The Consultative Committee for Space Data Systems

CCSDS NETWORK LAYER SECURITY ADAPTATION PROFILE TEST

DRAFT CCSDS RECORD

CCSDS 356.1-Y-2

Yellow Book

October 2017

DOCUMENT CONTROL

Document	Title and Issue	Date	Status
CCSDS 000.1-R-1	CCSDS NETWORK LAYER SECURITY ADAPTATION PROFILE, Draft CCSDS Record, Issue 1	August 2013	draft

FOREWORD

Through the process of normal evolution, it is expected that expansion, deletion, or modification of this document may occur. This document is therefore subject to CCSDS document management and change control procedures, which are defined in the *Procedures Manual for the Consultative Committee for Space Data Systems*. Current versions of CCSDS documents are maintained at the CCSDS Web site:

http://www.ccsds.org/

Questions relating to the contents or status of this document should be addressed to the CCSDS Secretariat at the address indicated on page i.

At time of this publication, the active Member and Observer Agencies of the CCSDS were:

Member Agencies

- Agenzia Spaziale Italiana (ASI)/Italy.
- British National Space Centre (BNSC)/United Kingdom.
- Canadian Space Agency (CSA)/Canada.
- Centre National d'Etudes Spatiales (CNES)/France.
- China National Space Administration (CNSA)/People's Republic of China.
- Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)/Germany.
- European Space Agency (ESA)/Europe.
- Federal Space Agency (FSA)/Russian Federation.
- Instituto Nacional de Pesquisas Espaciais (INPE)/Brazil.
- Japan Aerospace Exploration Agency (JAXA)/Japan.
- National Aeronautics and Space Administration (NASA)/USA.

Observer Agencies

- Austrian Space Agency (ASA)/Austria.
- Belgian Federal Science Policy Office (BFSPO)/Belgium.
- Chinese Academy of Sciences (CAS)/China.
- Chinese Academy of Space Technology (CAST)/China.
- China Satellite Launch and Tracking Control General, (CLTC)/China.
- Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
- Departamento De Ciência E Tecnologia Aeroespacial (DCTA)/Brazil.
- Danish National Space Center (DNSC)/Denmark.
- Electronics and Telecommunications Research Institute (ETRI)/Korea
- European Organization for the Exploitation of Meteorological Satellites (EUMETSAT)/Europe.
- European Telecommunications Satellite Organization (EUTELSAT)/Europe.
- Geo-Informatics and Space Technology Development Agency (GISTDA)/Thailand
- Hellenic National Space Committee (HNSC)/Greece.
- Institute of Space Research (IKI)/Russian Federation.
- Indian Space Research Organization (ISTRAC)/India.
- Korea Aerospace Research Institute (KARI)/Korea.
- KFKI Research Institute for Particle and Nuclear Physics (RMKI)/Hungary
- Ministry of Communications (MOC)/Israel.
- Naval Center for Space Technology (NCST)/USA.
- National Institute of Information and Communications Technology (NICT)/Japan.
- National Oceanic and Atmospheric Administration (NOAA)/USA.
- National Space Agency of the Republic of Kazakhstan (Kazcosmos) (NSARK)/Republic of Kazakhstan.
- National Space Organization (NSPO)/ Taiwan.
- South African National Space Agency (SANSA)/ South Africa.
- Swedish Space Corporation (SSC)/Sweden.
- Swiss Space Office (SSO)/Swiss Confederation.
- Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
- Central Research Institute of Machine Building (TsNIIMash)/ Russian Federation.
- The Scientific and Technological Research Council of Turkey (TUBITAK)/ Turkey
- United States Geological Survey (USGS)/USA.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CCSDS NETWORK LAYER SECURITY ADAPTATION PROFILE TEST

1.0 Introduction

1.1 Purpose

The purpose of this document is to describe the compatibility testing conducted for the CCSDS Network Layer Security Adaptation Profile. Define CCSDS. Ensure that all acronyms are defined.

1.2 Scope

The scope of this document is the testing results of the Network Layer Security Adaptation Profile which will be implemented and used for CCSDS missions.

1.3 Applicability

This recommendation applies to any CCSDS mission using the Internet Protocol and requiring end-to-end confidentiality, authentication, or integrity from the sender to the receiver regardless of the number of intermediate hops between them.

1.4 Rationale

Many CCSDS missions require security services to protect commanding (command authentication, command confidentiality, command integrity) and payload data (confidentiality, integrity). Missions using the Internet Protocol (IP) may utilize link layer security services such as the Space Data Link Security (SDLS) Protocol which provides hop-by-hop security between two points (e.g., a ground station and a satellite). If end-to-end security is required, such as between a principal investigator and a payload instrument onboard a spacecraft through intermediary hops, then the IP Security (IPsec) protocol should be used. CCSDS has documented a "profile" of IPsec for use by CCSDS missions. This document discusses interoperability testing of the CCSDS profile.

1.5 Document Structure

This document describes the tests, configurations tested and not tested, and test results from the Network Layer Security Adaptation Profile interoperability testing.

1.6 References

The following documents are informative references used to accomplish testing.

[1] Internet Engineering Task Force (IETF); Kent, S; Seo, K; Security Architecture for the Internet Protocol; Request for Comments (RFC) 4301; http://datatracker.ietf.org/doc/rfc4301; Dec. 2005.

[2] IETF; Kent, S; IP Authentication Header; RFC 4302; http://datatracker.ietf.org/doc/rfc432; Dec. 2005.

[3] IETF; Kent, S; IP Encapsulating Security Payload (ESP); RFC 4303; http://datatracker.ietf.org/doc/rfc4303; Dec. 2005.

[4] IETF; Kaufman, C; Internet Key Exchange (IKEv2) RFC 4306; http://datatracker.ietf.org/doc/rfc4306; Dec. 2005.

[5] IETF; Shacham, A; Monsour, B; Pereira, R; Thomas M; IP Payload Compression Protocol (IPComp); Request for Comments (RFC) 3173; http://datatracker.ietf.org/doc/rfc3173; Sep. 2001.

[6] CCSDS; CCSDS Cryptographic Algorithms; CCSDS 352.0-B-1; Blue Book; Issue 1; Nov. 2012.
[7] CCSDS; IP over CCSDS Space Links; CCSDS 702.1-B-1; Blue Book; Issue 1; Sep. 2012.

2.0 Overview

Many CCSDS missions require security services such as confidentiality, integrity, and authentication to protect spacecraft commands, software uploads, engineering telemetry, and science payload data.

IPsec consists of two protocols: the Authentication Header (AH) and the Encapsulating Security Payload (ESP). AH provides only authentication and integrity services for the security payload and portions of the IP header. However, AH does not provide confidentiality. ESP, on the other hand, provides confidentiality, integrity, and authentication. Authentication with ESP is not as robust as with AH because it does not cover as much of the external headers but is quite adequate. ESP can be also be used to provide only authentication with the use of a null encryption algorithm.

CCSDS has decided that ESP is the only IPsec protocol that shall be supported.

3.0 Summary of Interoperability and Compatibility Testing

IPsec compatibility testing was successful; however, some challenges were encountered. Some of the issues were that some commercial vendors no longer support various IPsec options as specified in the CCSDS Network Layer Security Adaptation Profile. Vender routers and firewalls do not support manual keying and Vendors have also removed the capability to control the rekeying.

Connectivity between National Aeronautics and Space Administration (NASA) Glenn Research Center and NASA’s Independent Verification and Validation (IV&V) endpoint systems was successfully established.

4.0 Algorithm Testing Goals

4.1 General

This profile adopts RFC 4301 and RFC 4303 except as specified in 4.2-4.9, inclusive.

4.2 Supported protocols

For CCSDS mission implementations, IPsec shall support only ESP.

4.3 ESP mode

For CCSDS mission implementations, IPsec shall support only tunnel mode.

4.4 ESP authenticated encryption service

For CCSDS mission implementations, IPsec shall support confidentiality and integrity security service (authenticated encryption).

4.5 ESP Integrity service

For CCSDS mission implementations, IPsec shall support an integrity-only service.

4.6 ESP Non-Authenticated Encryption

For CCSDS mission implementations, only authenticated encryption shall be used.

4.7 ESP Manual Key Management

For CCSDS mission implementations, IPsec shall support manual key management.

4.8 ESP Automatic Key Management

For CCSDS mission implementations, IPsec shall support automated key management as described in RFC 4306 with an extension to inhibit rekey or to rekey only upon command.

NOTE: this extension is required to ensure that a rekey does not occur during a critical phase of the mission potentially resulting in a system lockout or loss of mission.

4.9 ESP Cipher Suite

For CCSDS mission implementations, IPsec shall employ the algorithms described in the CCSDS Cryptographic Algorithms recommendations [6].

5.0 Tests Details

The testing between NASA GRC's end-point and NASA's IV&V Facility end-point was conducted at the NASA's Independent Verification and Validation (IV&V) Facility.

Process note: Tunnels are brought down in-between each test to ensure no miss configured states.

Table 1 lists equipment and software utilized during testing. The operator must have an understanding of the software systems being utilized and a knowledge of Internet Protocol.

Table 2 synopsizes the IPsec modes performed and results from local testing. This table highlights the different configurations that are to be built and utilized during the interoperability testing.

TABLE 1.—TESTED END POINT ITEMS

NASA GRC	NASA IV&V
Hardware	**Hardware**
Cisco 892 FSP router IOS 15.5(3)M4a	Cisco 892 FSP router IOS 15.5(3)M4a
HP Z-Book	Dell XFR0630
Software	**Software**
Ubuntu v16.04.2 LTS	Ubuntu v16.04.2 LTS
Minicom 2.7	Minicom 2.7
Cisco Configuration Professional Express 3.3	Cisco Configuration Professional Express 3.3
StrongSwan 5.5.3	StrongSwan 5.5.3
Open SSL 1.0.2G	Open SSL 1.0.2G
WireShark v2.26	WireShark v2.26

TABLE 2.—IPSEC TESTS

IPV4 test no.	ESP	Tunnel	Integrity	Authenticated encryption	Confidentiality	Manual key	Auto key	No rekey
1	X	X	X	X	--	--	X	X
2	X	X	X		X	--	X	X
3	X	X	X	X	--	X	--	--
4	X	X	X	--	X	X	--	--

5.1 IPV4 Authenticated Automatic Keying #1

5.1.1 Test Description

IPV4 addresses using encapsulated tunnel mode with integrity using authentication and automatic keying with no rekeying. Endpoints will use a certificate server to acquire the same 128-bit public key and then negotiate the private key.

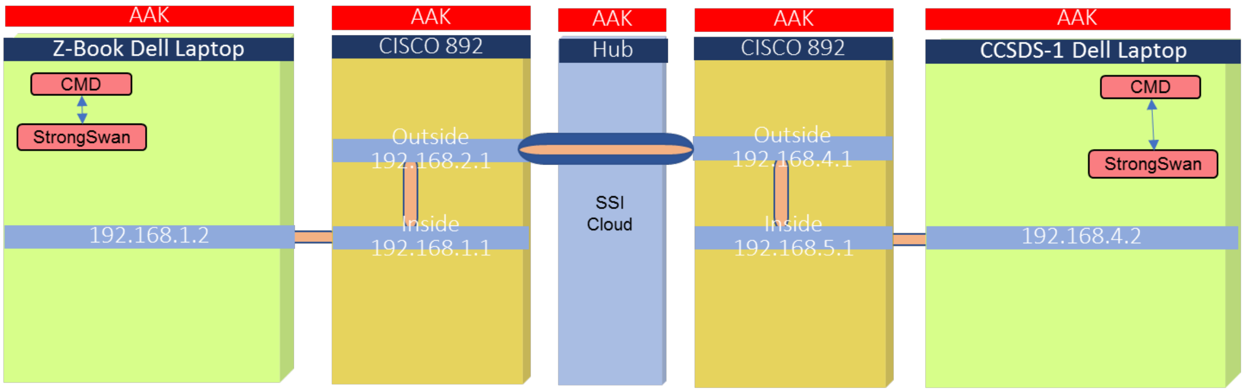
Preshared keys with, IPV4 addresses of firewalls and endpoints not provided in this document.

Figure 1 Test diagram of Authenticated Automatic Keying Reference Architecture for Space Data Systems (RASDS) view. RASDS view is intended to illustrate the layers of the Open Systems Interconnection model that this testing will work through however this is only a network layer test.

Figure 2 Test diagram of Authenticated Automatic Keying wire diagram view. The wire diagram shows how the protocol test is physically connected.

5.1.2 Expected Results

The resultant encryption/decrypted logs match, the test is successful.

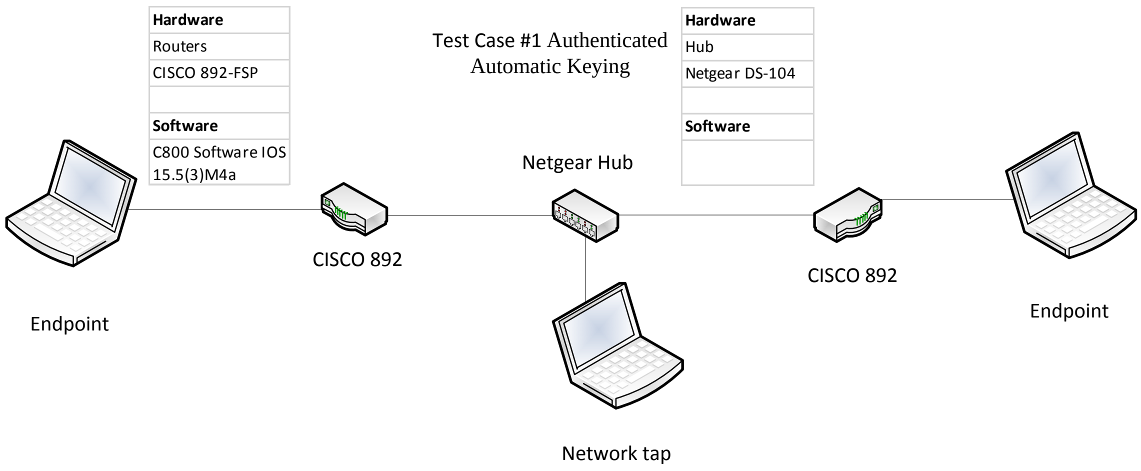


CCSDS laptops Sets up the security association, sets the pre-shared keys. StrongSwan will auto negotiate the keying and re-keying

The Hub represents the internet and its many hops. Dark Blue is Generic Routing Encapsulation (**GRE**) not part of the security.

CCSDS-2 Tap sniffing, SSI Cloud
192.168.12.4

Figure 1.—RASDAS view of test.



Hardware
Routers
CISCO 892-FSP
Software
C800 Software IOS 15.5(3)M4a

Hardware
Hub
Netgear DS-104
Software

Hardware
CCSDS-1 = IV&V
Dell XFR0630
Software
WireShark 2.26
minicom 2.7
Cisco Configuration Professional Express 3.3
StronSwan 5.5.3
Ubuntu 16.04.2 LTS
Open SSL 1.0.2G

Hardware
CCSDS-2 = Tap
Dell XFR0630
Software
WireShark 2.26
minicom 2.7
Cisco Configuration Professional Express 3.3
Ubuntu 16.04.2 LTS
Open SSL 1.0.2G

Hardware
Z-Book = GRC
HP z-Book
Software
WireShark 2.26
minicom 2.7
Cisco Configuration Professional Express 3.3
StronSwan 5.5.3
Ubuntu 16.04.2 LTS
Open SSL 1.0.2G

Figure 2.—Wireline diagram of the test.

128-Bit Key: 000102030405060708090a0b0c0d0e0f

5.2 IPV4 Confidentiality Automatic Keying #2

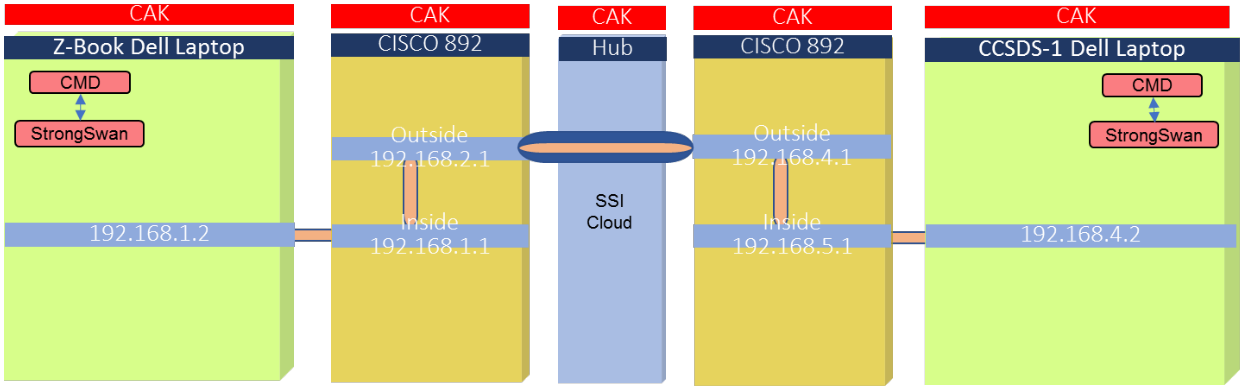
5.2.1 Test Description

IPV4 addresses using encapsulated tunnel mode with integrity using authentication and automatic keying with no rekeying. Endpoints will use a certificate server to acquire the same 128-bit public key and then negotiate the private key.

Pre shared IPV4 addresses of firewalls and endpoints not provided in this document.

Figure 3 Test diagram of Confidentiality Automatic Keying RASDS view. RASDS view is intended to illustrate the layers of the Open Systems Interconnection model that this testing will work through however this is only a network layer test.

Figure 4 Test diagram wire of Confidentiality Automatic Keying wire diagram view. The wire diagram shows how the protocol test is physically connected.



CCSDS laptops Sets up the security association, sets the pre-shared keys. StrongSwan will auto negotiate the keying and re-keying

The Hub represents the internet and its many hops. Dark Blue is Generic Routing Encapsulation (**GRE**) not part of the security.

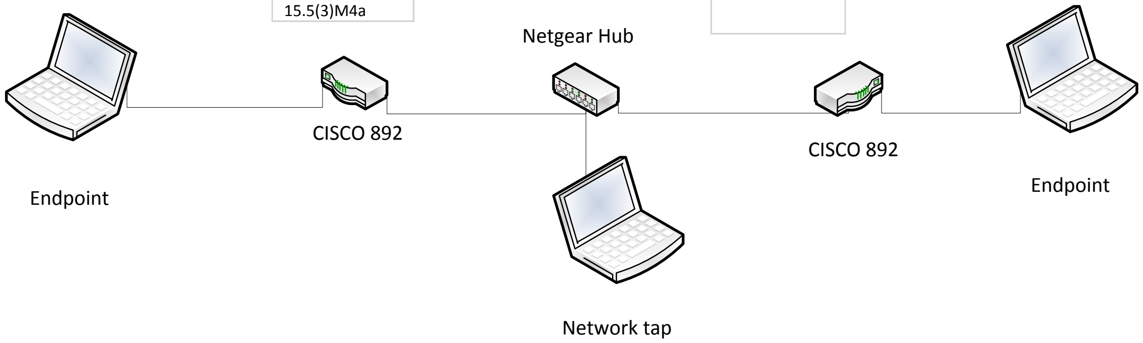
CCSDS-2 Tap sniffing, SSI Cloud
192.168.12.4

Figure 3.—RASDAS view of test.

Hardware
Routers
CISCO 892-FSP
Software
C800 Software ICS 15.5(3)M4a

Test Case #2 Confidentiality
Automatic Keying

Hardware
Hub
Netgear DS-104
Software



Hardware	**Hardware**	**Hardware**
CCSDS-1 = IV&V	CCSDS-2 = Tap	Z-Book = GRC
Dell XFR0630	Dell XFR0630	HP z-Book
Software	Software	**Software**
WireShark 2.26	WireShark 2.26	WireShark 2.26
minicom 2.7	minicom 2.7	minicom 2.7
Cisco Configuration Professional Express 3.3	Cisco Configuration Professional Express 3.3	Cisco Configuration Professional Express 3.3
StronSwan 5.5.3		StronSwan 5.5.3
Ubuntu 16.04.2 LTS	Ubuntu 16.04.2 LTS	Ubuntu 16.04.2 LTS
Open SSL 1.0.2G	Open SSL 1.0.2G	Open SSL 1.0.2G

Figure 4.—Wireline diagram of the test.

Pre shared Keying: 128-Bit Key: 000102030405060708090a0b0c0d0e0f

5.2.2 Expected Results

If the resultant encryption/decrypted logs match, the test is successful.

5.3 IPV4 Authenticated Manual Key #3

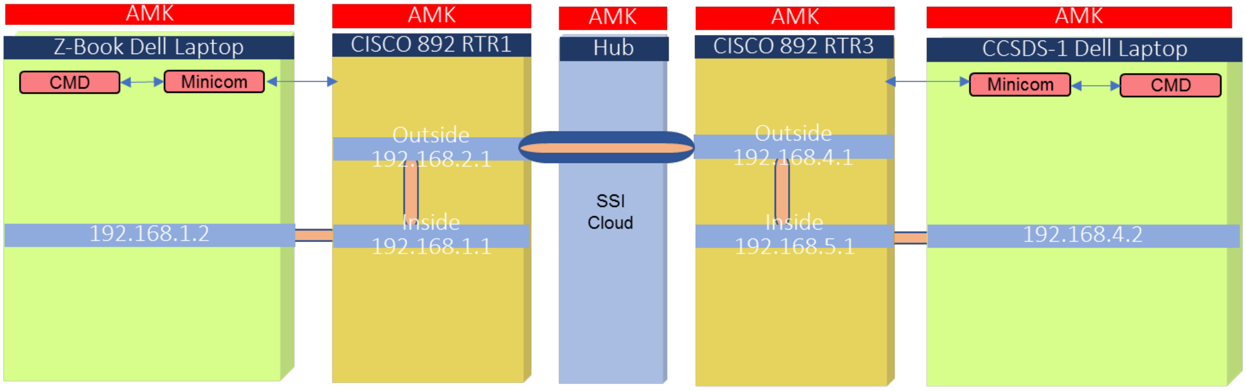
5.3.1 Test Description

IPV4 addresses using encapsulated tunnel mode with integrity using authentication and manual keying. Endpoint one will encrypt data using a 128-bit test key. The resultant cipher data will be sent to a second endpoint recipient via a network connection. The recipient will use the same 128-bit test key to decrypt the cipher text.

Pre shared IPV4 addresses of firewalls and end points not provided in this document.

Figure 5 shows a test diagram of Authenticated Manual Keying RASDS view. RASDS view is intended to illustrate the layers of the Open Systems Interconnection model that this testing will work through however this is only a network layer test.

Figure 6 is a test diagram of Authenticated Manual Keying wire diagram view. The wire diagram shows how the protocol test is physically connected.



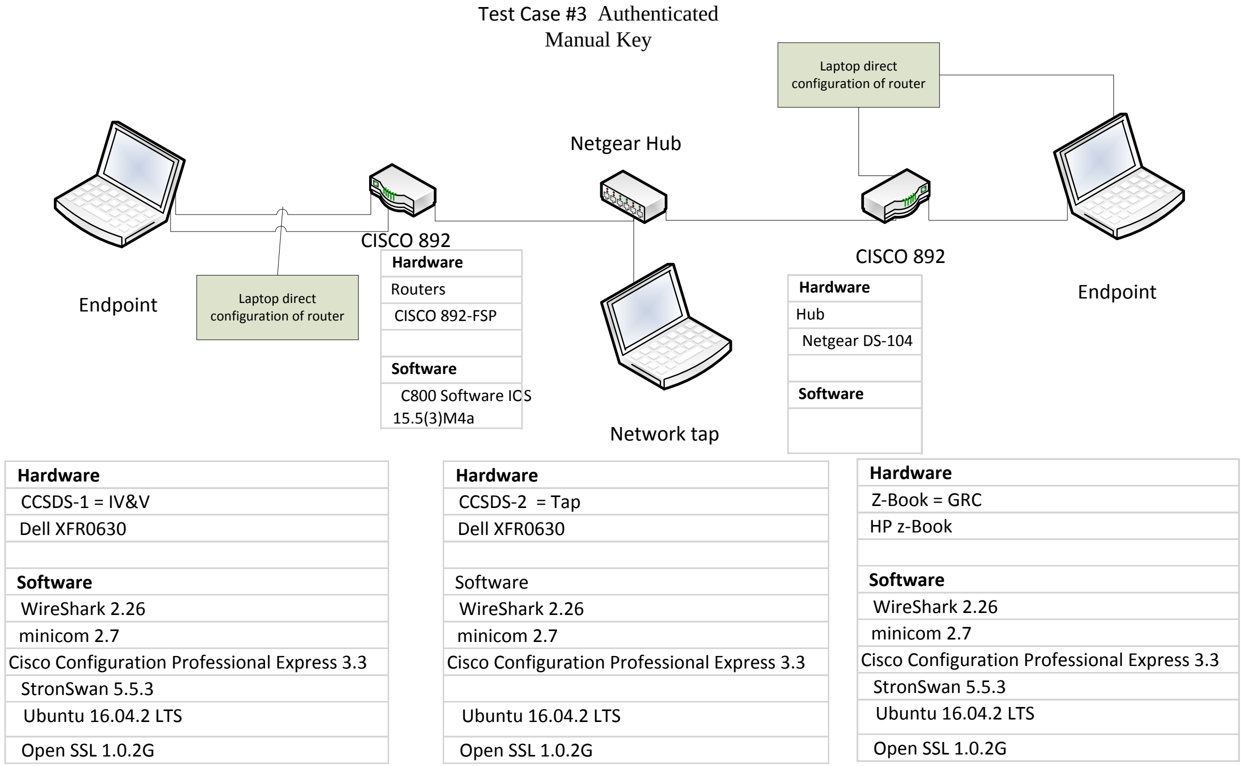
CCSDS laptops manually configure the CISCO 892 routers, provides the addresses and the pre-shared keys. Builds the Phase 1 and Phase 2 tunnels.

Flesh tone is the secure tunnel; Phase 1 tunnel the two endpoints authenticate one another and negotiate keying material.
Phase 2: the two endpoints use the secure tunnel created in Phase 1 to negotiate ESP SAs. The ESP SAs are what are used to encrypt the actual user data that is passed between the two endpoints.

The Hub represents the internet and its many hops. Dark Blue is Generic Routing Encapsulation (**GRE**) not part of the security.

CCSDS-2 Tap sniffing, SSI Cloud
192.168.12.4

Figure 5.—RASDAS view of test.



Hardware
CCSDS-1 = IV&V
Dell XFR0630
Software
WireShark 2.26
minicom 2.7
Cisco Configuration Professional Express 3.3
StronSwan 5.5.3
Ubuntu 16.04.2 LTS
Open SSL 1.0.2G

Hardware
CCSDS-2 = Tap
Dell XFR0630
Software
WireShark 2.26
minicom 2.7
Cisco Configuration Professional Express 3.3
Ubuntu 16.04.2 LTS
Open SSL 1.0.2G

Hardware
Z-Book = GRC
HP z-Book
Software
WireShark 2.26
minicom 2.7
Cisco Configuration Professional Express 3.3
StronSwan 5.5.3
Ubuntu 16.04.2 LTS
Open SSL 1.0.2G

Figure 6.—Wireline diagram of the test.

Pre shared Keying: 128-Bit Key: 000102030405060708090a0b0c0d0e0f

5.3.2 Expected Results

Encryption/decrypted numbers match or off by one and tunnel established the test is successful.

5.4 IPV4 Confidentiality Manual Key #4

5.4.1 Test Description

IPV4 addresses using encapsulated tunnel mode with integrity using confidentiality and manual keying. Endpoint one will encrypt data using a 128-bit test key. The resultant cipher data will be sent to a second endpoint recipient via a network connection. The recipient will use the same 128-bit test key to decrypt the cipher text.

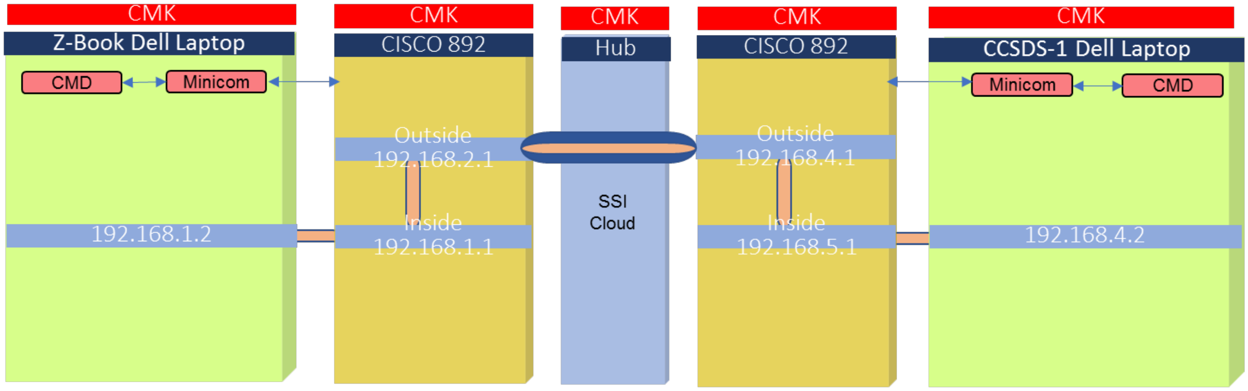
Pre shared IPV4 addresses of firewalls and endpoints not provided in this document.

Figure 7 shows a test diagram of Confidentiality Manual Keying RASDS view. RASDS view is intended to illustrate the layers of the Open Systems Interconnection model that this testing will work through however this is only a network layer test.

Figure 8 shows a test diagram of Confidentiality Manual Keying wire diagram view. The wire diagram shows how the protocol test is physically connected.

5.4.2 Expected Results

Encryption/decrypted numbers match or off by one and tunnel established the test is successful.



CCSDS laptops manually configure the CISCO 892 routers, provides the addresses and the pre-shared keys. Builds the Phase 1 and Phase 2 tunnels.

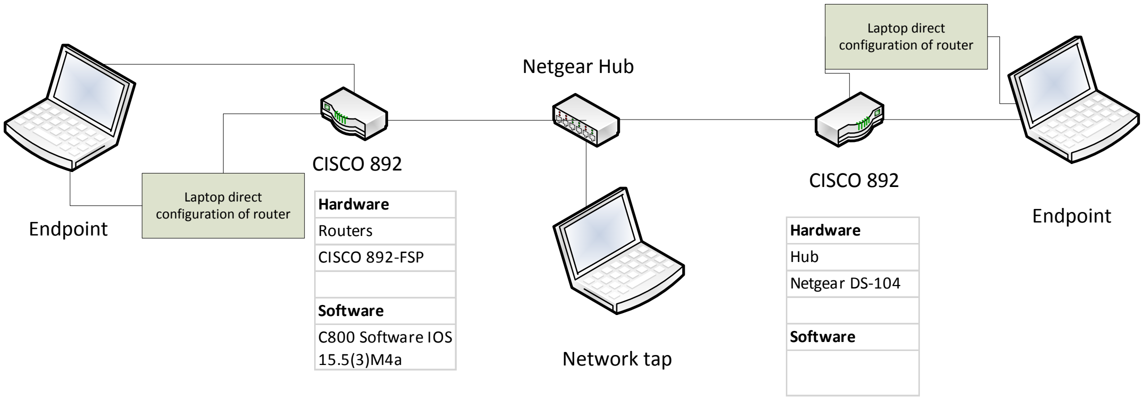
Flesh tone is the secure tunnel; Phase 1 tunnel the two endpoints authenticate one another and negotiate keying material.
Phase 2: the two endpoints use the secure tunnel created in Phase 1 to negotiate ESP SAs. The ESP SAs are what are used to encrypt the actual user data that is passed between the two endpoints.

The Hub represents the internet and its many hops. Dark Blue is Generic Routing Encapsulation (**GRE**) not part of the security.

CCSDS-2 Tap sniffing, SSI Cloud
192.168.12.4

Figure 7.—RASDAS view of test.

Test Case #4 Confidentiality
Manual Key


Netgear Hub
Laptop direct configuration of router
CISCO 892
Endpoint
Laptop direct configuration of router
CISCO 892
Endpoint
Network tap

Hardware
Routers
CISCO 892-FSP
Software
C800 Software IOS 15.5(3)M4a

Hardware
Hub
Netgear DS-104
Software

Hardware
CCSDS-1 = IV&V
Dell XFR0630
Software
WireShark 2.26
minicom 2.7
Cisco Configuration Professional Express 3.3
StronSwan 5.5.3
Ubuntu 16.04.2 LTS
Open SSL 1.0.2G

Hardware
CCSDS-2 = Tap
Dell XFR0630
Software
WireShark 2.26
minicom 2.7
Cisco Configuration Professional Express 3.3
Ubuntu 16.04.2 LTS
Open SSL 1.0.2G

Hardware
Z-Book = GRC
HP z-Book
Software
WireShark 2.26
minicom 2.7
StronSwan 5.5.3
Ubuntu 16.04.2 LTS
Open SSL 1.0.2G

Figure 8.—Wireline diagram of the test.

Pre shared Keying: 128-Bit Key: 000102030405060708090a0b0c0d0e0f

6.0 Compatibility Testing Between NASA GRC and NASA IV&V

Compatibility testing is used to measure how well software applications or hardware devices function in concert with relevant hardware, software, operating systems or network environments.

NASA GRC and IV&V are only testing the IPV4 configurations (Figure 9). Appropriate documentation was exchanged between NASA centers in order to configure the path and encrypt the tunnels.

Table 3 is the summary of the IPsec tests modes performed and results from compatibility testing between NASA centers.

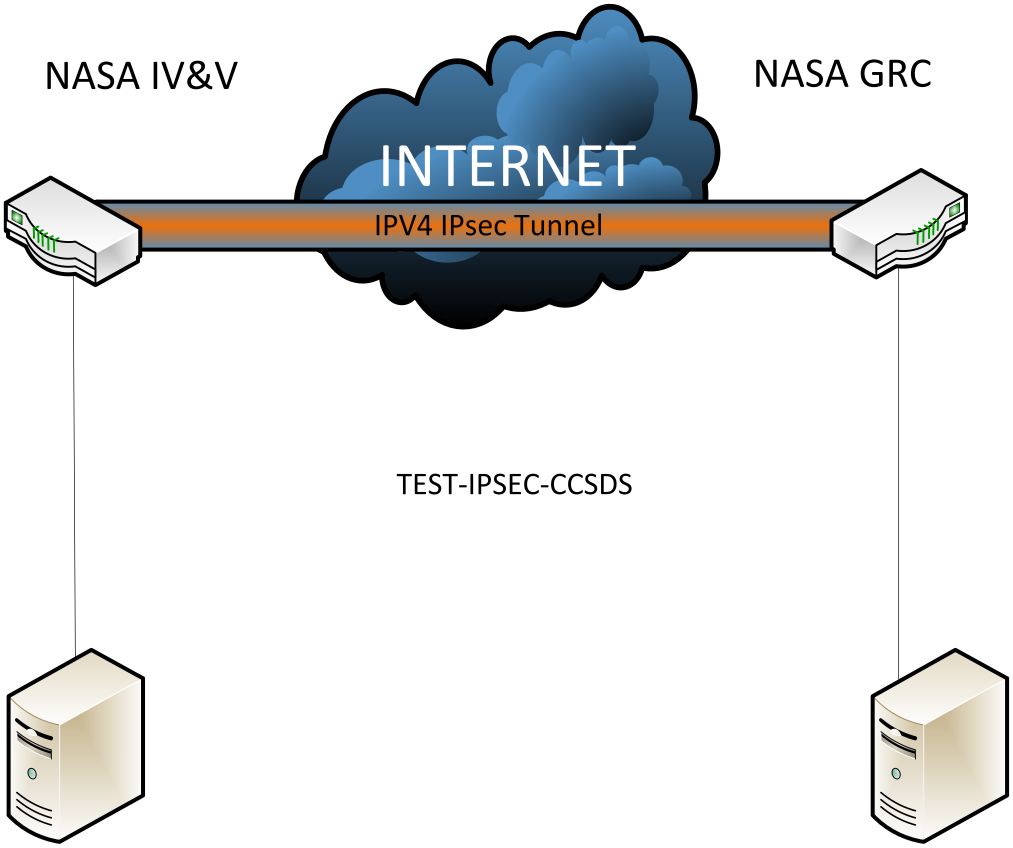


Figure 9.—GRC-IV&V test setup.

TABLE 3.—COMPATIBILITY TESTS AND RESULTS

IPV4 test #	ESP	Tunnel	Integrity	Authenticated encryption	Confidentiality	Manual key	Auto key	No rekey	Interoperability test
1	X	X	X	X	--	X	--	--	
2	X	X	X	--	X	X	--	--	
3	X	X	X	X	--	--	X	X	
4	X	X	X	--	X	--	X	X	

6.1 IPV4 Compatibility Test Results

Table 4 shows the details of Test Case 3, Authenticated Manual Key.

TABLE 4.—TEST CASE 3, AUTHENTICATED MANUAL KEY

1.	Test Date: 10/16/17	
2.	Program under test:	Network Layer Security Adaptation Profile
3.	Test Case:	3, Authenticated Manual Key
4.	Agencies Participating in this Test Case:	NASA GRC and NASA IV&V Facility
5.	IV&V Point of Contact:	Brandon Bailey
6.	IV&V Test Engineer:	Adam Alley ENGILITY Corp.
7.	GRC Point of Contact:	Charles Sheehe
8.	GRC Test Engineer:	John Wang
9.	Results (Pass, Partial Pass, Fail):	**Pass**
10.	Variances from Expected Result:	None
11.	Comments:	

The following are the log validating the test conducted:

IV&V: Configured Router

GRC: Configured Router

IV&V: Pinged distant end point

GRC: Pinged distant end point

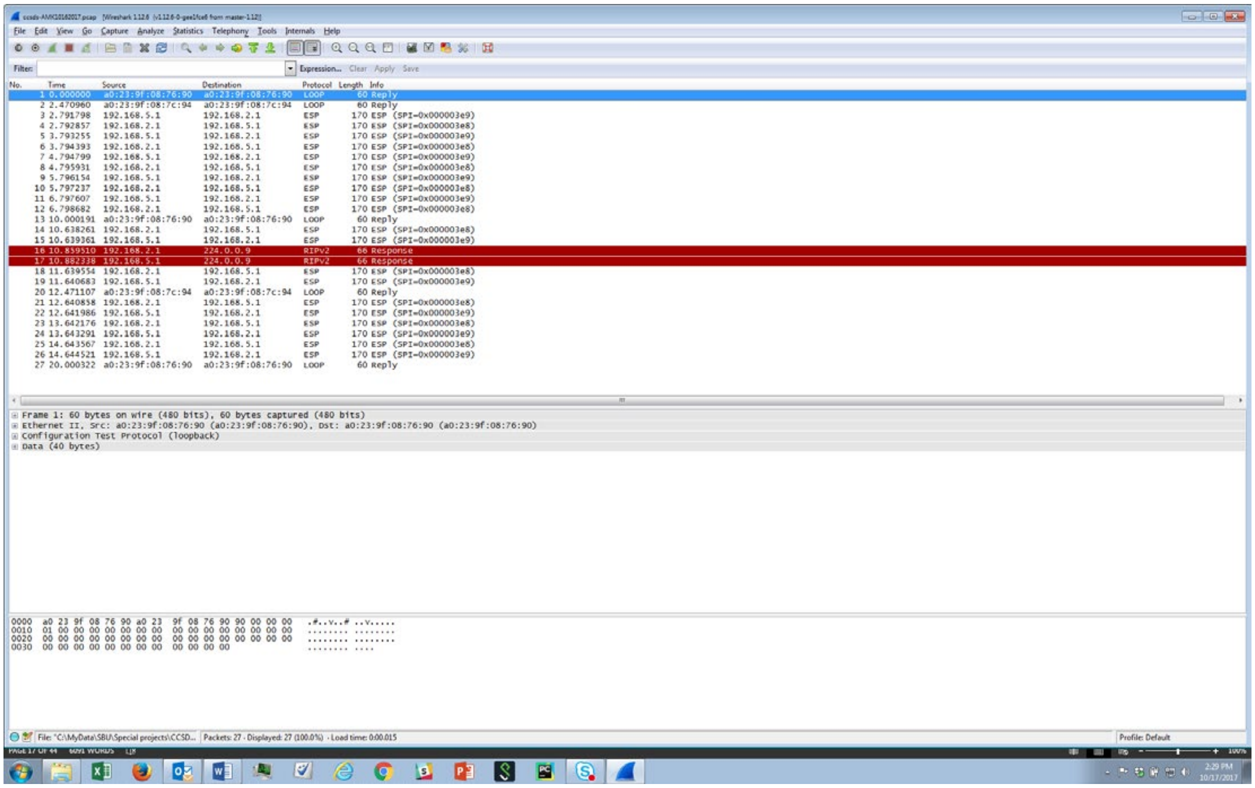
Bytes and Packets counters before traffic:

Bytes and Packets counters after ping from IV&V:

Bytes and Packets counters after ping from GRC:

Wire Shark capture of traffic/pings: File below:

ccsds-AMK10162017.pcap


ccsds-AMK10162017.pcap [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
Profile: Default

```
No.  Time       Source              Destination         Protocol Length Info
  1 0.000000   a0:23:9f:08:76:90   a0:23:9f:08:76:90   LOOP      60 Reply
  2 2.470960   a0:23:9f:08:7c:94   a0:23:9f:08:7c:94   LOOP      60 Reply
  3 2.791798   192.168.5.1         192.168.2.1         ESP      170 ESP (SPI=0x000003e9)
  4 2.792857   192.168.2.1         192.168.5.1         ESP      170 ESP (SPI=0x000003e8)
  5 3.793255   192.168.5.1         192.168.2.1         ESP      170 ESP (SPI=0x000003e9)
  6 3.794393   192.168.2.1         192.168.5.1         ESP      170 ESP (SPI=0x000003e8)
  7 4.794799   192.168.5.1         192.168.2.1         ESP      170 ESP (SPI=0x000003e9)
  8 4.795931   192.168.2.1         192.168.5.1         ESP      170 ESP (SPI=0x000003e8)
  9 5.796154   192.168.5.1         192.168.2.1         ESP      170 ESP (SPI=0x000003e9)
 10 5.797237   192.168.2.1         192.168.5.1         ESP      170 ESP (SPI=0x000003e8)
 11 6.797607   192.168.5.1         192.168.2.1         ESP      170 ESP (SPI=0x000003e9)
 12 6.798682   192.168.2.1         192.168.5.1         ESP      170 ESP (SPI=0x000003e8)
 13 10.000191  a0:23:9f:08:76:90   a0:23:9f:08:76:90   LOOP      60 Reply
 14 10.638261  192.168.2.1         192.168.5.1         ESP      170 ESP (SPI=0x000003e8)
 15 10.639361  192.168.5.1         192.168.2.1         ESP      170 ESP (SPI=0x000003e9)
 16 10.839510  192.168.2.1         224.0.0.9           RIPv2     66 Response
 17 10.882338  192.168.5.1         224.0.0.9           RIPv2     66 Response
 18 11.639554  192.168.2.1         192.168.5.1         ESP      170 ESP (SPI=0x000003e8)
 19 11.640683  192.168.5.1         192.168.2.1         ESP      170 ESP (SPI=0x000003e9)
 20 12.471107  a0:23:9f:08:7c:94   a0:23:9f:08:7c:94   LOOP      60 Reply
 21 12.640858  192.168.2.1         192.168.5.1         ESP      170 ESP (SPI=0x000003e8)
 22 12.641986  192.168.5.1         192.168.2.1         ESP      170 ESP (SPI=0x000003e9)
 23 13.642176  192.168.2.1         192.168.5.1         ESP      170 ESP (SPI=0x000003e8)
 24 13.643291  192.168.5.1         192.168.2.1         ESP      170 ESP (SPI=0x000003e9)
 25 14.643567  192.168.2.1         192.168.5.1         ESP      170 ESP (SPI=0x000003e8)
 26 14.644521  192.168.5.1         192.168.2.1         ESP      170 ESP (SPI=0x000003e9)
 27 20.000322  a0:23:9f:08:76:90   a0:23:9f:08:76:90   LOOP      60 Reply
```

```
⊞ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
⊞ Ethernet II, Src: a0:23:9f:08:76:90 (a0:23:9f:08:76:90), Dst: a0:23:9f:08:76:90 (a0:23:9f:08:76:90)
⊞ Configuration Test Protocol (loopback)
⊞ Data (40 bytes)
```

```
0000  a0 23 9f 08 76 90 a0 23  9f 08 76 90 90 00 00 00   .#..v..# ..v.....
0010  01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

File: "C:\MyData\SBU\Special projects\CCSD... Packets: 27 · Displayed: 27 (100.0%) · Load time: 0:00.015

Figure 10.—Wire Shark screen capture for Test Case 3, Authenticated Manual Key.

Wire Shark screen capture for Authenticated Manual Key is shown in Figure 10.

<BREAK>

Table 5 list details of Test Case 4, Confidentiality Manual Key.

TABLE 5.—TEST CASE 4, CONFIDENTIALITY MANUAL KEY

1.	Test Date:10/16/17	
2.	Program under test:	Network Layer Security Adaptation Profile
3.	Test Case:	4, Confidentiality Manual Key
4.	Agencies Participating in this Test Case:	NASA GRC and NASA IV&V Facility
5.	IV&V Point of Contact:	Brandon Bailey
6.	IV&V Test Engineer:	Adam Alley ENGILITY Corp.
7.	GRC Point of Contact:	Charles Sheehe
8.	GRC Test Engineer:	John Wang
9.	Results (Pass, Partial Pass, Fail):	**Pass**
10.	Variances from Expected Result:	None
11.	Comments:	

The following are the log validating the test conducted:

IV&V: Configured Router

GRC: Configured Router

IV&V: Pinged distant end point

GRC: Pinged distant end point

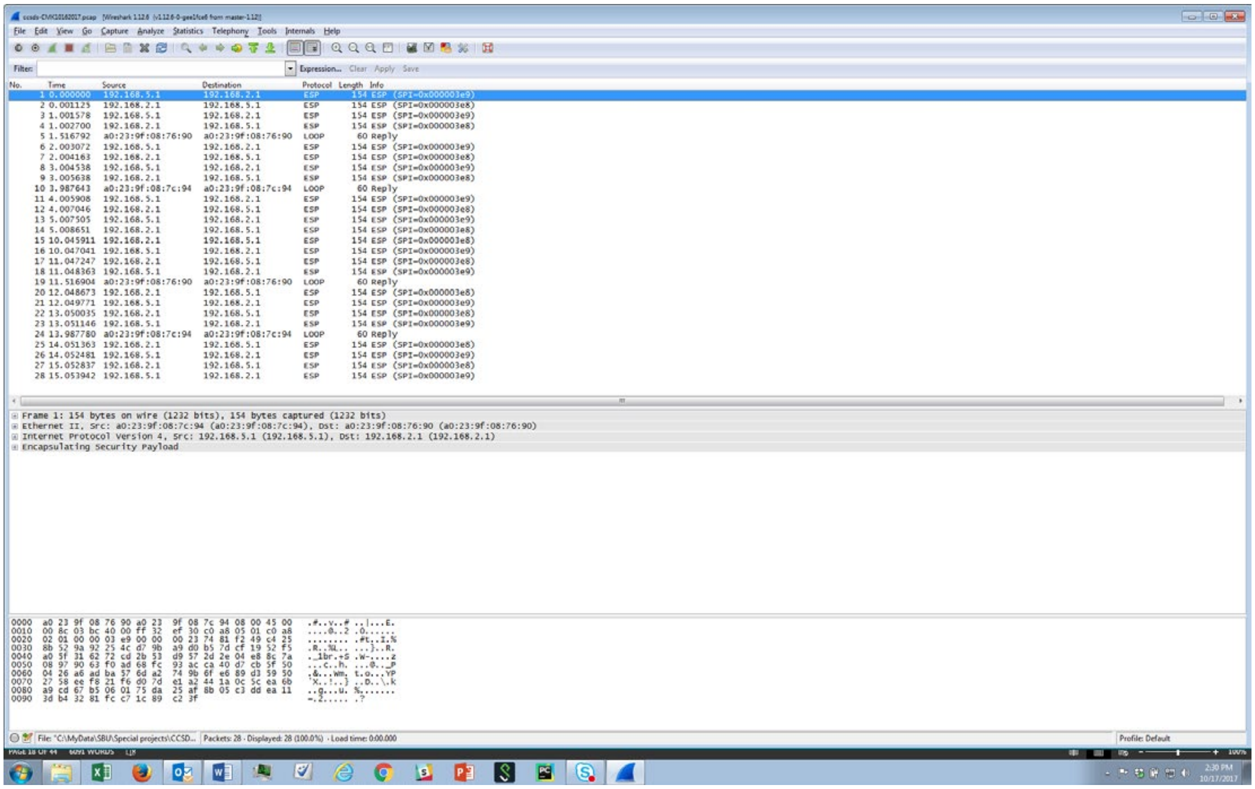
Bytes and Packets counters before traffic:

Bytes and Packets counters after ping from IV&V:

Bytes and Packets counters after ping from GRC:

Wire Shark capture of traffic/pings: File below

ccsds-CMK10162017.pcap


ccsds-CMK10162017.pcap [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
Profile: Default

```
No.  Time       Source             Destination        Protocol Length Info
   1 0.000000   192.168.5.1        192.168.2.1        ESP       154 ESP (SPI=0x000003e9)
   2 0.001125   192.168.2.1        192.168.5.1        ESP       154 ESP (SPI=0x000003e8)
   3 1.001578   192.168.5.1        192.168.2.1        ESP       154 ESP (SPI=0x000003e9)
   4 1.002700   192.168.2.1        192.168.5.1        ESP       154 ESP (SPI=0x000003e8)
   5 1.516792   a0:23:9f:08:76:90  a0:23:9f:08:76:90  LOOP       60 Reply
   6 2.003072   192.168.5.1        192.168.2.1        ESP       154 ESP (SPI=0x000003e9)
   7 2.004163   192.168.2.1        192.168.5.1        ESP       154 ESP (SPI=0x000003e8)
   8 3.004538   192.168.5.1        192.168.2.1        ESP       154 ESP (SPI=0x000003e9)
   9 3.005638   192.168.2.1        192.168.5.1        ESP       154 ESP (SPI=0x000003e8)
  10 3.987643   a0:23:9f:08:7c:94  a0:23:9f:08:7c:94  LOOP       60 Reply
  11 4.005908   192.168.5.1        192.168.2.1        ESP       154 ESP (SPI=0x000003e9)
  12 4.007046   192.168.2.1        192.168.5.1        ESP       154 ESP (SPI=0x000003e8)
  13 5.007505   192.168.5.1        192.168.2.1        ESP       154 ESP (SPI=0x000003e9)
  14 5.008651   192.168.2.1        192.168.5.1        ESP       154 ESP (SPI=0x000003e8)
  15 10.045911  192.168.2.1        192.168.5.1        ESP       154 ESP (SPI=0x000003e8)
  16 10.047041  192.168.5.1        192.168.2.1        ESP       154 ESP (SPI=0x000003e9)
  17 11.047247  192.168.2.1        192.168.5.1        ESP       154 ESP (SPI=0x000003e8)
  18 11.048363  192.168.5.1        192.168.2.1        ESP       154 ESP (SPI=0x000003e9)
  19 11.516904  a0:23:9f:08:76:90  a0:23:9f:08:76:90  LOOP       60 Reply
  20 12.048673  192.168.2.1        192.168.5.1        ESP       154 ESP (SPI=0x000003e8)
  21 12.049771  192.168.5.1        192.168.2.1        ESP       154 ESP (SPI=0x000003e9)
  22 13.050035  192.168.2.1        192.168.5.1        ESP       154 ESP (SPI=0x000003e8)
  23 13.051146  192.168.5.1        192.168.2.1        ESP       154 ESP (SPI=0x000003e9)
  24 13.987780  a0:23:9f:08:7c:94  a0:23:9f:08:7c:94  LOOP       60 Reply
  25 14.051363  192.168.2.1        192.168.5.1        ESP       154 ESP (SPI=0x000003e8)
  26 14.052481  192.168.5.1        192.168.2.1        ESP       154 ESP (SPI=0x000003e9)
  27 15.052837  192.168.2.1        192.168.5.1        ESP       154 ESP (SPI=0x000003e8)
  28 15.053942  192.168.5.1        192.168.2.1        ESP       154 ESP (SPI=0x000003e9)
```

```
⊞ Frame 1: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits)
⊞ Ethernet II, Src: a0:23:9f:08:7c:94 (a0:23:9f:08:7c:94), Dst: a0:23:9f:08:76:90 (a0:23:9f:08:76:90)
⊞ Internet Protocol Version 4, Src: 192.168.5.1 (192.168.5.1), Dst: 192.168.2.1 (192.168.2.1)
⊞ Encapsulating Security Payload
```

```
0000  a0 23 9f 08 76 90 a0 23  9f 08 7c 94 08 00 45 00   .#..v..# ..|...E.
0010  00 8c 03 bc 40 00 ff 32  ef 30 c0 a8 05 01 c0 a8   ....@..2 .0......
0020  02 01 00 00 03 e9 00 00  00 23 74 81 f2 49 c4 25   ........ .#t..I.%
0030  8b 52 9a 92 25 4c d7 9b  a9 d0 b5 7d cf 19 52 f5   .R..%L.. ...}..R.
0040  a0 5f 31 62 72 cd 2b 53  d9 57 2d 2e 04 e8 8c 7a   ._1br.+S .W-....z
0050  08 97 90 63 f0 ad 68 fc  93 ac ca 40 d7 cb 5f 50   ...c..h. ...@.._P
0060  04 26 a6 ad ba 57 6d a2  74 9b 6f e6 89 d3 59 50   .&...Wm. t.o...YP
0070  27 58 ee f8 21 f6 d0 7d  e1 a2 44 1a 0c 5c ea 6b   'X..!..} ..D..\.k
0080  a9 cd 67 b5 06 01 75 da  25 af 8b 05 c3 dd ea 11   ..g...u. %.......
0090  3d b4 32 81 fc c7 1c 89  c2 3f                     =.2..... .?
```

File: "C:\MyData\SBU\Special projects\CCSD... Packets: 28 · Displayed: 28 (100.0%) · Load time: 0:00.000

Figure 11.—Wire Shark screen capture for Test Case 4, Confidentiality Manual Key.

Wire Shark screen capture for Confidentiality Manual Key can be seen in Figure 11.

<BREAK>

The process for AAK StrongSwan will be:

```
sudo ipsec start

sudo ipsec up ccsds-AAK

ping neighboring machine

sudo ipsec down ccsds-AAK

sudo ipsec stop
```

Table 6 shows some details from Test Case 1, Authenticated Automatic Keying.

TABLE 6.—TEST CASE 1, AUTHENTICATED AUTOMATIC KEYING

1.	Test Date: 10/16/17	
2.	Program under test:	Network Layer Security Adaptation Profile
3.	Test Case:	1, Authenticated Automatic Keying
4.	Agencies Participating in this Test Case:	NASA GRC and NASA IV&V Facility
5.	IV&V Point of Contact:	Brandon Bailey
6.	IV&V Test Engineer:	Adam Alley ENGILITY Corp.
7.	GRC Point of Contact:	Charles Sheehe
8.	GRC Test Engineer:	John Wang
9.	Results (Pass, Partial Pass, Fail):	**Pass**
10.	Variances from Expected Result:	None
11.	Comments:	

The following are the log validating the test conducted:

IV&V: Configured StrongSwan

GRC: Configured StrongSwan

IV&V: Pinged distant end point

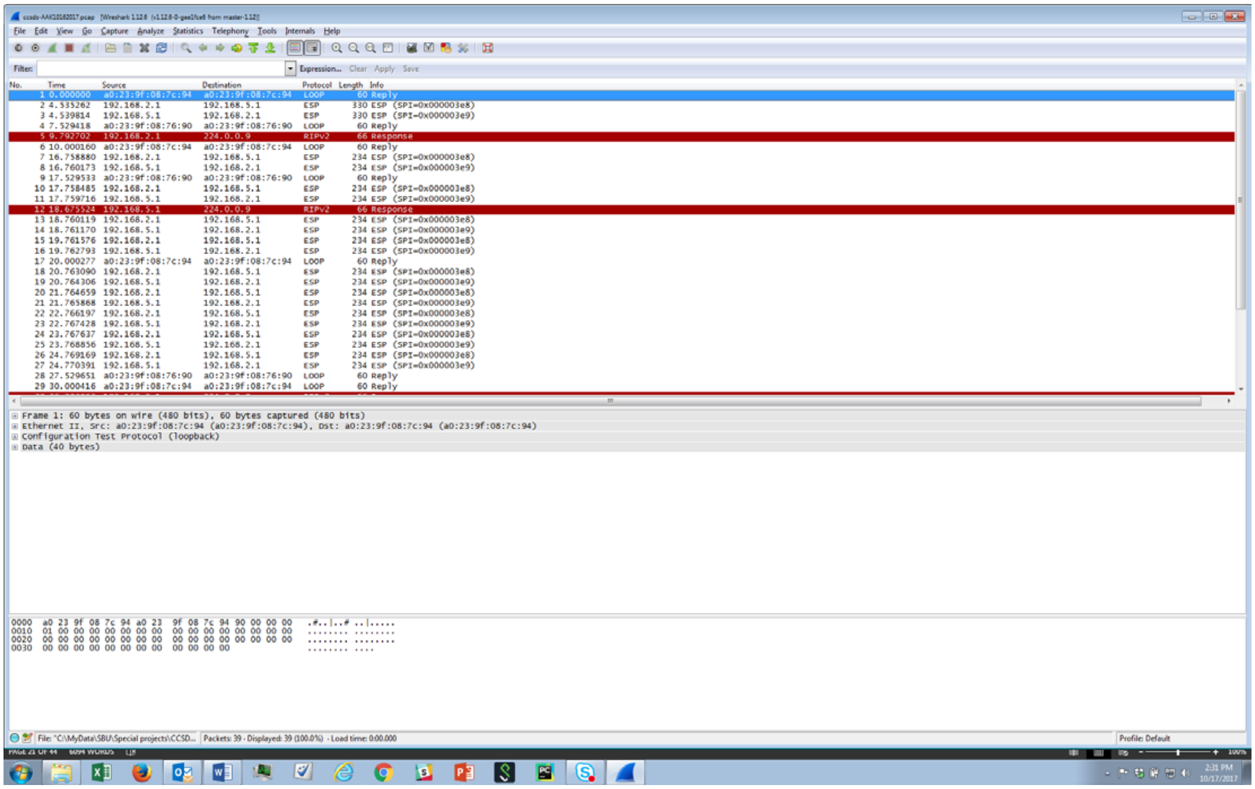
GRC: Pinged distant end point

Bytes and Packets counters before traffic:

Bytes and Packets counters after ping from IV&V:

Bytes and Packets counters after ping from GRC:

Wire Shark capture of traffic/pings: File below ccsds-AAK10162017.pcap


ccsds-AAK10162017.pcap [Wireshark 1.12.8 (v1.12.8-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
Profile: Default

```
No.  Time      Source             Destination        Protocol Length Info
   1 0.000000  a0:23:9f:08:7c:94  a0:23:9f:08:7c:94  LOOP       60 Reply
   2 4.535262  192.168.2.1        192.168.5.1        ESP       330 ESP (SPI=0x000003e8)
   3 4.539814  192.168.5.1        192.168.2.1        ESP       330 ESP (SPI=0x000003e9)
   4 7.529418  a0:23:9f:08:76:90  a0:23:9f:08:76:90  LOOP       60 Reply
   5 9.792702  192.168.2.1        224.0.0.9          RIPv2      66 Response
   6 10.000160 a0:23:9f:08:7c:94  a0:23:9f:08:7c:94  LOOP       60 Reply
   7 16.758880 192.168.2.1        192.168.5.1        ESP       234 ESP (SPI=0x000003e8)
   8 16.760173 192.168.5.1        192.168.2.1        ESP       234 ESP (SPI=0x000003e9)
   9 17.529533 a0:23:9f:08:76:90  a0:23:9f:08:76:90  LOOP       60 Reply
  10 17.758485 192.168.2.1        192.168.5.1        ESP       234 ESP (SPI=0x000003e8)
  11 17.759716 192.168.5.1        192.168.2.1        ESP       234 ESP (SPI=0x000003e9)
  12 18.675524 192.168.5.1        224.0.0.9          RIPv2      66 Response
  13 18.760119 192.168.2.1        192.168.5.1        ESP       234 ESP (SPI=0x000003e8)
  14 18.761170 192.168.5.1        192.168.2.1        ESP       234 ESP (SPI=0x000003e9)
  15 19.761576 192.168.2.1        192.168.5.1        ESP       234 ESP (SPI=0x000003e8)
  16 19.762793 192.168.5.1        192.168.2.1        ESP       234 ESP (SPI=0x000003e9)
  17 20.000277 a0:23:9f:08:7c:94  a0:23:9f:08:7c:94  LOOP       60 Reply
  18 20.763090 192.168.2.1        192.168.5.1        ESP       234 ESP (SPI=0x000003e8)
  19 20.764306 192.168.5.1        192.168.2.1        ESP       234 ESP (SPI=0x000003e9)
  20 21.764659 192.168.2.1        192.168.5.1        ESP       234 ESP (SPI=0x000003e8)
  21 21.765868 192.168.5.1        192.168.2.1        ESP       234 ESP (SPI=0x000003e9)
  22 22.766197 192.168.2.1        192.168.5.1        ESP       234 ESP (SPI=0x000003e8)
  23 22.767428 192.168.5.1        192.168.2.1        ESP       234 ESP (SPI=0x000003e9)
  24 23.767637 192.168.2.1        192.168.5.1        ESP       234 ESP (SPI=0x000003e8)
  25 23.768856 192.168.5.1        192.168.2.1        ESP       234 ESP (SPI=0x000003e9)
  26 24.769169 192.168.2.1        192.168.5.1        ESP       234 ESP (SPI=0x000003e8)
  27 24.770391 192.168.5.1        192.168.2.1        ESP       234 ESP (SPI=0x000003e9)
  28 27.529651 a0:23:9f:08:76:90  a0:23:9f:08:76:90  LOOP       60 Reply
  29 30.000416 a0:23:9f:08:7c:94  a0:23:9f:08:7c:94  LOOP       60 Reply
```

```
⊞ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
⊞ Ethernet II, Src: a0:23:9f:08:7c:94 (a0:23:9f:08:7c:94), Dst: a0:23:9f:08:7c:94 (a0:23:9f:08:7c:94)
⊞ Configuration Test Protocol (loopback)
⊞ Data (40 bytes)
```

```
0000  a0 23 9f 08 7c 94 a0 23  9f 08 7c 94 90 00 00 00   .#..|..# ..|.....
0010  01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

File: "C:\MyData\SBU\Special projects\CCSD... Packets: 39 · Displayed: 39 (100.0%) · Load time: 0:00.000

Figure 12.—Wire Shark screen capture for Test Case 1, Authenticated Automatic Keying.

Figure 12 is a Wire Shark screen capture for Authenticated Automatic Keying.

<BREAK>

The process for CAK StrongSwan will be:

sudo ipsec start

sudo ipsec up ccsds-CAK

ping neighboring machine

sudo ipsec down ccsds-CAK

sudo ipsec stop

Table 7 illustrates Test Case 2, Confidentiality Automatic Keying.

TABLE 7.—TEST CASE 2, CONFIDENTIALITY AUTOMATIC KEYING

1.	Test Date:10/16/17	
2.	Program under test:	Network Layer Security Adaptation Profile
3.	Test Case:	2, Confidentiality Automatic Keying
4.	Agencies Participating in this Test Case:	NASA GRC and NASA IV&V Facility
5.	IV&V Point of Contact:	Brandon Bailey
6.	IV&V Test Engineer:	Adam Alley ENGILITY Corp
7.	NASA Point of Contact:	Charles Sheehe
8.	NASA Test Engineer:	John Wang
9.	Results (Pass, Partial Pass, Fail):	**Pass**
10.	Variances from Expected Result:	None
11.	Comments:	

The following are the log validating the test conducted:

IV&V: Configured StrongSwan

GRC: Configured StrongSwan

IV&V: Pinged distant end point

GRC: Pinged distant end point

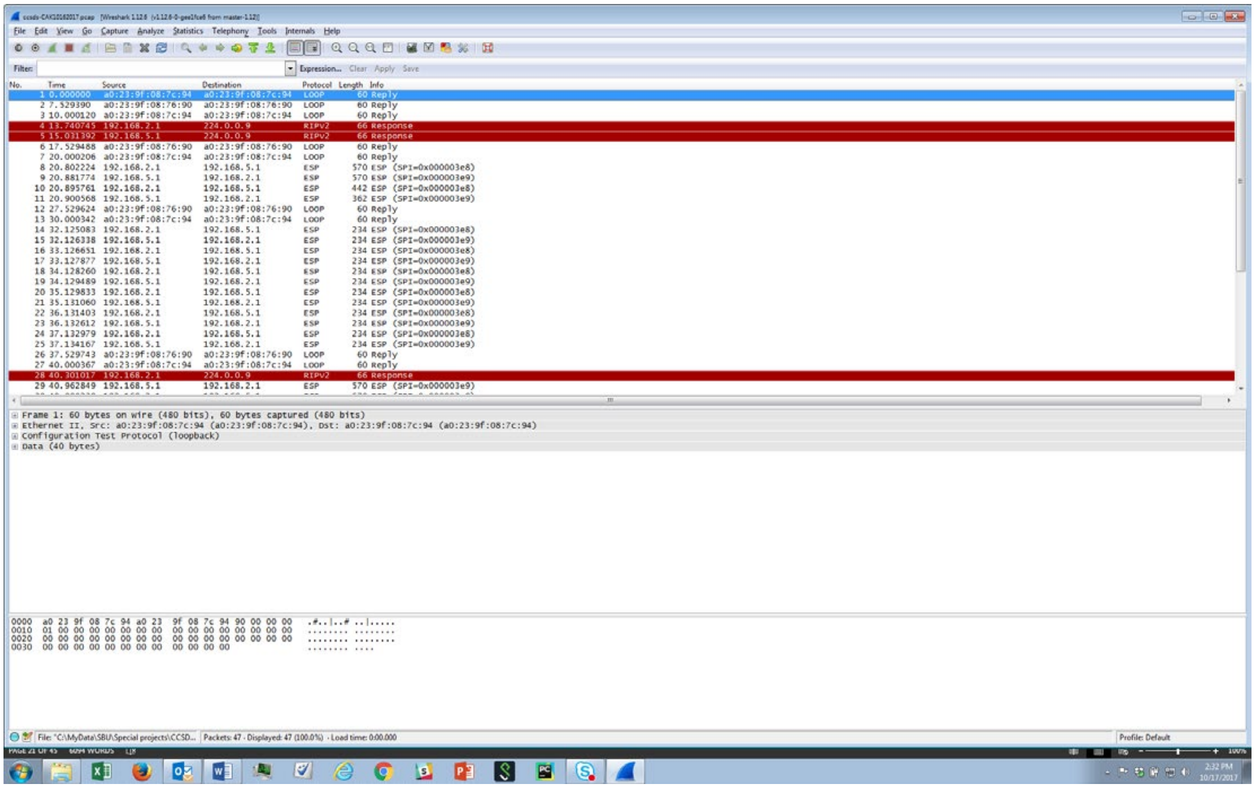
Bytes and Packets counters before traffic:

Bytes and Packets counters after ping from IV&V:

Bytes and Packets counters after ping from GRC:

Wire Shark capture of traffic/pings: File below

ccsds-CAK10162017.pcap


ccsds-CAK10162017.pcap [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
Profile: Default

```
No.  Time       Source             Destination        Protocol Length Info
   1 0.000000   a0:23:9f:08:7c:94  a0:23:9f:08:7c:94  LOOP       60 Reply
   2 7.529390   a0:23:9f:08:76:90  a0:23:9f:08:76:90  LOOP       60 Reply
   3 10.000120  a0:23:9f:08:7c:94  a0:23:9f:08:7c:94  LOOP       60 Reply
   4 13.740745  192.168.2.1        224.0.0.9          RIPv2      66 Response
   5 15.031392  192.168.5.1        224.0.0.9          RIPv2      66 Response
   6 17.529488  a0:23:9f:08:76:90  a0:23:9f:08:76:90  LOOP       60 Reply
   7 20.000206  a0:23:9f:08:7c:94  a0:23:9f:08:7c:94  LOOP       60 Reply
   8 20.802224  192.168.2.1        192.168.5.1        ESP       570 ESP (SPI=0x000003e8)
   9 20.881774  192.168.5.1        192.168.2.1        ESP       570 ESP (SPI=0x000003e9)
  10 20.895761  192.168.2.1        192.168.5.1        ESP       442 ESP (SPI=0x000003e8)
  11 20.900568  192.168.5.1        192.168.2.1        ESP       362 ESP (SPI=0x000003e9)
  12 27.529624  a0:23:9f:08:76:90  a0:23:9f:08:76:90  LOOP       60 Reply
  13 30.000342  a0:23:9f:08:7c:94  a0:23:9f:08:7c:94  LOOP       60 Reply
  14 32.125083  192.168.2.1        192.168.5.1        ESP       234 ESP (SPI=0x000003e8)
  15 32.126338  192.168.5.1        192.168.2.1        ESP       234 ESP (SPI=0x000003e9)
  16 33.126651  192.168.2.1        192.168.5.1        ESP       234 ESP (SPI=0x000003e8)
  17 33.127877  192.168.5.1        192.168.2.1        ESP       234 ESP (SPI=0x000003e9)
  18 34.128260  192.168.2.1        192.168.5.1        ESP       234 ESP (SPI=0x000003e8)
  19 34.129489  192.168.5.1        192.168.2.1        ESP       234 ESP (SPI=0x000003e9)
  20 35.129833  192.168.2.1        192.168.5.1        ESP       234 ESP (SPI=0x000003e8)
  21 35.131060  192.168.5.1        192.168.2.1        ESP       234 ESP (SPI=0x000003e9)
  22 36.131403  192.168.2.1        192.168.5.1        ESP       234 ESP (SPI=0x000003e8)
  23 36.132612  192.168.5.1        192.168.2.1        ESP       234 ESP (SPI=0x000003e9)
  24 37.132979  192.168.2.1        192.168.5.1        ESP       234 ESP (SPI=0x000003e8)
  25 37.134167  192.168.5.1        192.168.2.1        ESP       234 ESP (SPI=0x000003e9)
  26 37.529743  a0:23:9f:08:76:90  a0:23:9f:08:76:90  LOOP       60 Reply
  27 40.000367  a0:23:9f:08:7c:94  a0:23:9f:08:7c:94  LOOP       60 Reply
  28 40.301017  192.168.2.1        224.0.0.9          RIPv2      66 Response
  29 40.962849  192.168.5.1        192.168.2.1        ESP       570 ESP (SPI=0x000003e9)
```

```
⊞ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
⊞ Ethernet II, Src: a0:23:9f:08:7c:94 (a0:23:9f:08:7c:94), Dst: a0:23:9f:08:7c:94 (a0:23:9f:08:7c:94)
⊞ Configuration Test Protocol (loopback)
⊞ Data (40 bytes)
```

```
0000  a0 23 9f 08 7c 94 a0 23  9f 08 7c 94 90 00 00 00   .#..|..# ..|.....
0010  01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

File: "C:\MyData\SBU\Special projects\CCSD... Packets: 47 · Displayed: 47 (100.0%) · Load time: 0:00.000

Figure 13.—Wire Shark screen capture for Test Case 2, Confidentiality Automatic Keying.

Figure 13 shows a Wire Shark screen capture for Confidentiality Automatic Keying.

7.0 Observations

Due to limited budgets for compatibility testing and increased emphasis on institutional network security, it became increasingly difficult to implement legacy configurations that required manual keying or automatic keying with controllable rekeying. Static keys are considered risky and major terrestrial vendors and institutions no longer support this configuration. Automatic keying life time have been reduced and the no-rekeying function has been removed from many vendors' products. Terrestrial network/firewall vendors are responding to networking needs of the internet world and flexibility is reduced in favor of security.

If manual keying, controlled automatic rekeying configurations are needed for space flight, then an effort needs to be undertaken to support these space flight operational modes with vendors to keep these functions within their actively supported equipment and software.

Annex A

Configuration files and Photographs

Hardware and software configuration captures. Photos of the test setup.

Router #1 Configuration File:

```
rtr1#sho run
Building configuration...

Current configuration : 9454 bytes
!
! Last configuration change at 15:14:27 GMT Mon Oct 16 2017 by rtr1
!
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname rtr1
!
boot-start-marker
boot system flash:/c800-universalk9-mz.SPA.155-3.M4a.bin
boot-end-marker
!
!
logging buffered 51200 warnings
enable secret 5 $1$1hWo$QJ7U6E2xJFFZlyUXazD.1.
enable password 7 051B071C325B411B1D52
!
aaa new-model
!
!
aaa authentication login local_access local
!
!
!
!
!
aaa session-id common
ethernet lmi ce
clock timezone GMT -4 0
!
crypto pki trustpoint TP-self-signed-146701208
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-146701208
 revocation-check none
 rsakeypair TP-self-signed-146701208
```

```
!
!
crypto pki certificate chain TP-self-signed-146701208
 certificate self-signed 01
  30820229 30820192 A0030201 02020101 300D0609 2A864886 F70D0101
05050030
  30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D
43657274
  69666963 6174652D 31343637 30313230 38301E17 0D313730 36323132
31303433
  335A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403
1325494F
  532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3134
36373031
  32303830 819F300D 06092A86 4886F70D 01010105 0003818D 00308189
02818100
  EB4B0194 689603BC E94550FA 32E297CA 055FEEBD 8752ECA3 47F2F741
40CCE57B
  5DA272E0 2BF9DA47 78BF3663 40221135 2768F2B3 6CE3B1AA ECCFD52C
EC8A051F
  5A940C45 8802CB39 CDFFB050 BF6336DE B2C14CDF 8A4E34B2 6FFD7468
E6E3E2CA
  4242BC1B B8E6A2B7 AEA1D48A 00818615 6848AC53 D488CC0C C6B72A69
B770F321
  02030100 01A35330 51300F06 03551D13 0101FF04 05300301 01FF301F
0603551D
  23041830 168014E8 7D62DDE3 42144329 09CD28B0 B02E4683 623EAA30
1D060355
  1D0E0416 0414E87D 62DDE342 14432909 CD28B0B0 2E468362 3EAA300D
06092A86
  4886F70D 01010505 00038181 00B6234B A59DEB28 9E748122 A23EBDC1
E199E417
  E0490026 C8D65B73 FF0D6D6B 25FED6F7 92604993 FB430BD0 B6D97BA4
3A679A8E
  084E1B4D AB06BE9B EA1BBF45 511D5594 436AF932 28103443 E5EEAF59
393781ED
  3E21A258 6DC64318 CED63065 7505299C 9081FA9D 9E7964A4 7C159D57
86961612
  8F2BADBF EEB8D105 19D34A98 87
        quit
!
!
!
!
!
!
!
!
!
!
!
!
```

```
ip nbar http-services
!
!
!
!
!


!
ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.2.1
!
ip dhcp pool ccp-pool
 import all
 network 192.168.2.0 255.255.255.128
 default-router 192.168.2.1
 lease 0 2
!
!
!
ip domain name nasa_grc
ip cef
no ipv6 cef
!
!
flow record nbar-appmon
 match ipv4 source address
 match ipv4 destination address
 match application name
 collect interface output
 collect counter bytes
 collect counter packets
 collect timestamp absolute first
 collect timestamp absolute last
!
!
flow monitor application-mon
 cache timeout active 60
 record nbar-appmon
!
parameter-map type inspect global
 max-incomplete low 18000
 max-incomplete high 20000
 nbar-classify
!
!
!
!
multilink bundle-name authenticated
!
!
!
```

```
!
!
!
!
license udi pid C892FSP-K9 sn FJC2124L0Z1
!
!
object-group network Others_dst_net
 any
!
object-group network Others_src_net
 any
!
object-group service Others_svc
 ip
!
object-group network Web_dst_net
 any
!
object-group network Web_src_net
 any
!
object-group service Web_svc
 ip
!
object-group network local_cws_net
!
object-group network local_lan_subnets
 any
 192.168.1.0 255.255.255.128
 192.168.2.0 255.255.255.128
!
object-group network vpn_remote_subnets
 any
!
username rtr1 privilege 15 secret 5 $1$cCSv$Ij/xZqjTNwHtvcCYuVfo/0
!
!
!
no crypto engine software ipsec
!
no cdp run
!
!
class-map type inspect match-any INTERNAL_DOMAIN_FILTER
 match protocol msnmsgr
 match protocol ymsgr
class-map type inspect match-any Others_app
 match protocol https
 match protocol smtp
 match protocol pop3
 match protocol imap
 match protocol sip
 match protocol ftp
 match protocol dns
 match protocol icmp
class-map type inspect match-any Web_app
 match protocol http
class-map type inspect match-all Others
 match class-map Others_app
 match access-group name Others_acl
class-map type inspect match-all Web
 match class-map Web_app
 match access-group name Web_acl
!
policy-map type inspect LAN-WAN-POLICY
 class type inspect Web
  inspect
 class type inspect Others
  inspect
 class class-default
  drop log
!
zone security LAN
zone security WAN
zone security VPN
zone security DMZ
zone-pair security LAN-WAN source LAN destination WAN
 service-policy type inspect LAN-WAN-POLICY
!
!
crypto isakmp policy 1
 encr aes
 hash sha256
 authentication pre-share
 group 16
 lifetime 60
crypto isakmp key 000102030405060708090a0b0c0d0e0f address 192.168.5.1
no-xh
crypto isakmp keepalive 12
!
crypto ipsec security-association lifetime kilobytes 2560
crypto ipsec security-association lifetime seconds 120
!
crypto ipsec transform-set ccsdsset esp-aes esp-sha256-hmac
 mode tunnel
crypto ipsec transform-set ccsdsset-no-esp esp-null esp-sha256-hmac
 mode tunnel
crypto ipsec transform-set ccsdsset-no-auth esp-aes
 mode tunnel
!
crypto ipsec profile ccsds_ipsec
 set security-association lifetime kilobytes disable
 set security-association lifetime days 30
```

```
!
crypto ipsec profile default
 set security-association lifetime kilobytes disable
 set security-association lifetime days 30
!
crypto ipsec profile protect-gre
 set security-association lifetime kilobytes disable
 set security-association lifetime seconds 120
 set transform-set ccsdsset
!
crypto map AMK 1 ipsec-manual
 set peer 192.168.5.1
 set session-key inbound esp 1001 cipher
000102030405060708090a0b0c0d0e0f authe
 set session-key outbound esp 1000 cipher
000102030405060708090a0b0c0d0e0f auth
 set transform-set ccsdsset
 match address 101
crypto map CMK 1 ipsec-manual
 set peer 192.168.5.1
 set session-key inbound esp 1001 cipher
000102030405060708090a0b0c0d0e0f authe
 set session-key outbound esp 1000 cipher
000102030405060708090a0b0c0d0e0f auth
 set transform-set ccsdsset-no-auth
 match address 101
!

!
!
!
!
!
interface GigabitEthernet0
 no ip address
!
interface GigabitEthernet1
 no ip address
 shutdown
!
interface GigabitEthernet2
 no ip address
 shutdown
!
interface GigabitEthernet3
 no ip address
 shutdown
!
interface GigabitEthernet4
 no ip address
 shutdown
!
```

```
interface GigabitEthernet5
 no ip address
 shutdown
!
interface GigabitEthernet6
 no ip address
 shutdown
!
interface GigabitEthernet7
 no ip address
 shutdown
!
interface GigabitEthernet8
 description PrimaryWANDesc_
 ip address 192.168.2.1 255.255.255.0
 ip nbar protocol-discovery
 ip tcp adjust-mss 1412
 duplex auto
 speed auto
 pppoe enable group global
 pppoe-client dial-pool-number 4
 crypto map AMK
!
interface GigabitEthernet9
 no ip address
 ip nat inside
 ip virtual-reassembly in
 ip tcp adjust-mss 1412
 shutdown
 duplex auto
 speed auto
!
interface Vlan1
 description $ETH_LAN$
 ip address 192.168.1.1 255.255.255.0
 ip nbar protocol-discovery
 ip tcp adjust-mss 1412
!
interface Dialer4
 no ip address
!
router rip
 version 2
 network 192.168.1.0
 network 192.168.2.0
 network 192.168.4.0
 network 192.168.5.0
 network 192.168.8.0
 network 192.168.9.0
 neighbor 192.168.9.1
 neighbor 192.168.5.1
 no auto-summary
```

```
!
ip forward-protocol nd
ip http server
ip http upload enable path flash:
ip http upload overwrite
ip http authentication local
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
!
ip dns server
ip nat inside source list nat-list interface Dialer4 overload
ip route 0.0.0.0 0.0.0.0 GigabitEthernet8
!
ip access-list extended GRE-tunnel
 permit gre host 192.168.2.1 host 192.168.5.1
ip access-list extended Others_acl
 permit object-group Others_svc object-group Others_src_net object-
group Otherst
ip access-list extended Web_acl
 permit object-group Web_svc object-group Web_src_net object-group
Web_dst_net
ip access-list extended nat-list
 permit ip object-group local_lan_subnets any
!
!
access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.4.0 0.0.0.255
access-list 102 permit ip any any
access-list 103 permit ip 192.168.2.0 0.0.0.255 192.168.5.0 0.0.0.255
access-list 104 permit ip host 192.168.2.1 host 192.168.5.1
!
!
!
control-plane
!
!
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
!
!
!
!
!
!
line con 0
 login authentication local_access
 no modem enable
line aux 0
line vty 0 4
 access-class 23 in
 privilege level 15
 password 7 00141215174C04140B76
 login authentication local_access
 transport input telnet ssh
line vty 5 15
 access-class 23 in
 privilege level 15
 password 7 140713181F132539207F
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
end
```

Router #3 Configuration File:

```
RTR3#sh conf
Using 10123 out of 262136 bytes
!
! Last configuration change at 19:02:12 GMT Tue Sep 5 2017 by rtr3
!
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname RTR3
!
boot-start-marker
boot system flash:/c800-universalk9-mz.SPA.155-3.M4a.bin
boot-end-marker
!
!
logging buffered 51200 warnings
enable secret 5 $1$ZDRe$ro0z8ubVcfRxsGwfSyuhk/
enable password 7 13151601181B0B382F73
!
aaa new-model
!
!
aaa authentication login local_access local
!
!
```

```
!
!
!
aaa session-id common
ethernet lmi ce
clock timezone GMT -4 0
!
crypto pki trustpoint TP-self-signed-3604603593
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3604603593
 revocation-check none
 rsakeypair TP-self-signed-3604603593
!
!
crypto pki certificate chain TP-self-signed-3604603593
 certificate self-signed 01 nvram:IOS-Self-Sig#1.cer
!
!
!
!
!
!
!
!
!
!
!
!
ip nbar http-services
!
!
!
!
!



!
ip dhcp excluded-address 192.168.4.1
ip dhcp excluded-address 192.168.5.1
!
ip dhcp pool ccp-pool
 import all
 network 192.168.4.0 255.255.255.128
 default-router 192.168.4.1
 dns-server 192.168.4.1
 lease 0 2
!
!
!
ip domain name nasa_ivv
ip cef
no ipv6 cef
```

```
!
!
flow record nbar-appmon
 match ipv4 source address
 match ipv4 destination address
 match application name
 collect interface output
 collect counter bytes
 collect counter packets
 collect timestamp absolute first
 collect timestamp absolute last
!
!
flow monitor application-mon
 cache timeout active 60
 record nbar-appmon
!
parameter-map type inspect global
 max-incomplete low 18000
 max-incomplete high 20000
 nbar-classify
!
!
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
license udi pid C892FSP-K9 sn FJC2125L1PP
!
!
object-group network Others_dst_net
 any
!
object-group network Others_src_net
 any
!
object-group service Others_svc
 ip
!
object-group network Web_dst_net
 any
!
object-group network Web_src_net
 any
!
object-group service Web_svc
```

```
 ip
!
object-group network local_cws_net
!
object-group network local_lan_subnets
 any
 192.168.4.0 255.255.255.128
 192.168.5.0 255.255.255.128
!
object-group network vpn_remote_subnets
 any
!
username rtr3 privilege 15 secret 5 $1$H0WQ$ZsyyAzgcILofJbwz7F4k40
!
!
!
no crypto engine software ipsec
!
no cdp run
!
!
class-map type inspect match-any INTERNAL_DOMAIN_FILTER
 match protocol msnmsgr
 match protocol ymsgr
class-map type inspect match-any Others_app
 match protocol https
 match protocol smtp
 match protocol pop3
 match protocol imap
 match protocol sip
 match protocol ftp
 match protocol dns
 match protocol icmp
class-map type inspect match-any Web_app
 match protocol http
class-map type inspect match-all Others
 match class-map Others_app
 match access-group name Others_acl
class-map type inspect match-all Web
 match class-map Web_app
 match access-group name Web_acl
!
policy-map type inspect LAN-WAN-POLICY
 class type inspect Web
  inspect
 class type inspect Others
  inspect
 class class-default
  drop log
!
zone security LAN
zone security WAN
zone security VPN
zone security DMZ
zone-pair security LAN-WAN source LAN destination WAN
 service-policy type inspect LAN-WAN-POLICY
!
!
crypto isakmp policy 1
 encr aes
 hash sha256
 authentication pre-share
 group 16
 lifetime 60
crypto isakmp key 000102030405060708090a0b0c0d0e0f address 192.168.2.1
no-xauth
crypto isakmp keepalive 12
!
crypto ipsec security-association lifetime kilobytes 2560
crypto ipsec security-association lifetime seconds 120
!
crypto ipsec transform-set ccsdsset esp-aes esp-sha256-hmac
 mode tunnel
crypto ipsec transform-set ccsdsset-no-esp esp-null esp-sha256-hmac
 mode tunnel
crypto ipsec transform-set ccsdsset-no-auth esp-aes
 mode tunnel
!
crypto ipsec profile ccsds_ipsec
 set security-association lifetime kilobytes disable
 set security-association lifetime days 30
!
crypto ipsec profile default
 set security-association lifetime kilobytes disable
 set security-association lifetime days 30
!
crypto ipsec profile protect-gre
 set security-association lifetime kilobytes disable
 set security-association lifetime seconds 120
 set transform-set ccsdsset
!
crypto map AMK 1 ipsec-manual
 set peer 192.168.2.1
 set session-key inbound esp 1000 cipher
000102030405060708090a0b0c0d0e0f authenticator 20
 set session-key outbound esp 1001 cipher
000102030405060708090a0b0c0d0e0f authenticator 20
 set transform-set ccsdsset
 match address 101
!
crypto map CMK 1 ipsec-manual
 set peer 192.168.2.1
 set session-key inbound esp 1000 cipher
000102030405060708090a0b0c0d0e0f authenticator 20
```

```
 set session-key outbound esp 1001 cipher
000102030405060708090a0b0c0d0e0f authenticator 20
 set transform-set ccsdsset-no-auth
 match address 101
!
!
!
!
!
interface Tunnel0
 ip address 192.168.50.1 255.255.255.0
 shutdown
 tunnel source GigabitEthernet8
 tunnel mode ipsec ipv4
 tunnel destination 192.168.2.1
 tunnel protection ipsec profile protect-gre
!
interface GigabitEthernet0
 description eth0
 no ip address
!
interface GigabitEthernet1
 description eth1
 no ip address
 shutdown
!
interface GigabitEthernet2
 no ip address
 shutdown
!
interface GigabitEthernet3
 no ip address
 shutdown
!
interface GigabitEthernet4
 no ip address
 shutdown
!
interface GigabitEthernet5
 no ip address
 shutdown
!
interface GigabitEthernet6
 no ip address
 shutdown
!
interface GigabitEthernet7
 no ip address
 shutdown
!
interface GigabitEthernet8
 description PrimaryWANDesc_
 ip address 192.168.5.1 255.255.255.0
 ip nbar protocol-discovery
 ip tcp adjust-mss 1412
 duplex auto
 speed auto
 pppoe enable group global
 pppoe-client dial-pool-number 4
!
interface GigabitEthernet9
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Vlan1
 description $ETH_LAN$
 ip address 192.168.4.1 255.255.255.0
 ip nbar protocol-discovery
 ip tcp adjust-mss 1412
!
interface Dialer4
 no ip address
!
router rip
 version 2
 network 192.168.1.0
 network 192.168.2.0
 network 192.168.4.0
 network 192.168.5.0
 network 192.168.8.0
 network 192.168.9.0
 neighbor 192.168.9.1
 neighbor 192.168.2.1
 bfd all-interfaces
 no auto-summary
!
ip forward-protocol nd
ip http server
ip http upload enable path flash:
ip http upload overwrite
ip http access-class 23
ip http authentication local
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
!
ip dns server
ip nat inside source list nat-list interface Dialer4 overload
ip route 0.0.0.0 0.0.0.0 GigabitEthernet8
!
ip access-list extended GRE-tunnel
 permit gre host 192.168.5.1 host 192.168.2.1
```

```
ip access-list extended Others_acl
 permit object-group Others_svc object-group Others_src_net object-
group Others_dst_net
ip access-list extended Web_acl
 permit object-group Web_svc object-group Web_src_net object-group
Web_dst_net
ip access-list extended nat-list
 permit ip object-group local_lan_subnets any
!
!
access-list 101 permit ip 192.168.4.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 102 permit ip any any
access-list 104 permit ip host 192.168.5.1 host 192.168.2.1
!
!
!
control-plane
!
!
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
!
!
!
!
!
banner exec ^CC
% Password expiration warning.
----------------------------------------------------------------------
-

Cisco Configuration Professional (Cisco CP) is installed on this
device
and it provides the default username "cisco" for  one-time use. If you
have
already used the username "cisco" to login to the router and your IOS
image
supports the "one-time" user option, then this username has already
expired.
You will not be able to login to the router with this username after
you exit
this session.

It is strongly suggested that you create a new username with a
privilege level
of 15 using the following command.
```

```
username <myuser> privilege 15 secret 0 <mypassword>

Replace <myuser> and <mypassword> with the username and password you
want to use.

----------------------------------------------------------------------
-
^C
banner login ^CC
----------------------------------------------------------------------
-
Cisco Configuration Professional (Cisco CP) is installed on this
device.
This feature requires the one-time use of the username "cisco" with
the
password "cisco". These default credentials have a privilege level of
15.

YOU MUST USE CISCO CP or the CISCO IOS CLI TO CHANGE THESE
PUBLICLY-KNOWN CREDENTIALS

Here are the Cisco IOS commands.

username <myuser>  privilege 15 secret 0 <mypassword>
no username cisco

Replace <myuser> and <mypassword> with the username and password you
want
to use.

IF YOU DO NOT CHANGE THE PUBLICLY-KNOWN CREDENTIALS, YOU WILL
NOT BE ABLE TO LOG INTO THE DEVICE AGAIN AFTER YOU HAVE LOGGED OFF.

For more information about Cisco CP please follow the instructions in
the
QUICK START GUIDE for your router or go to
http://www.cisco.com/go/ciscocp
----------------------------------------------------------------------
-
^C
!
line con 0
 login authentication local_access
 no modem enable
line aux 0
line vty 0 4
 access-class 23 in
 privilege level 15
 password 7 00141215174C04140B76
 login authentication local_access
 transport input telnet ssh
```

```
line vty 5 15
 access-class 23 in
 privilege level 15
 password 7 06160E325F59060B0140
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
end
```

StrongSwan Configuration File for CCSDS1:

```
config setup
      charondebug="all"
      strictcrlpolicy=no
      uniqueids=yes

# Add connections here

# Sample VPN connections
# For host @ccsds1

conn ccsds-AAK
      authby = secret
      auto = add
      keyexchange = ikev2
      ike = aes256-sha2_256-modp2048
      left = 192.168.4.2
      leftid = @ccsds1
      leftfirewall = no
      right = 192.168.1.2
      rightid = @zbook
      rightfirewall = no
      type = tunnel
      esp = aes256-sha2_256
      reauth = no
      rekey = no

conn ccsds-CAK
      authby = secret
      auto = add
      keyexchange = ikev2
      ike = aes256-sha256-modp2048!
      left = 192.168.4.2
      leftid = @ccsds1
      leftfirewall = no
      right = 192.168.1.2
      rightid = @zbook
      rightfirewall = no
      type = tunnel
```

```
     esp = null-sha256, aes256-sha2_256!
     reauth = no
     rekey = no
```

StrongSwan Configuration File for Zbook:

```
config setup
     charondebug="all"
     strictcrlpolicy=no
     uniqueids = yes

# Add connections here.

# Sample VPN connections
# For host @zbook


conn ccsds-CAK
     authby=secret
     auto=add
     keyexchange=ikev2
     ike=aes256-sha256-modp2048!
     left=192.168.1.2
     leftid=@zbook
     leftfirewall=no
     right=192.168.4.2
     rightid=@ccsds1
     rightfirewall=no
     type=tunnel
     esp=null-sha256, aes256-sha2_256!
     reauth=no
     rekey=no

conn ccsds-AAK
     authby = secret
     auto = add
     keyexchange = ikev2
     ike = aes256-sha2_256-modp2048!
     left = 192.168.1.2
     leftid = @zbook
     leftfirewall = no
     right = 192.168.4.2
     rightid = @ccsds1
     rightfirewall = no
     type = tunnel
     esp = aes256-sha2_256!
     reauth = no
     rekey = no
```

StrongSwan Secrets file:

```
# ipsec.secrets - strongSwan IPsec secrets file

@ccsds1 @zbook : PSK 0x000102030405060708090a0b0c0d0e0f

@ccsds1 %any : PSK 0xf00102030405060708090a0b0c0d0e0f

192.168.4.2 %any : PSK 0x000102030405060708090a0b0c0d0e0f
```

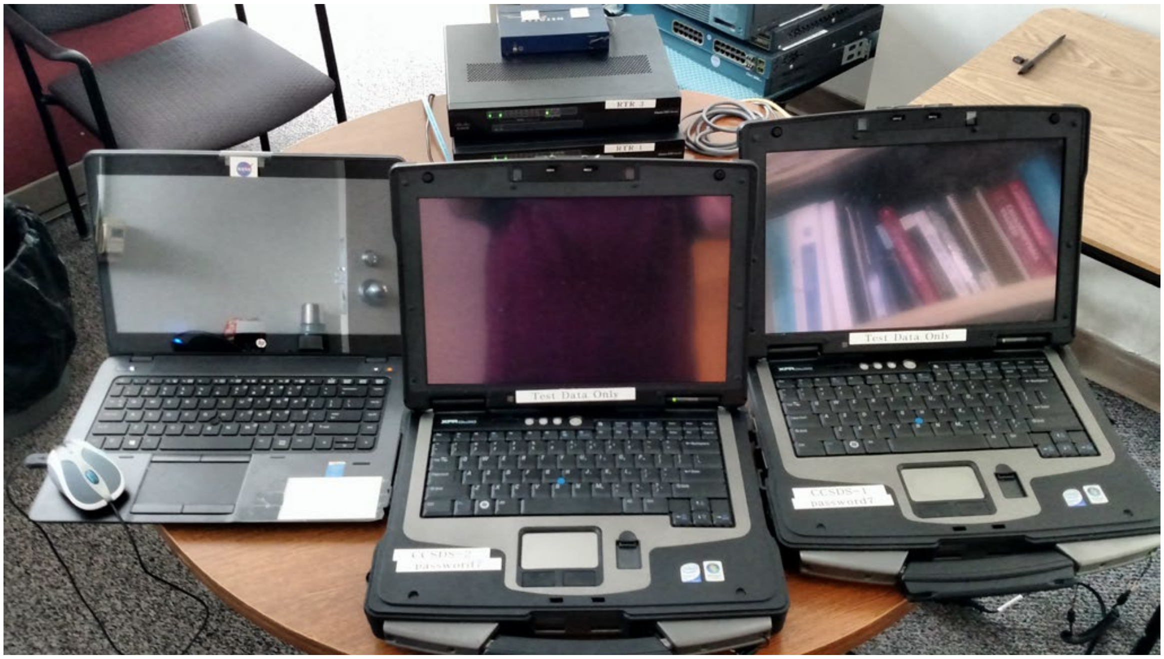


Figure 14.—Photo #1 of the test setup.

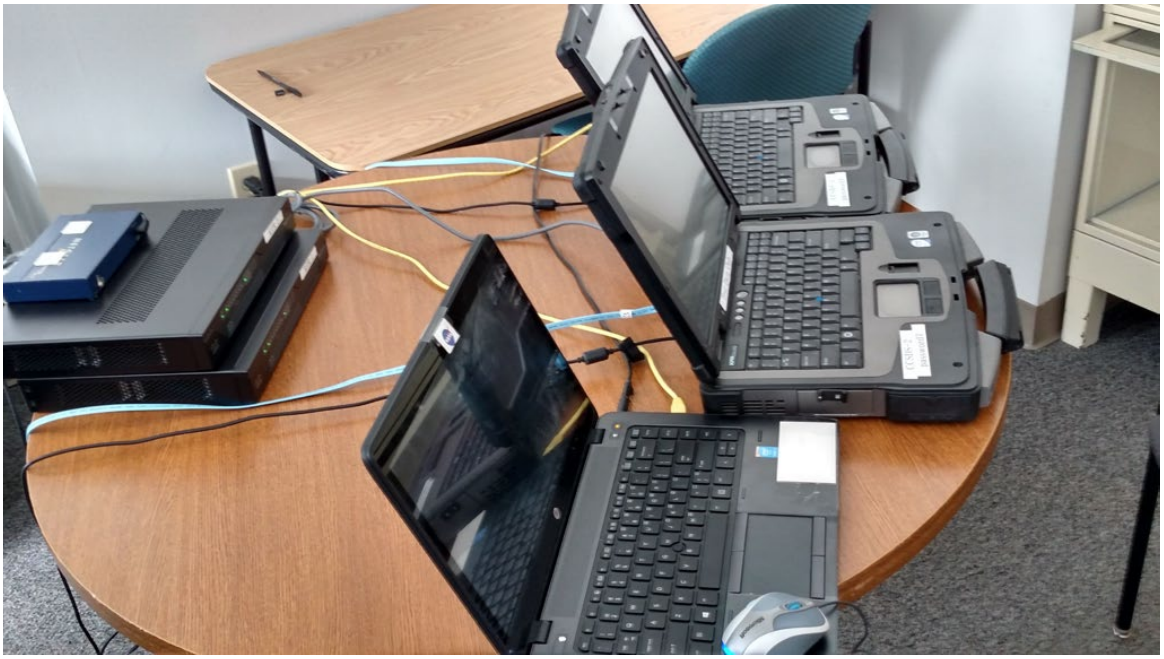


Figure 15.—Photo #2 of the test setup.

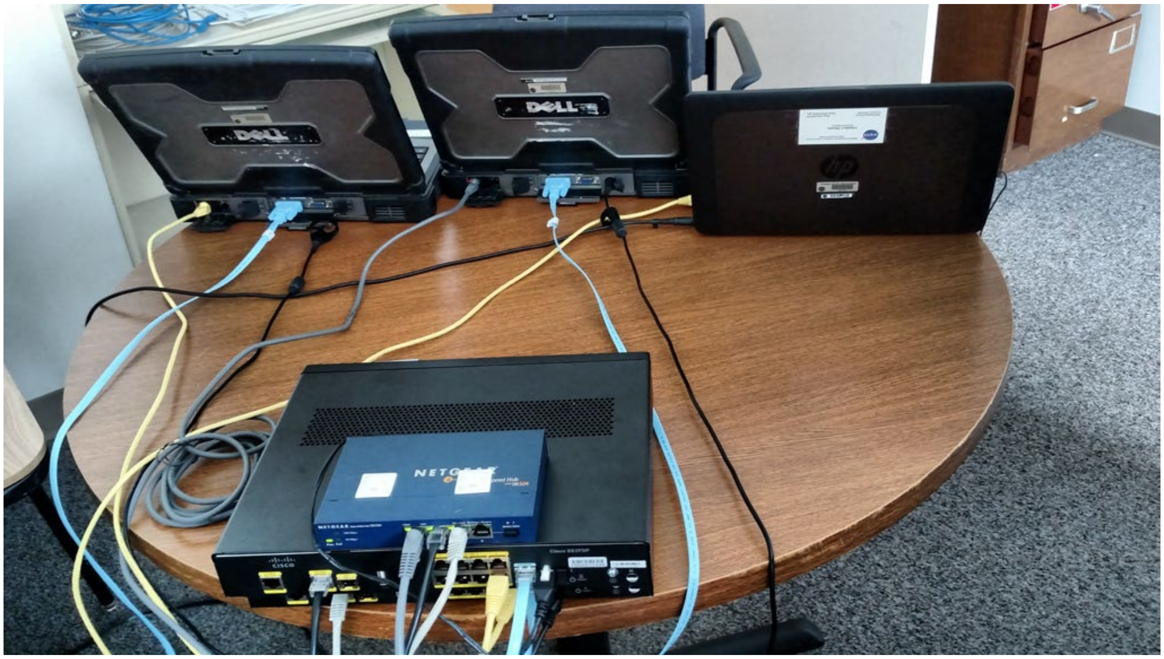


Figure 16.—Photo #3 of the test setup.

Figure 17.—Photo #4 of the testing at IV&V facility.