between the Automation System and the SonicWall router
- The gateway allows traffic flow between the Automation System and the SonicWall router
- The Automation System (Windows™) Host firewall allows two-way traffic flow to the SonicWall

Serial Connection to the Automation System

Figure 3 below details the network arrangement that supports a serial connection from the UltraSync network with the Automation System.

The LANtronix EDS2100 or equivalent is used to convert the IP UltraSync traffic from the SonicWall router into serial for the Automation System. As shown in Figure 3 below the LANtronix device is connected to Port X3 of the SonicWall router.

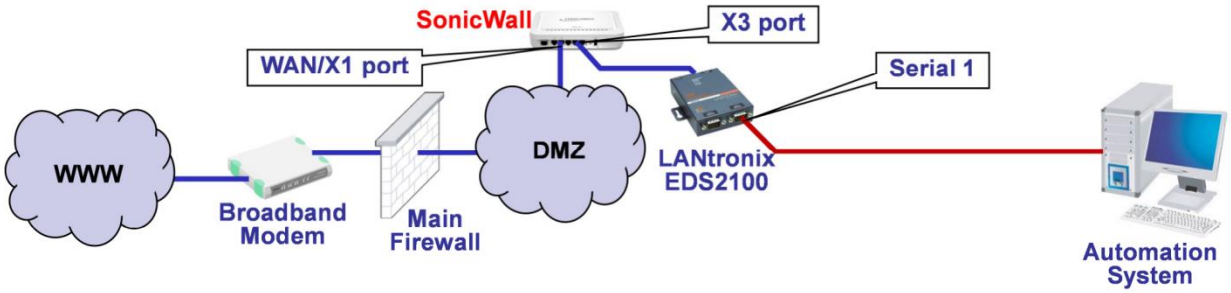

Figure 3: Serial Connection to Automation System

Before installing, use the reset switch to default the LANtronix unit.

The LANtronix EDS2100 (or EDS1100 – single port variant) is configured as follows:

Parameter	Default Value
SonicWall Port:	X3
LANtronix IP Address:	Dynamic – DHCP (default)
LANtronix Serial Port:	Port 1
Serial Baud Rate:	9600 bps (default)
Serial Data:	8 bits (default)
Serial Parity:	None (default)
Serial Cable (EDS2100):	9-Pin DTE, ports used: Tx, Rx, GND – see table below
Serial Cable (EDS1100):	25-Pin DCE, ports used: Tx, Rx, GND – see table below

Table 4

Device Pin function	EDS2100 (9-pin male - DTE) – PIN:	EDS1100 (25-pin female - DCE) – PIN:
Serial Input	2	2
Serial Output	3	3
GND	5	7

Table 5

The Automation System serial port parameters should also be configured as per the LANtronix above.

Configuration of the Automation System

At the central station the Automation System has to be configured to receive alarms from the UltraSync network. That is the Automation System is the TCP/IP client while the UltraSync network is the TCP/IP server.

The table below provides a summary of the requirements:

Automation System Requirements: Surgard	Connection Type	
	IP	Serial
Activate two Surgard receiver tasks (main & backup) in the Automation Software	✓	✓
Setup receiver tasks in the Automation Software as IP clients	✓	
Enter the SonicWall IP address for each receiver task in the Automation Software	✓	
Enter IP Port 4000 for each receiver task in the Automation Software	✓	
Allocate two serial ports (main and backup) on the Automation System Host		✓
Configure the serial ports as: 9600 bps, 8-bits, No parity		✓
Prepare serial cables from LANtronix devices to Automation System Host		✓
UltraSync sends the Automation System an idle message every 50 seconds which is Acknowledged by the Automation System by sending the ASCII 'Ack' character. Configure the Automation System to look for an idle message every five minutes to filter out short duration network disruptions. UltraSync idle message: 1011<11 spaces (ASCII 32)>@<4 spaces (ASCII 32)> <DC4 (ASCII 20)> Note that the '<' & '>' characters are delimiters and do not form part of the string. Automation software response = ASCII 6 'Ack'	✓	✓

Table 6a

Automation System Requirements: Ademco685	Connection Type	
	IP	Serial
Activate two Ademco685 receiver tasks (main & backup) in the Automation Software	✓	✓
Setup receiver tasks in the Automation Software as IP clients	✓	
Enter the SonicWall IP address for each receiver task in the Automation Software	✓	
Enter IP Port 4000 for each receiver task in the Automation Software	✓	
Allocate two serial ports (main and backup) on the Automation System Host		✓
Configure the serial ports as: 9600 bps, 8-bits, No parity		✓
Prepare serial cables from LANtronix devices to Automation System Host		✓
Set the Automation System receiver polling period to 30 seconds Automation System poll message = 'S' UltraSync response = ASCII 6 'Ack'	✓	✓

Table 6b

Trouble Shooting the Connection

1. If the VPN does not establish, additional diagnostic information can be obtained by logging into the SonicWall router using the access credentials noted above.

   Refer to Figure 4 below, the process is as follows:
   a. Login to the SonicWall router
   b. Select System
   c. Select Diagnostic Tools
   d. Select Check Network Setting
   e. Press the Test button on each row labelled DNS Server

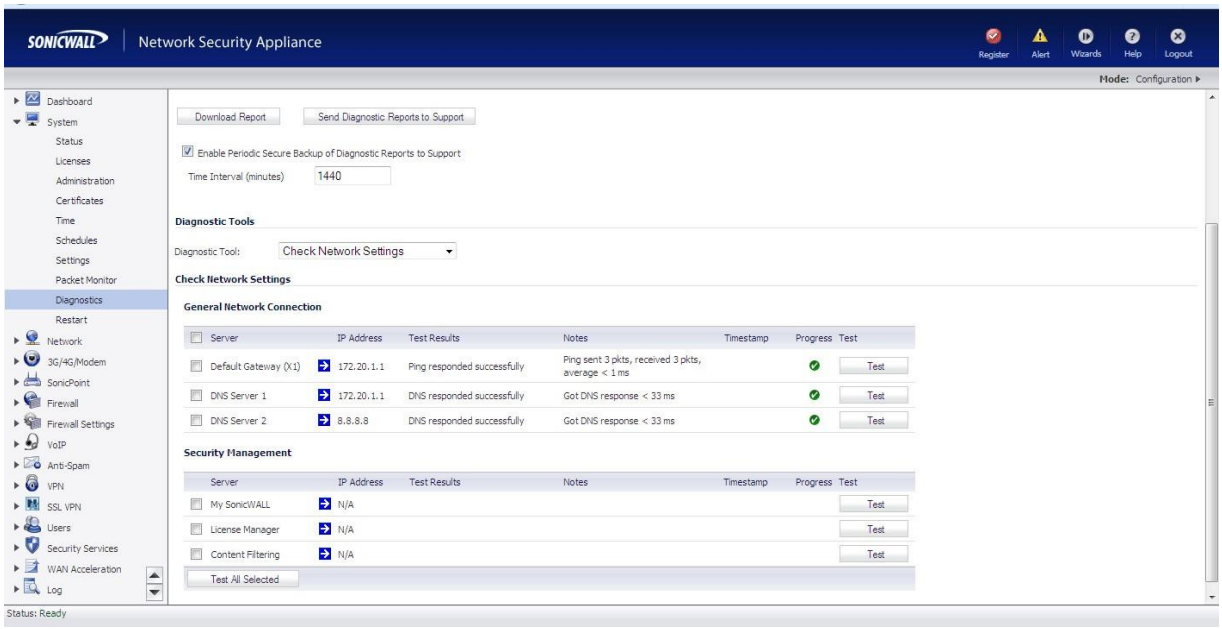

Figure 4: SonicWall Diagnostics

In the column labelled Test Results, each DNS test should return "DNS responded successfully".

2. Use the netcat PC software to diagnose the connection between the SonicWall router and the Automation System.
   a. Obtain a copy of from the UTC Network Engineer and install on a PC
   b. Unplug the SonicWall and plug in the PC into the same router port as the SonicWall router
   c. Configure the PC with the same IP address as the SonicWall router
   d. At the command prompt enter the following to run the netcat program: `ncat -vk1 4000`

   The netcat program can be expected to print the following results:

Result	Comment
`Ncat: Version 6.46 ( http://nmap.org/ncat )`	Printed immediately
`Ncat: Listening on :::4000`	Printed immediately
`Ncat: Listening on 0.0.0.0:4000`	Printed immediately
`Ncat: Connection from 192.168.10.71.`	Printed when a connection is established
`Ncat: Connection from 192.168.10.71:43619.`	Printed when a connection is established

Table 7

In the above example:

- 4000 is the port used by the Automation System to connect to the SonicWall router
- 192.168.10.71 is the IP address of the Automation System – this is setup dependent
- 43619 is the Automation System source IP port – This port is setup dependent and can be expected to vary

If there is no connection to the Automation System, the netcat printout will stop at:

```
Ncat: Listening on 0.0.0.0:4000
```