U.S. DEPARTMENT OF ENERGY

PNNL-19266

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Second Line of Defense Virtual Private Network Guidance for Deployed and New CAS Systems

SV Singh AI Thronas

January 2010

Pacific Northwest NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-ACO5-76RL01830

Printed in the United States of America
Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576 5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service,
U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161
ph: (800) 553-6847
fax: (703) 605-6900
email: orders@nits.fedworld.gov
online ordering: http://www.ntis.gov/ordering.htm

Acronyms

AT	Acceptance Test
CAS	Central Alarm Station
SLAT	System Level Acceptance Testing
SLD	Second Line of Defense
VPN	Virtual Private Network

Contents

1.0 Overview 1
2.0 Background 1
3.0 Requirements 1
3.1 Assumptions 1
3.2 Hardware/Software 1
3.3 Client Software 2
3.4 Help Desk Requirement 2
4.0 Deployment 2
5.0 Maintenance 2
6.0 Sustainability 3
Appendix A—Functional Requirements 4

1.0 Overview

This paper discusses the importance of remote access via virtual private network (VPN) for the Second Line of Defense (SLD) Central Alarm System (CAS) sites, the requirements for maintaining secure channels while using VPN and implementation requirements for current and future sites.

2.0 Background

There has been no standardized method of establishing remote access for sites currently participating in the SLD program. Many sites that are installed with VPN are vendor controlled, which can constitute a conflict of interest between a paid vendor having control of both the installed systems and access to those systems to repair them. Other sites have not established a method for remote access.

Additionally, at some sites the remote access is enabled but is not secured properly, possibly allowing malicious attackers originating from the internet to gain access to information without a legitimate need to know. The attacker could also install viruses or other control software on attacked machines, which typically run in a non-patched state, causing them to distribute virus code, send spam out and perform slowly, frustrating the sites and causing an increase in the number of SLD Helpdesk Service Requests received.

Finally, the implementation of VPN is not done with consistency at each site, making support and sustainability more complex, increasing costs over the supported lifetime of the system. The program needs to be able to implement a consistent VPN solution that is robust, upgradeable and replicable, increasing uptime for our customers and reducing costs.

3.0 Requirements

3.1 Assumptions

- Country is allowing remote access for SLD staff members or vendors
- Country has a working infrastructure to maintain an internet connection

3.2 Hardware/Software

Consistent hardware is paramount to being able to have a supportable and sustainable solution that can be implemented for all sites. Also, the hardware should not interrupt normal operations for the site. The hardware should function in a secure manner and not require frequent updating in order to maintain remote functionality. The hardware should be configurable to match the needs of the site, should that be a simple, secure remote connection or two-factor authentication. The hardware should also be able to maintain a log of the user who used a remote access capability to include user identifiable information, time the system was accessed, and duration of the access. The hardware and software should accommodate a large number of users.

The recommended hardware to be implemented is the Cisco ASA 5500 series appliance as it offers firewall, router, VPN, and comprehensive logging capability in one device. Available in different sizes, Cisco ASA appliances can be pre-configured and distributed to the SLD sites.

3.3 Client Software

A consistent software base, supported by the manufacturer, is also necessary from a supportability standpoint. The software should be able to accommodate installation of multiple profiles because of the likelihood that an SLD staff member or a vendor will be supporting sites totaling more than one.

The client recommendation, if using a client-to-site VPN model, is Cisco IPSEC VPN client. This client allows us to enforce a full tunnel between the end points. This means that all traffic when using VPN is routed between the two computers only and no other network traffic is allowed (i.e., a computer that is connecting with VPN will not be able to access local resources like shares and printers or the internet, only remote resources). Using a third party client can lead to a possible split tunnel, which allows access to local and remote resources and the internet, creating a possible security vulnerability.

3.4 Help Desk Requirement

It is recommended that the SLD Helpdesk serve as the single point of contact for all account operations regarding SLD sites with VPN access. Working in close coordination with DOE-HQ, the SLD Helpdesk can serve as the clearinghouse for all VPN requests and will grant or revoke access requests from vendors and SLD staff members. The SLD Helpdesk will maintain records of access requests and be able to provide reporting on remote access usage when necessary. The SLD Helpdesk will also require renewal of all VPN access requests once per year for SLD staff members and vendors. The SLD Helpdesk will also control two-factor authentication token distribution and keep records of who has two-factor authentication tokens and request their return upon a staff member or vendor no longer requiring the token. Finally, the SLD Helpdesk will maintain VPN profile information for all sites and be able to distribute the profile information when it is deemed necessary.

4.0 Deployment

Hardware and software deployment details are to be determined by site and schedule requirements. Complete deployment should be reasonably completed within one year. New sites should have a contingency written for System Level Acceptance Testing (SLAT)/Acceptance Test (AT) that requires remote VPN access be implemented following this guidance document. All sites, if capable, will have VPN remote access capability.

5.0 Maintenance

Updates to VPN hardware operating systems will be coordinated by the SLD Helpdesk and deployed by an SLD Helpdesk Service Request Manager or a knowledgeable delegate.

Updates to VPN client software will be coordinated by the SLD Helpdesk and communicated via e-mail. The SLD Helpdesk will maintain a share or website with current software for deployment to SLD staff members or vendors. Users having outdated client software will not be able to connect via VPN until after the update to supported software is complete. The SLD Helpdesk will not support VPN software on outdated operating systems or on recently deployed operating systems for which a client may not be available from the VPN hardware/software vendor.

6.0 Sustainability

Upgrades to standardized equipment and software will be coordinated through the SLD Helpdesk via a Service Request. Testing of software and hardware upgrades will also be done by the SLD Helpdesk in an offline testing prior to deployment on other SLD systems. Communication will be done via e-mail prior to deploying any updates. Sites will allow for remote upgrades of equipment or take responsibility for deployed equipment and its hardware or software maintenance.

Appendix A—Functional Requirements

REQ 1 – Remote access will be secure.

REQ 2 – Remote access will be reliable.

REQ3 – Remote access will not impede bandwidth to a point that it is unusable.

REQ4 – Remote access will be able to be controlled, managed and tracked from a central location.

REQ5 – Remote access software will not adversely affect normal operations of client or remote client systems.