Realize your vision

Samsung SDS
EMM

Configuration Guide for Ipsec settings in Microsoft Windows Server 2016/2019 for Common Criteria Evaluation

Solution version 2.2.5

Published: 27th January 2023

Manual version 2.2.5b

SAMSUNG SDS SAMSUNG

Before using this information and the product it supports, be sure to read the general information on this page.

Publisher	Samsung SDS Co., Ltd
Address	125, 35-Gil, Olympic-Ro, Songpa-Gu, Seoul, South Korea.
Email	ems.support@samsung.com
Website	www.samsungsds.com

Samsung SDS Co., Ltd. has verified the information contained in this document. However, Samsung SDS is not responsible for any circumstances which arise from inaccurate content or typographical errors.

The content and specifications in this document are subject to change without notice.

DFARS Limited Rights Notice

LIMITED RIGHTS

Contractor Name: Samsung SDS Co. Ltd., *via its distributor in the U.S.,* Samsung SDS America, Inc.

Contractor Address: Samsung SDS America, Inc.: 100 Challenger Road, 6th Fl., Ridgefield Park, NJ 07660 U.S.A.

The US Government's rights to use, modify, reproduce, release, perform, display, or disclose these technical data are restricted by paragraph (b)(3) of the Rights in Technical Data--Noncommercial Items clause contained in the US Government contract under which the US Government has obtained a license to use this computer software. Any reproduction of technical data or portions thereof marked with this legend must also reproduce the markings. Any person, other than the US Government, who has been provided access to such data must promptly notify the above named Contractor.

(End of legend)

FAR Limited Rights Notice

Limited Rights Notice (Dec 2007)

(a) These data are submitted with limited rights under the US Government contract under which the US Government has obtained a license to use these data. These data may be reproduced and used by the US Government with the express limitation that they will not, without written permission of the Contractor, be used for purposes of manufacture nor disclosed outside the US Government; except that the US Government may disclose these data outside the US Government for the following purposes, if any; provided that the US Government makes such disclosure subject to prohibition against further use and disclosure (if any).

(b) This notice shall be marked on any reproduction of these data, in whole or in part.

(End of notice)

DISCLAIMER

Samsung SDS may alter, change, modify or delete a part of or whole contents of this guide at any time by its sole discretion for the purpose of providing better information.

PREFACE

This guide describes how to set up IPsec configuration on Microsoft Windows Server 2016 for the mutual authentication among the servers installed in Samsung SDS EMM as the environment for Common Criteria evaluation to MDMPP v4.0. The guide outlines the followings:

1. host to host communication (transport mode)
2. Standalone Machine (not Domain-joined Machine)
3. Settings of Main mode vs Quick mode
4. Select Authentication Methods
   - PSK
   - Not Kerberos
   - Not Certificate (from CA, local)
5. Select Security Method
   - integrity : SHA-256
   - Encryption : AES-CBC 256
   - key exchange : DH Group 14
6. Enable FIPS feature in Microsoft Windows

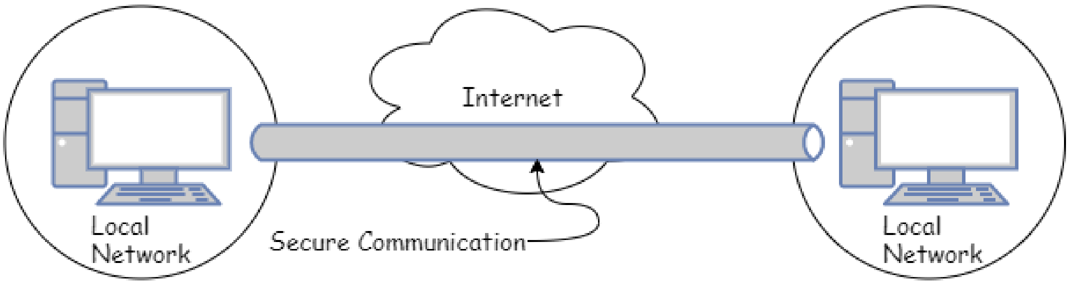
Note: This guides how to set up the IPsec in MS Windows Server 2016/2019 for establishing the secure communication channel between the EMM server and the external server (e.g., DBMS).

Revision History

Solution version	Manual version	Manual revised date	Revised details
2.2.5	2.2.5a	October 2019	Initially published.
2.2.5	2.2.5b	January 2023	Add the settings for Windows Server 2019

□ Abstract

- This guide shows how to set up the secure communication between the servers in terms of the components of Samsung SDS EMM.



□ Test environment

- Create 2 of Virtual Machines (hereinafter VM)
  . VM A IP : 10.0.222.54
  . VM B IP : 10.0.222.159

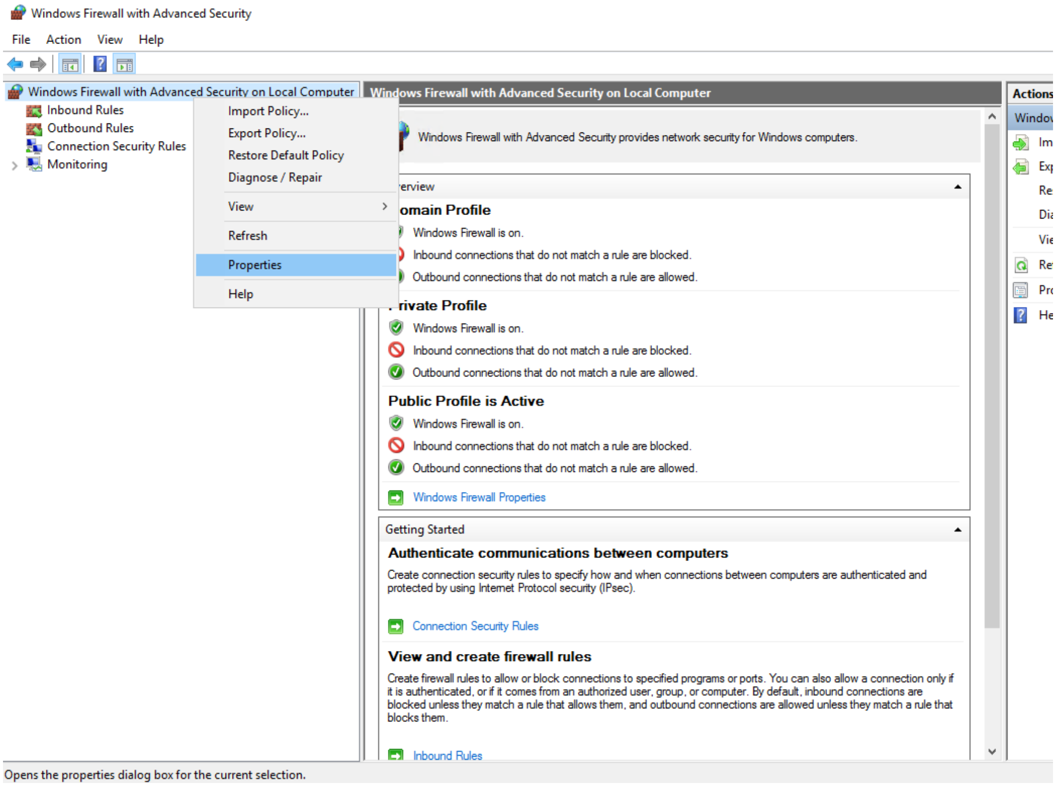
□ Practice

1. Go to [Control Panel] → [Administrative Tools] → [Windows Firewall with Advanced Security]

   - In the case of Windows Server 2019, go to [Server Manager] → [Tools] → [Windows Defender Firewall with Advanced Security]

2. Click [Properties] while the task bar selected and right-click on [Windows Firewall with Advanced Security on Local Computer]

   - In the case of Windows Server 2019, click [Properties] while the task bar selected and right-click on [Windows Defender Firewall with Advanced Security on Local Computer]



Windows Firewall with Advanced Security on Local Computer

Windows Firewall with Advanced Security provides network security for Windows computers.

erview

omain Profile

Windows Firewall is on.

Inbound connections that do not match a rule are blocked.

Outbound connections that do not match a rule are allowed.

rivate Profile

Windows Firewall is on.

Inbound connections that do not match a rule are blocked.

Outbound connections that do not match a rule are allowed.

Public Profile is Active

Windows Firewall is on.

Inbound connections that do not match a rule are blocked.

Outbound connections that do not match a rule are allowed.

Authenticate communications between computers

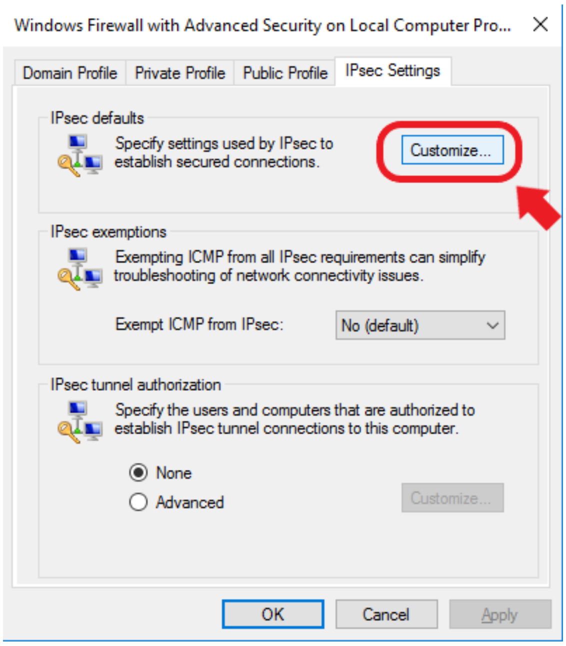
Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that blocks them.

Opens the properties dialog box for the current selection.

3. Go to [IPsec Settings] → [IPsec defaults], and click [Customize]



Specify settings used by IPsec to establish secured connections.

Exempting ICMP from all IPsec requirements can simplify troubleshooting of network connectivity issues.

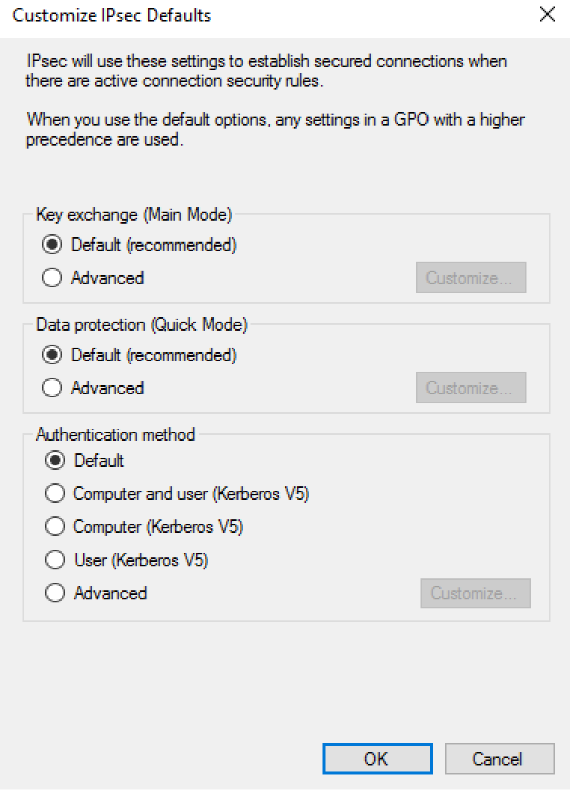
Exempt ICMP from IPsec: No (default)

Specify the users and computers that are authorized to establish IPsec tunnel connections to this computer.

● None

○ Advanced

Check the default settings and click OK



Customize IPsec Defaults

IPsec will use these settings to establish secured connections when there are active connection security rules.

When you use the default options, any settings in a GPO with a higher precedence are used.

Key exchange (Main Mode)

● Default (recommended)
○ Advanced

Data protection (Quick Mode)

● Default (recommended)
○ Advanced

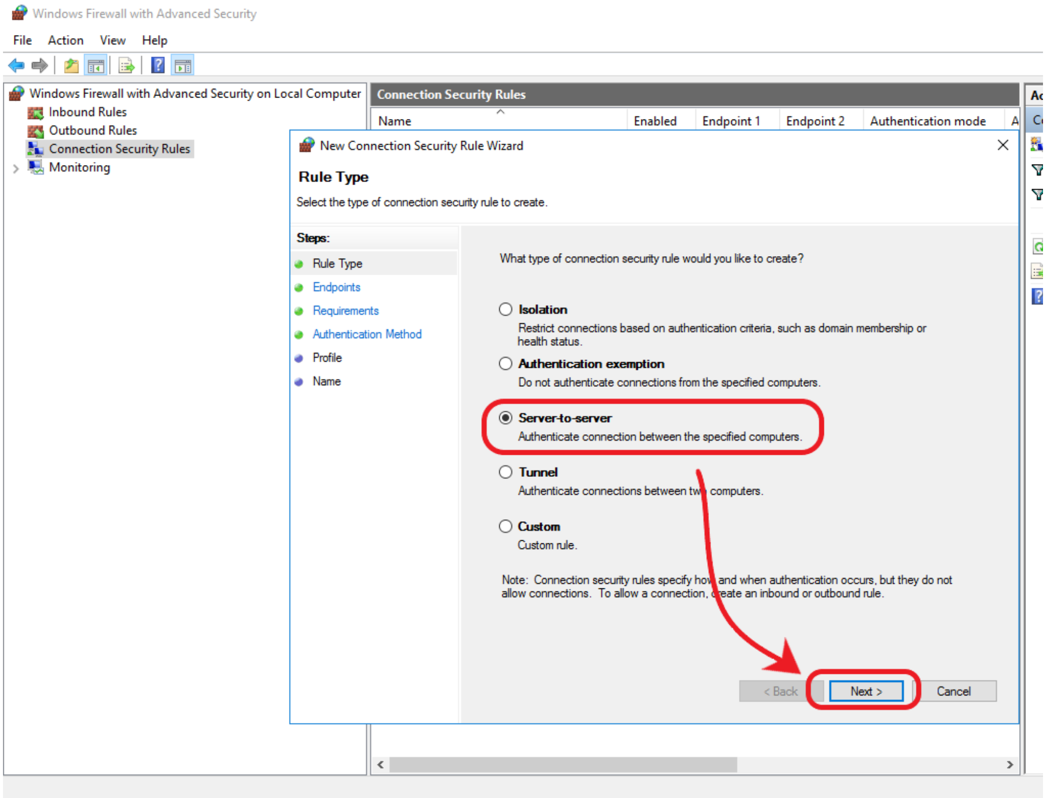
Authentication method

● Default
○ Computer and user (Kerberos V5)
○ Computer (Kerberos V5)
○ User (Kerberos V5)
○ Advanced

4. Set up the algorithm by referring the 3 modes below for CC evaluation

Key exchange (Main Mode)	. Select [Advanced], and click [Customize...] . Delete the [Security methods], click [Add...] . Click [OK] after setting as * Integrity algorithm : SHA-256 * Encryption algorithm : AES-CBC 256 * Key exchange algorithm : Diffie-Hellman Group 14 . Click [OK]
Data protection (Quick Mode)	. Select [Advanced], and click [Customize...] . Check '√ ' at [Require encryption for all connection security rules that use these settings] . Delete the [Data integrity and encryption], click [Add...] . Select [ESP(recommended)] . Click [OK] after setting as * Integrity algorithm : AES-GMAC 256 * Encryption algorithm : AES-GCM 256 . Click [OK]
Authentication method	. Select [Advanced], and click [Customize...] . Delete the [First authentication methods], click [Add...] . Click [OK] after setting as * Select [Preshared key] and enter the desired value . Click [OK]

5. Double click [Connection Security Rules],
select [Rule Type] in [New Connection Security Rules Wizard] window,
Select [Rule Type] in Steps, [New Rule...], [Server-to-server] for IPsec setting
. Click [Next]



Rule Type

Select the type of connection security rule to create.

What type of connection security rule would you like to create?

○ **Isolation**
Restrict connections based on authentication criteria, such as domain membership or health status.

○ **Authentication exemption**
Do not authenticate connections from the specified computers.

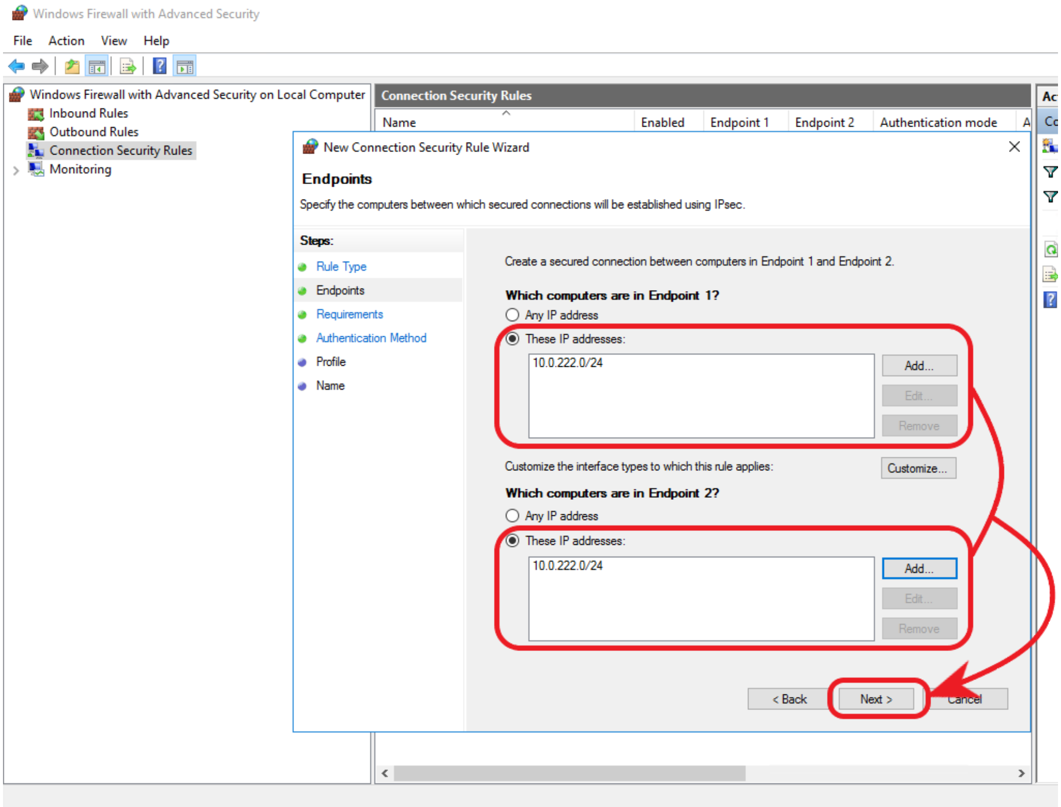
● **Server-to-server**
Authenticate connection between the specified computers.

○ **Tunnel**
Authenticate connections between two computers.

○ **Custom**
Custom rule.

Note: Connection security rules specify how and when authentication occurs, but they do not allow connections. To allow a connection, create an inbound or outbound rule.

In [Endpoints] steps, a second connection is needed.
Note: This guide shows the setting per subnet. Please set up for respective use.



Endpoints

Specify the computers between which secured connections will be established using IPsec.

Create a secured connection between computers in Endpoint 1 and Endpoint 2.

Which computers are in Endpoint 1?

○ Any IP address

● These IP addresses:

10.0.222.0/24

Customize the interface types to which this rule applies:

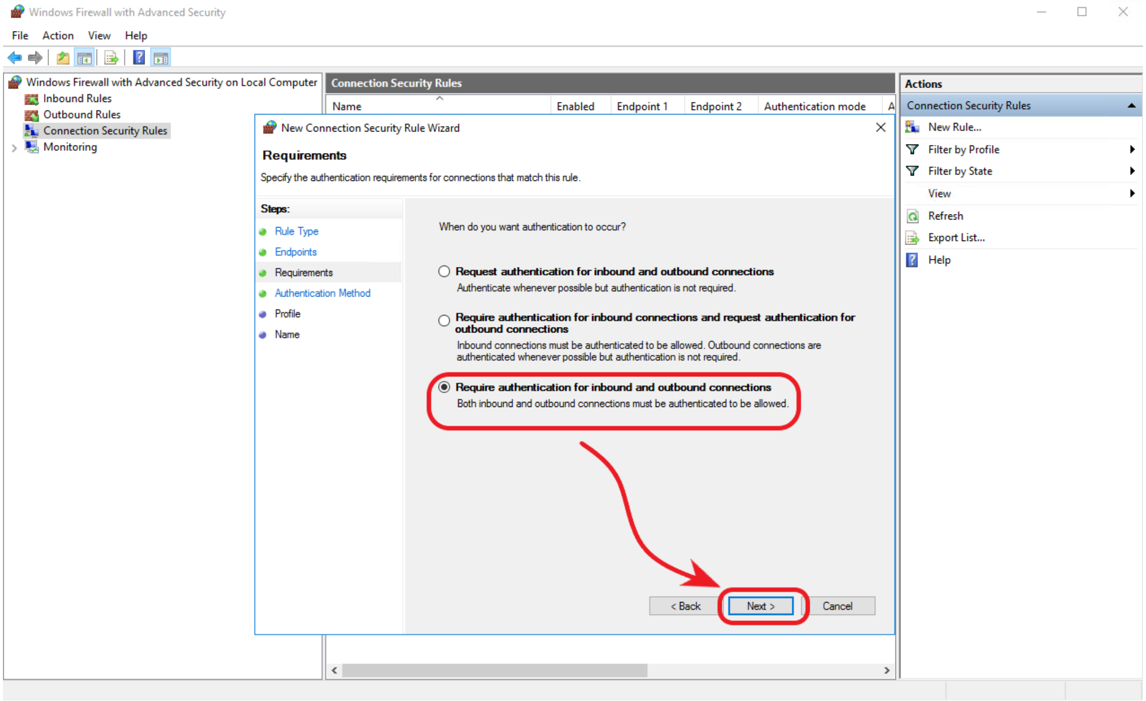
Which computers are in Endpoint 2?

○ Any IP address

● These IP addresses:

10.0.222.0/24

In [Requirements], please refer to the settings as below
Select [Require authentication for inbound and outbound connections], click [Next]



New Connection Security Rule Wizard

Requirements

Specify the authentication requirements for connections that match this rule.

Steps: Rule Type, Endpoints, Requirements, Authentication Method, Profile, Name

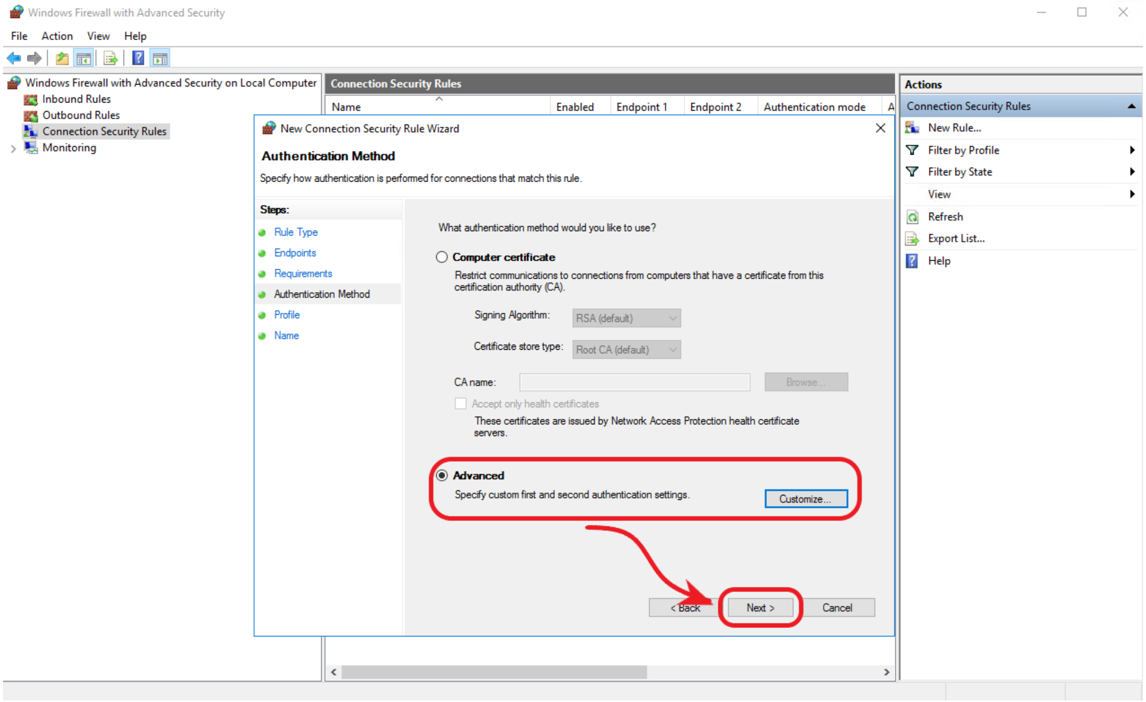
When do you want authentication to occur?

○ **Request authentication for inbound and outbound connections**
Authenticate whenever possible but authentication is not required.

○ **Require authentication for inbound connections and request authentication for outbound connections**
Inbound connections must be authenticated to be allowed. Outbound connections are authenticated whenever possible but authentication is not required.

● **Require authentication for inbound and outbound connections**
Both inbound and outbound connections must be authenticated to be allowed.

In [Authentication Method], select [Advanced], click [Next]
Note: This guide shows the PSK setting by applying Preshared Key in [Customize].



New Connection Security Rule Wizard

Authentication Method

Specify how authentication is performed for connections that match this rule.

Steps: Rule Type, Endpoints, Requirements, Authentication Method, Profile, Name

What authentication method would you like to use?

○ **Computer certificate**
Restrict communications to connections from computers that have a certificate from this certification authority (CA).

Signing Algorithm: RSA (default)

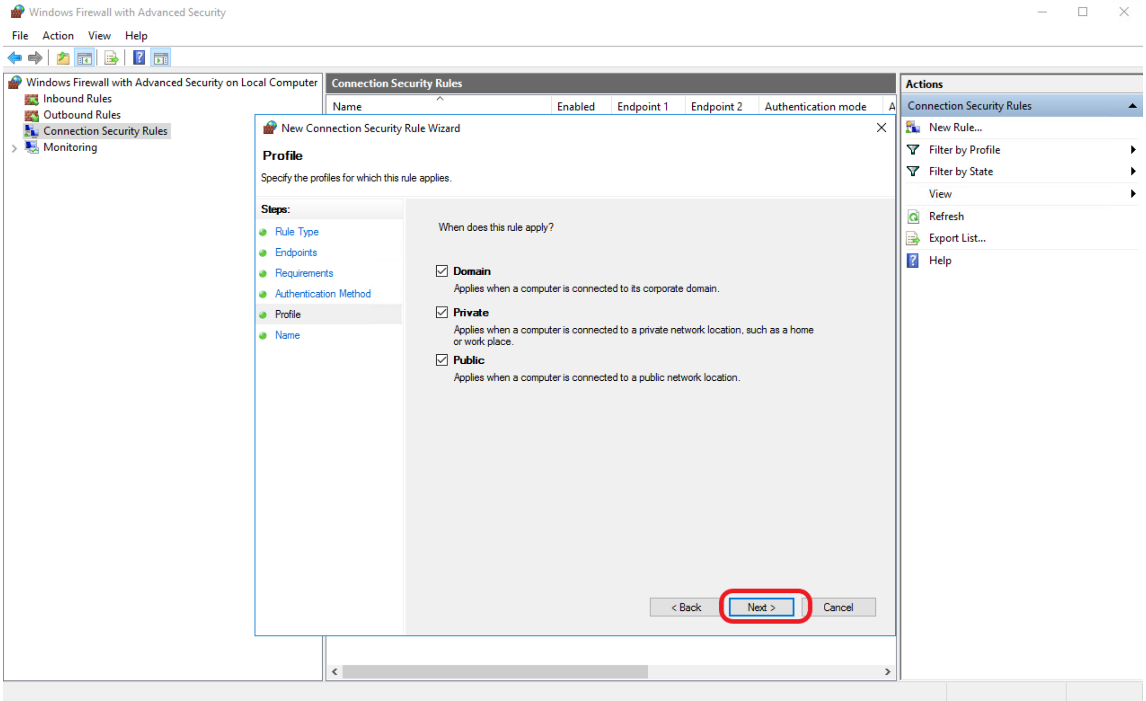
Certificate store type: Root CA (default)

CA name:

□ Accept only health certificates
These certificates are issued by Network Access Protection health certificate servers.

● **Advanced**
Specify custom first and second authentication settings.

In [Profile], check '√ ' at Domain, Private and Public and click [Next]



New Connection Security Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:
- Rule Type
- Endpoints
- Requirements
- Authentication Method
- Profile
- Name

When does this rule apply?

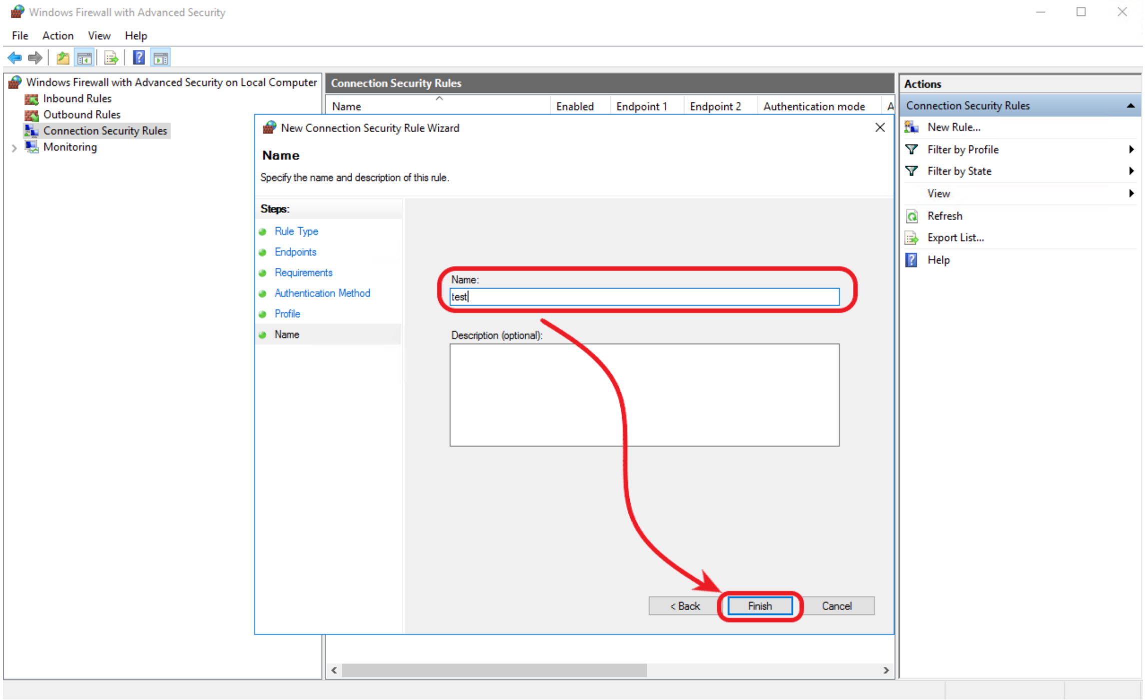
☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☑ **Public**
Applies when a computer is connected to a public network location.

< Back | Next > | Cancel

In [Name], please enter the appropriate name (and Description as an option).
Click [Finish].
Note: This setting should be exactly same to each Host.



New Connection Security Rule Wizard

Name

Specify the name and description of this rule.

Steps:
- Rule Type
- Endpoints
- Requirements
- Authentication Method
- Profile
- Name

Name:
test

Description (optional):

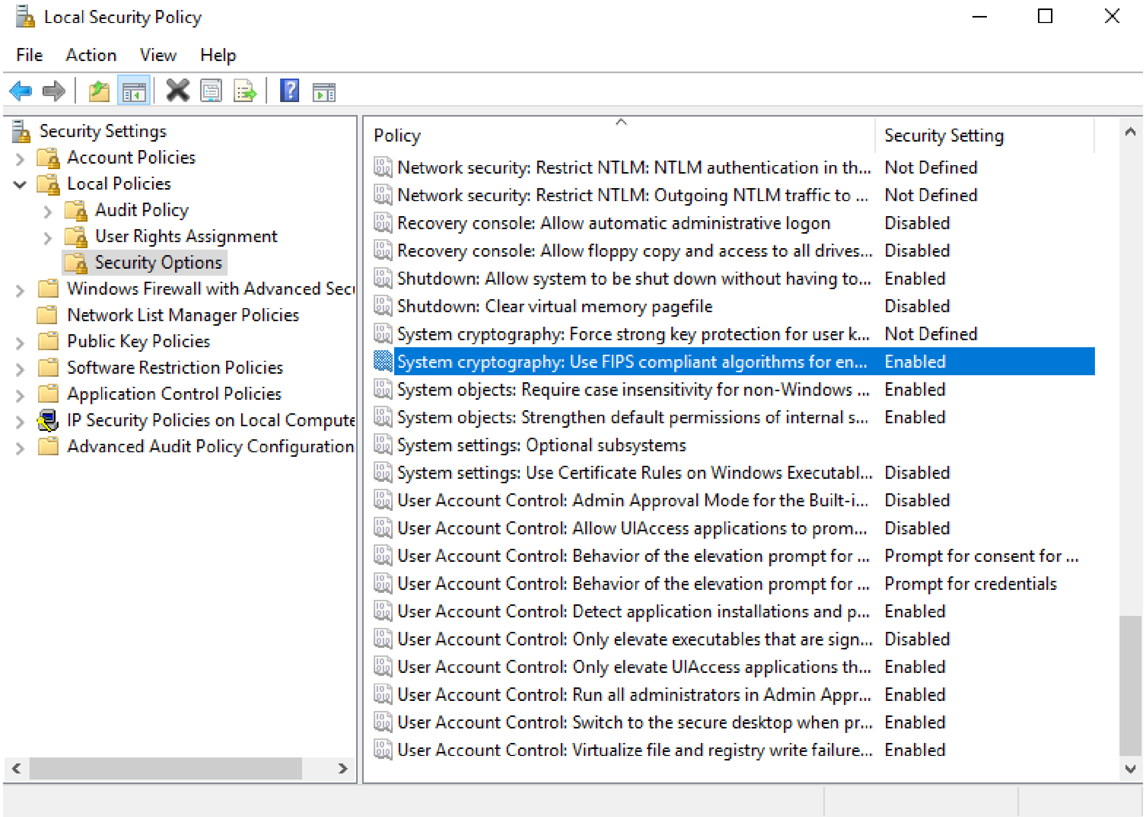
< Back | Finish | Cancel

□ Option) FIPS setting for CC evaluation

1. Go to [Control Panel] → [Administrative Tools] → run [Local Security Policy]

- In the case of Windows Server 2019, go to [Server Manager] → [Tools] →→ run [Local Security Policy]

2. Go to [Security Settings] → [Local Policies] → [Security Options] →
   Select [System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing] Enabled (please see below)

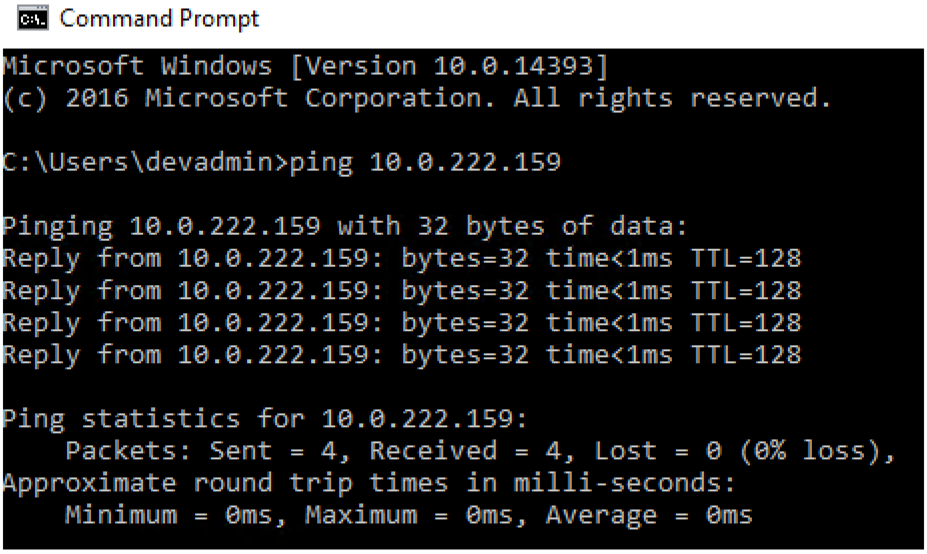

Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Network security: Restrict NTLM: NTLM authentication in th...	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to ...	Not Defined
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives...	Disabled
Shutdown: Allow system to be shut down without having to...	Enabled
Shutdown: Clear virtual memory pagefile	Disabled
System cryptography: Force strong key protection for user k...	Not Defined
System cryptography: Use FIPS compliant algorithms for en...	Enabled
System objects: Require case insensitivity for non-Windows ...	Enabled
System objects: Strengthen default permissions of internal s...	Enabled
System settings: Optional subsystems	
System settings: Use Certificate Rules on Windows Executabl...	Disabled
User Account Control: Admin Approval Mode for the Built-i...	Disabled
User Account Control: Allow UIAccess applications to prom...	Disabled
User Account Control: Behavior of the elevation prompt for ...	Prompt for consent for ...
User Account Control: Behavior of the elevation prompt for ...	Prompt for credentials
User Account Control: Detect application installations and p...	Enabled
User Account Control: Only elevate executables that are sign...	Disabled
User Account Control: Only elevate UIAccess applications th...	Enabled
User Account Control: Run all administrators in Admin Appr...	Enabled
User Account Control: Switch to the secure desktop when pr...	Enabled
User Account Control: Virtualize file and registry write failure...	Enabled

□ Test

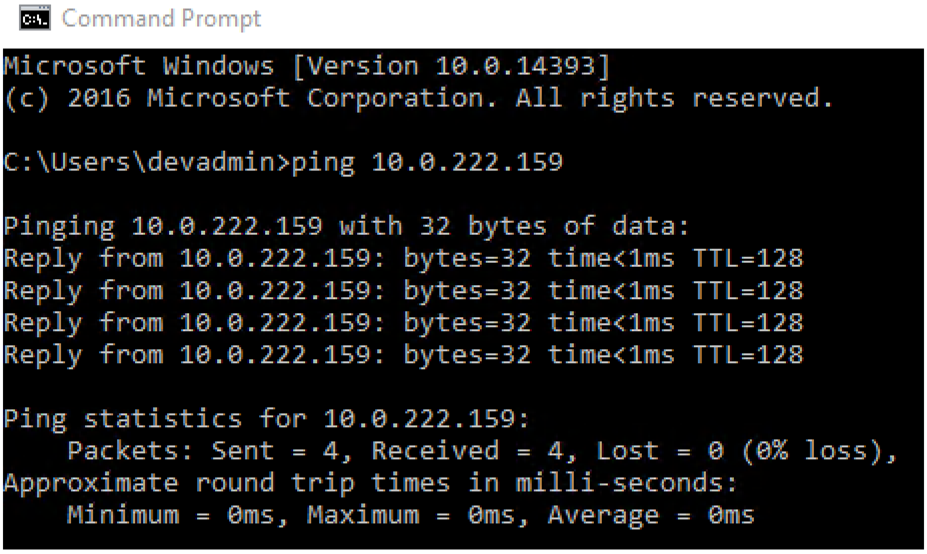
1. Run Command prompt by entering [cmd] in search field (magnifier icon at the bottom left of the screen) > test the ping and check the status

Host A



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\devadmin>ping 10.0.222.159

Pinging 10.0.222.159 with 32 bytes of data:
Reply from 10.0.222.159: bytes=32 time<1ms TTL=128
Reply from 10.0.222.159: bytes=32 time<1ms TTL=128
Reply from 10.0.222.159: bytes=32 time<1ms TTL=128
Reply from 10.0.222.159: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.222.159:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Host B

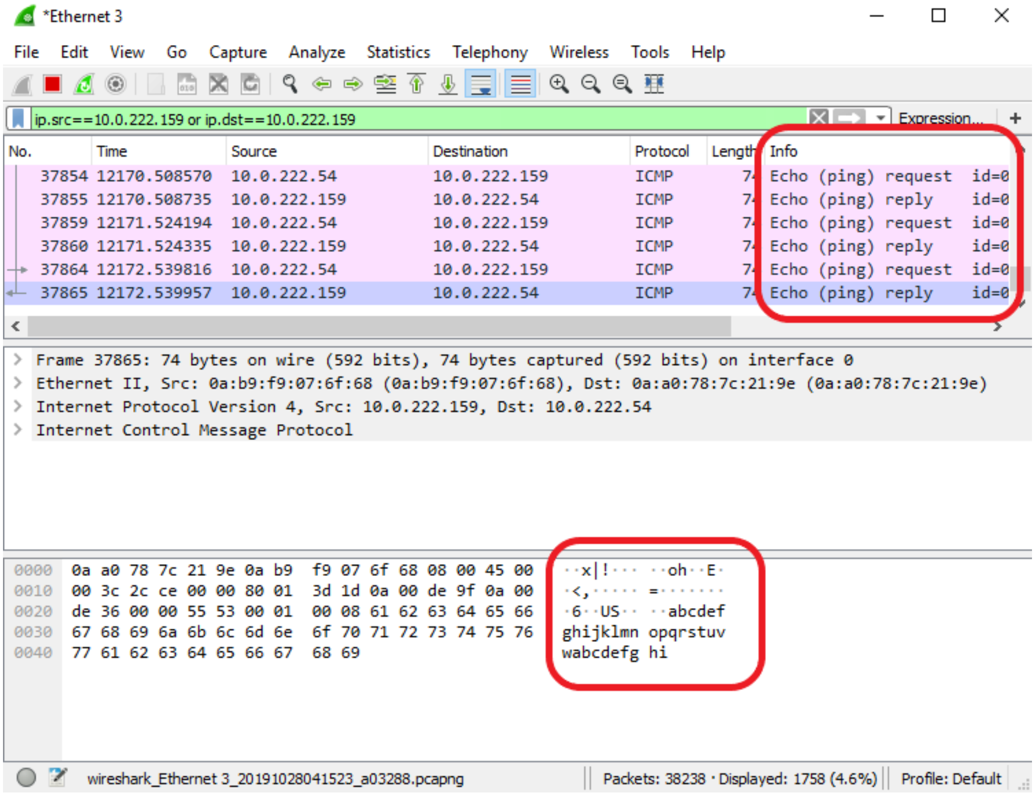


```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\devadmin>ping 10.0.222.159

Pinging 10.0.222.159 with 32 bytes of data:
Reply from 10.0.222.159: bytes=32 time<1ms TTL=128
Reply from 10.0.222.159: bytes=32 time<1ms TTL=128
Reply from 10.0.222.159: bytes=32 time<1ms TTL=128
Reply from 10.0.222.159: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.222.159:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2. Run Packet monitoring by WireShark

[Before applying IPsec]

Host A


*Ethernet 3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

ip.src==10.0.222.159 or ip.dst==10.0.222.159

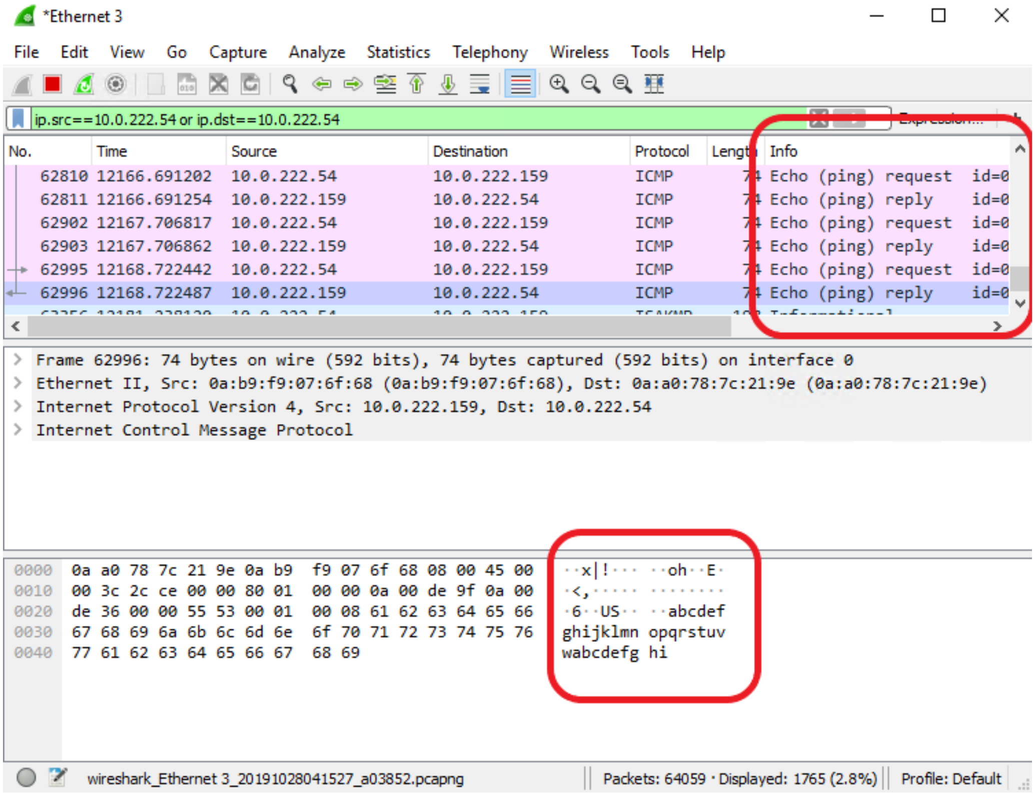
```
No.   Time          Source         Destination    Protocol  Length  Info
37854 12170.508570  10.0.222.54    10.0.222.159   ICMP      74      Echo (ping) request  id=0
37855 12170.508735  10.0.222.159   10.0.222.54    ICMP      74      Echo (ping) reply    id=0
37859 12171.524194  10.0.222.54    10.0.222.159   ICMP      74      Echo (ping) request  id=0
37860 12171.524335  10.0.222.159   10.0.222.54    ICMP      74      Echo (ping) reply    id=0
37864 12172.539816  10.0.222.54    10.0.222.159   ICMP      74      Echo (ping) request  id=0
37865 12172.539957  10.0.222.159   10.0.222.54    ICMP      74      Echo (ping) reply    id=0
```

```
> Frame 37865: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: 0a:b9:f9:07:6f:68 (0a:b9:f9:07:6f:68), Dst: 0a:a0:78:7c:21:9e (0a:a0:78:7c:21:9e)
> Internet Protocol Version 4, Src: 10.0.222.159, Dst: 10.0.222.54
> Internet Control Message Protocol
```

```
0000  0a a0 78 7c 21 9e 0a b9  f9 07 6f 68 08 00 45 00   ··x|!···  ··oh··E·
0010  00 3c 2c ce 00 00 80 01  3d 1d 0a 00 de 9f 0a 00   ·<,·····  =·······
0020  de 36 00 00 55 53 00 01  00 08 61 62 63 64 65 66   ·6··US··  ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn  opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg  hi
```

wireshark_Ethernet 3_20191028041523_a03288.pcapng | Packets: 38238 · Displayed: 1758 (4.6%) | Profile: Default

Host B


*Ethernet 3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

ip.src==10.0.222.54 or ip.dst==10.0.222.54

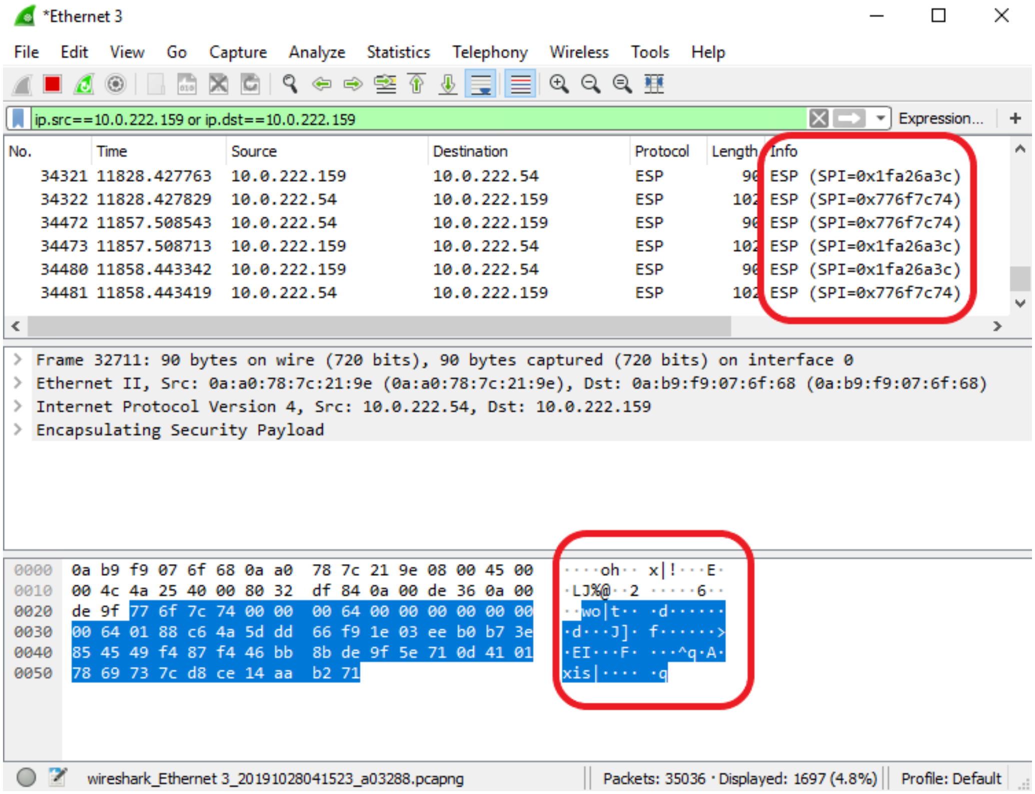
```
No.   Time          Source         Destination    Protocol  Length  Info
62810 12166.691202  10.0.222.54    10.0.222.159   ICMP      74      Echo (ping) request  id=0
62811 12166.691254  10.0.222.159   10.0.222.54    ICMP      74      Echo (ping) reply    id=0
62902 12167.706817  10.0.222.54    10.0.222.159   ICMP      74      Echo (ping) request  id=0
62903 12167.706862  10.0.222.159   10.0.222.54    ICMP      74      Echo (ping) reply    id=0
62995 12168.722442  10.0.222.54    10.0.222.159   ICMP      74      Echo (ping) request  id=0
62996 12168.722487  10.0.222.159   10.0.222.54    ICMP      74      Echo (ping) reply    id=0
```

```
> Frame 62996: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: 0a:b9:f9:07:6f:68 (0a:b9:f9:07:6f:68), Dst: 0a:a0:78:7c:21:9e (0a:a0:78:7c:21:9e)
> Internet Protocol Version 4, Src: 10.0.222.159, Dst: 10.0.222.54
> Internet Control Message Protocol
```

```
0000  0a a0 78 7c 21 9e 0a b9  f9 07 6f 68 08 00 45 00   ··x|!···  ··oh··E·
0010  00 3c 2c ce 00 00 80 01  00 00 0a 00 de 9f 0a 00   ·<,·····  ········
0020  de 36 00 00 55 53 00 01  00 08 61 62 63 64 65 66   ·6··US··  ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn  opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg  hi
```

wireshark_Ethernet 3_20191028041527_a03852.pcapng | Packets: 64059 · Displayed: 1765 (2.8%) | Profile: Default

[After applying IPsec]
The packet shows its encapsulation after applying IPsec as below.
Host A


*Ethernet 3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

ip.src==10.0.222.159 or ip.dst==10.0.222.159

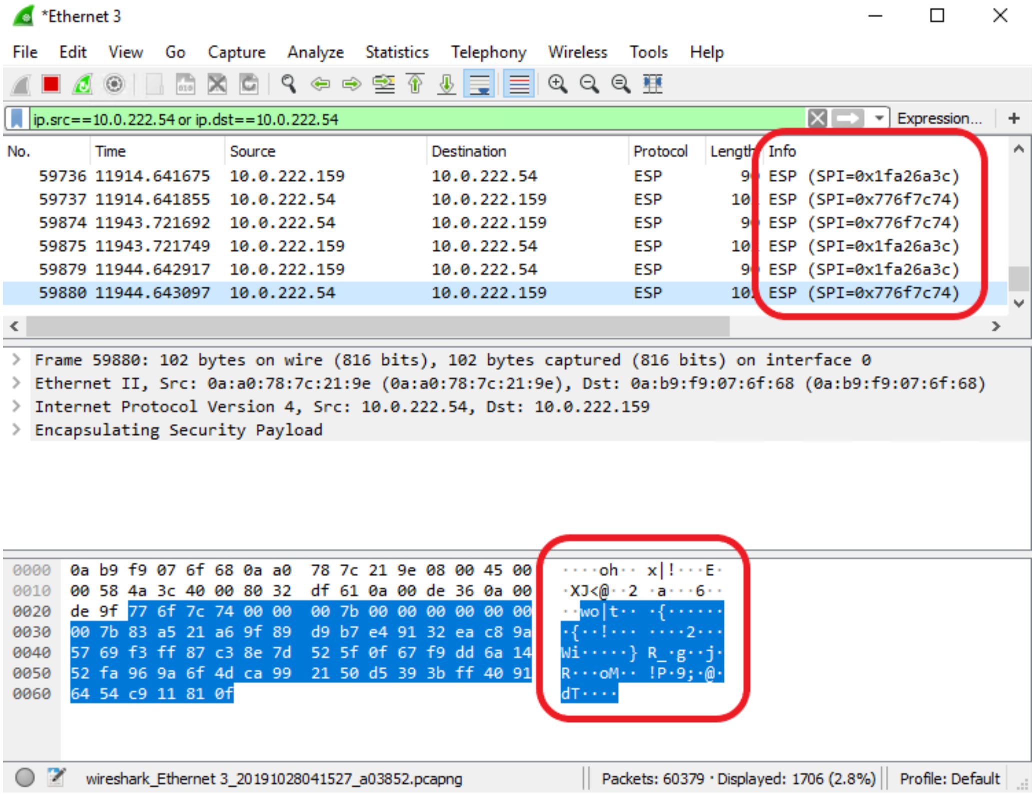
```
No.     Time         Source         Destination    Protocol  Length Info
  34321 11828.427763 10.0.222.159   10.0.222.54    ESP        90 ESP (SPI=0x1fa26a3c)
  34322 11828.427829 10.0.222.54    10.0.222.159   ESP       102 ESP (SPI=0x776f7c74)
  34472 11857.508543 10.0.222.54    10.0.222.159   ESP        90 ESP (SPI=0x776f7c74)
  34473 11857.508713 10.0.222.159   10.0.222.54    ESP       102 ESP (SPI=0x1fa26a3c)
  34480 11858.443342 10.0.222.159   10.0.222.54    ESP        90 ESP (SPI=0x1fa26a3c)
  34481 11858.443419 10.0.222.54    10.0.222.159   ESP       102 ESP (SPI=0x776f7c74)
```

```
> Frame 32711: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
> Ethernet II, Src: 0a:a0:78:7c:21:9e (0a:a0:78:7c:21:9e), Dst: 0a:b9:f9:07:6f:68 (0a:b9:f9:07:6f:68)
> Internet Protocol Version 4, Src: 10.0.222.54, Dst: 10.0.222.159
> Encapsulating Security Payload
```

```
0000  0a b9 f9 07 6f 68 0a a0  78 7c 21 9e 08 00 45 00   ····oh·· x|!···E·
0010  00 4c 4a 25 40 00 80 32  df 84 0a 00 de 36 0a 00   ·LJ%@··2 ·····6··
0020  de 9f 77 6f 7c 74 00 00  00 64 00 00 00 00 00 00   ··wo|t·· ·d······
0030  00 64 01 88 c6 4a 5d dd  66 f9 1e 03 ee b0 b7 3e   ·d···J]· f······>
0040  85 45 49 f4 87 f4 46 bb  8b de 9f 5e 71 0d 41 01   ·EI···F· ···^q·A·
0050  78 69 73 7c d8 ce 14 aa  b2 71                     xis|···· ·q
```

wireshark_Ethernet 3_20191028041523_a03288.pcapng | Packets: 35036 · Displayed: 1697 (4.8%) | Profile: Default

Host B


*Ethernet 3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

ip.src==10.0.222.54 or ip.dst==10.0.222.54

```
No.     Time         Source         Destination    Protocol  Length Info
  59736 11914.641675 10.0.222.159   10.0.222.54    ESP         9 ESP (SPI=0x1fa26a3c)
  59737 11914.641855 10.0.222.54    10.0.222.159   ESP        10 ESP (SPI=0x776f7c74)
  59874 11943.721692 10.0.222.54    10.0.222.159   ESP         9 ESP (SPI=0x776f7c74)
  59875 11943.721749 10.0.222.159   10.0.222.54    ESP        10 ESP (SPI=0x1fa26a3c)
  59879 11944.642917 10.0.222.159   10.0.222.54    ESP         9 ESP (SPI=0x1fa26a3c)
  59880 11944.643097 10.0.222.54    10.0.222.159   ESP        10 ESP (SPI=0x776f7c74)
```

```
> Frame 59880: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
> Ethernet II, Src: 0a:a0:78:7c:21:9e (0a:a0:78:7c:21:9e), Dst: 0a:b9:f9:07:6f:68 (0a:b9:f9:07:6f:68)
> Internet Protocol Version 4, Src: 10.0.222.54, Dst: 10.0.222.159
> Encapsulating Security Payload
```

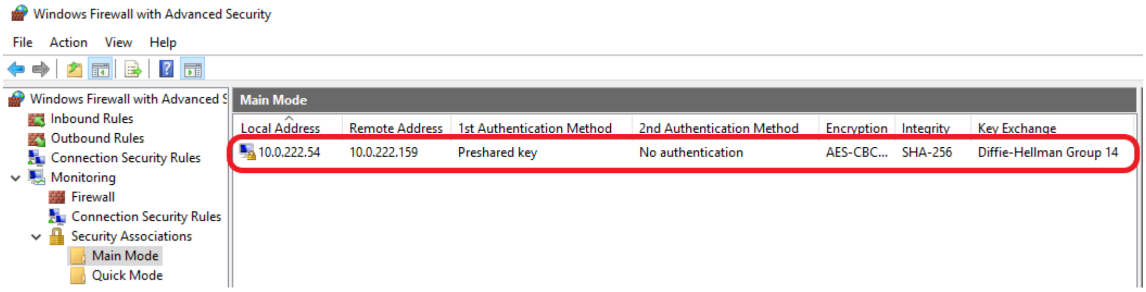
```
0000  0a b9 f9 07 6f 68 0a a0  78 7c 21 9e 08 00 45 00   ····oh·· x|!···E·
0010  00 58 4a 3c 40 00 80 32  df 61 0a 00 de 36 0a 00   ·XJ<@··2 ·a···6··
0020  de 9f 77 6f 7c 74 00 00  00 7b 00 00 00 00 00 00   ··wo|t·· ·{······
0030  00 7b 83 a5 21 a6 9f 89  d9 b7 e4 91 32 ea c8 9a   ·{··!··· ····2···
0040  57 69 f3 ff 87 c3 8e 7d  52 5f 0f 67 f9 dd 6a 14   Wi·····} R_·g··j·
0050  52 fa 96 9a 6f 4d ca 99  21 50 d5 39 3b ff 40 91   R···oM·· !P·9;·@·
0060  64 54 c9 11 81 0f                                  dT····
```

wireshark_Ethernet 3_20191028041527_a03852.pcapng | Packets: 60379 · Displayed: 1706 (2.8%) | Profile: Default

3. Verify SA

Main mode

Go to [Monitoring] → [Security Associations] → Main Mode

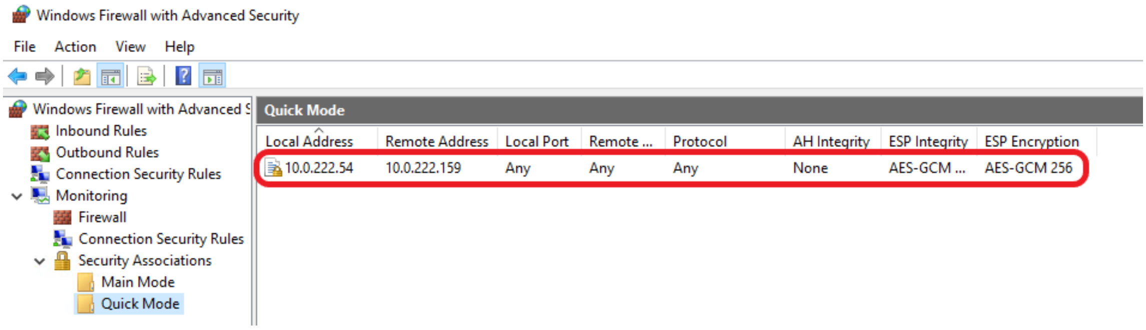

Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advanced S
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Firewall
Connection Security Rules
Security Associations
Main Mode
Quick Mode

Main Mode

Local Address	Remote Address	1st Authentication Method	2nd Authentication Method	Encryption	Integrity	Key Exchange
10.0.222.54	10.0.222.159	Preshared key	No authentication	AES-CBC...	SHA-256	Diffie-Hellman Group 14

Quick mode

Go to [Monitoring] → [Security Associations] → Main Mode


Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advanced S
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Firewall
Connection Security Rules
Security Associations
Main Mode
Quick Mode

Quick Mode

Local Address	Remote Address	Local Port	Remote ...	Protocol	AH Integrity	ESP Integrity	ESP Encryption
10.0.222.54	10.0.222.159	Any	Any	Any	None	AES-GCM ...	AES-GCM 256

(End of document)

Realize your vision SAMSUNG SDS

www.samsungsds.com