

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

Lab Answers



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

Lab L01 Lab Environment Answers	3
Part 1	3
Part 3	3
Lab L02 SYSLOGD Answers	4
Part 1	4
Part 2	4
Lab L03 Policy Agent Answers	5
Part 1	5
Part 2	5
Part 3	5
Lab L04 Certificate Cleanup Answers	7
Part 1	7
Part 12	7
Lab L05 Certificate Creation Answers	8
Part 1	8
Part 2	9
Lab L06 AT-TLS Errors Answers	10
Part 1	10
Lab L07 AT-TLS FTP Answers	11
Part 2	11
Part 3	11
Lab L08 AT-TLS TN3270 Answers	13
Part 1	13
Part 3	13
Part 5	13
Lab L09 IP Filters Answers	14
Part 1	14
Lab L10 TRMD Answers	15
Part 1	15
Part 2	15
Lab L11 IP Filter Testing Answers	16
Part 2	16
Lab L12 IPsec VPN Answers	17
Part 1	17
Part 2	17
Lab L13 IPsec Errors Answers	18
Part 1	18
Lab L14 IDS Answers	19
Part 3	19
Lab L15 IPsec VPN Preshare Mode Answers	20
Part 1	20
Part 2	20
Lab L16 NSSD Answers	21
Part 2	21
Lab L17 DMD Answers	22

Warning! Numbers may not match due to lab updates!

Lab L01 Lab Environment Answers

Part 1

1.d.i. Write down here the address of your workstation (DNS Suffix = dmz).

192.168.215.156 (example)

The class subnet is 192.168.0.0 so your workstation address used in this class starts with 192.168. Your address may be different than this one.

Part 3

2.a.i. Are you a superuser? No

Superuser has Unix ID (UID) of 0 (zero) and allows greater authority than other users.

2.a.ii. What is your UNIX identity? 531(USER21) (example) (where 531 is your UID and 21 is your team number.

Your UID is some number other than 0 (zero).

4.a.i. What is your UNIX identity now? 0 (the userid is the last one that executed a unix command in superuser mode.

6.b. Do you see a mount for /var? Yes

7.a.i. Name of directory: /u/usernx

9.b. What is the Process ID (PID) of the Syslog Daemon? 17170439 (example)

PID numbers can be any whole number greater than 0 (zero).

Lab L02 SYSLOGD Answers

Part 1

- 4.a. What is the Job Name of the SYSLOG Daemon? [SYSLOGDC](#)
- 4.b. What address space is it running in? [003D](#) (example)
The address space ID (ASID) is some 4 digit hex number.
- 4.c. Which UNIX owner is associated with the SYSLOG Daemon? [OMVSKERN](#)
The user ID OMVSKERN is associated with the started procedure SYSLOGDC in RACF.
- 4.d. What is the UNIX Process ID of the SYSLOG Daemon? [34013190](#) (example)
Process ID (PID numbers) can be any whole number greater than 0 (zero).
9. How did SYSLOGD obtain the job name that you saw on the MVS console?
[BPX JOBNAME='SYSLOGDC'](#) is specified on the syslog start command.
11. Write down here the UNIX Process ID (PID) of the running SYSLOGD.
[34013190](#) (example)
- 12.a. "-c" parameter: [create log files and directories automatically](#)
The start parameters are documented in the IP Configuration Guide and the IP Configuration Reference.
- 12.b. "-i" parameter: [start in local-only mode. Do not receive messages from network.](#)
- 12.c. "-u" parameter: [include userid and job name in the record](#)
- 12.d. "-f" parameter: [specifies the configuration file name](#)

Part 2

- 6.a. Is the PID number the same or different from what it was before? [Same](#)
7. Why is it important for SYSLOGD to continue to execute when the configuration file is refreshed? [So that important messages are not lost](#)
- 9.b. Do you find the directory named "CSLOG"? [Yes](#)
- 19.b. What types of messages are now in the log? [Not much because of the low log level](#)
- 22.a. Do you find CRON as a running process? [Yes](#)

Lab L03 Policy Agent Answers

Part 1

- 7.b. What RACF userid is associated with the OMVS segment that PAGENTT requires for successful startup? [TCPIP](#)
- 9.a. ...the path and name of the main PAGENT configuration file: [/etc/PAGT1/pagentt.conf](#)
-c is the start parameter that defines the configuration file.
- 9.b. Where is Policy Agent logging its messages? [SYSLOGD](#)
-l is the start parameter that defines the log.
- 9.c. ..."_CEE_ENVFILE=" [DD:STDENV](#)
The data definition card defines the Standard Environment file variable.
- 9.d. ...the path and name of the Language Environment file? [/etc/PAGT1/pagentt.env](#)
The STDENV DD card defines the Standard Environment file.
- 12.a. ..."_CEE_ENVFILE=" [DD:STDENV](#)
- 12.b. Does the basic procedure indicate where Policy Agent is to log its messages? [No, -l=SYSLOGD is commented out](#)
- 12.c. Does the basic procedure indicate where Policy Agent is to find its Main Configuration File? [No, -c is commented out](#)
- 12.d. Does the basic procedure give you information on how to code the location of the PAGENT logging and of the Main Configuration File directly on the PAGENT EXEC statement? [Yes, Policy Agent parameters are detailed](#)
- 12.e. Name the five environment variables that you might include in the STDENV file:
[PAGENT CONFIG FILE](#)
[PAGENT LOG FILE](#)
[PAGENT LOG FILE CONTROL](#)
[LIBPATH](#)
[TZ](#)
[All five environment variables are documented in the IP Configuration Reference.](#)
- 12.f.i. Configuration file default: [/etc/pagent.conf](#)
[This is documented in both the IP Configuration Guide and the IP Configuration Reference.](#)
- 12.g.i. Log messages in [/tmp/pagent.log](#)
[This is documented in both the IP Configuration Guide and the IP Configuration Reference.](#)
13. Name several differences in our customized version of the PAGENT procedure and the default sample...: [PARM=POSIX\(ON\), ALL31\(ON\)...-c /etc/PAGT1/pagentt.conf, -l SYSLOGD, STDENV=/etc/PAGT1/pagentt.env](#)
[POSIX stands for Portable Operating System Interface, and is an IEEE standard designed to facilitate application portability. POSIX is an attempt by a consortium of vendors to create a single standard version of UNIX.](#)
[ALL31 indicates that a program must receive control in 31-bit addressing mode.](#)

Part 2

- 6.c. Do you see many samples for getting started with an LDAP repository ("ldif" files)? [Yes](#)
- 6.d. Do you see many samples for getting started using text files ("conf" files)? [Yes](#)
- 6.e. Do you see the Main Pagent Configuration File? [Yes, pagent.conf](#)

Part 3

- 5.b.i. Do you see evidence of the two MODIFY commands? [Yes, EZZ8443I PAGENT MODIFY COMMAND ACCEPTED](#)
- 6.b.i. Loglevel at which PAGENTT was started: [31](#)

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

8. Is the QoS policy stored locally or was it retrieved from a Central Policy Agent Server?
ConfigLocation: Local
9. From which file did PAGENTT read the QoS policy RULES and ACTIONS? **Base configuration file.**
Remember you just edited the file and copied it to /etc/PAGT1/pagentt.conf.
10. Is PAGENTT reading the policies from an LDAP Server? **No, LDAPServer: False**
Remember we did not define an LDAP server in the configuration file.
11. Are the policies to be flushed and purged? **Yes, ApplyFlush: True and ApplyPurge: True**
Remember we coded that in the pagent configuration file.
15. What is the name of the ACTION that matches this RULE? **batch1**
16. How many Policy ACTIONS are associated with this RULE? **1**
17. During what time frame is the rule active? **All the time**
18. Which networking interfaces does this rule apply to? **InInterface: All**
19. Are there any restrictions on the Source or Destination IP addresses that this rule is using?
No,
SourceIpFrom: All
SourceIpTo: All
DestIpFrom: All
DestIpTo: All
20. What are the source ports for this policy? **SourcePortFrom: 20 SourcePortTo: 21**
21. Which protocol does this rule apply to? **ProtocolNumFrom: 6 ProtocolNumTo: 6;**
protocol 6 is TCP.
Protocol numbers are assigned by the Internet Assigned Numbers Authority (IANA). A simple Internet search can provide a number of sites that list them.
22. When was the policy last created and when was it last updated? **Today**
- 26.a. DEBUG LEVEL 31: **Base, LDAP, Sysplex, and Memory trace data**
- 26.b. LOGLEVEL 127: **Base, LDAP, Sysplex, Memory trace, Policy Install trace, and Lock trace**
28. Do you think you would want to run constantly with the enhanced levels? **No**
- 28.a. Why not? **Because it would fill the logs quickly.**

Lab L04 Certificate Cleanup Answers

Part 1

5. If any of the items exist in step 5 you should notify the instructor which ones exist in step 6.

Part 12

12.a. How many certificates are in the “chain of trust” for this certificate? [The only certificate in the “chain of trust” is the certificate itself.](#)

16.a. What is the certificate being used for? [Yes, yes, yes](#)

18.a. How many certificates are in the “chain of trust” for this certificate? [The only certificate in the “chain of trust” is the certificate itself.](#)

Lab L05 Certificate Creation Answers

Part 1

- 6.a. Does the certificate have a unique certificate ID? Yes
The display doesn't come out and tell you this. In the lab description it is mentioned that all the certificates are on a shared RACF database and therefore there are no duplicate certificate ID.
- 6.b. Is the certificate in TRUST Status? Yes
When you create your own certificates, always check to make sure they have status TRUST, otherwise RACF will not allow them to be used.
- 6.c. Is this certificate expired or not? No
If today's date falls within the date range then the certificate has not expired.
- 6.d. What is the Serial Number assigned by RACF, the CA issuer? 36 (example)
- 6.e. What is the Issuer's Name, that is, who signed this certificate?
CN=WSCCA.LABS.IBM.COM.O=IBM.C=US
- 6.f. CN= FTP .WSC.LABS.IBM.COM.O=IBM.C=US
- 6.g. What is the size of the Private Key? 2048
- 6.h. What key rings is the cert. connected to ("owner"/"ringname")? FTPD/ServerRing1
8. Cert Owner = ID(TCPIP)
- 10.a. Does the certificate have a unique certificate number? Yes
The display doesn't come out and tell you this. In the lab description it is mentioned that all the certificates are on a shared RACF database and therefore there are no duplicate certificate ID.
- 10.b. Is the certificate in TRUST Status? Yes
When you create your own certificates, always check to make sure they have status TRUST, otherwise RACF will not allow them to be used.
- 10.c. Is this certificate expired or not? No
If today's date falls within the date range then the certificate has not expired.
- 10.d. What is the Serial Number assigned by RACF, the CA issuer? 41 (example)
- 10.e. What is the Issuer's Name, that is, who signed this certificate?
CN=CA.WSC.LABS.IBM.COM.O=IBM.C=US
- 10.f. What is the Subject's Fully Distinguished Name?
CN=USERnx.WSC.LABS.IBM.COM.O=IBM.C=US
- 10.g. What is the size of the Private Key? 2048
- 10.h. What key rings is the certificate connected to ("owner"/"ringname")?
USERnx/LabClientRing
- 12.a. How many default certificates are on the ring? 1
There is only one default certificate on each keyring.
- 12.b. Who owns the default certificate? USERnx
Your userid owns the default certificate.
- 12.c. Can the owner of this default certificate find his certificate by pointing to the key ring name alone? Yes
Without identifying the label name the default certificate will be used.
- 12.d. How many CA Certificates are on the ring? 1
13. Why is there only one CA Certificate on this ring? CA certificate signed both server and client certificate.
There is only a single CA Certificate because we used the same CA Certificate to sign both the server and client certificate. Typically when client authentication is used there are two CA Certificates on each keyring, both the CA Certificate that signed the server certificate and the CA Certificate that signed the client certificate.
- 14.b. Is this the same CA Certificate that signed the FTP Server Certificate? Yes
- 16.a. Who owns this key ring? FTPD

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

- 16.b. How many default certificates are on the ring? 1
There is only one default certificate on each keyring.
- 16.c. Who owns the default certificate? USER1
- 16.d. How many individual user clients can point to this key ring if they are asked to present a client certificate? Multiple
- 16.e. They must identify their own certificate by specifying the Label name of the certificate. To identify any certificate on a keyring, other than the default certificate, requires the Label Name.
- 16.f. How many CA Certificates are on the ring? 1
- 18.a. Does the certificate have a unique ID? Yes
The display doesn't come out and tell you this. In the lab description it is mentioned that all the certificates are on a shared RACF database and therefore there are no duplicate certificate ID.
- 18.b. Is the certificate in TRUST Status? Yes
- 18.c. Is this CA Certificate expired or not? No
- 18.d. What is the Serial Number assigned to this Root, CA Certificate? 8C (example)
- 18.e. CN= MVS1CA .LABS.IBM.COM.O=MVS1 CA.C=US
- 18.f. CN= WSCCA .LABS.IBM.COM.O=IBM.C=US
- 18.g. What is the size of the Private Key? 1024
- 18.h. What is this certificate used for? CERTSIGN
Signing other certificates.
- 18.i. Does this CA Certificate reside on the FTP Client Ring owned by YOUR Userid which is named "USERnx/LabClientRing"? Yes
- 18.j. Does this CA Certificate reside on the Server Ring owned by userid FTPD which is named "FTPD/ServerRing1"? Yes
19. Why do the ServerRing1 and the LabClientRing require only one CA certificate? The server and client are both signed by the same CA certificate

Part 2

- 18.c. How many CA Certificates need to be on each key ring now? 2
Because the server and client certificates are signed by different CA certificates, both CA certificates are needed on the keyring.

Lab L06 AT-TLS Errors Answers

Part 1

1. SSL Return Code 6: The requested key label is not found in the key database.
2. SSL Return Code 7: The key database does not contain any certificates.
3. SSL Return Code 8: An error is detected while validating a certificate. This error can occur if a root CA certificate is not found in the key database or if the certificate is not marked as a trusted certificate or if the certificate requires an algorithm or key size that is non-FIPS while executing in FIPS mode.
4. SSL Return Code 109: The key database does not contain any valid certification authority certificates.
5. SSL Return Code 202: An error is detected while opening the key database. This error can occur if no name is supplied or the database does not exist.
6. SSL Return Code 417: A self-signed certificate cannot be validated because it is not in the key database.
7. SSL Return Code 435: The key database does not contain a certificate for the certification authority.
8. SSL Return Code 437: A close notification has been received from or sent to the peer application.
9. SSL Return Code 443: Access of key via default status could not be resolved because multiple keys are marked as the default key.
10. SSL Return Code 448: The TLS server has been unable to match the server names supplied in a "Server Name Indication" type TLS extension, and either the TLS server or TLS client has determined this scenario to be fatal.
11. AT-TLS Return Code 5001: ClientAuthType is set to Required or SAFCheck, but the client did not provide a certificate.
12. AT-TLS Return Code 5002: ClientAuthType is set to SAFCheck, but the certificate supplied by the client is not defined to SAF subsystem.
13. AT-TLS Return Code 5006: The connection is using a TTLSEnvironmentAction statement that failed to initialize a System SSL environment.

Lab L07 AT-TLS FTP Answers

Part 2

- 8.b. IEF695I START FTPT WITH JOBNAME FTPT IS ASSIGNED TO USER TCPIP
GROUP=OMVSGRP
11. What is your access to this SERVAUTH resource? READ
- 13.a.i. Who owns the FTP Server Certificate with the label of "FTP on ANY ZOS"? ID(TCPIP)
- 13.a.ii. Is it the DEFAULT certificate on the ring? Yes
- 13.a.iii. Is this the right owner? Yes, back at the beginning of this section you found that user ID TCPIP is also the user ID associated with application FTPT.
- 13.a.iv. What is the other type of certificate on this ring? CA certificate
- 13.b.i. How many USER certificates are on "LabClientRing"? 1
- 13.b.ii. How many CERTAUTH certificates are here? 1
- 13.c.i. How many USER certificates are on "ClientRing1"? Multiple
- 13.c.ii. How many of these are the DEFAULT certificate? 1
- 13.c.iii. How many CERTAUTH certificates are on this ring? 1
- 45.a. What does LE variable "_BPXK_SETIBMOPT_TRANSPORT=TCPIPT" do for the FTP procedure? It binds FTPT to the TCPIPT stack.
Documented in the "IP Configuration Guide" and the "Unix System Services Planning" manuals.
- 45.b. What does TZ=EST5EDT do for the FTP procedure? Sets the time zone to Eastern Standard and Daylight Savings times.
The TZ variable was discussed in the class lecture and it is documented in the "IP Configuration Guide" and the "Unix System Services Command Reference" manuals.
- 46.a. What configuration dataset is this FTP server proc pointing to?
SYS1.CS.TCPPARMS(FTPSEC)

Part 3

- 9.b. Which traces are running? SEC
- 14.a. How many encryption and hashing algorithms have access to CPACF? 8
System SSL: SHA-1 crypto assist is available
System SSL: SHA-224 crypto assist is available
System SSL: SHA-256 crypto assist is available
System SSL: DES crypto assist is available
System SSL: DES3 crypto assist is available
System SSL: AES 128-bit crypto assist is available
System SSL: AES 256-bit crypto assist is not available
System SSL: AES-GCM crypto assist is available
- 15.d. Has ICSF been enabled for this MVS image? Yes
- 16.b. Do you see any TTLS sessions yet? No
- 30.c.i. What version of SSL or TLS has been negotiated? FC3204 authServerAttls: Using TLSv1.1 protocol
- 30.c.ii. What cipherspec was chosen? FC3226 authServerAttls: SSL cipher: 000A
- 30.c.iii. Has FTP with AT-TLS been enabled for FIPS-140? FC3171 authServerAttls: FIPS140 not enabled
- 30.c.iv. What is the meaning of this cipherspec? 3DES
Cipher 0A is the 3DES cipher. Ciphers are documented in the "IP Configuration Guide", the "IP Configuration Reference", and the "Cryptographic Services System Secure Sockets Layer Programming" manuals.
- 36.c. Do you see a session count now? Yes, CONNS 1
- 45.a. Is this an AT-TLS connection? Yes, FC0294 ftpAuth: security values: mech=TLS, tlsmech=ATTLS, tlsreuse=N, sFTP=R, sCC=P, sDC=P

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

45.b. Is the connection “application-controlled” or not? [Yes, FC2971 ftpAuthAttls: AT-TLS policy set as application controlled.](#)

You might remember from the lecture that both FTP and TN3270 are both AT-TLS application controlled.

45.c. What version of SSL or TLS has been negotiated? [FC3204 authServerAttls: Using TLSv1.1 protocol](#)

45.d. What cipher was chosen? [FC3226 authServerAttls: SSL cipher: 000A](#)

45.e. What is the meaning of this cipherspec? [3DES](#)

Cipher 0A is the 3DES cipher. Ciphers are documented in the “IP Configuration Guide”, the “IP Configuration Reference”, and the “Cryptographic Services System Secure Sockets Layer Programming” manuals.

45.f. Is FIPS-140 enabled or not? [No, FC3171 authServerAttls: FIPS140 not enabled](#)

Lab L08 AT-TLS TN3270 Answers

Part 1

- 7.a. USERnx on MVSn ID(USERnx) PERSONAL DEFAULT=YES
7.b. GBGCACnx LABS Client CA CERTAUTH CERTAUTH DEFAULT=NO
7.c. GBGCASnx LABS Server CA CERTAUTH CERTAUTH DEFAULT=NO
9.a. TN3270 on MVSn ID(TN3270) PERSONAL DEFAULT=YES
9.b. GBGCACnx LABS Client CA CERTAUTH CERTAUTH DEFAULT=NO
9.c. GBGCASnx LABS Server CA CERTAUTH CERTAUTH DEFAULT=NO
13.a. FORMAT(CERTDER)
13.b. Does the PCOMM application on the workstation need to have access to the private keys of the CA Certificates? Why or why not? No, they only need the public keys to authenticate.
13.c. Why is this Certificate Package Export format chosen? The private keys are not required.
13.d. Does this format export in Text or Binary mode? Binary
14.a. FORMAT(PKCS12DER)
14.b. Does the PCOMM application on the workstation need to have access to the private keys of the Client Certificates? Yes
14.c. Why is this Certificate Package Export format chosen? So that the private key is included.
14.d. Does this format export in Text or Binary mode? Binary
14.e. Is the protected password in Upper Case or Lower Case? Upper

Part 3

- 8.a. My Private Key password is: USERLABS

Part 5

- 8.b.i. What is the CONNTYPE: CONNTYPE SECURE
8.b.ii. What is the Port's Key Ring name? TTLS/**N/A**
This indicates that AT-TLS is being used and therefore the key ring is defined in the policy rather than the PROFILE.
8.b.ii.1. Why is the name of the Key Ring not displayed? Because it is defined in Policy rather than the TN3270 profile.
8.b.iii. What is the Encryption Type: TTLS
This indicates that AT-TLS is being used and therefore the ciphers are defined in the policy rather than the PROFILE.
8.b.iv. What type of CLIENTAUTH is valid: TTLS
This indicates that AT-TLS is being used and therefore the client authentication is defined in the policy rather than the PROFILE.
10. Write down the Connection ID number of your TN3270 session: 0000001F (example)
11.b. Is Client Authentication in Use? Yes, CLIENTAUTH USERID: USERnx
11.c. What is the USERID that is associated with the TN3270 ATTLS Connection? USERnx
11.d. What type of Access is coded for this TN3270 Port? ACCESS: SECURE
11.e.i. Which Cipher Specs are represented? ACCESS: SECURE 000A TLSV1 means TLS RSA WITH 3DES EDE CBC SHA
Cipher suites definitions are located in the manual z/OS Cryptographic Services System Secure Sockets Layer Programming, SC14-7495.
11.f. What is the name of the TTLS Rule? TTLSRULE: TN3270-WS-to-Host~1
12.a. LUNAME: TCPS2A01 (example)
12.b. APPL: F0010002

Lab L09 IP Filters Answers

Part 1

21. Why are we creating IP Filter rules for FTP between VIPAs when we have already implemented AT-TLS policies for this traffic? Packets are checked at the IP layer prior to the Transport layer by IP Filters. If there is not an IP Filter PERMIT rule for the traffic it will be discarded and not passed up to the Transport layer for the AT-TLS policy to be applied.

You must make sure all your AT-TLS traffic has corresponding IP Filter PERMIT rules unless IP Filter and IPsec are not implemented, no IPCONFIG IPSECURITY.

Lab L10 TRMD Answers

Part 1

- 9.a. Does the procedure point to a REAL or a DUMMY standard environment file? DUMMY as defined by: //STDENV DD DUMMY
- 9.b.i. How does it know which TCP/IP Stack it is to be associated with? There is no Environment variable BPX_JOBNAME= or resolver RESOLVER_CONFIG= defined so it should bind with the "default" TCP/IP stack (defined in BPXPRMxx or whichever stack started first).
- 9.b.ii. How does it know the TIMEZONE variable it is to use for the messages printed to the log? Event detection in UTC time (Greenwich Mean Time)
Recording time (according to Timezone variable) TZ is not defined in this proc so it will use the Unix setting for Timezone.

Part 2

- 2.a. _CEE_ENVFILE= No (STDENV DD DUMMY instead)
- 2.b. How does the procedure point to the TCP/IP stack it is to be associated with? Resolver RESOLVER_CONFIG="//&CS..CS.TCPPARMS(&DATA)" which defaults to SYS1.CS.DATnA
- 2.c. How does the procedure indicate the timestamp to be associated with the logging time of the messages? TZ=EST5EDT

Lab L11 IP Filter Testing Answers

Part 2

Part 2A

3.a. Because my userid or my group was permitted to the SERVAUTH class named:

[EZB.IPSECCMD.*.*](#)

[This is documented in the IP Configuration Guide.](#)

15.c.i. SYSDEFAULT [RULE.x](#)

15.c.ii. SYSDEFAULT [DENYRULE](#)

2.b.i. Why does this connection fail? [The AT-TLS TN3270 policy is for connections to the VIPA address \(192.168.20.10n\) only and not to the OSA address \(192.168.20.9n\).](#)

Part 2B

8. Which policies are in effect? [Stack Profile filters are now in effect](#)

12. Which policies are in effect? [Stack Policy filters now in effect](#)

19.b.i. What is the name of the SERVAUTH class that permitted you to execute the "pasearch" command? [EZB.PAGENT.sysname.tcpstack.ptype](#)

[EZB.PAGENT is documented in the IP Configuration Guide manual.](#)

24.a. The Default Stack Filters? [No](#)

24.b. The Policy Filters? [Yes](#)

Lab L12 IPSec VPN Answers

Part 1

- 1.a. Local Data Endpoint (LDE at your ZOSn): 192.168.20. 9n
- 1.b. Remote Data Endpoint (RDE at ZOS1): 192.168.20. 91
- 2.a. Local Security Endpoint (LSE at your ZOSn): 192.168.20. 9n
- 2.b. Remote Security Endpoint (RSE at ZOS1): 192.168.20. 91
- 3.a. Host to Host? Yes
- 3.b. Host to Gateway? No
- 3.c. Gateway to Host? No
- 3.d. Gateway to Gateway? No
- 4.a. Certificate ALTNAME of IPADDR? Yes
- 4.b. Certificate ALTNAME of FQDN? No
- 4.c. Certificate ALTNAME of USER@FQDN? No
- 4.d. Certificate ALTNAME of SUBJECT NAME of X.500 DN? No
- 5.a. Certificate ALTNAME of IPADDR? Yes
- 5.b. Certificate ALTNAME of FQDN? No
- 5.c. Certificate ALTNAME of USER@FQDN? No
- 5.d. Certificate ALTNAME of SUBJECT NAME of X.500 DN? No
- 6. Who owns the IKED Keyring and what is the name of the IKED Keyring that contains the appropriate X.509 certificates? IKED/IKEDnRING
- 2.b.i. Certificate label from the correct IKED ring for our lab: 'IKEDn at ZOSn'
- 4.a. IP 192.168.20. 9n
- 5.b.i. Certificate label from the correct IKED ring for our lab: 'IKED1 at ZOS1'
- 7.a. IP 192.168.20. 91
- 2. Identify the name of the IKED key ring that you will be using: IKEDnRING

Part 2

- 4.c.i. What type of policies for IPSec have been loaded? Stack Policy Rules
- 13.f. Encr Alg AES-CBC
- 13.i. Hash Alg SHA1
- 13.l. Auth Method RsaSignature
- 14.c. Local IKE ID info : ID_IPV4_ADDR 192.168.20. 92
- 14.d. Remote IKE ID info : ID_IPV4_ADDR 192.168.20. 91
- 14.e. Local IKE IP : 192.168.20. 92 port 500
- 14.f. Remote IKE IP : 192.168.20. 91 port 500
- 14.k. Local IPSec upper-layer info : port 1025 (example)
- 14.l. Remote IPSec upper-layer info : port 21
- 14.m. Local IPSec IP info : 192.168.20. 92
- 14.n. Remote IPSec IP info : 192.168.20. 91

Lab L13 IPsec Errors Answers

Part 1

1. EZD1075I Received ISAKMP error notification message: No proposal chosen
The IKE daemon received an ISAKMP error notification message. This error indicates that a security association (SA) negotiation failure occurred.
2. EZD1040I Phase 1 security association retransmit timeout src IP: 192.168.20.121 dest IP: 192.168.20.95 src port: 500 protocol: UDP(17)
The IKE daemon exhausted the retransmit limit set for a single phase 1 or phase 2 message retransmission.
3. EZD1078I A security association (Phase 1 – SA ID 0) has been deactivated
This is an informational message to indicate that either a phase 1 (IKE) or phase 2 (dynamic) security association (SA) was deactivated. Multiple SAs are activated and deactivated to carry tunnel traffic. The deactivation of an SA does not imply that the tunnel has ended or is unavailable.
4. EZD1093I Policy mismatch: KeyExchangeOffer (1) requires parameter (DHGroup) with value (Group 1) but proposed (1) value is (Group 2)
The IKE daemon was unable to accept a proposal because there was a mismatch in the configured policy. IKE daemon processing continues to the next proposal. If no proposals are accepted, the security association negotiation will fail.
5. EZD1093I Policy mismatch: KeyExchangeOffer (1) requires parameter (HowToEncrypt) with value (AES) but proposal (1) value is (3DES)
The IKE daemon was unable to accept a proposal because there was a mismatch in the configured policy. IKE daemon processing continues to the next proposal. If no proposals are accepted, the security association negotiation will fail.
7. EZZ0751I Cannot start IPv4 Security after TCPIP is active.
The VARY TCPIP,,OBEYFILE command was issued including the IPSECURITY parameter on the IPCONFIG statement. IPv4 Security can be started only from an initial profile.
8. EZZ0754I IPSEC statement was not processed because IP Security is not enabled.
An IPSEC statement was configured in the profile but the IPSECURITY parameter was not coded on the IPCONFIG statement in the initial profile.
9. EZZ0802I GLOBALCONFIG ZIIP IPSECURITY is ignored – IP Security is not enabled.
The TCPIP profile requested IP security exploitation of the IBM System z9 Integrated Information Processor (zIIP), but IP security is not configured.
10. EZZ0804I ZIIP function IS ENABLED – ZIIPS ARE ONLINE
The IBM System z9 Integrated Information Processor (zIIP) function is enabled and there are zIIPs online.
11. EZZ8438I PAGENT POLICY DEFINITIONS CONTAIN ERRORS FOR image: type
The specified policies, which are defined in a configuration file or on an LDAP server, contain errors, or cannot be accessed, for the specified TCP/IP stack or remote policy client. The error might be caused by any of the following conditions:
 - ▣ The policy definitions contain one or more syntax or semantic errors.
 - ▣ The configuration file configured for the specified policy type does not exist or cannot be read.
 - ▣ The Policy Agent that is acting as a policy client does not have permission to access the specified policy type on the Policy Agent that is acting as a policy server.
 - ▣ The import requestor does not have permission to access the policy type on the Policy Agent.
12. EZZ8544I TRMD IPSEC LOGGING COULD NOT ACTIVATE
TRMD could not obtain storage for the IPsec log buffer. At least 2 megabytes of private storage is needed to process the IPsec log records.

Lab L14 IDS Answers

Part 3

- 6.b. Are IDS policies loaded for the TCPIPT stack? Yes
SCAN DETECTION, ATTACK DETECTION, and TRAFFIC REGULATION sections are all displayed.
- 6.c. Can you see that any connections have been rejected for Traffic Regulation? No
CONNREJECTED: 0
- 9.c. Have you been attacked in any way yet? No
- 2.b.i. Are the five connections successful? Yes
There may be a delay in starting so wait a minute and they should come up successfully.
- 2.b.ii. What percentage of the total available sessions do 3 connections represent? 3 because the total you set was 100 in the policy.
- 2.b.iii. Is this percentage what you configured in your TR Policy? Yes
- 3.a. What happens? It fails
- 3.b. Why did this happen with the 4th connection? Because the policy with 3% limit will only allow a maximum of 3 sessions from any given user.
- 5.b. Can you see that any connections have been rejected for Traffic Regulation? Yes, you should see that a connection has been rejected now.

Lab L15 IPSec VPN Preshare Mode Answers

Part 1

- 1.a. Local Data Endpoint (LDE at your ZOSn): 192.168.20. 12n
- 1.b. Remote Data Endpoint (RDE at ZOS1): 192.168.20. 121
- 2.a. Local Security Endpoint (LSE at your ZOSn): 192.168.20. 9n
- 2.b. Remote Security Endpoint (RSE at ZOS1): 192.168.20. 121
- 3.a. Host to Host? No
- 3.b. Host to Gateway? Yes
- 3.c. Gateway to Host? No
- 3.d. Gateway to Gateway? No
- 4.a. Host to Host? No
- 4.b. Host to Gateway? No
- 4.c. Gateway to Host? Yes
- 4.d. Gateway to Gateway? No
- 5.a. Certificate ALTNAME of IPADDR? No
- 5.b. Certificate ALTNAME of FQDN? No
- 5.c. Certificate ALTNAME of USER@FQDN? Yes
- 5.d. Certificate ALTNAME of SUBJECT NAME of X.500 DN? No
- 6.a. Certificate ALTNAME of IPADDR? No
- 6.b. Certificate ALTNAME of FQDN? Yes
- 6.c. Certificate ALTNAME of USER@FQDN? No
- 6.d. Certificate ALTNAME of SUBJECT NAME of X.500 DN? No

Part 2

- 7.a. Which Encryption Algorithm ("Encr Alg") is being proposed? AES-CBC
- 7.b. Which Hashing Algorithm ("Hash Alg") is being proposed? SHA1
- 7.c. Which Authentication Method ("Auth Method") is being proposed? PresharedKey
- 8.a. Local IKE ID info: IPv4 192.168.20. ID FQDN WSC.LABS.IBM.COM
- 8.b. Remote IKE ID info: IPv4 192.168.20. ID USER FQDN ZOS1@WSC.LABS.IBM.COM
- 8.c. Local IKE IP: 192.168.20. 9n Port: 500
- 8.d. Remote IKE IP: 192.168.20. 121 Port: 500
- 9.a. Local IPSec Client ID info: IPv4 192.168.20. 12n
- 9.b. Remote IPSec Client ID info: IPv4 192.168.20. 121

Lab L16 NSSD Answers

Part 2

4. Is an environment file specified in the NSSD proc? [No, STDENV DD DUMMY](#)
5. Is the NSSD configuration file specified in the NSSD proc? [No, the comments indicate that the configuration file may be specified in an environment file.](#)
6. What NSSD configuration file will be used? [The default /etc/security/nssd.conf, as documented in the IP Configuration Guide manual.](#)

Lab L17 DMD Answers

Part 1

8. Is an environment file specified in the DMD proc? [no](#)
9. Is the DMD configuration file specified in the DMD proc? [no](#)
10. What DMD configuration file will be used? [The default /etc/security/dmd.conf](#)

