SECURITY CORE FUNCTION AND DEFINITION REPORT

Prepared by:

EnerNex Corporation
170C Market Place Blvd
Knoxville, TN 37922-2337
USA
(865) 691-5540
www.enernex.com

Version 1
May 13, 2008

Table of Contents

1 Summary

The first phase of the Lemnos Interoperable Security Program shall lay the foundation for future work by providing a guiding example of the vocabulary, metrics, interoperability requirements and interoperability assurance methodologies used to create interoperable network security products. From a requirements definition perspective, this translates to:

1. **Functional Requirements:** What functions are being performed that are critical to be met to achieve interoperability? This is a set of binary questions, as the subject either does something (performs a specific function) or it does not. There is no measurement involved. Assurance mechanisms are defined to assure possibility of functional interoperability.
2. **Non-functional Requirements:** What bounds on function performance are required to achieve interoperability? This is a subsequent set of entirely "grayscale" questions, as they describe characteristics like how well, how much, and how fast specific functions are performed. Assurance mechanisms are defined to assure interoperability over the specified range.

1.1 Problem Statement

Consumers of control system network security products do not currently have a standardized or widely accepted mechanism for evaluation of product security functionality, security performance, and security interoperability. Product offerings from different vendors are usually described in terms and figures that are difficult if not impossible to compare without deep understanding of every potential product or technology function. Further, the functional scope of one offering rarely, if ever maps directly to the functional scope of another in a "one-to-one"

fashion. This lack of common definitions and metrics fundamentally limits an organization's ability to effectively evaluate and compare products and solutions.

The Lemnos Interoperable Security Program will directly address the needs of utilities in evaluating and comparing network security vendor products. Lemnos will accomplish this by establishing a reference vocabulary and set of metrics for describing a product's functionality within the network security domain. We will demonstrate to the industry how products and utility security need may be specified using. these tools through both a reference implementation and a commercial design. Figure 1 illustrates the challenge of mapping two products' functionality into the requirement of utility application. Without a basis in vocabulary and an agreed-upon set of security functionality, industry must forever make such comparisions at the least common denominator of functionality: empirical test.

1.2 Vision

By bringing technical clarity to the network security domain, the functional vocabulary and metrics will improve utilities' ability to match vendors' products to risk mitigation criteria. An important benefit of this approach is that vocabulary and metrics can form the foundation of interoperability definition by following the semantic model.

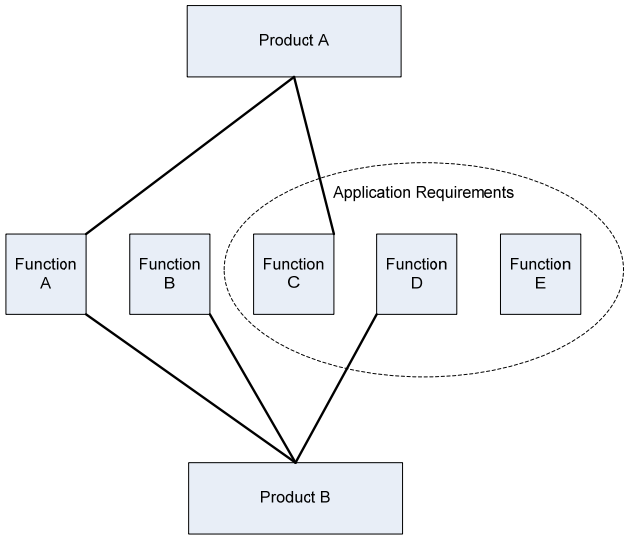


Figure 1: Functional Requirements Mapping & Comparison

Unlike other industries, technology in the utility industry was developed for long term use (20+ years). The major factor was reliability and availability. The need for security was either none existent and/or not needed. Now vendors and systems are playing 'catch up' on the network security domain. With developments and trends toward internet applications, automation products focus from availability and reliability are also adding security and assurance. Focus should be on manufacturing the system with security, by incorporating it in the beginning of the system development process. The system/product should be modular in design; able to incorporate different products (VPN, router, firewall, etc) into one physical product.

Improving the security of control systems in the energy sector is a complex task. High-priority needs include:

- Agreeing on metrics/standards for measuring security.
- Developing security test harnesses.
- Developing security architecture with plug-and-play compatibility.

This report documents the definitions, metrics and measurements for all fundamental network security functions. Table 1 list the core functional and the corresponding non-functional security

requirements for the device. From various meetings, the team decided on a list of 48 core security functions to be implemented in the system (or device).

The Lemnos architecture (or framework) will provide utilities and vendors a common means of measuring and testing security gateway devices. All aspects of utility security domain have been analyzed to define the security space that will be tested.

2 Security Function Table

2.1 Security core functional and nonfunctional Requirements

Functional requirements describe what are being performed. This is a set of binary questions, as the system either does something or it does not. There is usually no measurement or metric involved. Non-functional requirements assign metrics and measurements to the functions. They describe characteristics like how well, how much, and how fast specific functions are performed. The nonfunctionals map to functional requirements. In Appendix A, A1 is a list of functional and the corresponding nonfunctional requirement. Not all functional requirements have a mapping to a nonfunctional.

2.2 Functional/Nonfunctional Mapping

The Lemnos security architecture building block is the core security function. The core security functions that will be implemented in the reference architecture and included in the vendor implementation are:

CORE SECURITY FUNCTION	HOW IMPLEMENTED	REQUIREMENTS
Secure Communications Channel	VPN with IPSEC Protocol	2,3,4,5,6,7,26,41,43,
Messaging	SYSLOG	9,37

The following core security functions have been envisioned but will not be implemented, and are not described in depth:

CORE SECURITY FUNCTION	REQUIREMENTS
Network Intrusion Detection (NIDS)	27,31
Host Intrusion Detection (HIDS)	28
Antivirus	47

There are many other requirements in the master table that are not describing core security functions but are necessary for equipment operability and security.

SECURITY OR OPERATIONAL FEATURE	REQUIREMENT
Startup testing	13,14
Storage through Power Cycle	10,12
Date and Time	24,32,33
Diagnosis	1,13
Security	15,16,17,18,19,20,21,22,43,48
Configuration	11,30,48

Interoperability Definition

Outside vendors equipment wishing to interoperate with Lemnos compliant equipment should have the following functionality:

CORE SECURITY FUNCTION	HOW IMPLEMENTED	REQUIREMENTS
Secure Communications Channel	VPN with IPSEC Protocol	2,3,4,5,6,7
Messaging	SYSLOG	9, 37

3 Definitions and Terms

The definitions and terms are collections of technologies listed during the functional requirements list phase.

1. Access Control List (ACL)-users, groups, machines and process that have been given access to a resource(NIST IR 7298)
2. AES-Advanced Encryption Standard-A symmetric block cipher for encrypting and decrypting information.(NIST 1R 7298)
3. Alert Generation-the process of a device sending or generating status and alert messages, either to a central Syslog server or storing the messages locally.
4. Asset-tangible or intangible entity that has value to an organization(Catalog of Control Systems Security)
5. Authentication-confirming the identity of a user, process, or a device before access to resources is granted. (NIST IR 7298, 800-53)
6. Authenticity-confidence and trust that and entity has been verified and is genuine (NIST SP800-82)
7. Authorization-rights and permissions granted to an entity, process, or system to access a control (Catalog of Control Systems Security)
8. Availability-resource providing timely and reliable access to information(NIST SP800-82)
9. Certificate Authority-entity that issues and revokes public key certificates(NIST IR 7298)

10. Confidentiality-assurance that only authorized individuals, process, and devices have accessed information (Catalog of Control System Security)

11. Cryptography-the principles, means and methods for transforming data to hide and prevent modification from unauthorized users(NIST SP800-82)

12. Denial of Service(DoS)-Prevention or disruption of authorized access to a system, which delays system operations or process function(ISA99)

13. DHCP-Dynamic Host Configuration Protocol-protocol used to assign IP address to nodes(NIST SP800-82)

14. DMZ-Demilitarized Zone-External facing network and systems with interfaces located in un-trusted networks

15. Encryption-conversion of data into ciphertext, for security or privacy, which cannot be understood by unauthorized entities. (NIST SP800-82)

16. ESP-Electronic Security Perimeter-Logical border surrounding a network for which access in controlled (Catalog of Control Systems Security)

17. Event Storage-centralized storage and collection of system generated event messages

18. Event-an observable occurrence in an information system, usually monitored and generates an alarm to an event logging system (NIST SP800-82)

19. Firewall- a gateway that limits traffic between networks in accordance with security policies. Can be software or hardware. (NIST SP800-82)

20. HMI-Human Machine Interface-Hardware and/or software through which one interacts with a system or controller(NIST SP 800-82)

21. Identification-the process of verifying the identity of a device, user, or process before granting access to a resource. (NIST SP800-82)

22. Identity-a unique name that identifies and individual or service, with sufficient information to make the name unique (NIST SP800-82)

23. IED-Intelligent Electronic Device-A device capable of receiving or sending data or control information (NIST SP 500-82)

24. Interoperability-The ability of two or more systems or components to exchange information and to use the information that has been exchanged

25. IPSec-IP Security-the framework for securing IP traffic, including key management, for protection of Virtual Private Network communications, including the type of security for the VPN (NIST IR 7298)

26. Local Area Network (LAN)-communications infrastructure designed to connect computers and other communication devices, limited to a specific geographical location(ISA99)

27. Metric-Measurement used to quantify a component (www.thefreedictionary.com/metrics)

28. NIDS-Network Intrusion Detection System-software that looks for certain suspicious communication activity, based on predefined malicious signatures (NIST IR 7298)

29. OCSP-Online Certificate Status Protocol-Protocol used in the revocation status of X.509 digital certificates.(RFC 2560)

30. OPSAID-Open PCS Security Architecture for Interoperable Design-Joint government/industry project to develop a security architecture utilizing open source software and hardware. (http://www.automationworld.com/view-2974)

31. Password-a sting of characters used to authenticate identity or verify authorization(Catalog of Control Systems Security)

32. Proxy/Gateway-application that breaks a direct connection between server and client. This provides an indirect path from external to internal networks; acts as the entrance point to another network. (Catalog of Control System Security) (NIST SP800-82)

33. Remote Access-external access by users or processes outside the electronic security perimeter of the network(Catalog of Control Systems Security)

34. Router-a device that connects to physically different networks. Usually used to connect wide area networks.

35. SCADA-Supervisory Control and Data Acquisition-hardware and software used to acquire data for the purpose of monitoring and control (Catalog of Control Systems)

36. SNMP-Simple Network Management Protocol-protocol used for managing network devices; including monitoring network performance, packet loss, and error rates (NIST SP800-82)

37. SSL-Secure Sockets Layer-provides a secure encrypted channel between two devices(also known as HTTPS)(NIST SP 800-82)

38. Switch-an OSI layer 2/3 device that interconnects devices(Catalog of Control Systems Security)

39. TLS-Transport Layer Security-see Secure Socket Layer (SSL)

40. Use Case-technique for capturing functional and non-functional requirements and conveys how a system should interact with another system or end-user(ISA99)

41. VPN-Virtual Private Network-logical network that is established over an existing physical un-trusted network, by virtual tunneling across the real network (NIST IR 7298, NIST SP 800-82))

42. W3C-World Wide Web Consortium-Develops interoperable technologies, including specifications, guidelines, and tools, for the web.(www.w3c.org)

43. X.509 Certificate-public key, that is unforgeable by the digital signature of the certification authority that issued the certificate(NIST IR 7298)

4 System Test Scenarios

4.1 VPN component test scenarios

Test Scenario #1 – Pre Shared Passphrase

A VPN is configured between two Lemnos devices with the pre shared passphrase XXXXXXXX. The Lemnos device on the left is the SNL reference implementation and the OPSAID on the right is the SEL implementation. The two Lemnos devices communicate with each other through a WAN to establish Security Associations (SA) for the VPN tunnel. Once the SAs have been established the 192.168.1.0/24 network can securely communicate with the 10.0.1.0/24, with the encrypted channel represented by the green link between Lemnos devices. At the same time, syslog-ng messages are being sent to SNL Lemnos Master from both Lemnos devices.

Test Scenario #2 – Pre Shared X.509 Certs

A VPN is configured between two Lemnos devices, each possessing their own X.509 public / private key pair and the public key of the opposite Lemnos. The Lemnos device on the left is the SNL reference implementation and the Lemnos on the right is the SEL implementation. The two Lemnos devices communicate with each other through a WAN to establish Security Associations (SA) for the VPN tunnel. Once the SAs have been established the 192.168.1.0/24 network can securely communicate with the 10.0.1.0/24, with the encrypted channel represented by the green link between Lemnos devices. At the same time, syslog-ng messages are being sent to SNL Lemnos Master from both Lemnos devices.

Test Scenario #3 – CA Signed X.509 Certs

A VPN is configured between two Lemnos devices, each possessing their own CA signed X.509 public / private key pair and the public key of the SNL Lemnos Master. The SNL Lemnos Master device acts as the CA and digitally signs each OPSAIDs certificate so public keys do not have to be distributed prior to the VPN tunnel being established. The CA signature of each certificate verifies that each certificate is authentic. The Lemnos device on the left is the SNL reference implementation and the Lemnos on the right is the SEL implementation. The two Lemnos devices communicate with each other through a WAN to establish Security Associations (SA) for the VPN tunnel. Once the SAs have been established the 192.168.1.0/24 network can securely communicate with the 10.0.1.0/24, with the encrypted channel represented by the green link between Lemnos devices. At the same time, syslog-ng messages are being sent to SNL Lemnos Master from both Lemnos devices.

Test Scenario #4 – CA Signed X.509 Certs with OCSP

A VPN is configured between two Lemnos devices, each possessing their own CA signed X.509 public / private key pair and the public key of the SNL Lemnos Master. The SNL Lemnos Master device acts as the CA and digitally signs each Lemnos certificate so public keys do not have to be distributed prior to the VPN tunnel being established. The CA signature of each certificate verifies that each certificate is authentic. The Lemnos device on the left is the SNL reference implementation and the Lemnos on the right is the SEL implementation. The two Lemnos communicate with each other through a WAN to establish Security Associations (SA) for the VPN tunnel. Once the SAs have been established the 192.168.1.0/24 network can securely communicate with the 10.0.1.0/24, with the encrypted channel represented by the green link between Lemnos. If a certificate is added to the Certificate Revocation List (CRL) of the SNL Lemnos Master device then the new CRL will be sent out to each OPSAID device, represented by the blue dashed line. The certificates appearing on the new CRL will no longer be verified by the CA. At the same time, Syslog-ng messages are being sent to SNL Lemnos Master from both Lemnos devices.

4.2 Firewall Test Scenarios

Test Scenario #1 – No Firewall

The Lemnos device on the left is the SNL reference implementation and the Lemnos on the right is the SEL implementation. The two Lemnos communicate with each other through a WAN and act as a gateway for each of the end devices connected to them. All communications between host Eve and host MiscBox should be disallowed. However, without a firewall Eve and MiscBox have established a telnet session between each other, represented as the green link between them.

Test Scenario #2 – Firewall Port Filter

The Lemnos device on the left is the SNL reference implementation and the Lemnos on the right is the SEL implementation. The two Lemnos devices communicate with each other through a WAN and act as a gateway for each of the end devices connected to them. All communications between host Eve and host MiscBox should be disallowed. However, with a firewall only

filtering telnet traffic between Eve and MiscBox only port 23 (represented by the green link) is blocked, while the two parties can still ssh to each other via port 22, represented by the blue link.

Test Scenario #3 – Firewall IP Filter

The Lemnos device on the left is the SNL reference implementation and the Lemnos on the right is the SEL implementation. The two Lemnos devices communicate with each other through a WAN and act as a gateway for each of the end devices connected to them. All communications between host Eve and host MiscBox should be disallowed. Now, with a firewall filtering on IP, telnet traffic, ssh traffic, and all other traffic between the IPs of Eve and MiscBox are blocked by the firewall.

5 References

This report makes use of the following references:

1. Catalog of Control Systems Security: Recommendations for Standards Developers, January 2008, Department of Homeland Security
2. Instrumentation, Systems, and Automation Society Standards Committee, ISA99.00.01, Security Technologies for Industrial Automation and Control Systems, October 2007
3. International Organization for Standardization 17799, Code of Practice for Information Security Management, June 2005
4. National Institute of Standards and Technology Special Publications 800-53A, Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans, Final Public Draft, December 2007
5. National Institute of Standards and Technology Special Publication 800-110, Information System Security Reference Data Model (DRAFT), September 2007.
6. National Institute of Standards and Technology, NIST IR 7298, Glossary of Key Information Security Terms, April 2006.
7. North American Electric Reliability Council, Critical Infrastructure Protection (CIP-002-1 through CIP 009-1), May 2006
8. Sandia Report , OPSAID Initial Design and Testing Report, November 2007
9. http://www.thefreedictionary.com/metrics, 2008

Appendix A

A.1 Table 1 Functional and Nonfunctional

	Functional Security Requirement	Corresponding Non-functional Security Requirement
1.0	System shall provide automated diagnostics and reporting	The system shall provide automated diagnostics and reporting a minimum of 1 time per month
2.0	The authentication for the secure SCADA/PCS tunnel shall comply with the IPSec Standard[i]	VPN shall provide zero loss of communication
3.0	The cryptographic tunnel shall support AES, 3DES, SHA-1, SHA-256, and be compliant with strongSwans implementation[ii]	Cryptography shall have a minimum (AES,3DES) 128 bit encryption
4.0	The SCADA/PCS tunnel shall support pre-shared passphrases as a key[iii]	The passphrase shall be a minimum of 10 characters and a maximum of 128 characters
5.0	The SCADA/PCS tunnel shall support pre-shared x509 certificates as a key[iv]	The device shall have a minimum key of 1024, with support for 4028 and 4096
6.0	The SCADA/PCS tunnel shall support CA signed x509 certificates as a key[v]	
7.0	Key revocations shall support OCSP[vi]	The system shall check the CRL interval every 10 minutes
8.0	The device shall be interoperable with other certified devices[vii]	
9.0	Local events shall be reported in a format compatible with Syslog[viii]	
10.0	Settings shall be stored in nonvolatile memory	The system shall be configured without requiring a device reboot
11.0	There shall be a human readable way to configure settings (GUI, CLI, or through a PC) is up to the customer	
12.0	Date and time shall be maintained through a power cycle	The device shall hold the date/time setting for up to 10 minutes
13.0	Equipment self tests shall be performed prior to enabling the equipment	The system shall report once per month, through and in the form of Syslog messages
14.0	All self tests shall be performed prior to enabling the equipment	
15.0	The device shall provide user based password security	
16.0	The device shall support password protection[ix]	The device shall support password protection from 8-128 characters

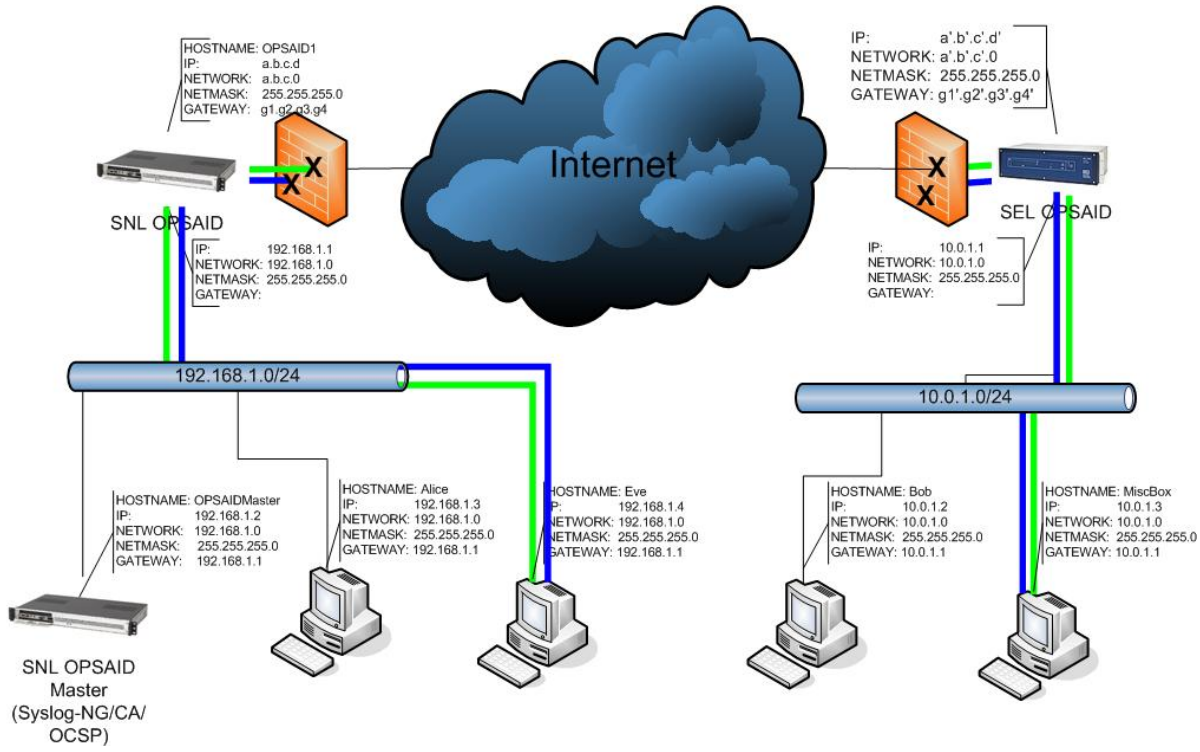
17.0	Password protection shall support all printable characters[x]	Passwords shall support all printable characters, from 7 bit ASCII set (0x20-0x70)
18.0	Passwords shall not be displayed at anytime	
19.0	This device shall trigger an alarm for all successful attempts to login as a user with write and/or modify rights	The alarm shall be generated and received within 30 seconds of the event from the user logging in
20.0	Warnings for invalid passwords shall be logged	The alarm shall be generated and received within 30 seconds of the invalid password event
21.0	Alarm shall be generated after three failed attempts to provide a legitimate password for an access request	The alarm shall be generated after 3 failed password attempts
22.0	The device shall provide the ability to lockout users	
23.0	The device shall provide a Syslog feature that logs successful access entries and failed access attempts	The alarm shall be generated and received within 30 seconds of the failed attempts
24.0	Date and data shall include day,month, and year and shall compensate for leap years.	
25.0	Product shall support a mechanism to filter undesired traffic[xi]	Users shall be able to create, at a minimum, 128 rules
26.0	VPN MIBs shall provide security status information[xii]	
27.0	Network Intrusion Detection System(NIDS) shall be targeted to SCADA protocols and updated as required	
28.0	Host Intrusion Detection System(HIDS) shall be considered for future implementation	
29.0	Event Storage, alert generation, and visualization shall be supported on remote systems	
30.0	Device configuration and system logging shall have a configuration interface.[xiii]	
31.0	Network Intrusion Detection System(NIDS) shall be supported on the device	

32.0	The system shall have a support for the selection of a time zone[xiv]	The system shall support a minimum of 12 hour offset
33.0	The system shall support date/time to be adjusted manually	
34.0	By default, the system shall drop all packets	
35.0	Default setting shall include a rule to allow the user to login to the management interface	
36.0	The system shall, at a minimum, allow filtering of IP traffic by the source and destination IP address range and the source and destination port number range of TCP and UDP packets	The system shall support ports 1-65534
37.0	Syslog events related to the firewall configuration shall be generated	
38.0	All Syslog events related to the modification of settings shall include the username of the user	
39.0	Allow the user to define the protocol-level static routes that control the flow of network traffic through the system	
40.0	System will be able to forward Syslog events to the Syslog server via the network	The system shall support a minimum of 2 Syslog servers
41.0	The system shall support public and private keys (using RSA encryption)[xv]	
42.0	The system shall support role based authorization.[xvi]	The system shall have a minimum of 2 roles, User and Administrator (Admin)
43.0	The system shall support third party authentication, such as pass tokens, smart cards, etc (Future use and implementation)	
44.0	The system shall support location based authentication, such as GPS. (Future use and implementation)	
45.0	The system shall support automated software management support, such as software patches, OS upgrades, etc. (Future use and implementation)	
46.0	If a BIOS is supported, settings shall	

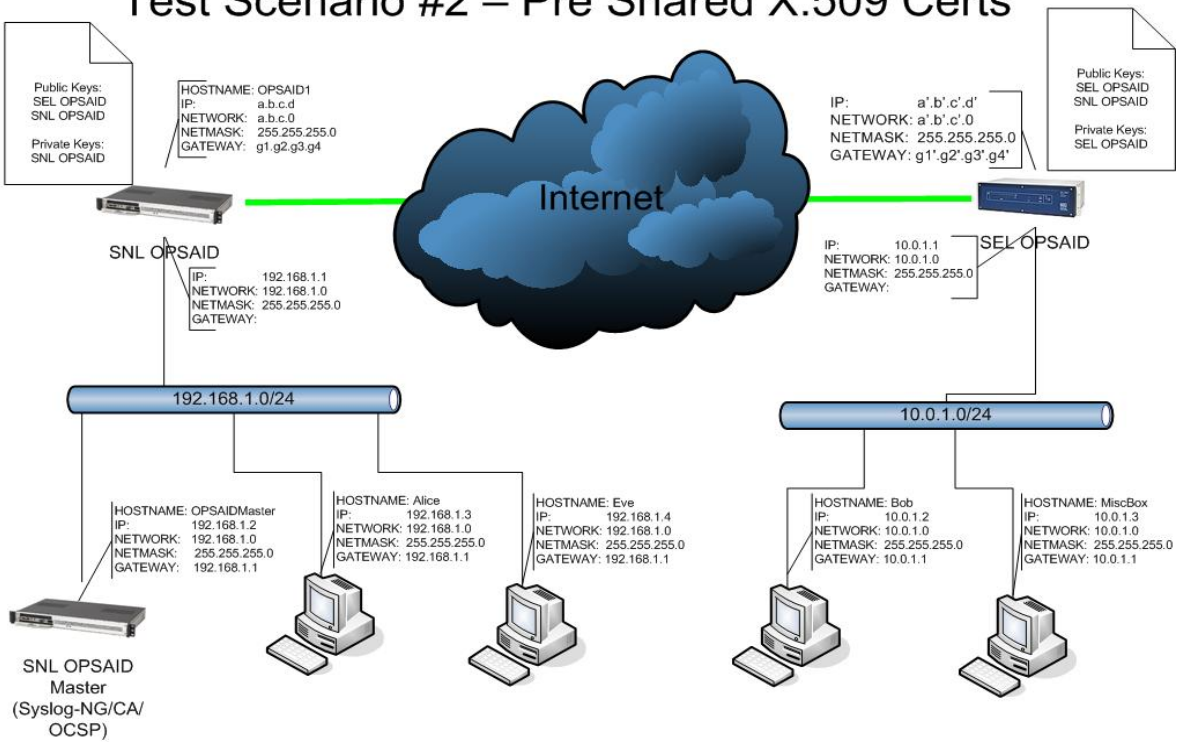
	be password protected (Future use and implementation)	
47.0	Anti-Virus software shall be supported on the implemented platform (Future use and implementation)	
48.0	Support for backup and recovery shall be available for configuration/system files (Future use and implementation)	

A.2 Supporting Test Scenarios Drawings

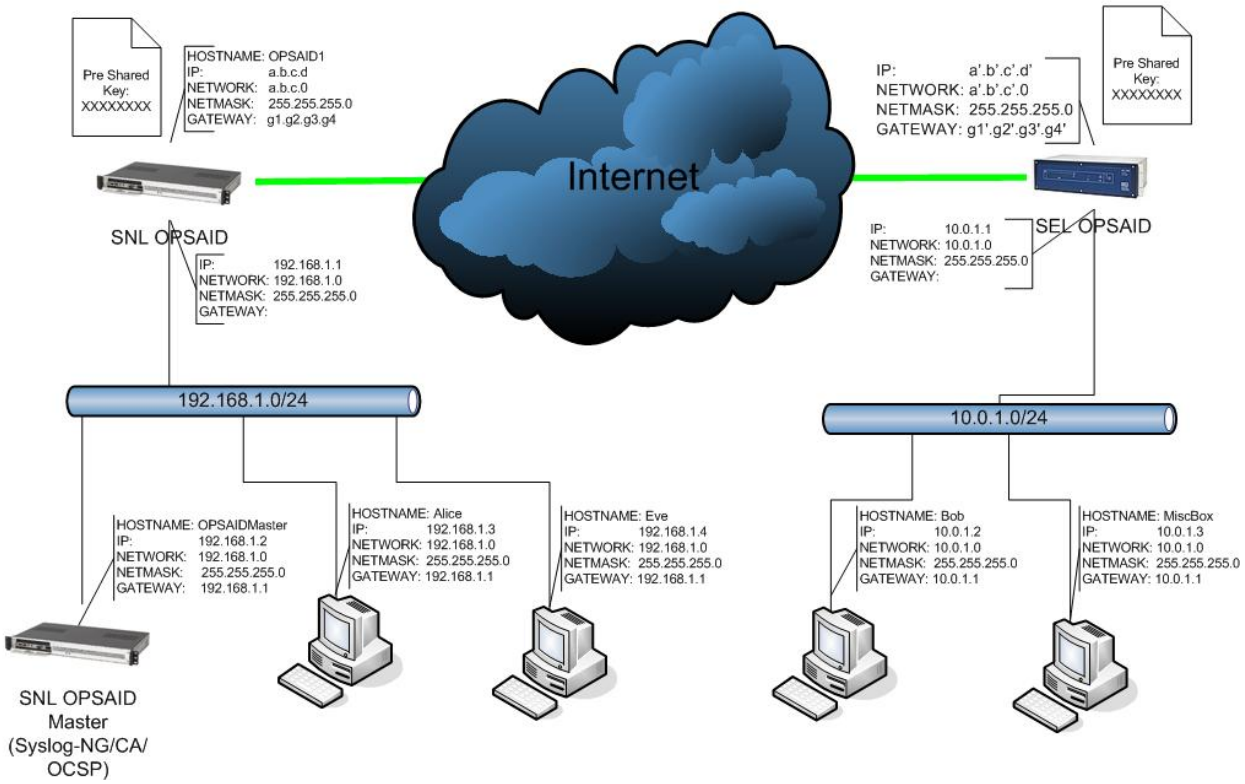
Test Scenario #3 – Firewall IP Filter



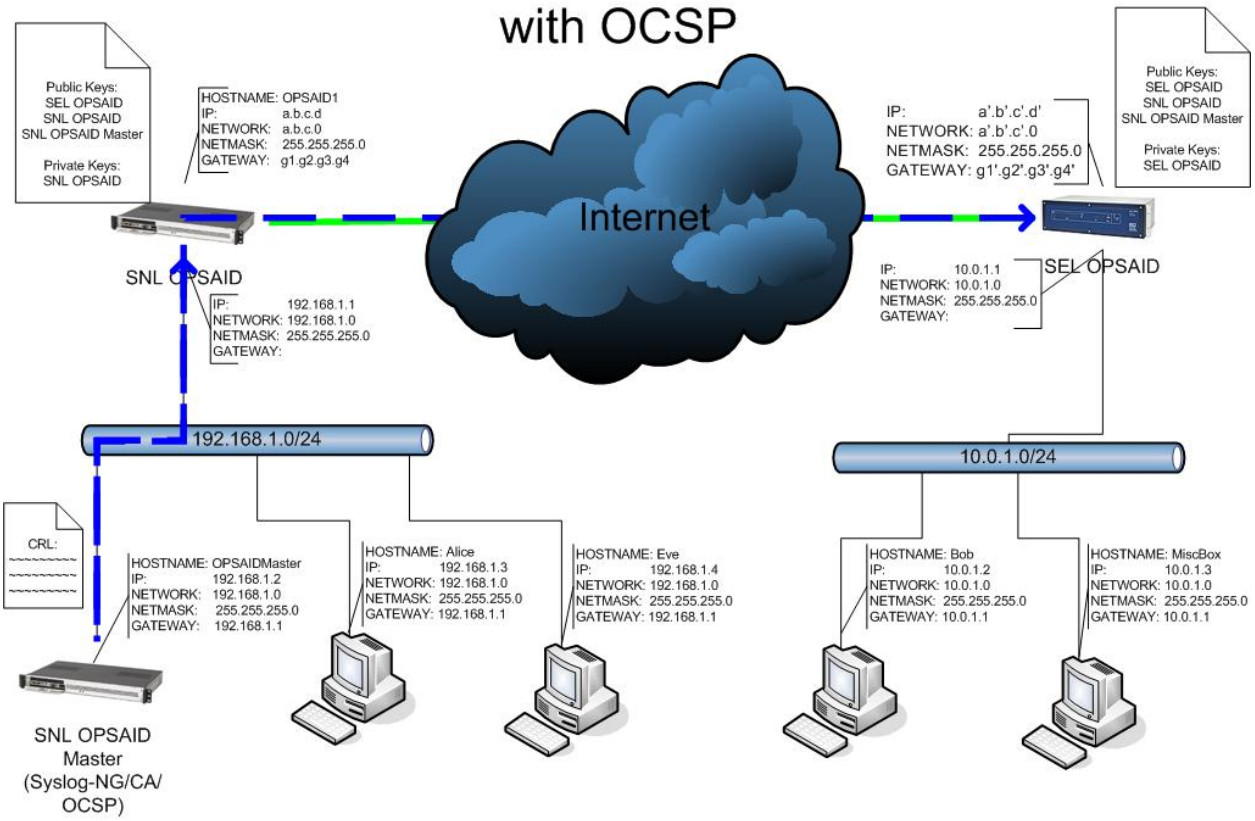
Test Scenario #2 – Pre Shared X.509 Certs



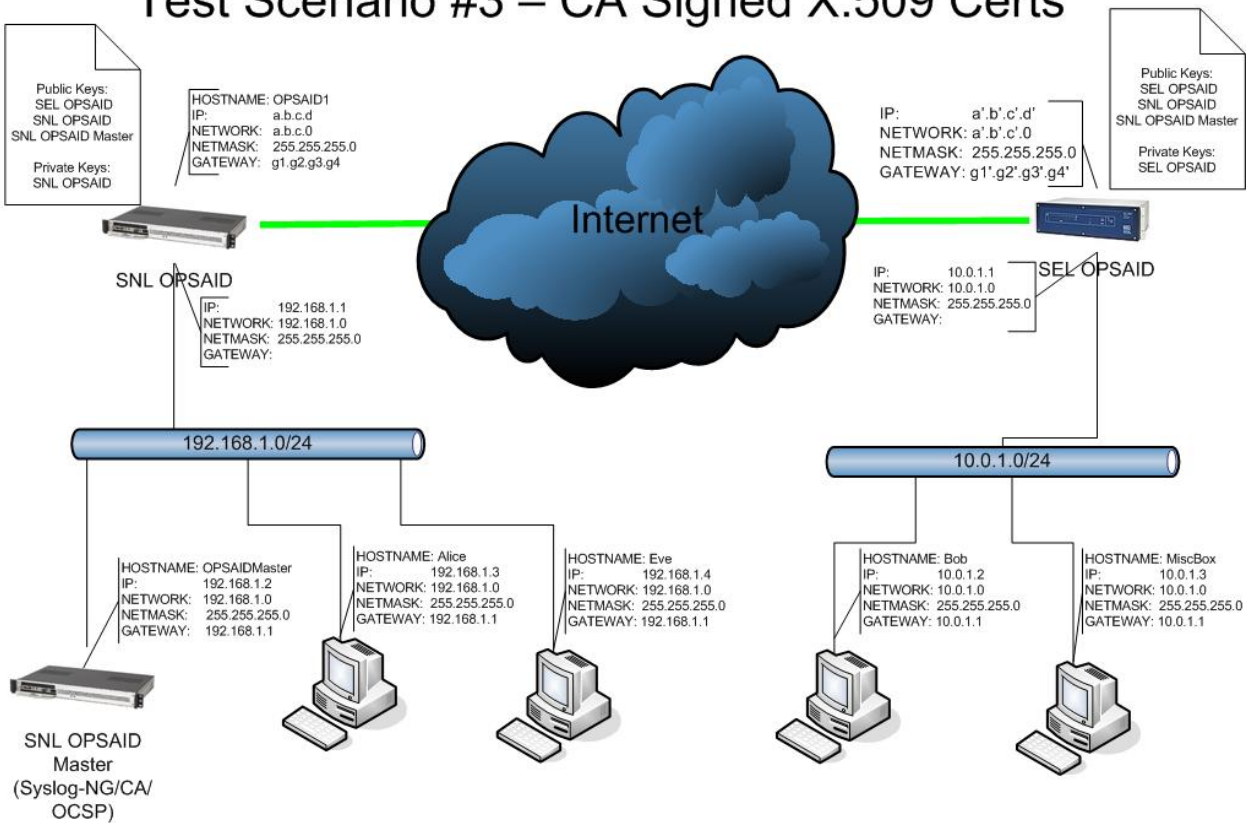
Test Scenario #1 – Pre Shared Passphrase



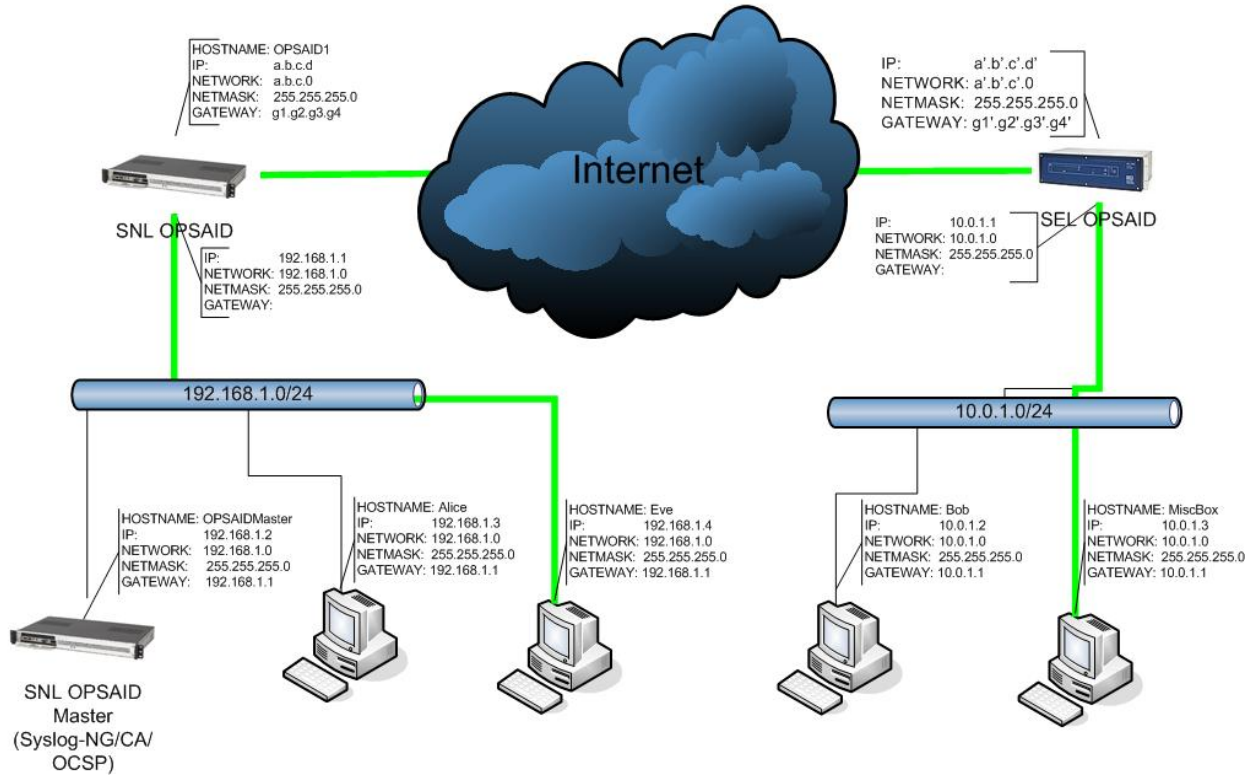
Test Scenario #4 – CA Signed X.509 Certs with OCSP

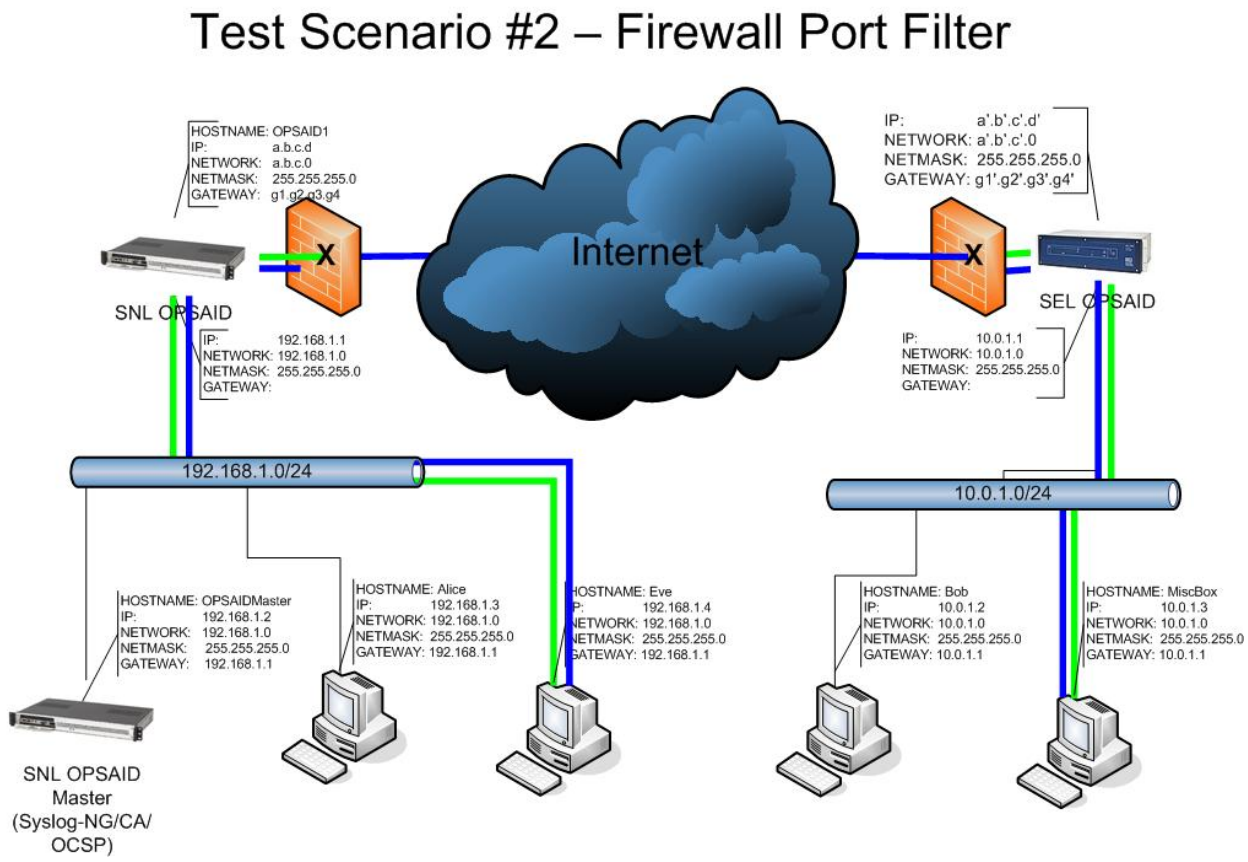


Test Scenario #3 – CA Signed X.509 Certs



Test Scenario #1 – No Firewall





A.3 Additional Information

A.3.1 Certificates for Securing IPSec Tunnels

This brief technology should give you some verbiage to explain why we chose X.509 certificates for securing our IPsec connections (in addition to offering the preshared key (PSK) protection).

Before we can talk about X.509 certificates, we need a brief review of asymmetric encryption. Remember that in asymmetric encryption (or public key) systems, the key used to encrypt the data is different from the key used to decrypt the data.

Asymmetric encryption algorithms generally have two key (which are composed of one or more numbers). Data can be encrypted with the public key and to a large degree of confidence we can be certain that the data can only be decrypted by the corresponding private key.

How is this useful for things like IPSec? Let's say Alice wants to authenticate Bob. Assume that Bob gave Alice his public key. Alice could create a random number X and encrypt X with Bob's public key. She could than send the encrypted version of X to Bob. If Bob can tell her the random number she chose, she can be pretty certain that Bob's private key was used to obtain the random number. Providing Bob is a good citizen and hasn't allowed his private key to be compromised (and ignoring MITM attacks for this illustration), Alice can proceed with confidence that Bob really is Bob.

The above scenario works great if Bob met Alice and gave her his public key, but doing so would require anyone who wants to talk to anyone else to have a face-to-face or semi-secure meeting. This quickly becomes difficult in a large group of people.

Enter PKI (Public key infrastructure). If Bob were to take his public key and put it in an envelope and mail it to Alice, Alice wouldn't be able to use the public key as she would be worried the carrier might have swapped it out for one of their keys.

One way to mitigate this problem would be to have an unbiased and trustworthy third party take the time to very that everyone's public key is actually tied to the person they say they are. Let's call this person Trent. If Bob went to Trent's office and showed Trent his birth certificate, driver's license, etc and convinced Trent that Bob really was Bob, Bob could put his public key in an envelope and Trent could sign the seal. Bob can now mail his key to Alice and since Alice also trusts Trent, she could see that Trent signed the envelope and thus Bob's key must have come from Bob.

We have solved one problem and introduced another? How does everyone learn what Trent's signature looks like? This is a little problematic, but it is easier to teach everyone what Trent's signature looks like then it is to exchange public keys between everyone in a large group.

Everything described above is applicable (with poetic license :-) to X.509 certificates. X.509 certificates encode a public key for an entity along with information stating who "owns" that public key. The entire certificate is than signed by a certificate authority who is in essence saying "I talk to the person who made this public key and I know that the person whose name is attached to this certificate really did make the certificate". This would generally be a CA like Thawte.

Using X.509 certificates bring stronger authentication to IPsec because:

- The keyspace is larger. Most RSA keys are 1024 random bits or more. Passphrases generally don't contain that much entropy.
- X.509 Certificates bind a specific public key (which is just a set of number) to an organization or a person.
- X.509 certificates are used ubiquitously. Every bank or SSL website makes use of an X.509 certificate.
- X.509 certificates can encode additional information about the key, such as the expiration date, start date, and group membership.

For more information on X.509 certificates see:
http://en.wikipedia.org/wiki/X509

A.3.2 Hurdles and Lessons Learned

- Interchangability generalizes the concept of modularity
- Interoperability generalizes the concept of interchangeability
- Application Requirements = Interoperability Requirements

- Assurance mechanisms/expectations need to be specified alongside interoperability requirements

---

[i] Functions of this component are authentication and integrity. Reference from ISA-TR99, NIST 800-53, and RFC 2401

[ii] The default is 128, mode is CBC and this is a minimum requirement. The components this is covering are confidentiality, integrity, authentication, and key management

[iii] IP address shall be used as the identifier for passphrase connections. IP Nat will not be supported by the IPSec endpoint. Use IKE v2, will support only tunnel mode. Source routing shall be supported. RSA keys by default with minimum size of 1024, but support 2048 and 4096. For perfect forward secrecy use Group 5 and PFS is required.

[iv] Can us V1,V2, and V3. PEM certification shall be used. Certificates will be verified, the subject has to match and the subject will be the identifier.

[v] Chaining is not developed on the certificates in this phase; will be added to future development.

[vi] Can support up to 2038.

[vii] Must have Ethernet IPv4.

[viii] Will provide specification of what to log at a future time.

[ix] With 1 to 128 characters

[x] From the ASCII set (ie. values between 0x21 and 0x7e) as password character security

[xi] Give users the options to drop ICMP ping; only encrypt traffic on the un-trusted interface; deny all by default. Per port actions include allow, drop or reject, enable the rule, select protocol.

[xii] MIBs will have security management

[xiii] Will employ tools and techniques to monitor events on the control system, detect attachment, and provide identification of unauthorized users of system; support near real time analysis of events, in support of detecting control system attacks. Integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attacks isolation and elimination; use common protocols; the control system monitors in bound and out bound communications from unusual or unauthorized activities and conditions

[xiv] Support for Day Light Savings time

[xv] Includes self-signed X.509, upload x.509 certificates and private keys; download certificates

[xvi] Provide support for central role based server