U.S. Department
of Transporation

Federal Aviation
Administration

Memorandum

Subject:	**INFORMATION**: Engineering Brief No. 84 Remote Maintenance and Monitoring of ALCMS and L-821 Computerized Control Panels	Date:	Feb 22, 2011
From:	Manager, Airport Engineering Division, AAS-100	Reply to Attn. of:	
To:	All Regions Attn: Manager, Airports Division		

ENGINEERING BRIEF NO. 84

Remote Maintenance and Monitoring of ALCMS and L-821 Computerized Control Panels

I. PURPOSE

This Engineering Brief provides guidance and information to airports, Airport District Offices (ADOs), and Architectural and Engineering (A&E) companies on the appropriate use of virtual private network (VPN) technology for secure remote maintenance and monitoring of airport lighting control management systems.

II. BACKGROUND

The support and troubleshooting of airport lighting control management systems (ALCMS) requires expert support personnel to be physically present on site, with remote troubleshooting being difficult, if not impossible. This situation is frequently defended via the claim of “better security”, but the result has been degraded response times for system repair, as well as significantly increased staff and travel costs for the industry. As ALCMS systems become increasingly based on complex computer technology, and expert knowledge is needed to effectively troubleshoot them, this situation will only get worse.

At the same time, secure remote access technology has matured significantly in the past half decade. Today, high risk processes such as hospital intensive care systems, oil and gas pipelines, and power transmission systems take advantage of carefully designed Virtual Private Network (VPN) architectures to allow support specialists to remotely connect to mission-critical systems in order to investigate and troubleshoot reported operations problems. The result is more timely response to issues, reduced system down time and better utilization of increasingly scarce expert resources. An unexpected benefit for companies using well architected systems is improved security, because other secondary uncontrolled access methods such as modems, mobile laptops and USB keys (e.g. storage devices) are no longer needed and all maintenance access can be managed through the system.

III. APPLICATION

Current L-890 ALCMS and possibly L-821 Computerized Control Panels.

IV. DESCRIPTION

This document provides guidance for the design and use of virtual private network (VPN) systems for secure remote maintenance and monitoring of airport lighting control management systems. It outlines the technology concepts and requirements to ensure secure remote maintenance and explains the functionality of the VPN server and client components that are needed for an appropriately designed system. An example user interface and security control interface is provided, along with an example installation and design recommendations. In addition, the test requirements to verify proper operation are described.

V. EFFECTIVE DATES

This engineering brief shall be effective after signature by the Manager of FAA Airport Engineering Division, AAS-100.

VI. APPLICABLE DOCUMENTS

FAA Advisory Circulars:

AC 150/5345-56, *Specification for L-890 Airport Lighting Control and Monitoring (ALCMS)*

AC 150/5345-3, *Specification for L-821 Panels for the Control of Airport Lighting*

Industry Standards:

IEC 60068-2-6, *Environmental Testing – Part 2:Tests – Test Fc: Vibration (sinusoidal)*

IEC 60068-2-27, *Amendment 1 – Basic Environmental Testing Procedures, Part 2-7: Tests – Test Ga and Guidance: Acceleration, Steady State*

EN 61326-1, *Electrical Equipment for Measurement, Control, and Laboratory use: General Requirements*

EN 61010-1, *Safety requirements for electrical equipment for measurement, control, and laboratory use – Part 1: General requirements*

1.0 Recommended Industry Best Practices.

Implement the highly secure Virtual Private Network (VPN) equipment described in this engineering brief to enable remote access to current ALCMS and L-821 Computerized Panels.

2.0 Understanding Remote Maintenance/Monitoring Requirements.

Remote maintenance and monitoring of critical control systems that are similar to ALCMS has been shown to increase support responsiveness, decrease total system downtime and reduce overall operating costs. The key is to design a remote access system that is provably secure so that security issues do not over shadow the benefits. In all cases, successful remote access systems are based on VPN technology that is designed and configured specifically to meet the needs of the control system environment. Sections 3 to 8 of this Engineering Brief describe what is needed in the ALCMS environment.

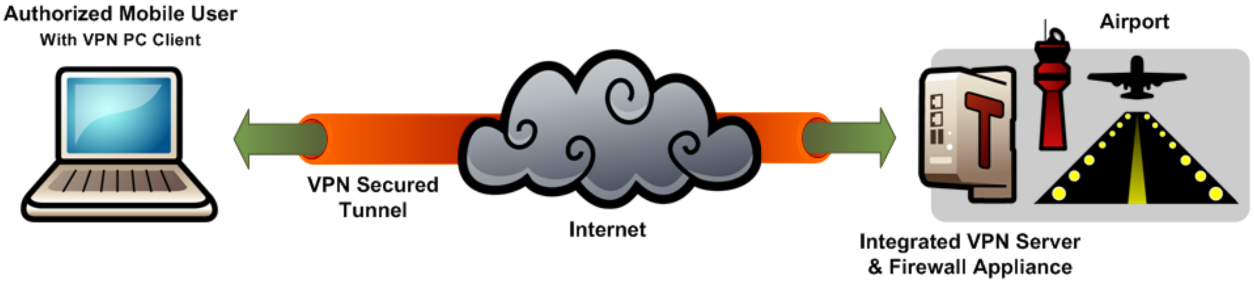


Figure 1. Secure access to critical systems for remote support personnel

2.1 How does VPN Technology Provide Reliable Security?

To understand how VPN provides security, consider this non-computer example - you have some secret information that you would like to discuss with a good friend. However, your friend lives several miles away from you, and the only way you can communicate with your friend is a two-way radio.

The first problem is, how can you keep your conversation secret? Because you are using a two-way radio, any person within range of your radio can hear everything you say. One way to keep your conversation private is to use a code that re-arranges the order of words, or substitutes different words, in a pre-agreed order. Any person listening to your conversation would not be able to understand what you are saying; only you and your friend know how to re-arrange the words from the 'scrambled' form back into a conversation that can be understood. This translation code provides the first key element of secure communications; ***Privacy***.

You have another problem however, when you communicate with a remote person; how do you know the person you are talking to is really your friend, and is not some stranger who is pretending to be your friend? On a good-quality two-way radio, you may be able to identify them by the sound of their voice over the radio; but for added protection, you will give your friend a secret phrase. When you ask for the secret phrase, your friend must tell it to you before you will begin the conversation. This secret phrase provides the second key element of secure communication; ***Authentication***.

Lastly, your friend and you are concerned that someone might inject some noise into the system that would make you misinterpret what your friend is saying. So you add a special closing to each message (such as how many times a certain set of letters was used) to validate each message and provide the final key element of secure communication; ***Integrity.***

VPN technologies create a secure 'tunnel' between two end points over an un-trusted network (such as the Internet) by electronically scrambling, authenticating and validating every message sent between the end points. In other words, VPNs provide three key capabilities:

- **Privacy**: VPNs encrypt the data passing between the two end points, so that any unauthorized person or device listening to the conversation cannot understand what is being communicated.

- **Authentication**: VPNs authenticate each end point to the other, so each party in the conversation can be sure that the other party really is who they say they are, and is not an imposter pretending to be an authorized party.
- **Integrity**: VPNs ensure that messages are not modified in transit between the sender and receiver.

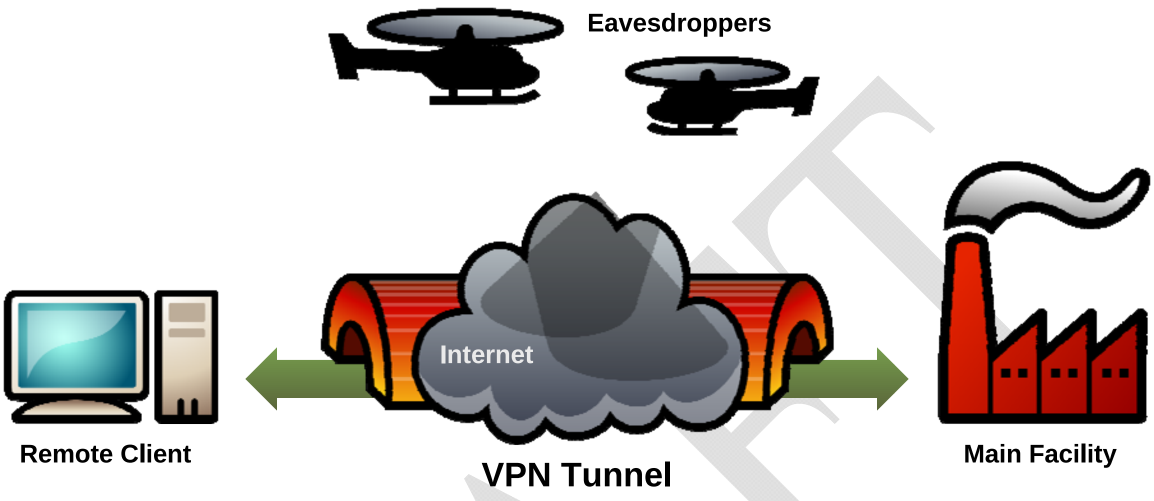


Figure 2. VPNs provide secure communication 'tunnels' across un-trusted networks

2.2 Core Components: VPN Clients and Servers.

All VPNs are designed to create point-to-point connections between a 'client' device and a 'server' device. Typically the client device is the one that initiates the connection, and the server device accepts and authenticates incoming connection requests from one or more client(s). For most ALCMS applications, a maintenance laptop might be the client and a VPN appliance might be the server. Once a VPN connection is authenticated and established between a client and a server, the networks behind the client and server are connected together such that network traffic may pass between them. In the case of a laptop client, the laptop would appear as if it was actually plugged into the network behind the VPN server – it would receive a new "virtual" IP address suitable for the local network and could access other devices just as if it was directly connected at the airport.

2.3 VPN Technology is One Piece of the Total Security Solution.

There is a common misconception that goes "if you use a VPN, then you are secure". This is not true! Once the endpoints are authenticated, a VPN lets all traffic through; it does not monitor or filter any of the traffic that passes through it. This means that if you connect a virus-infected laptop to the ALCMS control network through a VPN, the VPN will not prevent the virus from passing right through the tunnel and infecting PCs on the other end. Clearly this is not acceptable. To provide comprehensive security, a VPN must be combined with firewall capabilities on the VPN server to manage the traffic entering and leaving the VPN tunnel. The firewall should allow traffic rules to be defined on a per client basis and allow the security manager to restrict the devices that the computer can see on a strict as-needed basis. Finally, to reduce the possibility of security holes from configuration errors, seamless firewall and VPN interoperability is important – a single security console should be used for all VPN/firewall management.

2.4 Using VPN Technology to Enhance Local ALCMS Security.

One benefit from using a well-architected VPN solution is improved on-site security. When staff or suppliers bring mobile laptops and USB storage devices onto the site to perform maintenance activities, they can unintentionally introduce malware (i.e. viruses or worms) into the ALCMS.

Instead of leaving these secondary pathways uncontrolled, they can be managed through the VPN system by forcing all equipment that is not permanently on the site to connect through the VPN system even when physically in the maintenance center. This allows the firewall policies to take effect, restricting traffic on an as-needed basis.

In other words, while a computer connected directly to the ALCMS network would normally be completely unrestricted in terms of the traffic it could send on the network, a local laptop working through the VPN system could be restricted to communicating to a few ALCMS devices using only the appropriate ALCMS protocols. Since most malware does not use ALCMS protocols for propagation, this would effectively prevent the spread of Internet worms into the ALCMS. In addition, the event and alarm logging system would automatically record when maintenance activity was occurring and warn of potentially infected devices.

3.0 System Functional Block Diagram.

An ALCMS remote maintenance and monitoring system consists of the key components indicated in the block diagram below.

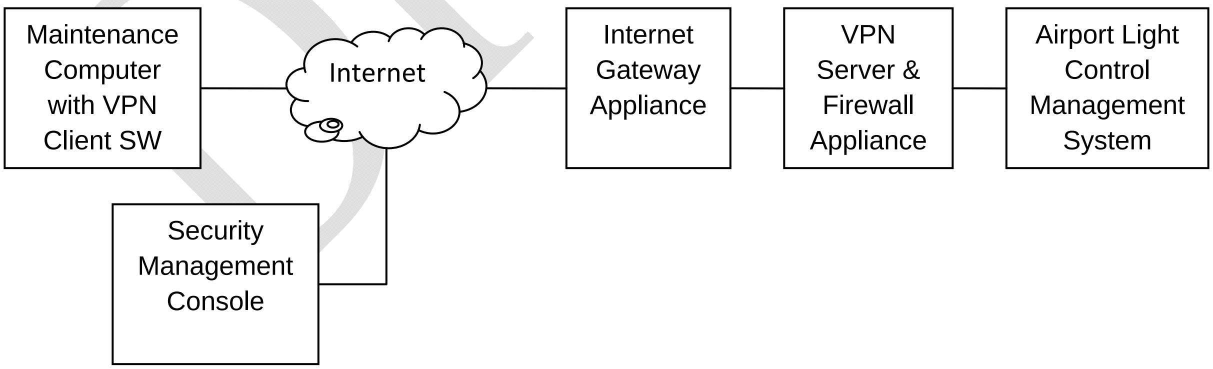

Maintenance Computer with VPN Client SW
Internet
Internet Gateway Appliance
VPN Server & Firewall Appliance
Airport Light Control Management System
Security Management Console

Figure 3. System Functional Block Diagram

3.1 Maintenance Computer with VPN Client Software.

This computer is a typical Windows-based computer (often a laptop) that is capable of connecting to the Internet (or other wide area networks) and contains software suitable for monitoring and maintaining the target ALCMS and VPN client software for connection to the designated VPN server at the airport.

3.2 External Network (Internet).

This is any wide area network that allows interconnectivity between the maintenance computer and the ALCMS. Typically it could be the Internet, but it could also be an internal airport network that is not normally secured for ALCMS use.

3.3 External Gateway Appliance.

This is a device that provides conversion/connectivity between the "Internet" and the ALCMS network. Typically it will be a device such as a DSL modem, cable modem, or wireless access point. It will provide conversion services between the internal ALCMS network and the external world. Figure 4 shows a typical device for connection to a cable broadband system. This may contain optional router services in cases where the maintenance Internet connection might be shared with other airport services.

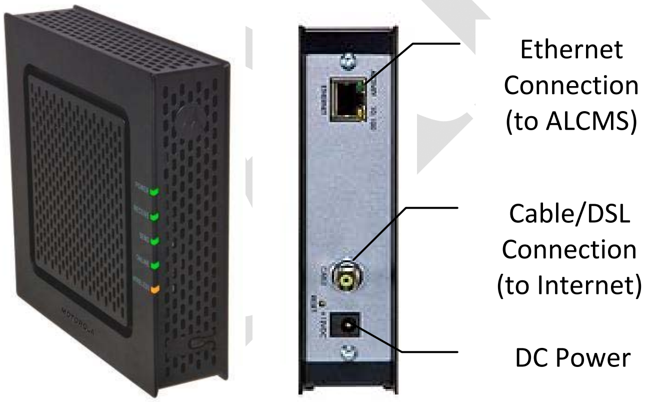

Ethernet Connection (to ALCMS)
Cable/DSL Connection (to Internet)
DC Power

Figure 4. Typical external gateway appliance (image courtesy of Motorola Inc.)

3.4 VPN Server & Firewall Appliance.

This is a hardware device that provides the VPN services at the ALCMS location. Figure 5 shows a typical integrated VPN/firewall appliance for securing mission-critical control systems.

The maintenance computer uses its VPN client software to request a connection from the VPN server by exchanging security certificates. The server then authenticates the VPN Client and if the authentication passes, determines what it is authorized to do (i.e. policy) and gives it a local IP address for the computer to use on the ALCMS network. It also exchanges one-time secret keys with the computer to use for the encryption for the duration of the connection.

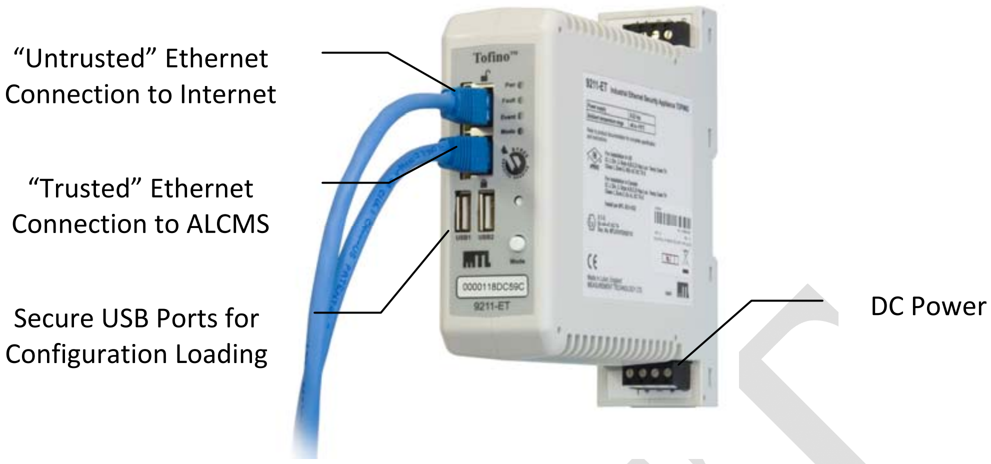

"Untrusted" Ethernet Connection to Internet
"Trusted" Ethernet Connection to ALCMS
Secure USB Ports for Configuration Loading
DC Power

Figure 5. Typical VPN server & firewall appliance (image courtesy of MTL Instruments)

The VPN server then decrypts all incoming traffic and encrypts all outgoing traffic. It also passes all traffic though the firewall policy rules to determine what devices on the ALCMS network the maintenance computer is authorized to communicate with and what network services it is allowed to use. Any traffic from the maintenance computer that does not match the policy is blocked and an alarm generated at the security management console.

3.5 Airport Light Control Management System.

These are L-890 ALCMS (and possibly L-821 Computerized Control Panels) used for airport operations. Typically this includes a number of hardened controllers and operator computers interconnected on an Ethernet network.

3.6 Security Management Console.

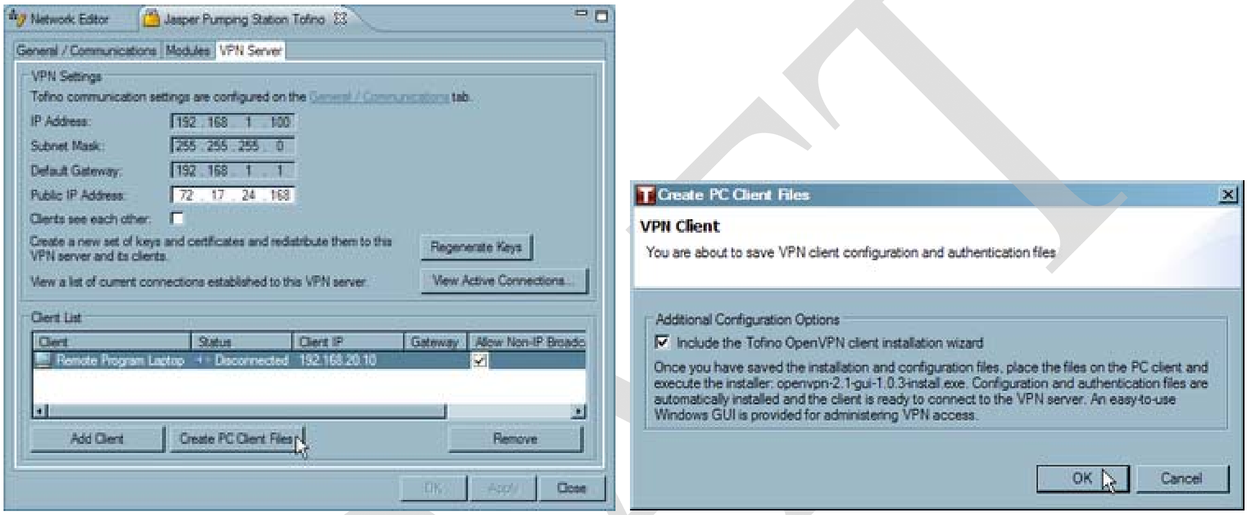
The security management console is a computer and software package that provides a centralized platform for configuring VPNs, defining security policies and rules and monitoring the system for security related events. The console could be located at the ALCMS site, but is recommended that it is located in at the ALCMS Supplier's central facility where it can be used to simultaneously monitor and coordinate security access across multiple facilities. Management connectivity between the VPN server appliances and the console is typically secured using similar VPN technology that is transparently embedded into the system.

The security management console creates and manages the security certificates used for authentication by the VPN clients and servers and centrally administers all firewall policy. It will also act as a central monitoring facility, recording all VPN connection activity (including failed attempts) and log all firewall policy violations. Finally it will monitor the health of the VPN server appliances.

4.0 Maintenance Computer User Interface.

4.1 Maintenance Computer VPN Client Installation.

Typically VPN PC client software is provided by the supplier of the VPN server, a highly recommended situation due the complexities of integrating clients and servers from different vendors. In more sophisticated products, the security management console automatically generates an installer package that integrates all the client software, VPN certificates and configuration settings into a single installation file, reducing the chance of error during VPN commissioning.



Tofino communication settings are configured on the General / Communications tab.

IP Address: 192 . 168 . 1 . 100

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 192 . 168 . 1 . 1

Public IP Address: 72 . 17 . 24 . 168

Clients see each other: □

Create a new set of keys and certificates and redistribute them to this VPN server and its clients.

View a list of current connections established to this VPN server.

Client	Status	Client IP	Gateway	Allow Non-IP Broadc
Remote Program Laptop	Disconnected	192.168.20.10		☑

VPN Client

You are about to save VPN client configuration and authentication files

Additional Configuration Options

☑ Include the Tofino OpenVPN client installation wizard

Once you have saved the installation and configuration files, place the files on the PC client and execute the installer: openvpn-2.1-gui-1.0.3-install.exe. Configuration and authentication files are automatically installed and the client is ready to connect to the VPN server. An easy-to-use Windows GUI is provided for administering VPN access.

Figure 6. Management Console creating an integrated package containing the client software, certificates and configuration settings for installation on the maintenance computer

4.2 Maintenance Computer VPN Client Usage.

The VPN client is typically started by clicking on the VPN icon on the Windows Task Bar and then selecting “Connect”. In cases where the maintenance computer is configured to service a number of different ALCMS systems, the user will select the appropriate target site.

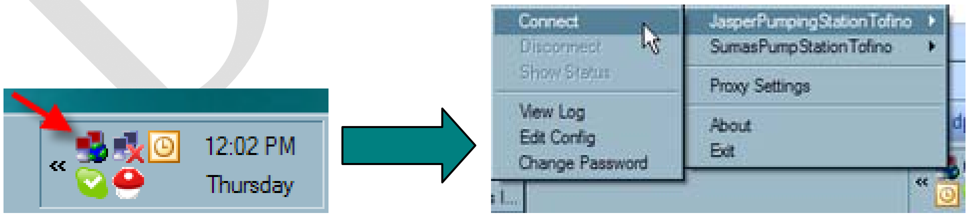


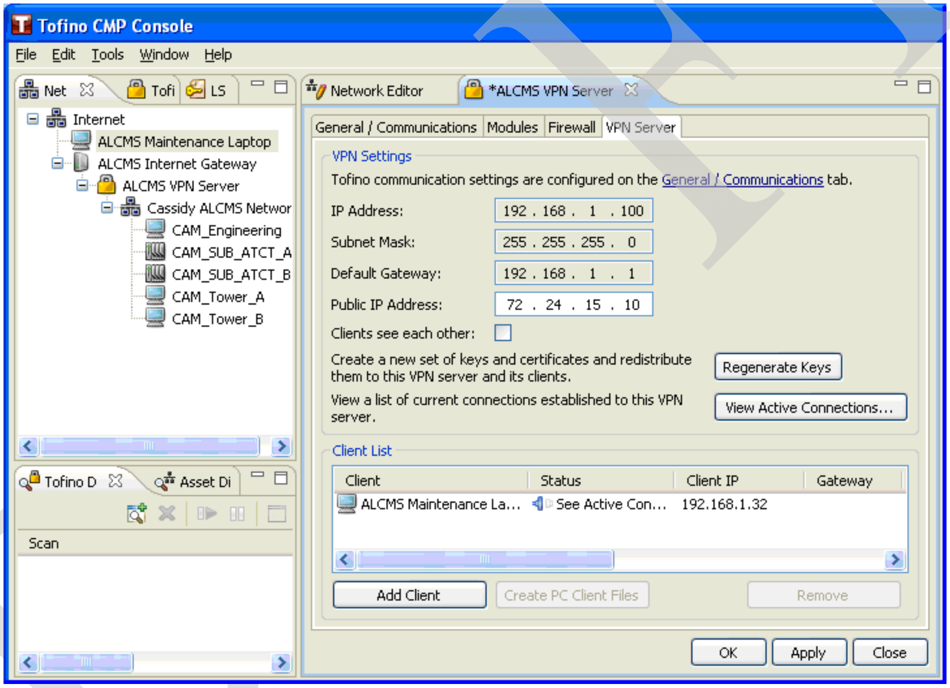
Figure 7. The VPN client is started by clicking on the VPN icon and selecting the target ALCMS

Once the VPN client is started, it will automatically connect to the appropriate VPN server at the ALCSM site and carry out all authentication tasks behind the scenes. If the authentication is accepted AND appropriate firewall rules are configured to allow it, the maintenance specialist can proceed to use any ALCMS software on the computer just as if he or she was connected to the network at the local site.

5.0 Security Management Control Interface.

A well integrated security management console is the key to a secure system. It is critical that it offers a single interface for configuring the VPNs, defining firewall security policies and monitoring the system for security related events.

Defining a VPN client to server connection involves creating identities or icons in the security management package to represent the VPN server and maintenance computer. Then to configure the VPN connection, the desired client is dragged and dropped on to the VPN Server. This will initiate the creation of unique cryptographic "certificates" that the two devices will later use to prove their identities to each other.



Tofino communication settings are configured on the General / Communications tab.

IP Address: 192 . 168 . 1 . 100

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 192 . 168 . 1 . 1

Public IP Address: 72 . 24 . 15 . 10

Clients see each other: □

Create a new set of keys and certificates and redistribute them to this VPN server and its clients.

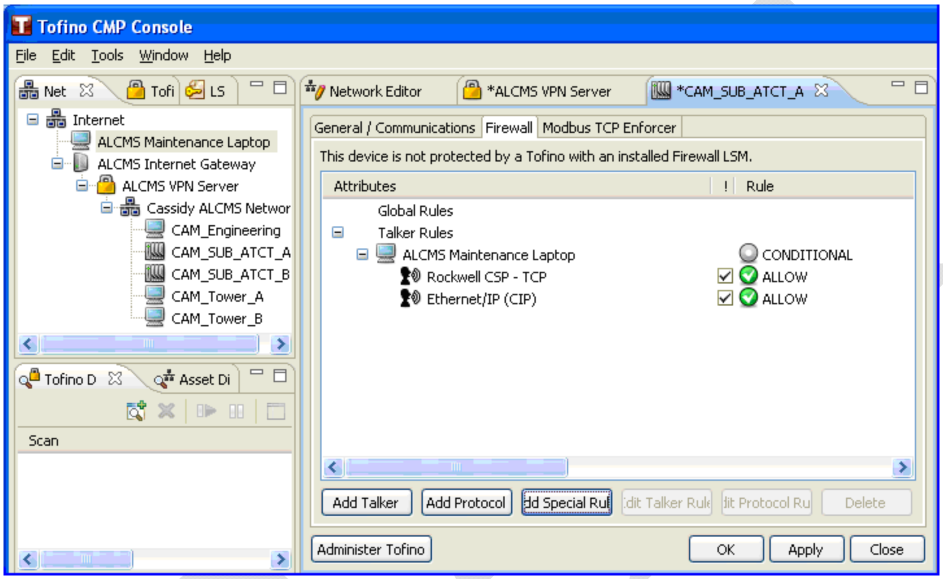
View a list of current connections established to this VPN server.

Client	Status	Client IP	Gateway
ALCMS Maintenance La...	See Active Con...	192.168.1.32	

Figure 8. Defining a new VPN connection by dragging the laptop icon onto the VPN server icon

After the VPN client to server connection is defined, the next step is to define firewall policy to manage which ALCMS devices the maintenance computer can interact. Typically this is defined on strict need-to connect basis. If required, different policies can be defined for various applications such as supervisor laptop policy for access to one set of equipment and a maintenance laptop policy for access to another set. Alternately, the VPN connection can be restricted to allowing the maintenance staff remote desktop access only to the same computers they would have access to when on site and then enforce a second login on these systems before accessing further into the ALCMS.

When the VPN and firewall configuration is complete, all information (including security certificates) needs to be transferred to both the VPN server and maintenance computer. In some systems, such as the Tofino Security Solution, the system will create custom install packages for every computer that contains both the VPN client software package and all required VPN configuration and certificate files so they can be installed on a Windows PC in a single process (see section 4.1). Similar configuration files are also created for the VPN server appliance that can be either downloaded over a network or installed via encrypted USB storage devices.

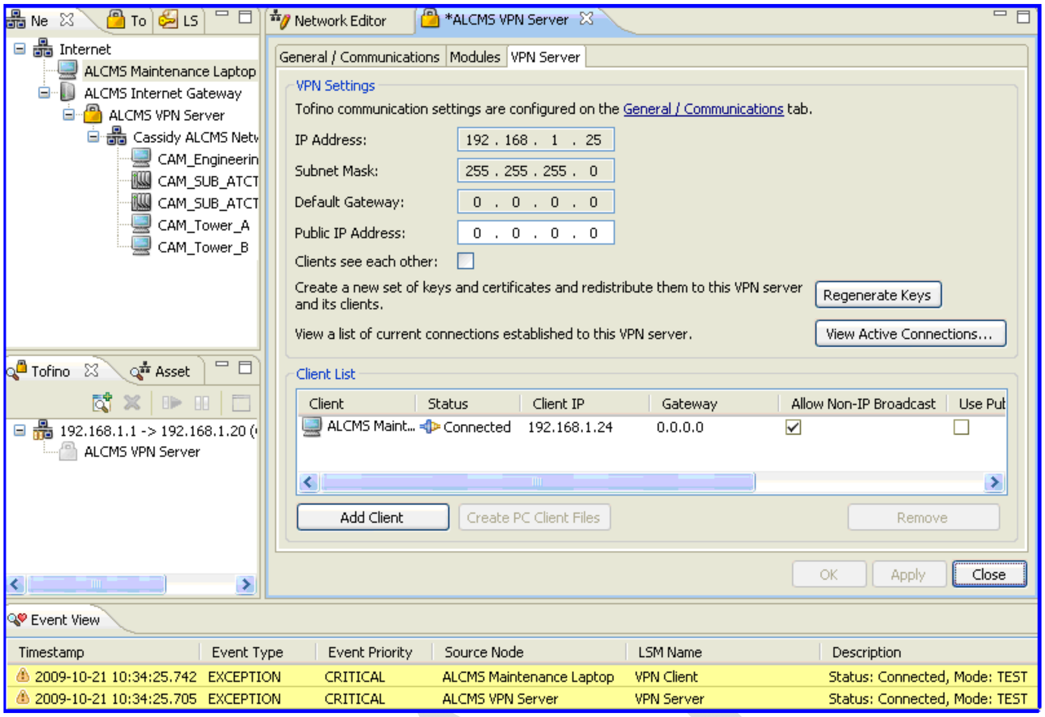


This device is not protected by a Tofino with an installed Firewall LSM.

Attributes	!	Rule
Global Rules		
⊟ Talker Rules		
⊟ ALCMS Maintenance Laptop		○ CONDITIONAL
Rockwell CSP - TCP	☑	✓ ALLOW
Ethernet/IP (CIP)	☑	✓ ALLOW

Figure 9. Defining the devices in the ALCMS that the maintenance laptop is permitted to communicate with

The final step is to set up monitoring for tracking both successful and failed VPN client to server connections and to log all firewall policy violations.



Tofino communication settings are configured on the General / Communications tab.

IP Address: 192 . 168 . 1 . 25

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 0 . 0 . 0 . 0

Public IP Address: 0 . 0 . 0 . 0

Clients see each other: □

Create a new set of keys and certificates and redistribute them to this VPN server and its clients.

View a list of current connections established to this VPN server.

Client	Status	Client IP	Gateway	Allow Non-IP Broadcast	Use Pul
ALCMS Maint...	Connected	192.168.1.24	0.0.0.0	☑	□

Timestamp	Event Type	Event Priority	Source Node	LSM Name	Description
2009-10-21 10:34:25.742	EXCEPTION	CRITICAL	ALCMS Maintenance Laptop	VPN Client	Status: Connected, Mode: TEST
2009-10-21 10:34:25.705	EXCEPTION	CRITICAL	ALCMS VPN Server	VPN Server	Status: Connected, Mode: TEST

Figure 10. VPN tunnel status along with logs showing VPN connection events

6.0 Design Considerations.

6.1 Maintenance Computer.

It is important that any maintenance computer be well secured with anti-virus software (with current signatures), host-based firewall software (such as Windows Firewall) and automatic software updates.

6.1 VPN Client Software.

It is recommended that the VPN PC client software be provided by the supplier of the VPN server, due the complexities of integrating clients and servers from different vendors. Certificate versus password authentication of both client and server is highly recommended, as any password that is difficult to crack is typically too difficult to remember too, resulting in people recording passwords on note pads or "post-it" notes.

6.2 External Gateway Appliance

This choice of device is typically dictated by the provider of the external network server (i.e. the Internet service provider). For ease of use, the gateway should have a static Internet Protocol (IP) address assigned.

6.3 VPN Server & Firewall Appliance.

The VPN server appliance is critical to the security and stability of the entire system. As a result, it is recommended that it meets the appropriate requirements as follows:

6.3.1 Environmental Requirements.

- Able to operate over an ambient temperature range of at least -40 to +70 degrees Celsius.
- Able to operate over a range of at least 10% to 90% relative humidity.
- Provide a facility for mounting to a standard 35mm DIN rail or a wall mount.
- Provide the ability to connect to two redundant power supply inputs. In the event that the main power supply fails, the security appliance shall draw power from the backup power supply without disruption to the operation of the security appliance and without disruption of network traffic passing through the security appliance.
- Shall accept an unregulated DC power source of between 12 and 36 volts DC.
- Shall meet or exceed the following standards for shock and vibration:
    - IEC 60068-2-6 (1g @ 20-500Hz)
    - IEC 60068-2-27 (30g for 11ms shock)
    - EN 61326 (EMC Annex A Industrial Locations)

6.3.2 Interface Requirements.

- Shall provide two Ethernet connections, both of which shall support the MDI / MDIX auto-crossover function.
- The security appliance shall offer the option of operating as an Ethernet layer 2 bridging device between its two Ethernet connections, and in this way eliminate the need to change network addressing of ALCMS devices connected to either Ethernet connection.
- Shall provide visible illuminated indicators on the front panel for each of the following:
    - Input power applied
    - Fault condition
    - Events
    - Operating mode
- Shall provide a USB connector and an operator control on the front panel to permit the operator to load configuration data into the security appliance from a USB storage device.
- Shall provide a USB connector and an operator control on the front panel to permit the operator to save log and diagnostic data to a USB storage device.
- The USB connector on the security appliance shall be completely non-functional except when specifically enabled by the operator using the operator control on the appliance front panel.
- The management software shall be able to disable the USB connector on the security appliance.
- The security appliance shall not load any files that have not been appropriately encrypted by the security appliance supplier’s management software.

6.2.3 Installation Requirements.

- The security appliance shall not require configuration of any DIP switches, jumpers or network settings prior to installation in the ALCMS network.
- The personnel performing installation of the security appliance shall not be required to complete any special training, nor shall they be required to have any knowledge of networking or firewall concepts or technologies.
- Only common hand tools such as a screwdriver shall be required to successfully install the security appliance in the ALCMS network.

6.2.4 Security Characteristics.

- The VPN server technology shall be Secure Sockets Layer (SSL) based using Advanced Encryption Standard (AES) - 128 encryption or better.
- The security appliance shall provide integrated firewall technology capable of specifying policy on an individual connection basis.
- The firewall technology shall implement full connection tracking to provide stateful inspection of each packet of network data that passes between the Ethernet interfaces.
- The security appliance shall allow the user to select, for each firewall rule, whether or not an alarm (log entry) is generated and sent to the management console.
- The security appliance shall implement an internal real-time (time of day) clock, and time-stamp all alarm reports with the time and date that the alarm report was generated.
- The security appliance and/or management software shall facilitate synchronization of its real-time clock with a central reference clock for the purpose of providing accurate time stamps in event alarm reports.
- The security appliance shall permit the operator to perform any of the following operations without disruption of the network traffic passing between its network connections:
    - edit and change the configuration of the appliance
    - install software upgrades and optional software modules into the security appliance
    - change the operating mode of the security appliance
- Remote access to the security appliance for configuration shall be controlled via a secure key/certificate controls. Password controlled access is not acceptable.

6.3 Security Management Console.

The security management console is the other critical component in the system. It should be installed on a well secured server that has controlled physical access and good account management. Server operating systems such as Windows Server 2003 or Windows Server 2008 is recommended over desktop operating systems. The access to the security management software should also be password protected and all accesses logged.

It should act as centralized platform for all VPN configuration, certificate management and firewall security policies definition. It should also provide the capability to monitor the VPN system for security related events. Management connectivity between the VPN server appliances and the console should be secured using VPN technology that is transparently embedded into the system rather than individual web or command line log-in that are password based.

For ease of deployment with centralized and coordinated security management, it is recommended that the security management console be installed at the ALCMS vendor or support provider.

7.0 Installation.

A typical installation of secure remote maintenance system for ALCMS is shown in Figure 11.

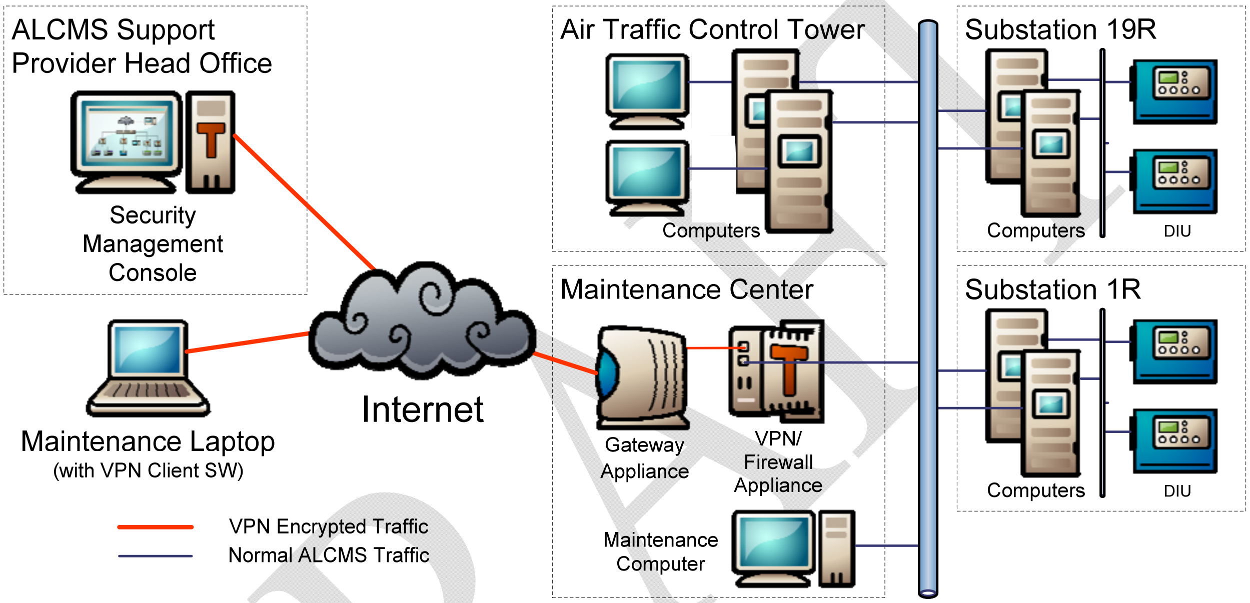


Figure 11. Typical installation of secure remote maintenance system for ALCMS

An Internet connection is brought into the ALCMS maintenance center and terminated into an Internet cable or DSL modem (the gateway appliance). This gateway is then connected to the “untrusted port” of the VPN/Firewall appliance. The “trusted port” of the VPN/Firewall appliance is connected to an existing Ethernet switch on the ALCMS network. Both the gateway appliance and the integrated VPN/Firewall appliance are supplied with DC power. See Figure 12.

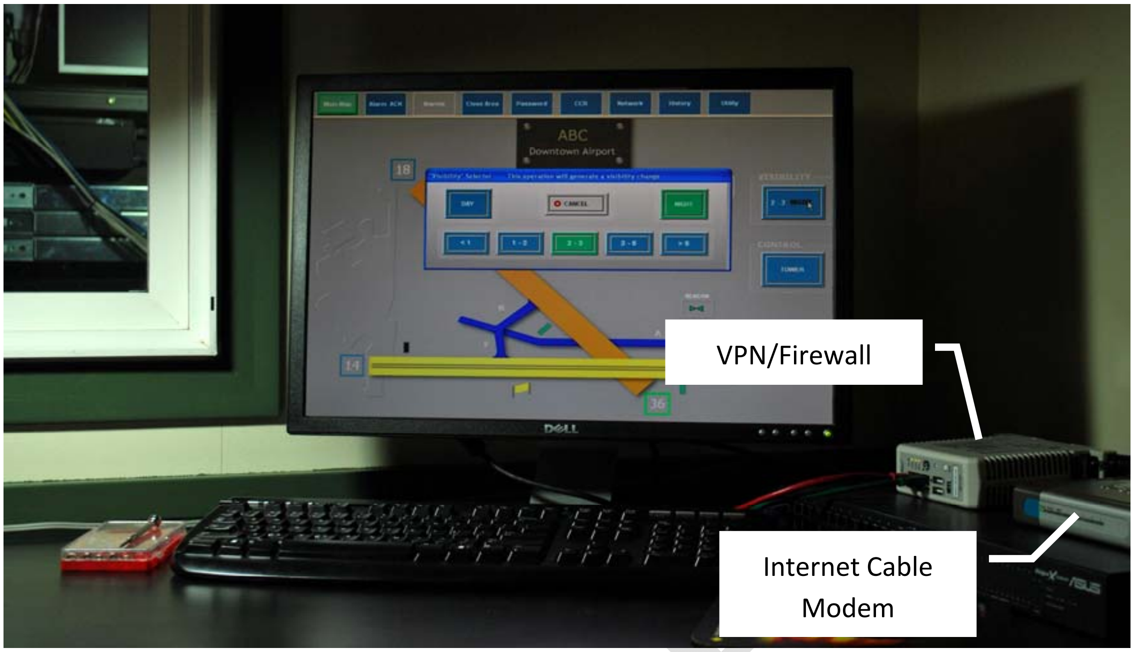


Figure 12. Typical installation of VPN appliance and cable modem in a maintenance room (both units were moved forward from the wall mount to make it possible to view them). The red cable connects to the cable modem and the black cable connects to the ALCMS network switch.

Once the hardware is in place, the ALCMS support provider would use the security management console to define policy and build encrypted VPN configuration files for both the maintenance laptop and the VPN/Firewall appliance and save these to two USB storage devices. One USB storage device would be sent to the support person possessing the maintenance laptop, while the other would be sent to the airport maintenance staff for uploading to the VPN/Firewall appliance. When the configuration files are loaded into both the laptop and VPN/Firewall appliance, the remote system would be ready for operation.

8.0 Testing Requirements.

Prior to using the VPN system, the following basic tests are recommended to prove the connectivity and security of the system. Ideally these tests should be conducted with a "dummy network" connected to the VPN server, prior to connecting the full ALCMS. This dummy network can be as simple as a laptop with an address set to represent a target ALCMS device.

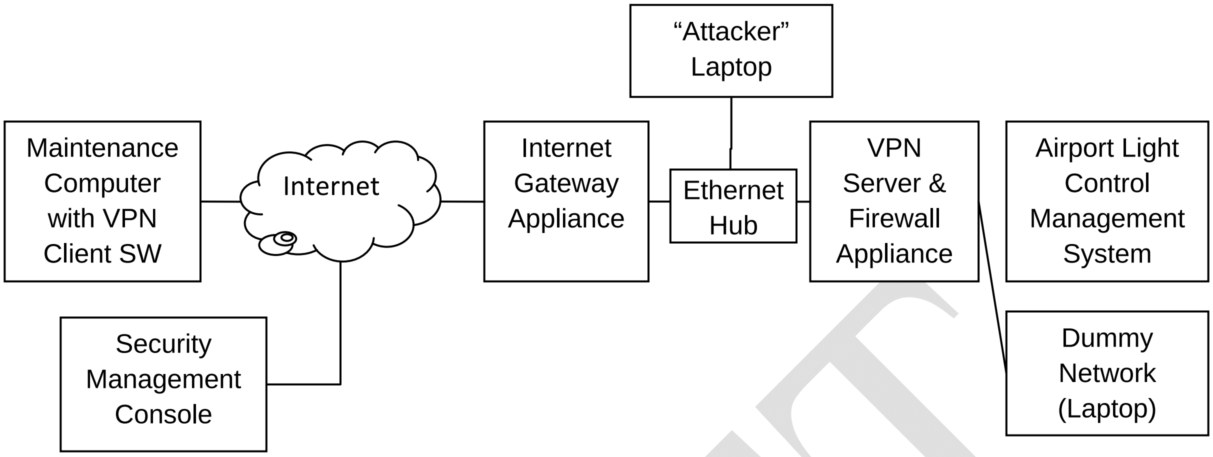


Figure 13. Test Setup

8.1 Connectivity Testing

To prove the connectivity of the system when the Internet gateway appliance, VPN Server & Firewall appliance and Dummy Network Laptop are in place and configured, the maintenance computer (with VPN client) should initiate a VPN connection to the VPN server with the server in test mode. Test mode is used to verify that the VPN tunnels can be successfully set up without actually passing traffic through the tunnel. This prevents accidental loss of critical ALCMS traffic due to a configuration issue. Review the VPN Server tab on the security management console to verify that the VPN tunnel is connected. Events will also show up in the event log indicating that the VPN tunnel is connected.

When the preceding test is passed, the next stage is to switch the VPN server to operational mode and confirm that the maintenance computer can ping the Dummy Network Laptop. This will require that a temporary firewall rule be added to allow ICMP (ping) traffic between the maintenance computer and the Dummy Network Laptop. If the ping test is successful, the VPN is fully operational.

8.2 Security Testing

The final set of tests are intended to prove the security of the system. An attacker laptop with traffic capture software such as WireShark® and network scanning software such as nmap® should inserted into the connection between the gateway and the server. This will require either an Ethernet switch with a spanning port or an Ethernet hub to allow the connection.

The nmap software should be used to scan the external IP address of the VPN server to see if there are any open TCP or UDP ports (other than the VPN port which is typically UDP port 1194 or TCP port 443). If there are no ports open, this indicates that only authenticated VPN traffic is being accepted into the ALCMS system by the VPN server.

If the port scan test passes, then the next stage is to do a test to determine if the VPN traffic is encrypted. The attacker laptop is switched to capture mode and the VPN client computer should start to ping the dummy network laptop. If the encryption is operational, the Wireshark software should only see traffic marked as SSL VPN traffic (typically UDP port 1194 or TCP port 443 traffic) and not be able to detect the ping traffic.

Finally, the firewall should be tested to determine if the rules will restrict the traffic flowing into the ALCMS. The command "tracert" should be used on the VPN client computer to a send a Trace Route UDP message to the dummy network laptop. If the firewall is operational, the Trace Route should fail and an alarm should appear in the event log indicating a message was blocked.

When all tests are passed, the appropriate firewall rules should be installed in the VPN server and the dummy network laptop replaced with a connection to the ALCMS network.

9.0 Conclusions

Remote maintenance and monitoring of critical ALCMS can increase support responsiveness, decrease total system downtime and reduce overall operating costs. The key is to design an access system that is provably secure, so that security issues do not over shadow the benefits. Remote access systems based around an integrated combination of VPN and firewall technology give ALCMS the ideal level of security – the VPN secures the critical traffic from all external attacks or events and the firewall ensures that only the approved devices in the ALCMS can be managed remotely. By using technologies and architectures configured specifically to meet the needs of the ALCMS environment, airports can achieve remote maintenance and monitoring solutions that both reduce cost and enhance overall security.