

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

**"Researching Common IPsec and
x.509 Certificate Errors"**

(Optional Paper Lab: IPsec and IKED Errors)



Table of Contents

Table of Contents.....	- 2 -
Part 0: Lab Description (Researching Common IPSec, IKED, and x.509 Certificate Errors)..	- 3 -
Part 1: What Causes the Following Error Messages related to IPSec or IKED Problems?	- 4 -
Part 2: Policy MisMatch Problem: Diffie-Hellman Group	- 5 -

Revision date -

Tuesday, 24 May 2022

This edition applies to IBM z/OS Configuration Assistant running in z/OSMF on
z/OS V2.4.

Attention:

Information in this document was developed in conjunction with use of the equipment
specified, and is limited in application to those specific hardware and software
products and levels.

Part 0: Lab Description (Researching Common IPSec, IKED, and x.509 Certificate Errors)

Please use the z/OS Communications Server manuals at your disposal to determine the meaning of the following common SSL/TLS Return Codes.

These return codes and error messages have been found in z/OS SYSLOGD, in console messages when the appropriate levels of logging have been enabled.

The manuals you may wish to consult are:

- *z/OS Cryptographic Services System Secure Sockets Layer Programming*
 - *also known as: System SSL Programming Guide*
- *z/OS Communications Server IP Diagnosis Guide*
- *z/OS Communications Server IP Messages: Vol. 1 (EZA)*
- *z/OS Communications Server IP Messages: Vol. 2 (EZB, EZD)*
- *z/OS Communications Server IP Messages: Vol. 3 (EZY)*
- *z/OS Communications Server IP Messages: Vol. 4 (EZZ, SNM)*
- *z/OS Security Server RACF Security Administrator's Guide*
- *z/OS Security Server RACF Command Language Reference*

The manuals are available on your workstation or on the IBM website at:

<http://www.ibm.com/systems/z/os/zos/bkserv/>

Part 1: What Causes the Following Error Messages related to IPSec or IKED Problems?

1. EZD1075I Received ISAKMP error notification message : No proposal Chosen
 - a. _____

2. EZD1040I Phase 1 security association retransmit timeout src IP : 192.168.20.121
dest IP : 192.168.20.95 src port : 500 dest port : 500 protocol : UDP(17)
 - a. _____

3. EZD1078I A security association (Phase 1 - SA ID 0) has been deactivated
 - a. _____

4. EZD1093I Policy mismatch : KeyExchangeOffer (1) requires parameter (DHGroup) with value (Group1) but proposal (1) value is (Group2)
 - a. _____

5. EZD1093I Policy mismatch : KeyExchangeOffer (1) requires parameter (HowToEncrypt) with value (AES) but proposal (1) value is (3DES)
 - a. _____

6. Examine the contents of Table 17 in the IP Diagnosis Manual. It shows you common messages for IKE problems:
 - a. EZD1065I
 - b. EZD0815I
 - c. EZD0965I
 - d. EZD0990I
 - e. EZD1030I
 - f. EZD1037I
 - g. EZD0981I
 - h. EZD1075I
 - i. EZD0902I
 - j. EZD0903I
 - k. EZD0918I
7. EZZ0751I Cannot start IPv4 Security after TCPIP is active.
 - a. _____

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

8. EZZ0754I IPSEC STATEMENT WAS NOT PROCESSED BECAUSE IP SECURITY IS NOT ENABLED
 - a. _____

9. EZZ0802I GLOBALCONFIG ZIIP IPSECURITY IS IGNORED - IP SECURITY IS NOT ENABLED
 - a. _____

10. EZZ0804I ZIIP *function* IS ENABLED - ZIIPS ARE ONLINE
 - a. _____

11. EZZ8438I PAGENT POLICY DEFINITIONS CONTAIN ERRORS FOR *image : type*
 - a. _____

12. EZZ8544I TRMD IPSEC LOGGING COULD NOT ACTIVATE
 - a. _____

Part 2: Policy MisMatch Problem: Diffie-Hellman Group

1. Problem: The Phase 1 Key Exchange setting at MVS6 has defaulted to VPN~A, which is for
 - a. **3DES,**
 - b. **SHA1, and a**
 - c. **Diffie-Hellman Group 2. (Group 2 is the problem.)**
2. Problem: The Phase 1 Key Exchange setting at MVS1 is using:
 - a. **AES,**
 - b. **SHA1, and a**
 - c. **Diffie-Hellman Group 1.**
3. Next look at these messages that will be logged at MVS1 if you leave these Key Exchange Proposals in place and then try to establish an IKE tunnel using these Key Exchange values:
 - a. EZD1093I Policy mismatch : KeyExchangeOffer (1) requires parameter (DHGroup) with value (Group1) but proposal (1) value is (Group2)
 - b. EZD1093I Policy mismatch : KeyExchangeOffer (1) requires parameter (HowToEncrypt) with value (AES) but proposal (1) value is (3DES)
 - c. IKE DEBUGSA : Proposal not accepted with tentative policy (TraffOSA2VIPAPreShMVS5~5) (TraffOSA2VIPAPreShMVS5)

Securing and Encrypting Network Traffic to z/OS Communications Server with Policy Agent

4. Message 1 tells you that ZOS6 proposed using DHGRoup 2 (Diffie Hellman Group 2) but ZOS1 was expecting DHGroup 1. So ZOS1 moved on to the next Key Exchange offer it would accept, and that was for AES. However
5. Message 2 tells you that ZOS6 proposed 3DES to you, but ZOS1 is now looking for AES. Therefore, ZOS1 rejects the Key Exchange Offer, as you see in Message 3.
6. Both ends of the connection must be synchronized to accept the offers made by each other. ***Therefore, you need to change your Key Exchange Offer to be something that ZOS1 will accept:***
 - a. AES
 - b. SHA1
 - c. **Diffie-Hellman Group 1**
7. NOTE: Always verify the Key Exchange Values that the peer for your IKE connection is expecting.

