Implemeting IPSec in Windows Domain – part 1

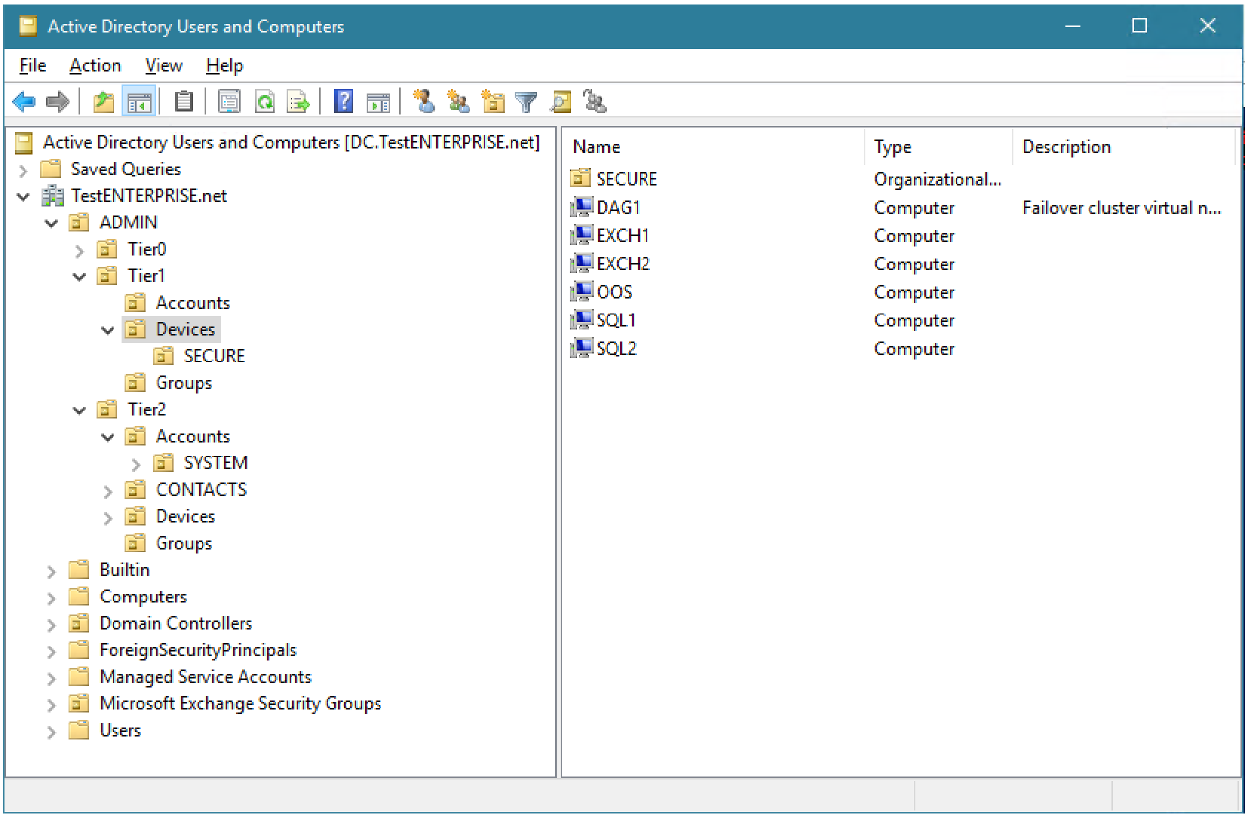
michaelfirsov.wordpress.com/implemeting-ipsec-in-windows-domain-part-1

October 31, 2019

In this article I'd like to show how administrators can use IPSec to protect the most valuable "assets" in their networks – for example, servers that runs HR or financial databases. Lots of articles on msdn/technet offer one of the following methods to secure the traffic – domain isolation or/and server isolation. The first one is supposed to restrict traffic flow only to the domain members while the latter is often regarded as the extra security layer to the domain isolation that further restricts access to some host(s) only to member of certain computer or user groups. My point is that sometimes we may deploy some form of server isolation by not restricting already established security policies (domain isolation) with the additional computer/user checking but simply by applying the connection security rules to the respective organizational units (OUs).

Consider the following task: only specific clients (say HR department users) should have access to the host with HR database. The easiest way to achieve this is to create a server GPO with the connection security rules which would require IPSec protection for all inbound traffic (and only request the protection for outbound traffic) and a client GPO which would request protection for both inbound and outbound traffic. Applying the server GPO to the OU containing the server computer account (or accounts) and the client GPO to the OU with the needed client computer accounts will result in the required server isolation – in this case grouping the server and client computer accounts into specific OUs will serve the same purpose as resticting access based on the computer/use group membership.

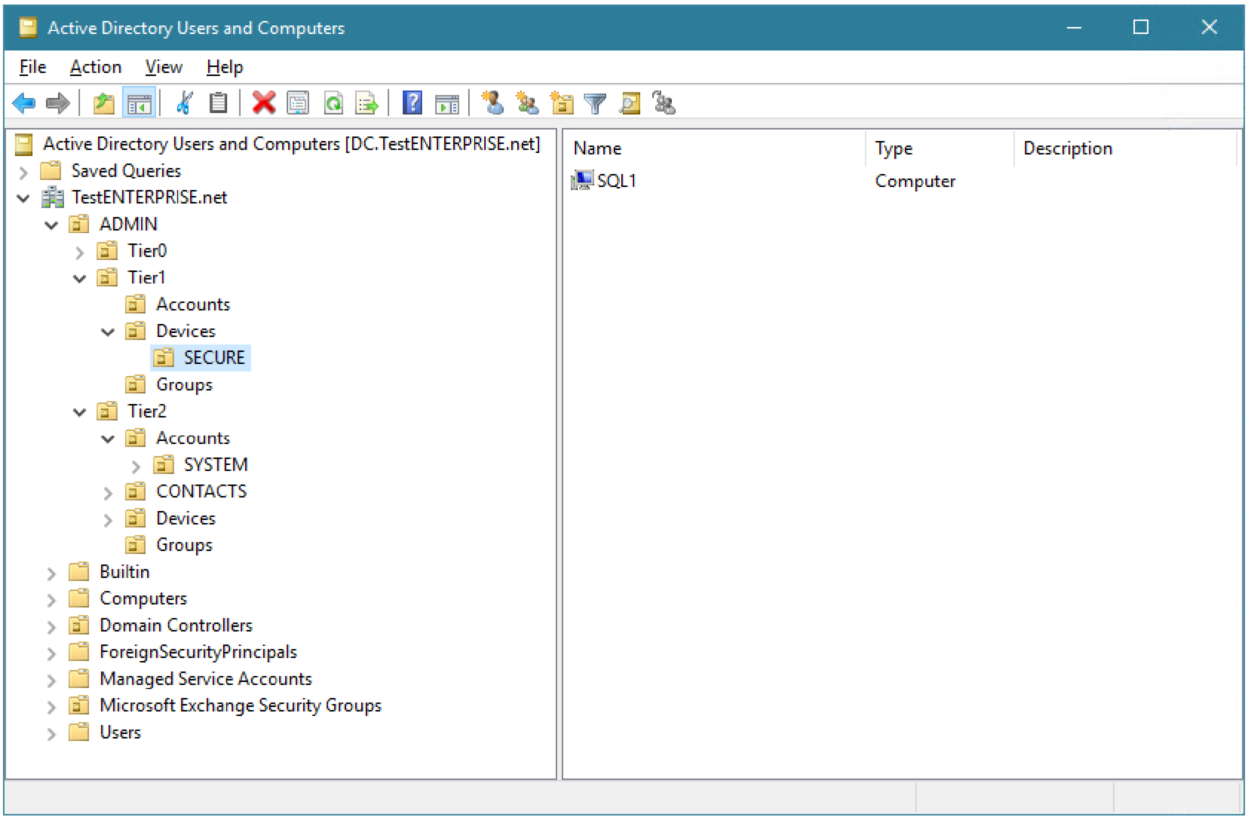
Suppose the server that hosts the database with sensitive information is SQL1 –



- Active Directory Users and Computers [DC.TestENTERPRISE.net]
  - Saved Queries
  - TestENTERPRISE.net
    - ADMIN
      - Tier0
      - Tier1
        - Accounts
        - Devices
          - SECURE
        - Groups
      - Tier2
        - Accounts
          - SYSTEM
        - CONTACTS
        - Devices
        - Groups
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - Managed Service Accounts
    - Microsoft Exchange Security Groups
    - Users

Name	Type	Description
SECURE	Organizational...	
DAG1	Computer	Failover cluster virtual n...
EXCH1	Computer	
EXCH2	Computer	
OOS	Computer	
SQL1	Computer	
SQL2	Computer	

so the first step is to create a new OU – Devices\SECURE – and move the server into it:

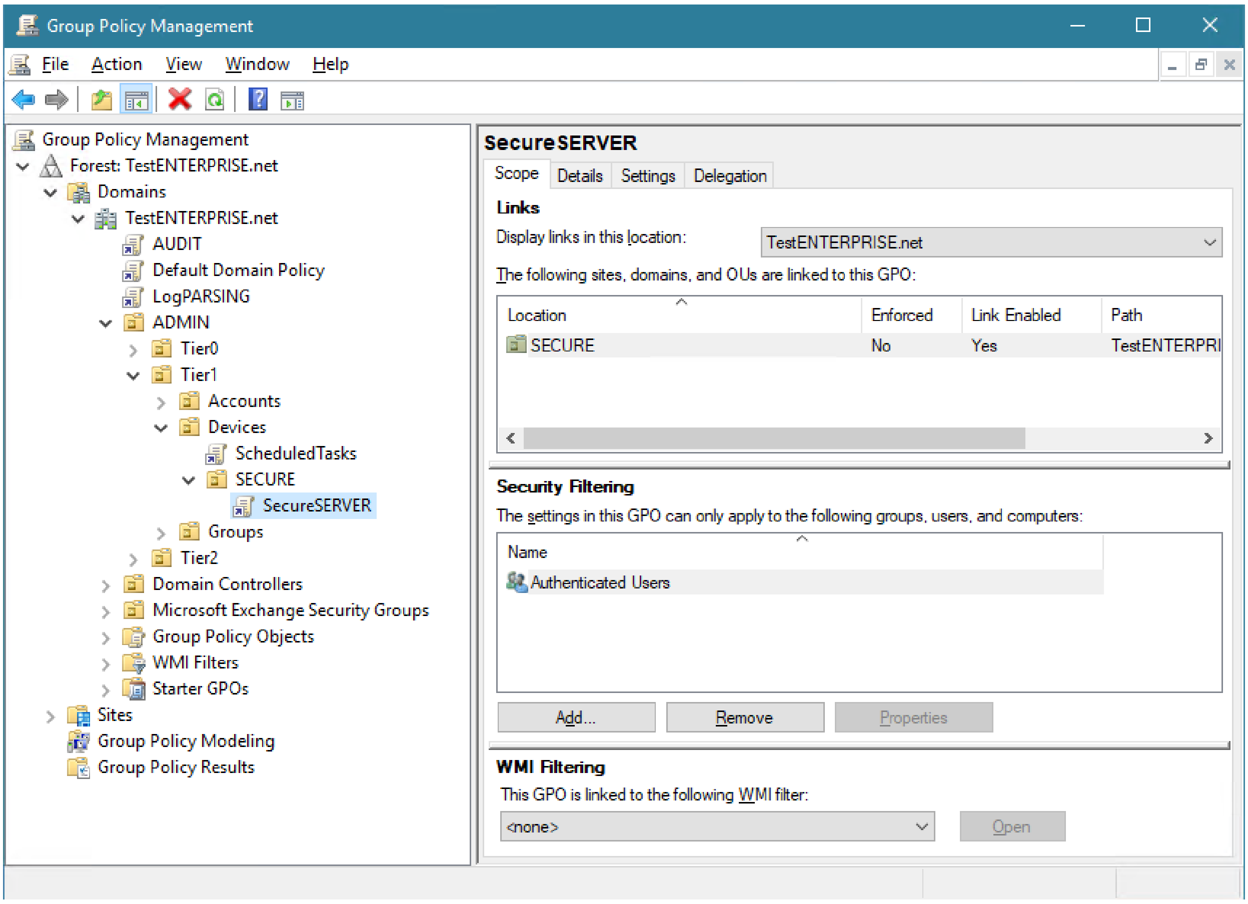


- Active Directory Users and Computers [DC.TestENTERPRISE.net]
  - Saved Queries
  - TestENTERPRISE.net
    - ADMIN
      - Tier0
      - Tier1
        - Accounts
        - Devices
          - SECURE
        - Groups
      - Tier2
        - Accounts
          - SYSTEM
        - CONTACTS
        - Devices
        - Groups
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - Managed Service Accounts
    - Microsoft Exchange Security Groups
    - Users

Name	Type	Description
SQL1	Computer	

Advertisements
Report this adPrivacy

SecureSERVER is a new GPO for which we'll create the new connection security rule that will require authentication for the inbound connections.



SecureSERVER

Links

Display links in this location: TestENTERPRISE.net

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
SECURE	No	Yes	TestENTERPRI

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

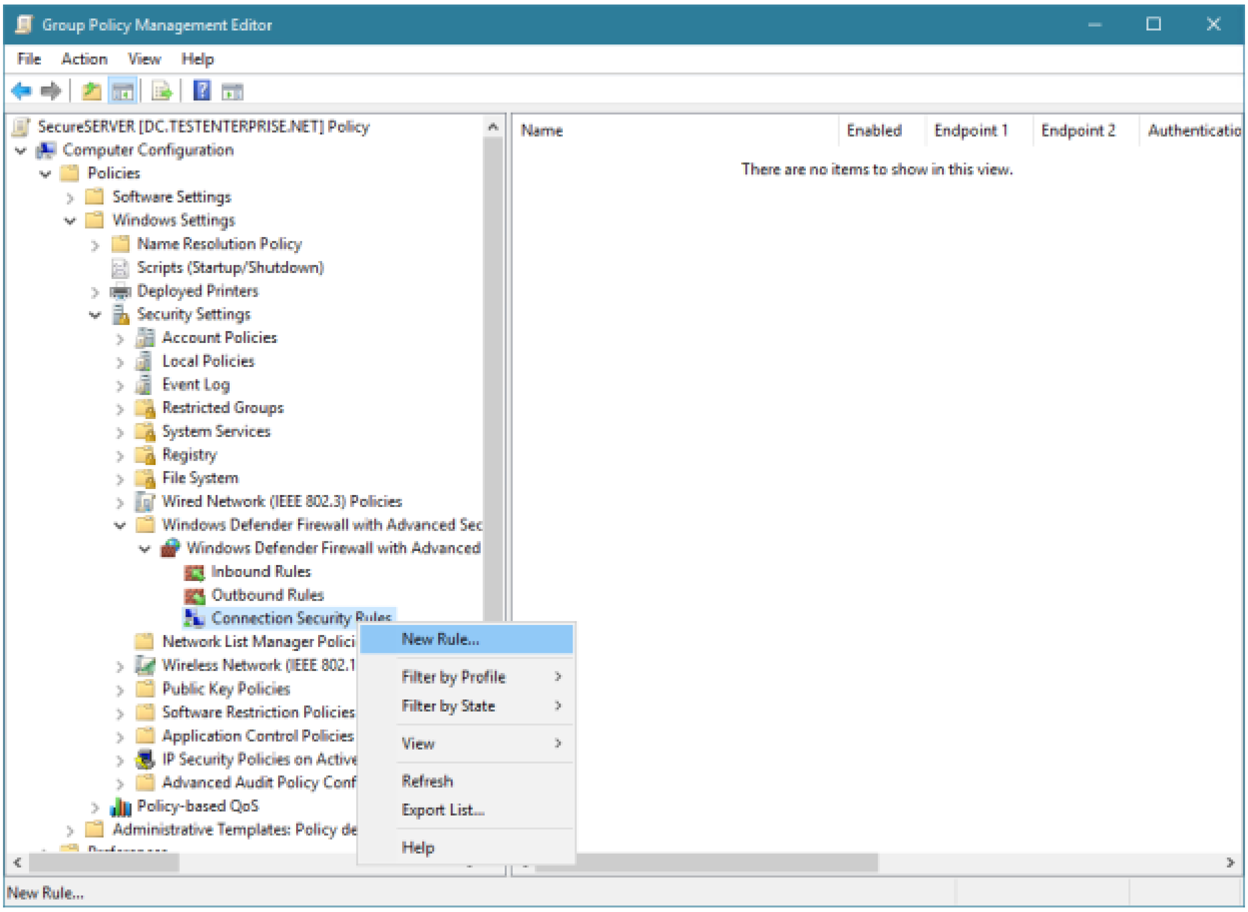
Name
Authenticated Users

WMI Filtering

This GPO is linked to the following WMI filter:

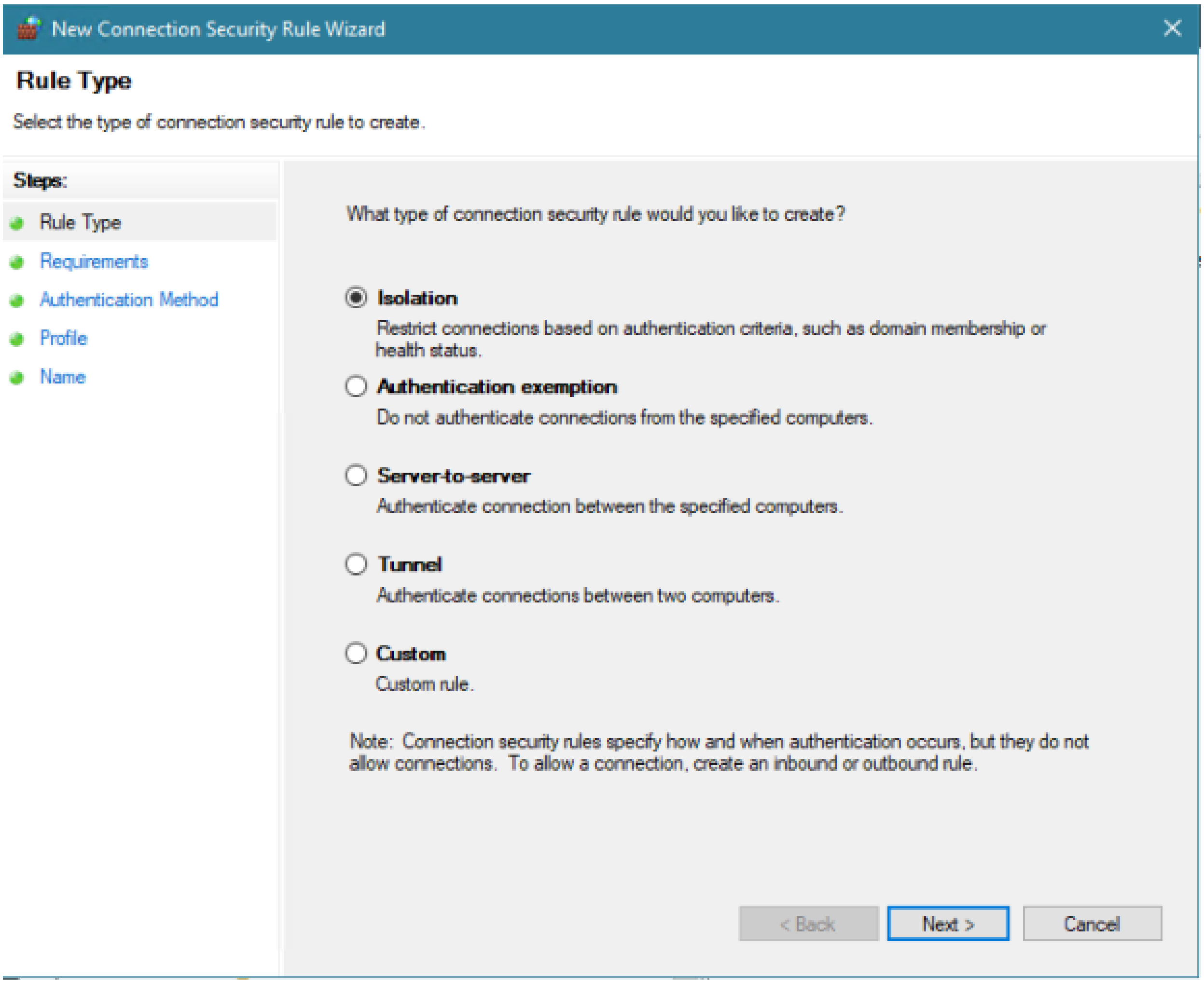
<none>

Now let’s create the new rule:


Group Policy Management Editor
File Action View Help
SecureSERVER [DC.TESTENTERPRISE.NET] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced Sec
Windows Defender Firewall with Advanced
Inbound Rules
Outbound Rules
Connection Security Rules
Network List Manager Polici
Wireless Network (IEEE 802.1
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active
Advanced Audit Policy Conf
Policy-based QoS
Administrative Templates: Policy de
New Rule...
Filter by Profile
Filter by State
View
Refresh
Export List...
Help
New Rule...

Name	Enabled	Endpoint 1	Endpoint 2	Authenticatio

There are no items to show in this view.



New Connection Security Rule Wizard

Rule Type

Select the type of connection security rule to create.

Steps:

- Rule Type
- Requirements
- Authentication Method
- Profile
- Name

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.

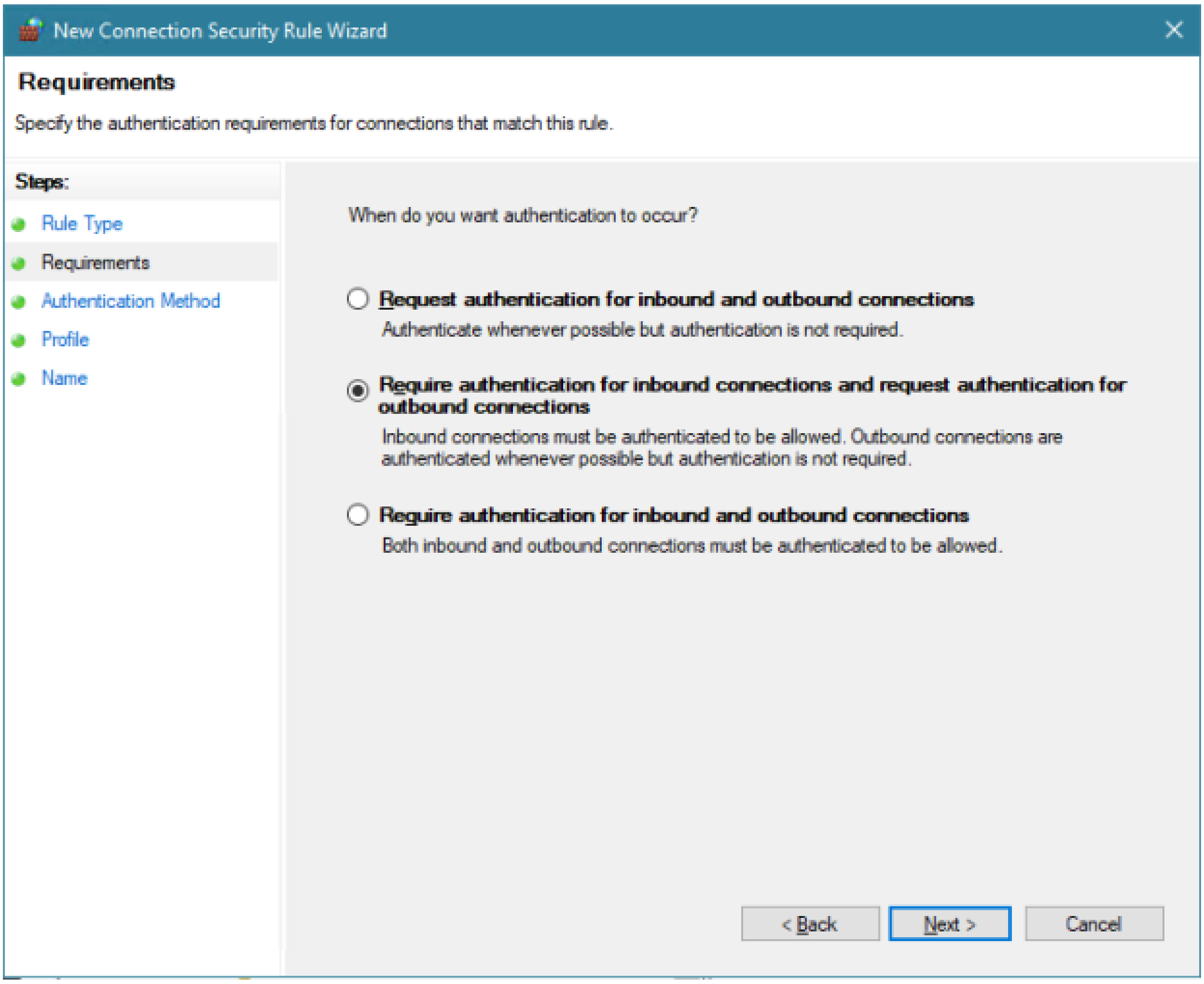
○ **Custom**
Custom rule.

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.

Advertisements

Report this adPrivacy

On the *Rule Type* page choose the type of the rule – **Isolation** and **Require authentication for inbound connections and request authentication for outbound connections** on the *Requirements* page:



New Connection Security Rule Wizard

Requirements

Specify the authentication requirements for connections that match this rule.

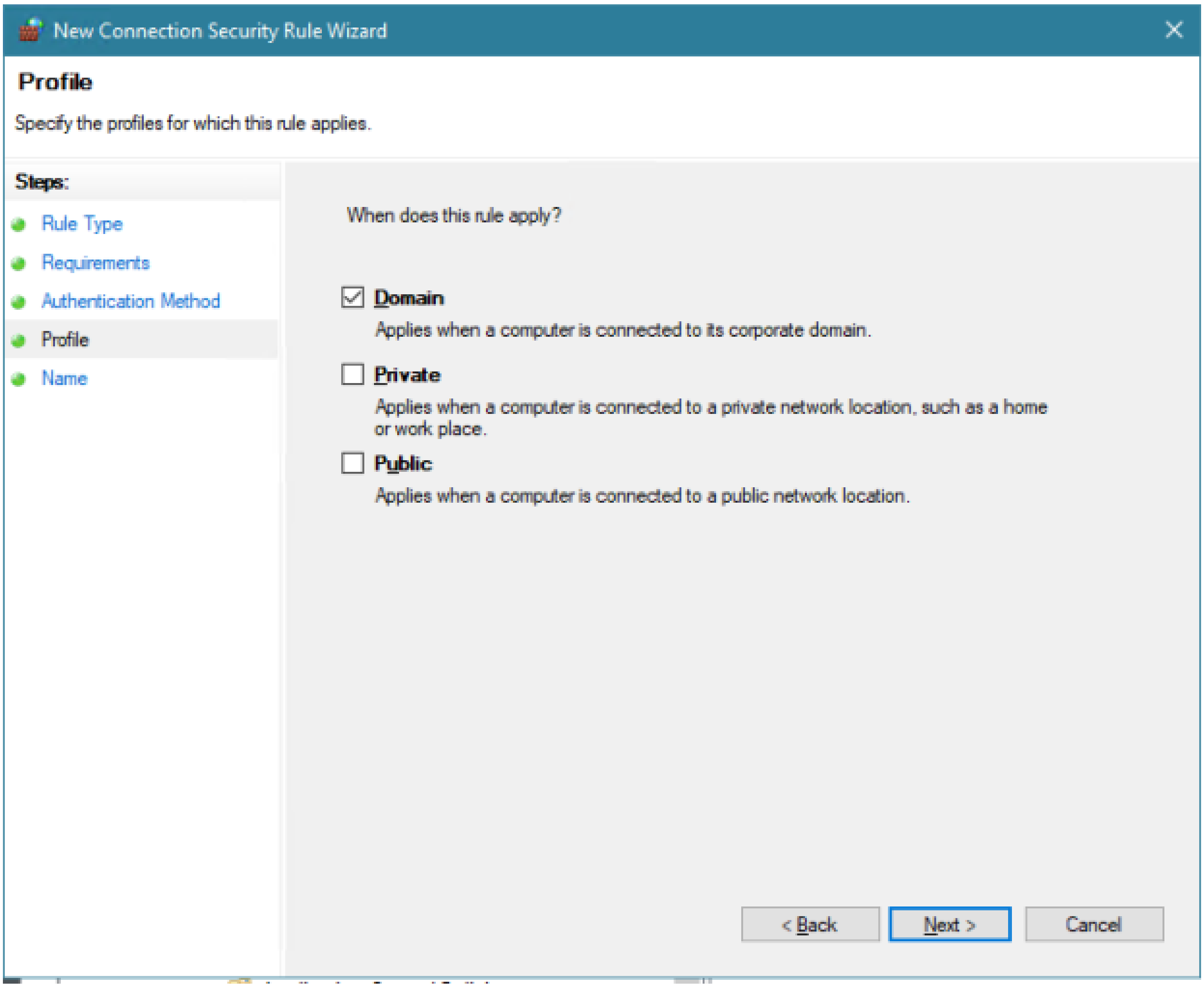
When do you want authentication to occur?

○ **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.

Since the new rule will use Kerberos authentication there's no need to choose anything except Domain here.



Profile

Specify the profiles for which this rule applies.

When does this rule apply?

☑ **Domain**

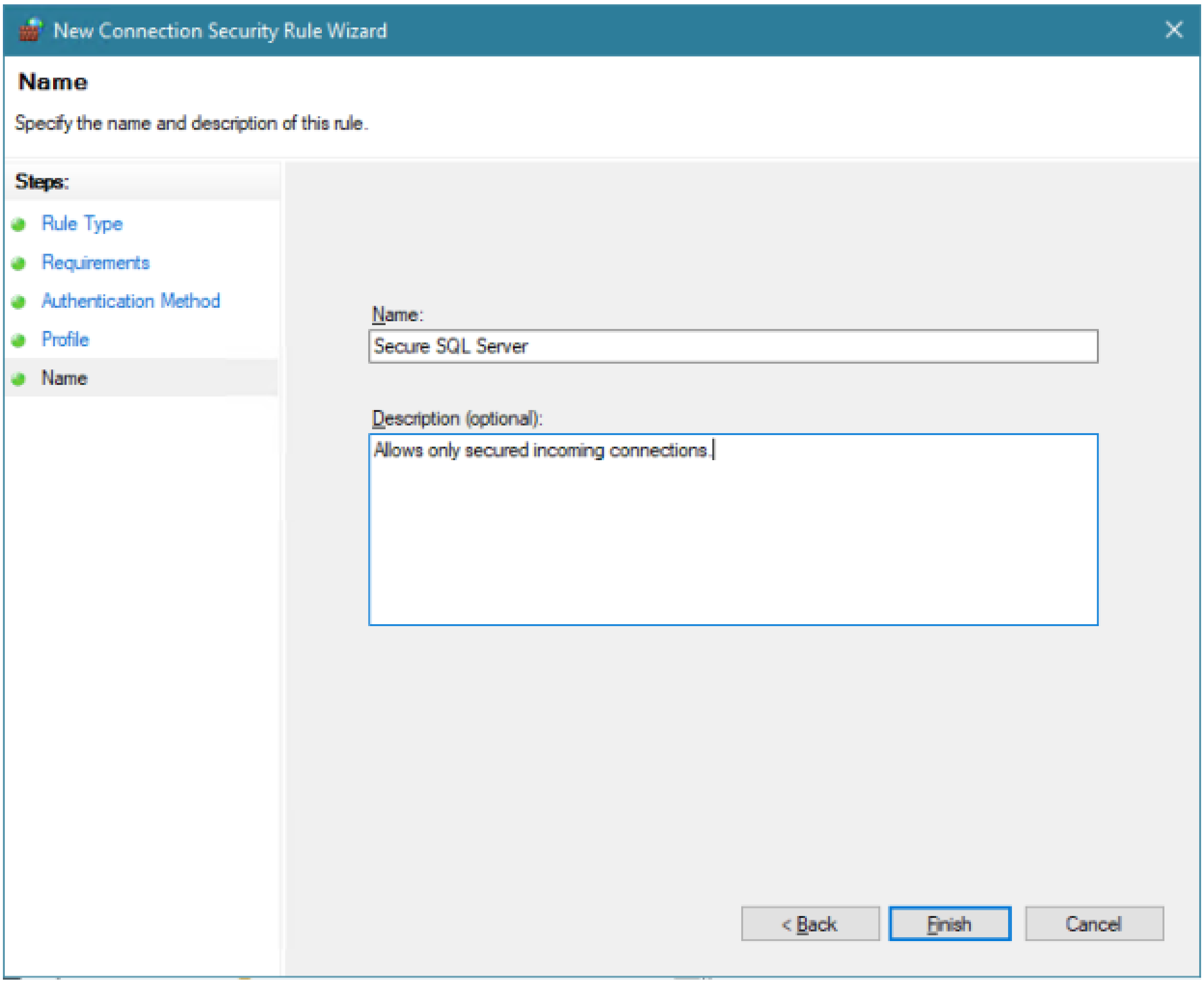
Applies when a computer is connected to its corporate domain.

□ **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.

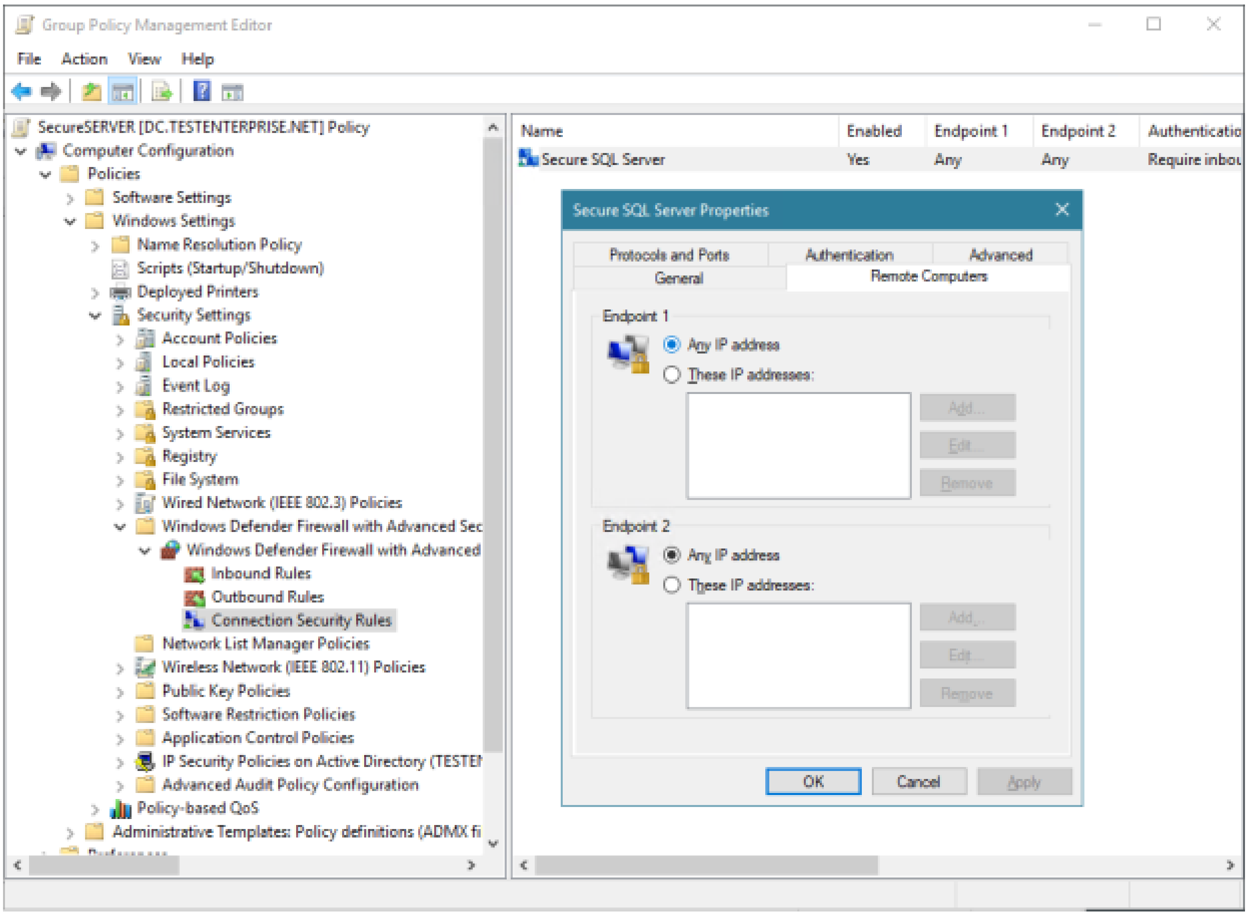

New Connection Security Rule Wizard
Name
Specify the name and description of this rule.
Steps:
Rule Type
Requirements
Authentication Method
Profile
Name
< Back
Finish
Cancel

Name: Secure SQL Server

Description (optional): Allows only secured incoming connections.

Advertisements
Report this adPrivacy

Again, since the target for this policy (and the rule) is defined by applying this GPO only to the specific OU, I won’t configure any endpoints for this rule.


Group Policy Management Editor
File Action View Help
SecureSERVER [DC.TESTENTERPRISE.NET] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced Sec
Windows Defender Firewall with Advanced
Inbound Rules
Outbound Rules
Connection Security Rules
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (TESTEN
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADMX fi
Secure SQL Server Properties
Protocols and Ports
Authentication
Advanced
General
Remote Computers
Add...
Edit...
Remove
OK
Cancel
Apply

Name	Enabled	Endpoint 1	Endpoint 2	Authenticatio
Secure SQL Server	Yes	Any	Any	Require inbou

Endpoint 1

● Any IP address

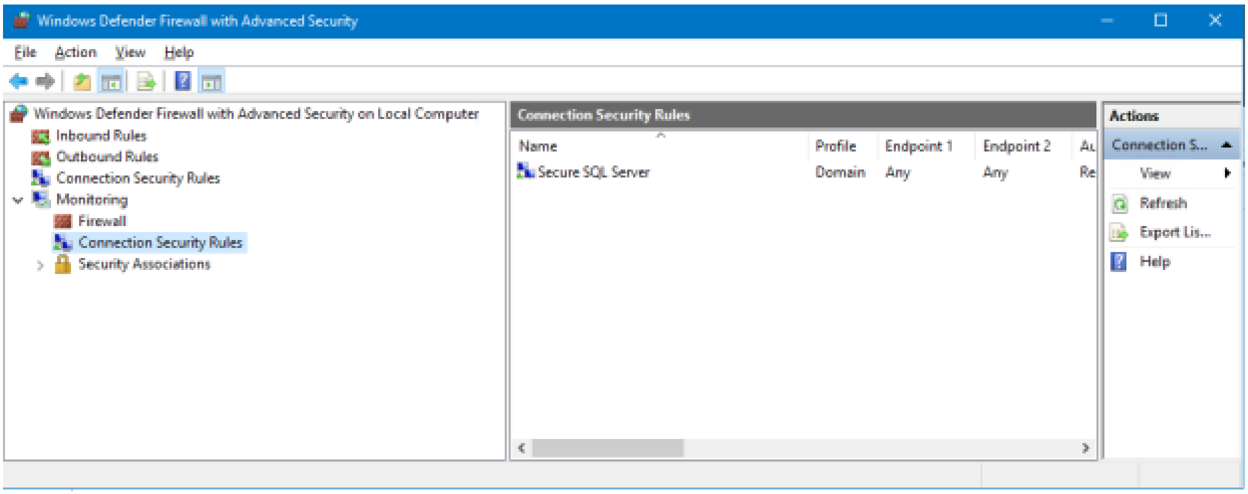
○ These IP addresses:

Endpoint 2

● Any IP address

○ These IP addresses:

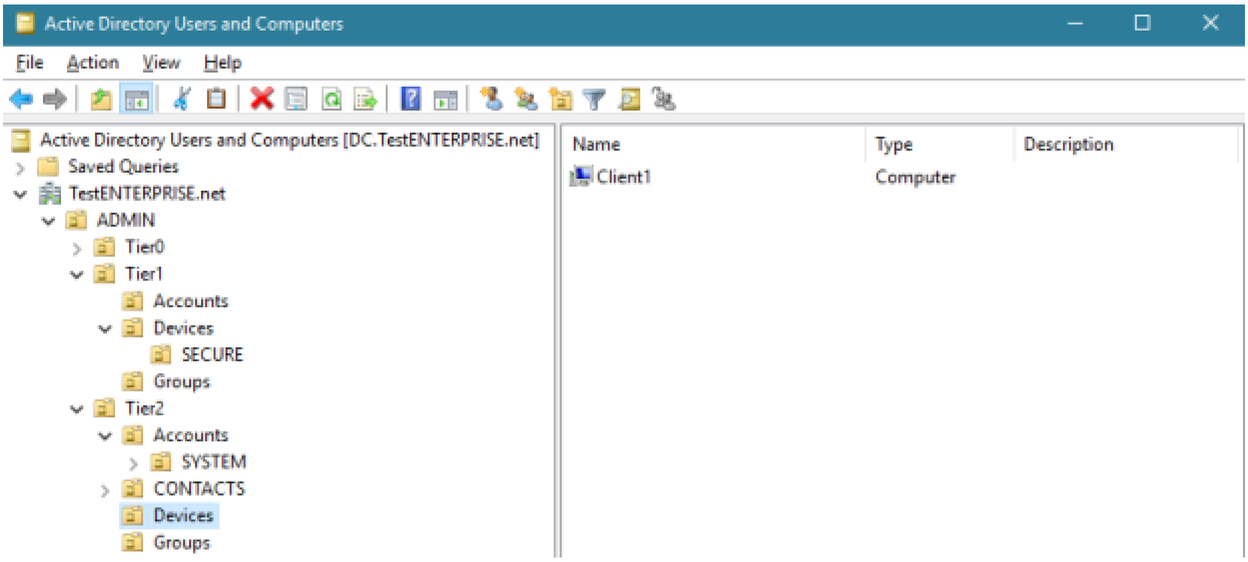
After running gpupdate /force on SQL1:


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall with Advanced Security on Local Computer
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Firewall
Connection Security Rules
Security Associations
Actions
Connection S...
View
Refresh
Export Lis...
Help

Connection Security Rules

Name	Profile	Endpoint 1	Endpoint 2	Au
Secure SQL Server	Domain	Any	Any	Re

The server-side policy is created – the next step is to create a GPO for users that should be able to connect to the SQL1 and create the client GPO – I'll create the SecureCONNECTIONS GPO and link it to the Tier2\Devices OU. It means any (client) computer which has its computer account placed in this GPO will be allowed to access the secure server (SQL1). In the production network it may be an OU at the deeper level but currently there's only one client computer account in my test network so I'll keep using this OU.



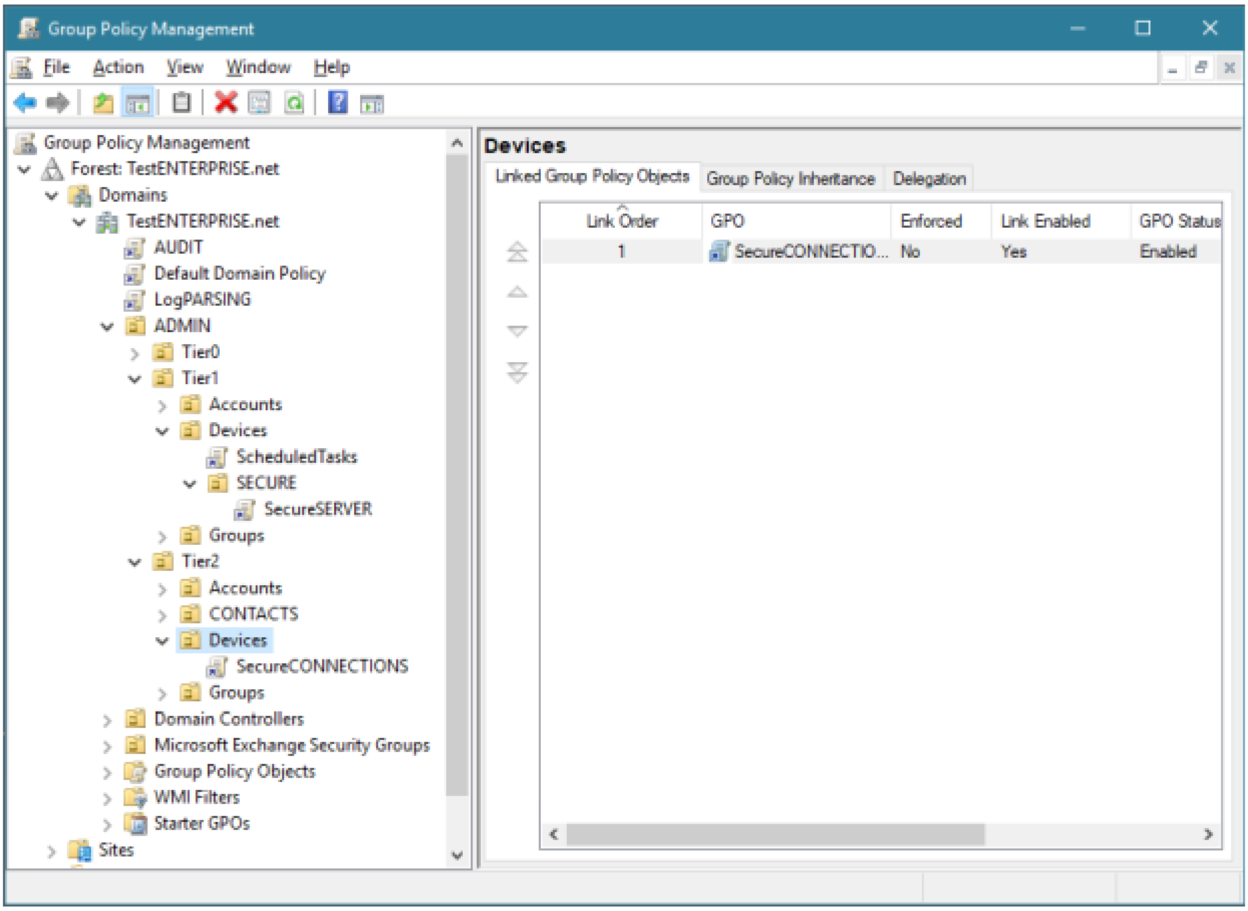
Active Directory Users and Computers

File Action View Help

Active Directory Users and Computers [DC.TestENTERPRISE.net]
- Saved Queries
- TestENTERPRISE.net
  - ADMIN
    - Tier0
    - Tier1
      - Accounts
      - Devices
        - SECURE
      - Groups
    - Tier2
      - Accounts
        - SYSTEM
      - CONTACTS
      - Devices
      - Groups

Name	Type	Description
Client1	Computer	

Advertisements
Report this adPrivacy



Group Policy Management

File Action View Window Help

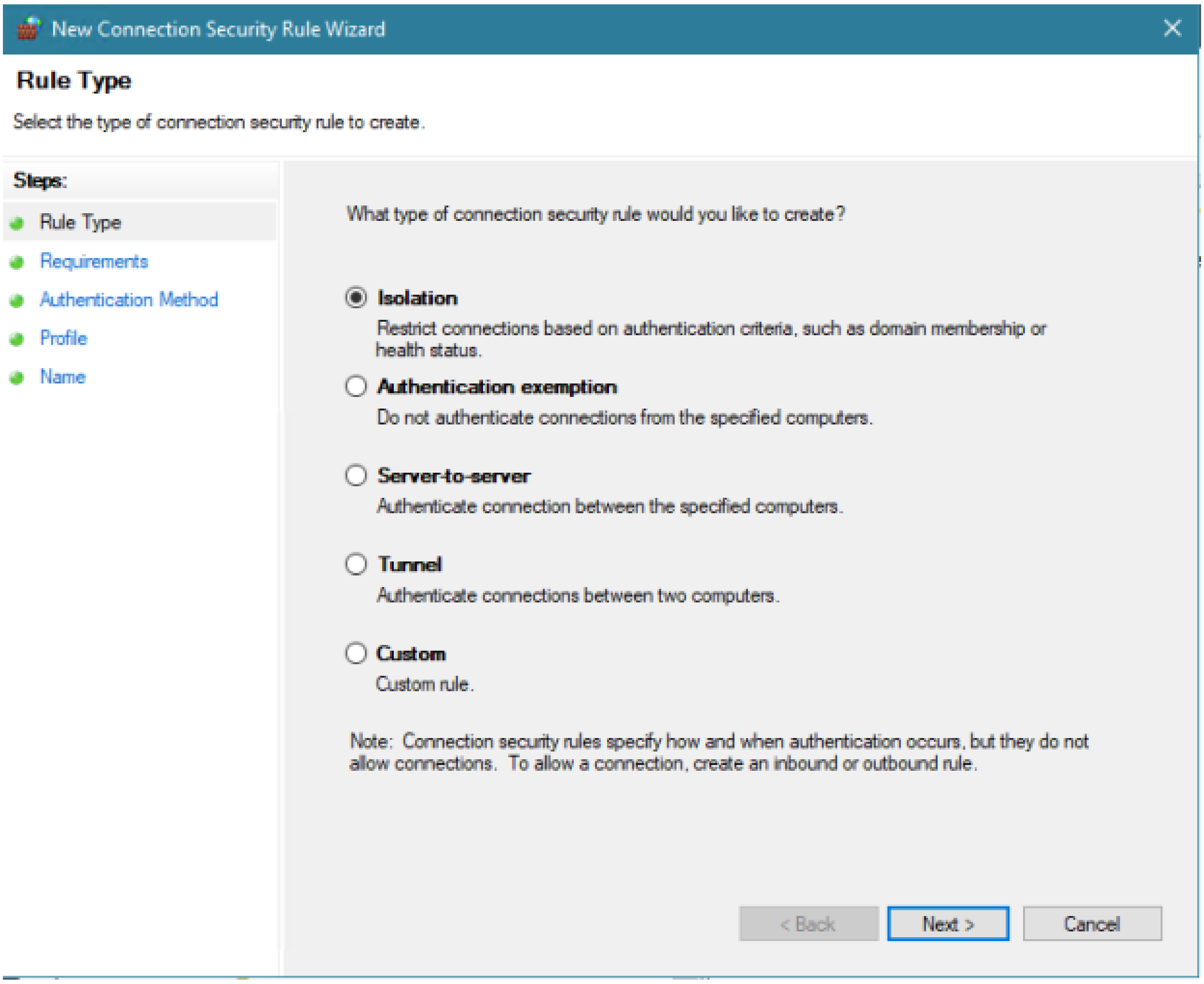
- Group Policy Management
  - Forest: TestENTERPRISE.net
    - Domains
      - TestENTERPRISE.net
        - AUDIT
        - Default Domain Policy
        - LogPARSING
        - ADMIN
          - Tier0
          - Tier1
            - Accounts
            - Devices
              - ScheduledTasks
              - SECURE
                - SecureSERVER
            - Groups
          - Tier2
            - Accounts
            - CONTACTS
            - Devices
              - SecureCONNECTIONS
            - Groups
        - Domain Controllers
        - Microsoft Exchange Security Groups
        - Group Policy Objects
        - WMI Filters
        - Starter GPOs
    - Sites

Devices

Linked Group Policy Objects | Group Policy Inheritance | Delegation

Link Order	GPO	Enforced	Link Enabled	GPO Status
1	SecureCONNECTIO...	No	Yes	Enabled

The new client connection security rule differs from the server one just in the **Requirements** tab (not speaking of the **Name** tab):



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.

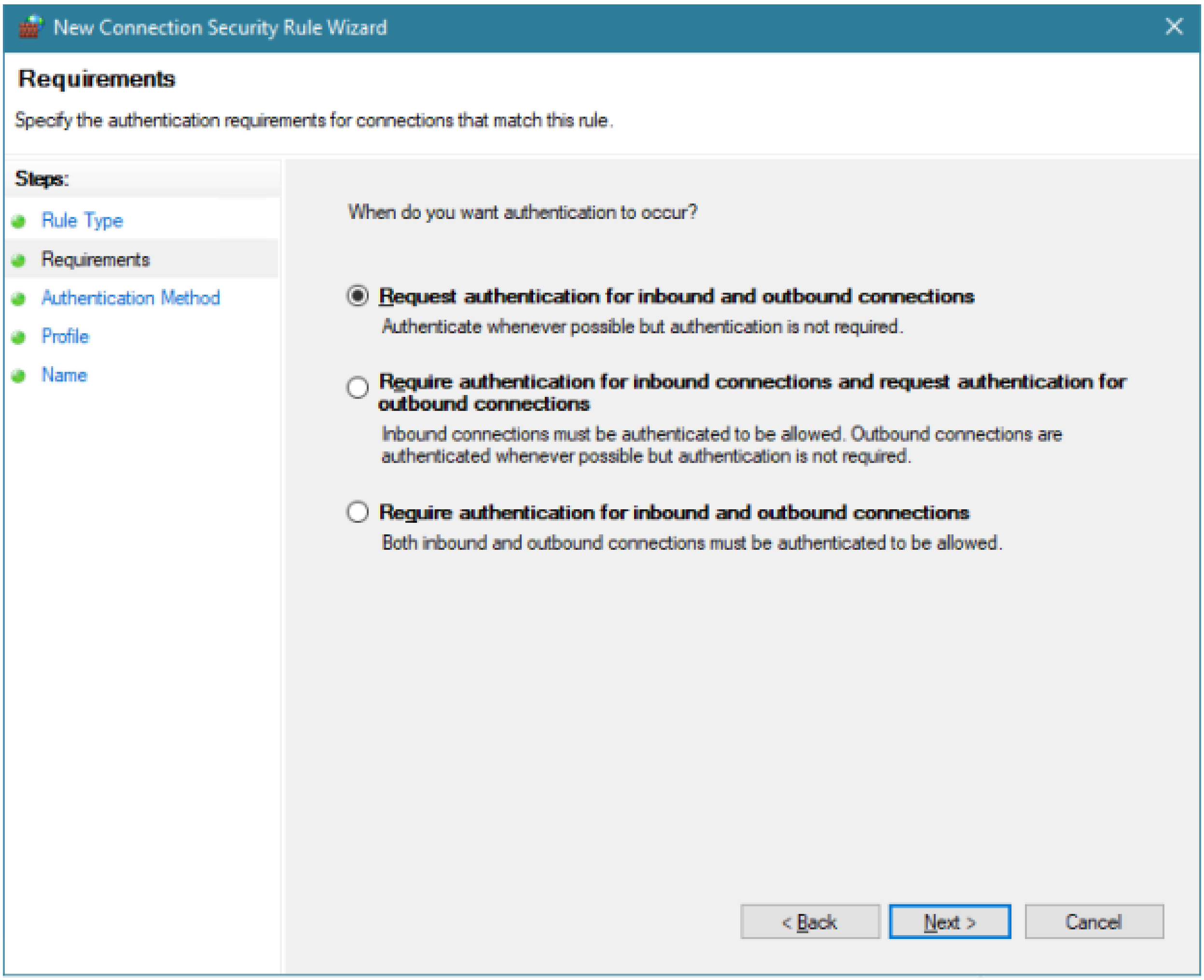
○ **Server-to-server**
Authenticate connection between the specified computers.

○ **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.

Clients should not require inbound connections to be authenticated – they just must be able to initiate a secure outbound connections (servers that require inbound authentication will respond with ipsec while all other hosts will reply as usually), so we select the first option here:



Requirements

Specify the authentication requirements for connections that match this rule.

When do you want authentication to occur?

● **Request authentication for inbound and outbound connections**

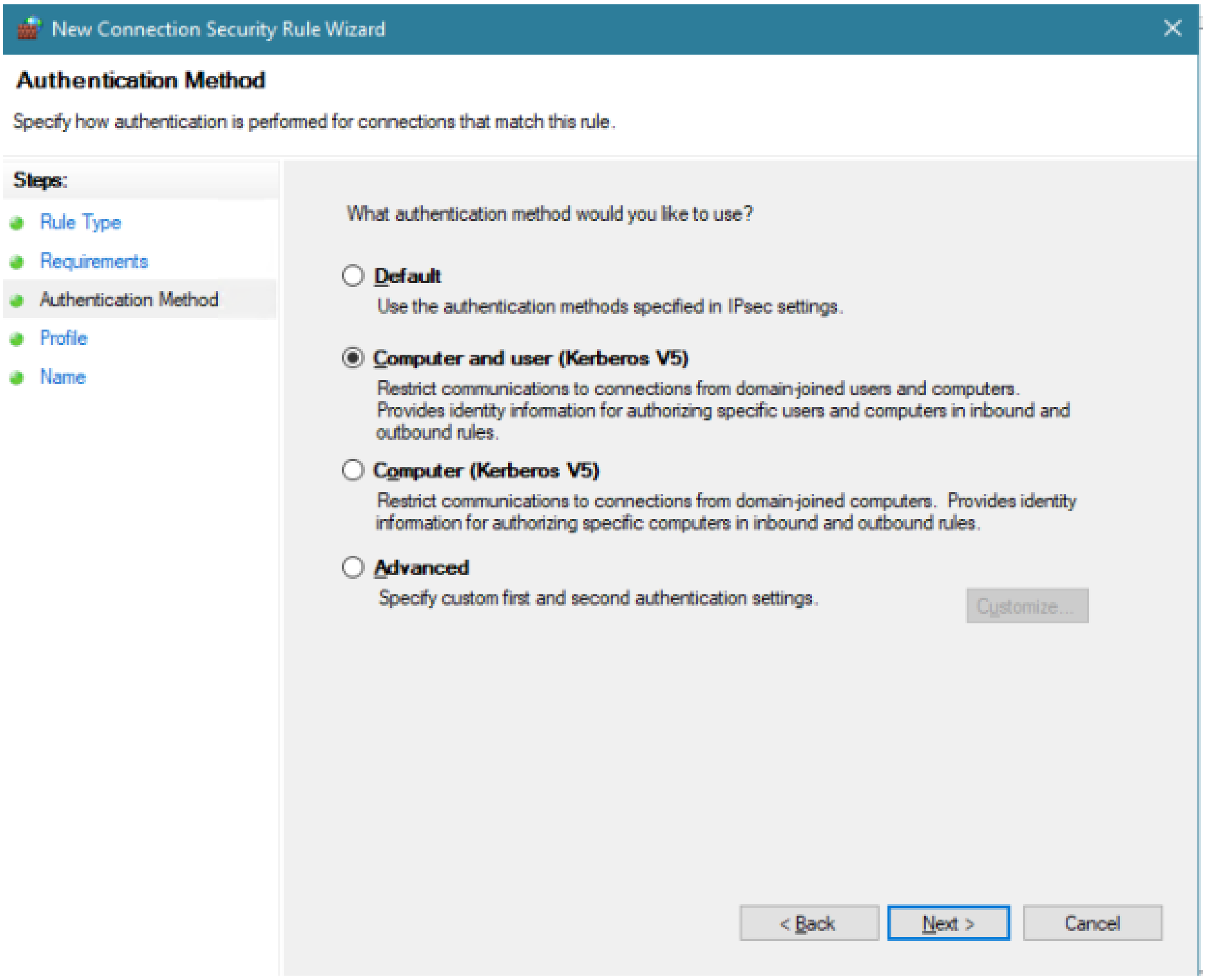
Authenticate whenever possible but authentication is not required.

○ **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.



New Connection Security Rule Wizard

Authentication Method

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

Steps:

- Rule Type
- Requirements
- Authentication Method
- Profile
- Name

What authentication method would you like to use?

○ **Default**

Use the authentication methods specified in IPsec settings.

● **Computer and user (Kerberos V5)**

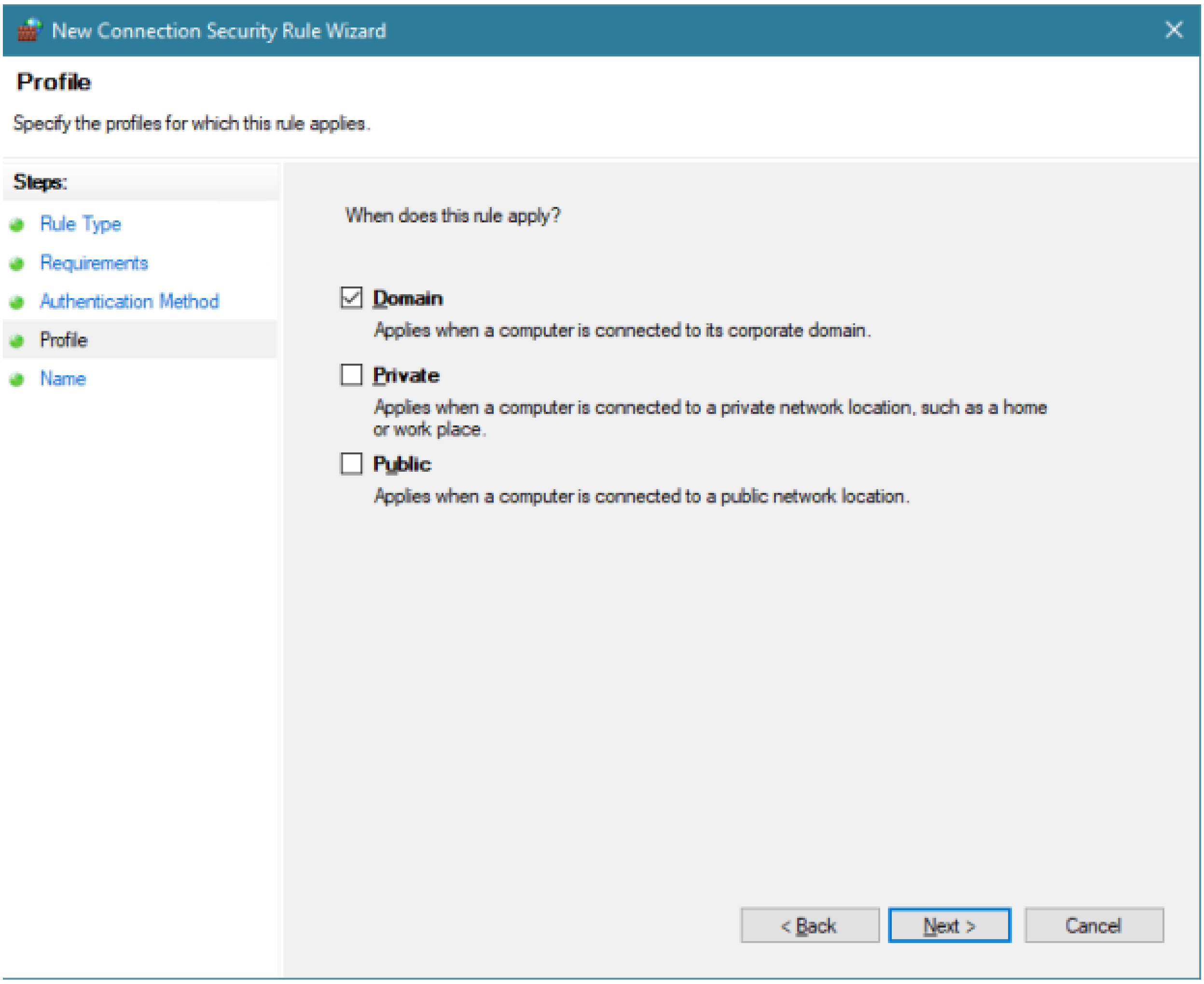
Restrict communications to connections from domain-joined users and computers. Provides identity information for authorizing specific users and computers in inbound and outbound rules.

○ **Computer (Kerberos V5)**

Restrict communications to connections from domain-joined computers. Provides identity information for authorizing specific computers in inbound and outbound rules.

○ **Advanced**

Specify custom first and second authentication settings.



New Connection Security Rule Wizard

Profile

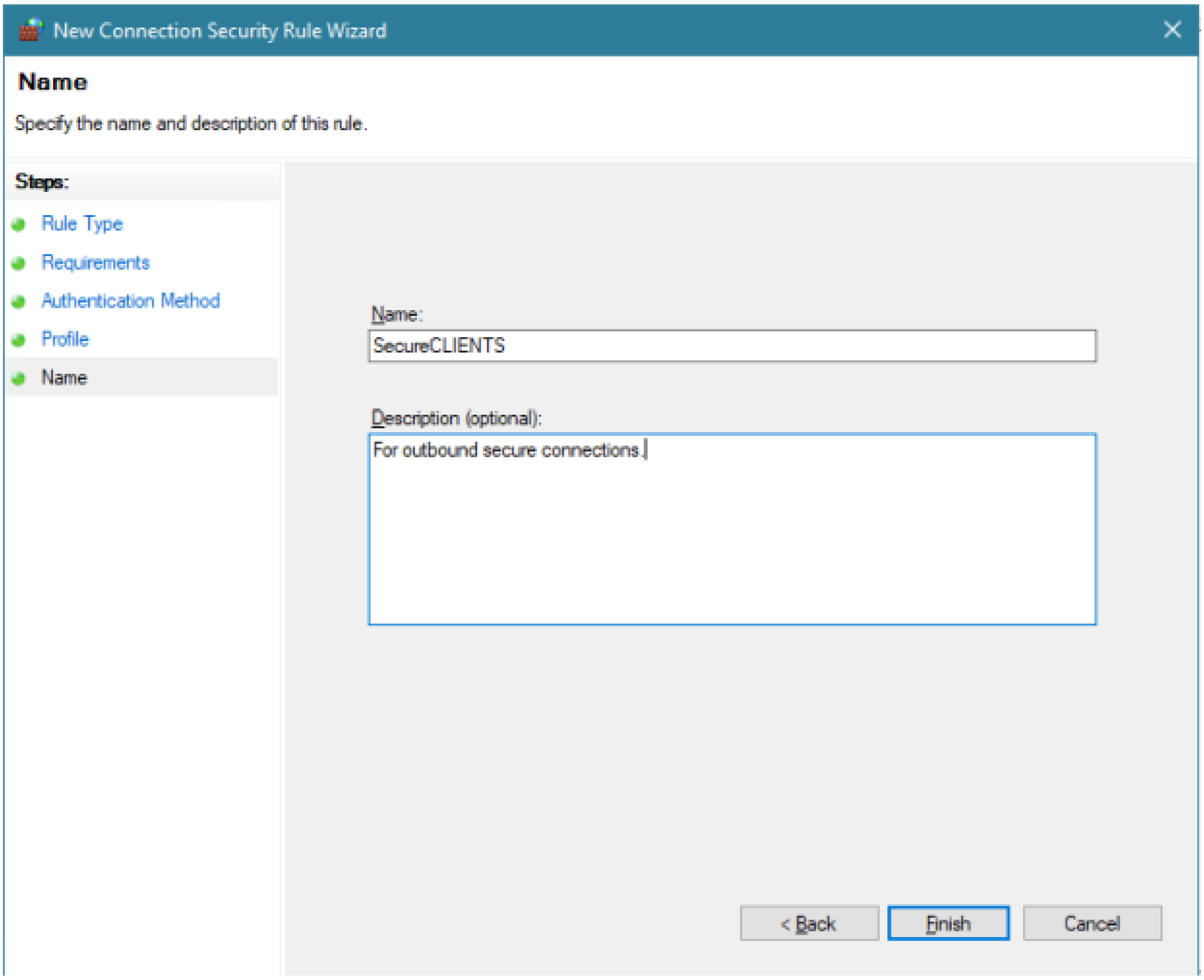
Specify the profiles for which this rule applies.

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.



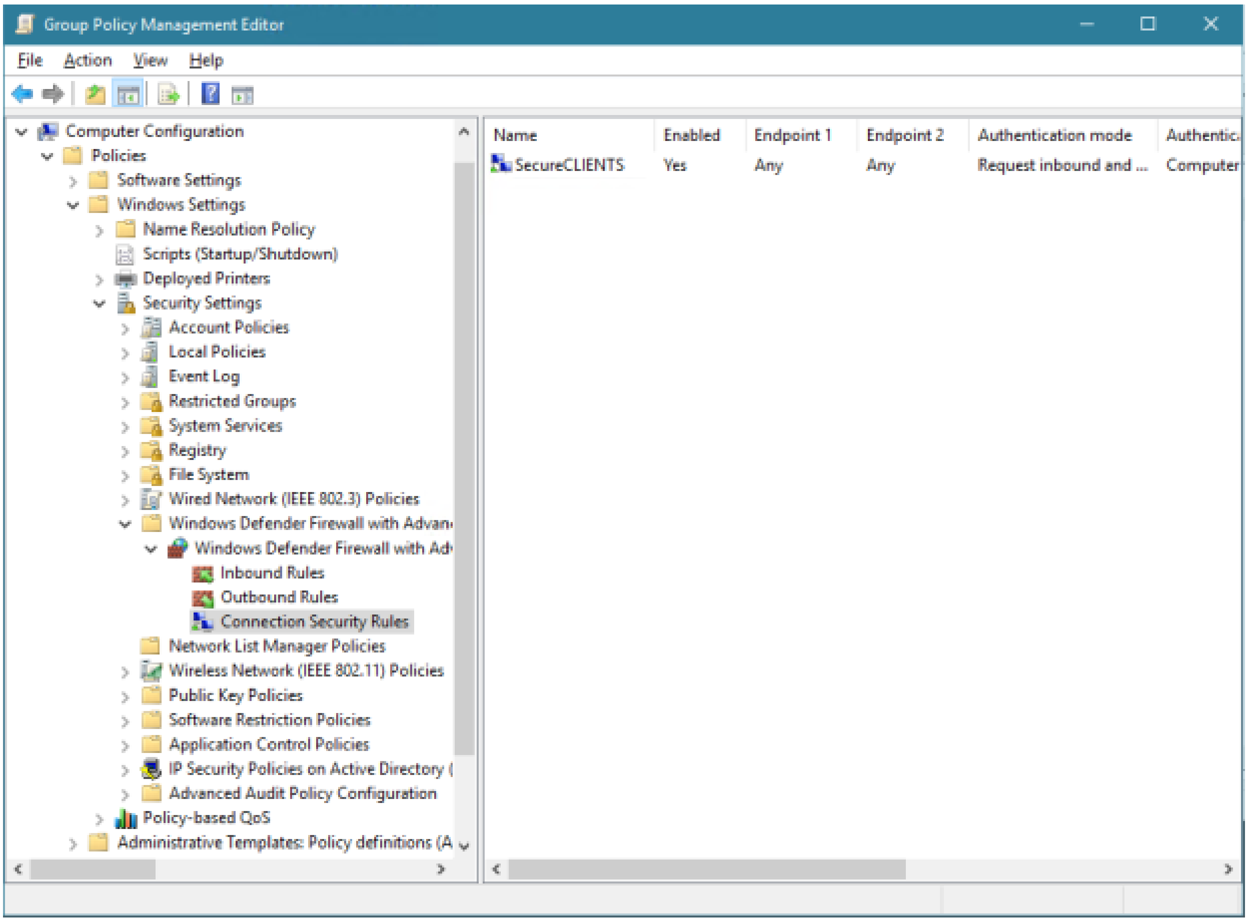
Name

Specify the name and description of this rule.

Name:
SecureCLIENTS

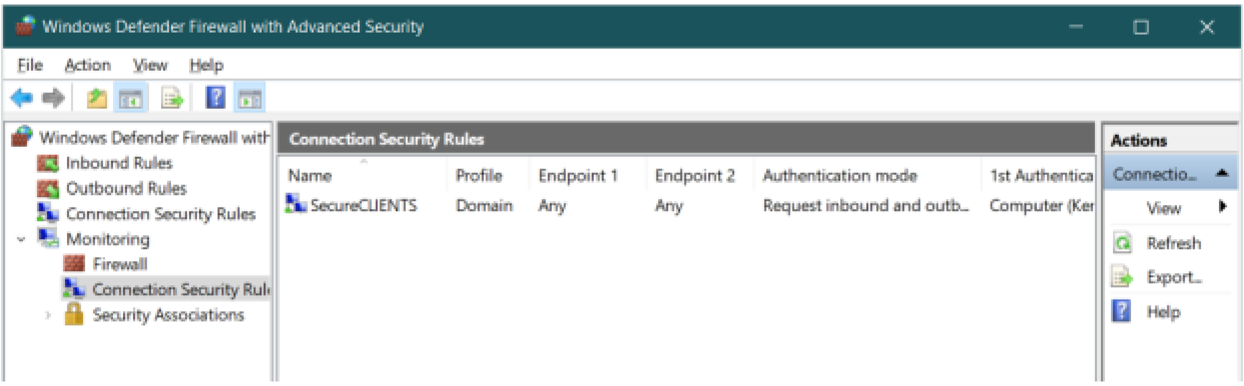
Description (optional):
For outbound secure connections.

Here’s the client rule:


Group Policy Management Editor
File
Action
View
Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advan
Windows Defender Firewall with Ad
Inbound Rules
Outbound Rules
Connection Security Rules
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (A

Name	Enabled	Endpoint 1	Endpoint 2	Authentication mode	Authentic
SecureCLIENTS	Yes	Any	Any	Request inbound and ...	Computer

After running gpupdate /force on Client1:

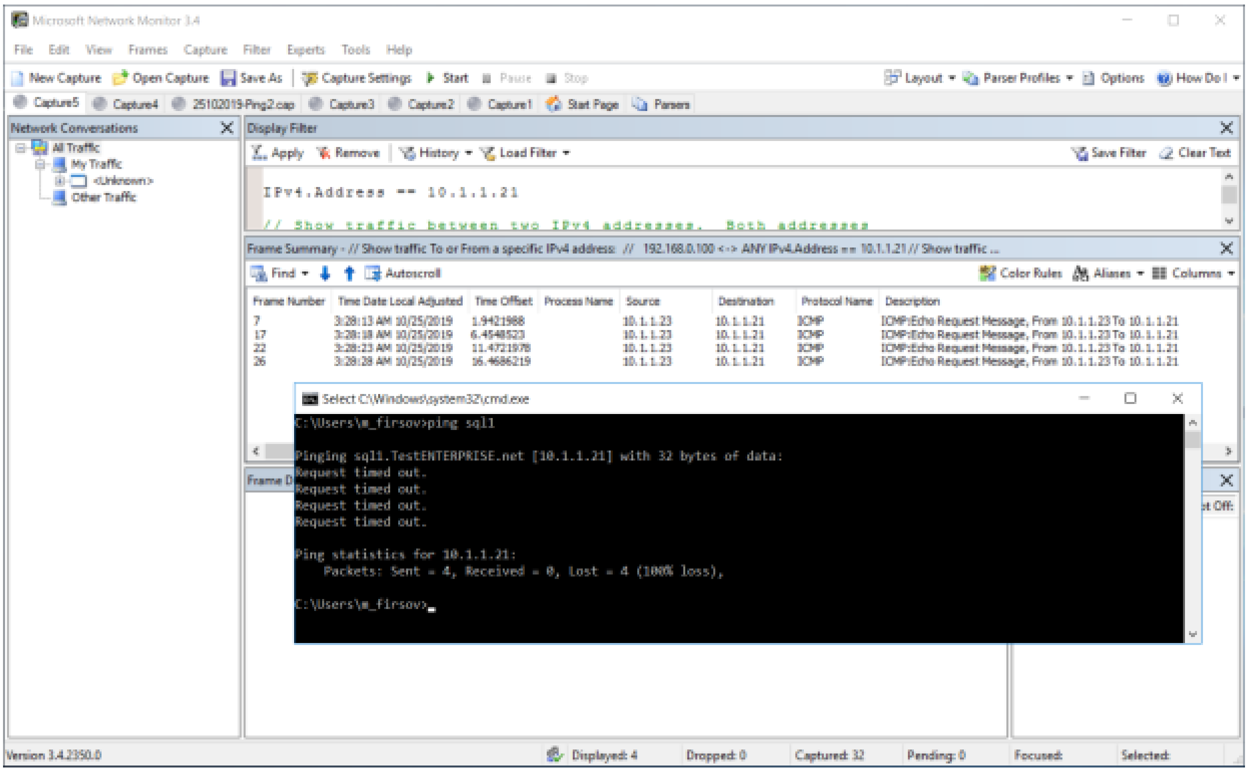


Name	Profile	Endpoint 1	Endpoint 2	Authentication mode	1st Authentica
SecureCLIENTS	Domain	Any	Any	Request inbound and outb...	Computer (Ker

Now let’s test it: computers in the Tier2\Devices (currently only Client1) should have access to SQL1 while any computers that are not in the Tier2\Devices OU should NOT. All connection attempts will be traced in Network Monitor.

Test 1: Connecting to SQL1 from Tier1\Devices\SQL2

1.1 Pinging SQL1 (the ip of SQL2 – 10.1.1.23):



```
IPv4.Address == 10.1.1.21

// Show traffic between two IPv4 addresses.  Both addresses
```

Frame Summary - // Show traffic To or From a specific IPv4 address: // 192.168.0.100 <-> ANY IPv4.Address == 10.1.1.21 // Show traffic ...

Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
7	3:28:13 AM 10/25/2019	1.9421988		10.1.1.23	10.1.1.21	ICMP	ICMP:Echo Request Message, From 10.1.1.23 To 10.1.1.21
17	3:28:18 AM 10/25/2019	6.4548523		10.1.1.23	10.1.1.21	ICMP	ICMP:Echo Request Message, From 10.1.1.23 To 10.1.1.21
22	3:28:23 AM 10/25/2019	11.4721978		10.1.1.23	10.1.1.21	ICMP	ICMP:Echo Request Message, From 10.1.1.23 To 10.1.1.21
26	3:28:28 AM 10/25/2019	16.4686219		10.1.1.23	10.1.1.21	ICMP	ICMP:Echo Request Message, From 10.1.1.23 To 10.1.1.21

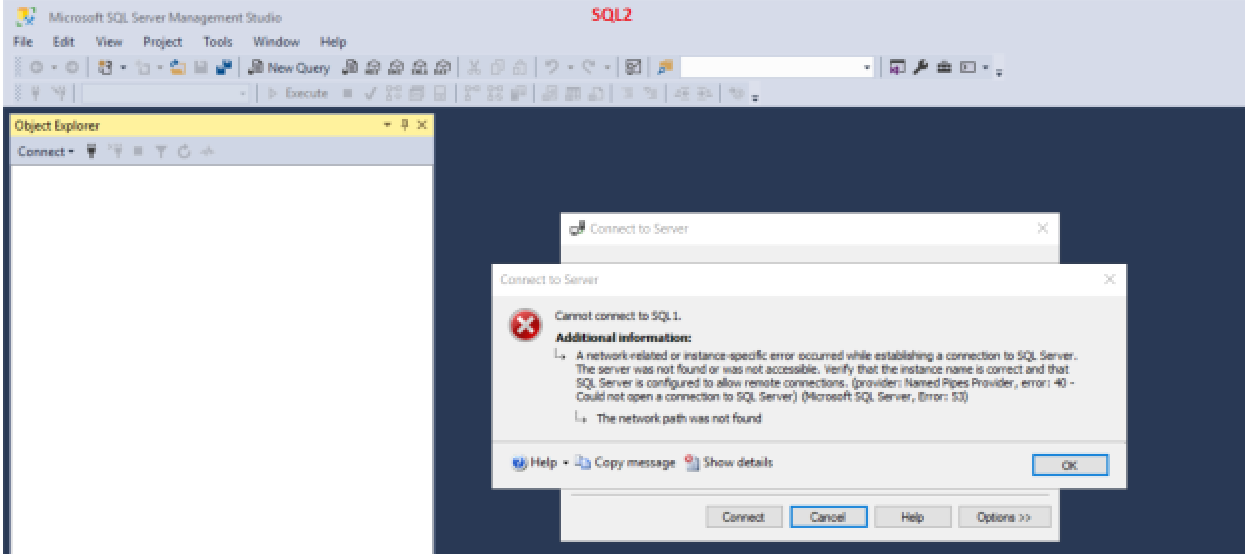
Select C:\Windows\system32\cmd.exe

```
C:\Users\m_firsov>ping sql1

Pinging sql1.TestENTERPRISE.net [10.1.1.21] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.1.1.21:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\m_firsov>
```

Version 3.4.2350.0 Displayed: 4 Dropped: 0 Captured: 32 Pending: 0 Focused: Selected:

The result: ping failed as expected – please note the trace does not contain the SQL1's authentication requests (AuthIP).

2.2 Connecting to SQL1 in SSMS



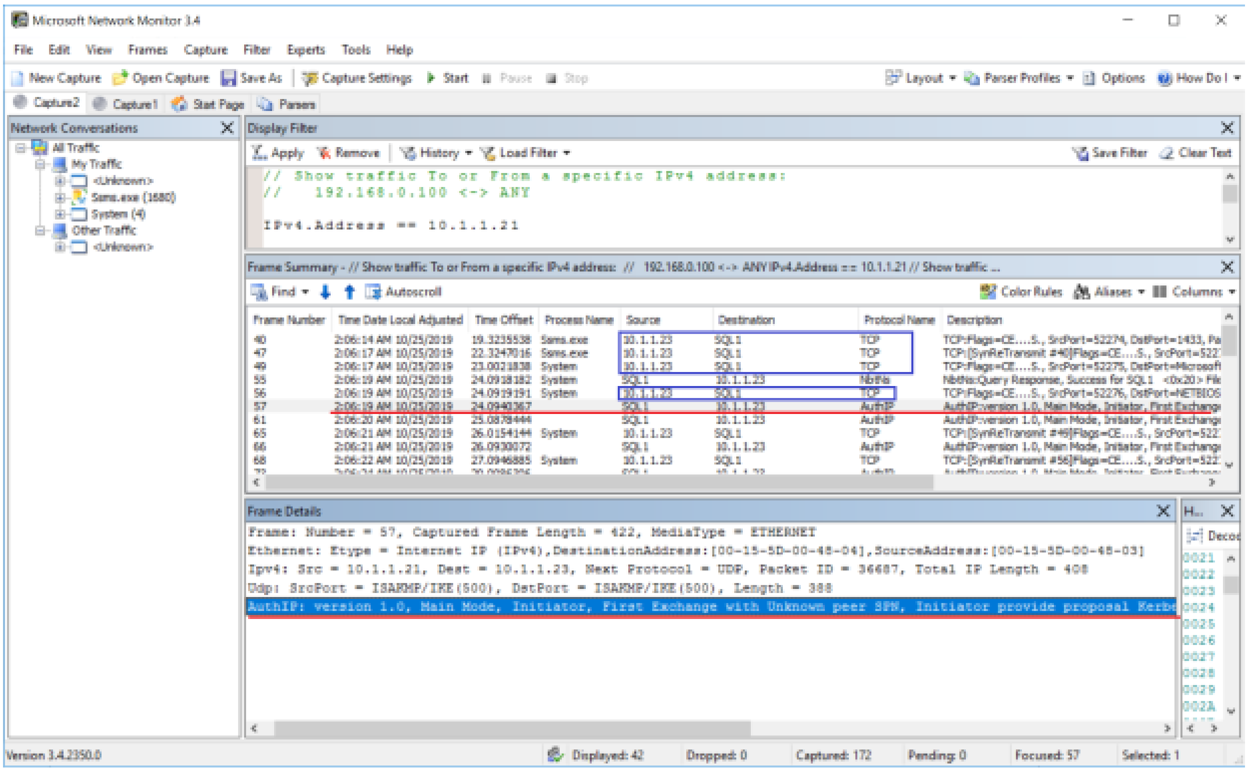
Connect to Server

Cannot connect to SQL1.

Additional information:

A network-related or instance-specific error occurred while establishing a connection to SQL Server. The server was not found or was not accessible. Verify that the instance name is correct and that SQL Server is configured to allow remote connections. (provider: Named Pipes Provider, error: 40 - Could not open a connection to SQL Server) (Microsoft SQL Server, Error: 53)

The network path was not found


Microsoft Network Monitor 3.4
File Edit View Frames Capture Filter Experts Tools Help
New Capture Open Capture Save As Capture Settings Start Pause Stop
Layout Parser Profiles Options How Do I
Capture2 Capture1 Start Page Parsers
Network Conversations
All Traffic
My Traffic
<Unknown>
Ssms.exe (1680)
System (4)
Other Traffic
<Unknown>
Display Filter
Apply Remove History Load Filter
Save Filter Clear Text
Find Autoscroll
Color Rules Aliases Columns
H...
Decod
Version 3.4.2350.0
Displayed: 42 Dropped: 0 Captured: 172 Pending: 0 Focused: 57 Selected: 1

```
// Show traffic To or From a specific IPv4 address:
//    192.168.0.100 <-> ANY

IPv4.Address == 10.1.1.21
```

Frame Summary - // Show traffic To or From a specific IPv4 address: // 192.168.0.100 <-> ANY IPv4.Address == 10.1.1.21 // Show traffic ...

Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
40	2:06:14 AM 10/25/2019	19.3235538	Ssms.exe	10.1.1.23	SQL1	TCP	TCP:Flags=CE....S., SrcPort=52274, DstPort=1433, Pa
47	2:06:17 AM 10/25/2019	22.3247016	Ssms.exe	10.1.1.23	SQL1	TCP	TCP:[SynReTransmit #40]Flags=CE....S., SrcPort=522
49	2:06:17 AM 10/25/2019	23.0021838	System	10.1.1.23	SQL1	TCP	TCP:Flags=CE....S., SrcPort=52275, DstPort=Microsoft
55	2:06:19 AM 10/25/2019	24.0918182	System	SQL1	10.1.1.23	NbtNs	NbtNs:Query Response, Success for SQL1 <0x20> File
56	2:06:19 AM 10/25/2019	24.0919191	System	10.1.1.23	SQL1	TCP	TCP:Flags=CE....S., SrcPort=52276, DstPort=NETBIOS
57	2:06:19 AM 10/25/2019	24.0940367		SQL1	10.1.1.23	AuthIP	AuthIP:version 1.0, Main Mode, Initiator, First Exchange
61	2:06:20 AM 10/25/2019	25.0878444		SQL1	10.1.1.23	AuthIP	AuthIP:version 1.0, Main Mode, Initiator, First Exchange
65	2:06:21 AM 10/25/2019	26.0154144	System	10.1.1.23	SQL1	TCP	TCP:[SynReTransmit #49]Flags=CE....S., SrcPort=522
66	2:06:21 AM 10/25/2019	26.0930072		SQL1	10.1.1.23	AuthIP	AuthIP:version 1.0, Main Mode, Initiator, First Exchange
68	2:06:22 AM 10/25/2019	27.0946885	System	10.1.1.23	SQL1	TCP	TCP:[SynReTransmit #56]Flags=CE....S., SrcPort=522

Frame Details

```
Frame: Number = 57, Captured Frame Length = 422, MediaType = ETHERNET
Ethernet: Etype = Internet IP (IPv4),DestinationAddress:[00-15-5D-00-48-04],SourceAddress:[00-15-5D-00-48-03]
Ipv4: Src = 10.1.1.21, Dest = 10.1.1.23, Next Protocol = UDP, Packet ID = 36687, Total IP Length = 408
Udp: SrcPort = ISAKMP/IKE(500), DstPort = ISAKMP/IKE(500), Length = 388
AuthIP: version 1.0, Main Mode, Initiator, First Exchange with Unknown peer SPN, Initiator provide proposal Kerbe
```

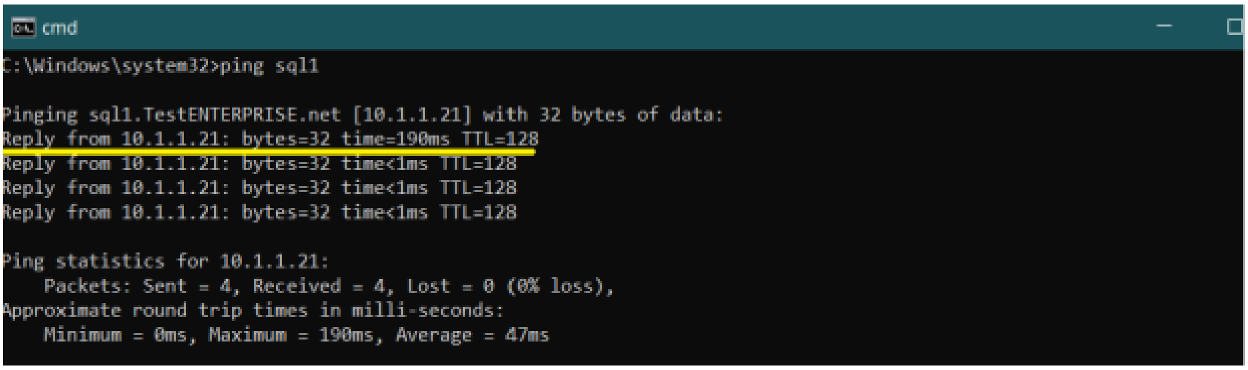
```
0021
0022
0023
0024
0025
0026
0027
0028
0029
002A
```

The result: the connection failed as expected and the trace does contain the SQL1's authentication requests (AuthIP) coming from SQL1 to SQL2. As SQL2 does not have any connection security rules applied it can't respond to the authentication requests that result in the failed connection.

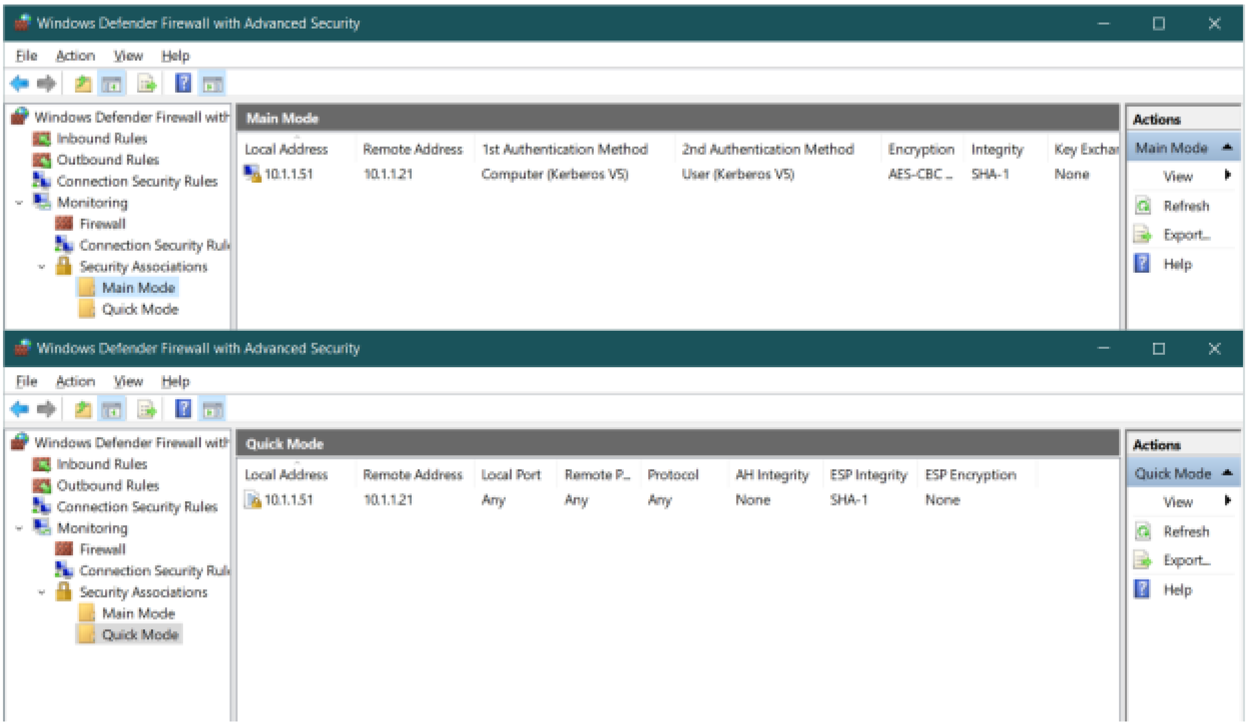
Test 2: Connecting to SQL1 from Tier2\Devices\Client1

2.1 Pinging SQL1

Please note the first packet's response time – it's due to the ipsec negotiation phase:



```
C:\Windows\system32>ping sql1

Pinging sql1.TestENTERPRISE.net [10.1.1.21] with 32 bytes of data:
Reply from 10.1.1.21: bytes=32 time=190ms TTL=128
Reply from 10.1.1.21: bytes=32 time<1ms TTL=128
Reply from 10.1.1.21: bytes=32 time<1ms TTL=128
Reply from 10.1.1.21: bytes=32 time<1ms TTL=128

Ping statistics for 10.1.1.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 190ms, Average = 47ms
```



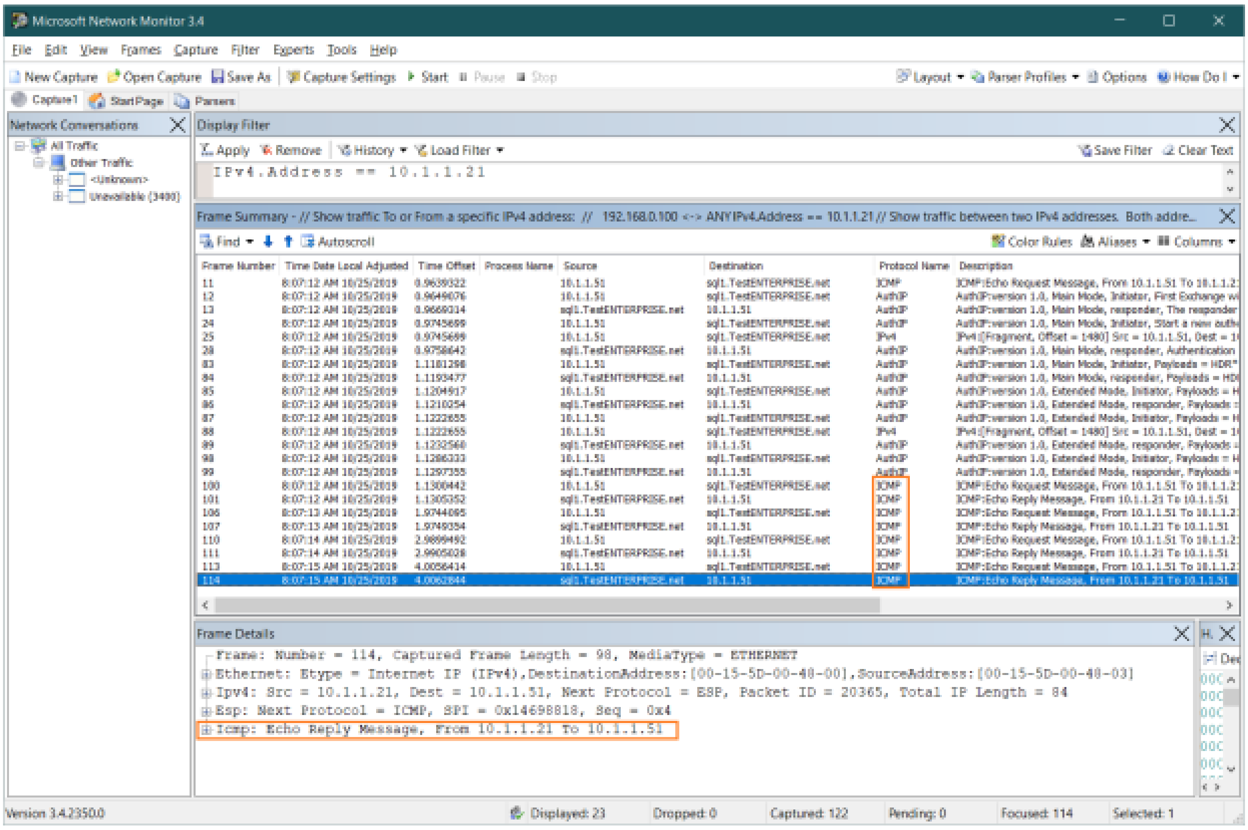
Main Mode

Local Address	Remote Address	1st Authentication Method	2nd Authentication Method	Encryption	Integrity	Key Exchar
10.1.1.51	10.1.1.21	Computer (Kerberos V5)	User (Kerberos V5)	AES-CBC ...	SHA-1	None

Quick Mode

Local Address	Remote Address	Local Port	Remote P...	Protocol	AH Integrity	ESP Integrity	ESP Encryption
10.1.1.51	10.1.1.21	Any	Any	Any	None	SHA-1	None

The trace:


Microsoft Network Monitor 3.4
File Edit View Frames Capture Filter Experts Tools Help
New Capture Open Capture Save As Capture Settings Start Pause Stop
Layout Parser Profiles Options How Do I
Capture1 Start Page Parsers
Network Conversations
All Traffic
Other Traffic
<Unknown>
Unavailable (3400)
Display Filter
Apply Remove History Load Filter
Save Filter Clear Text
Find Autoscroll
Color Rules Aliases Columns
Frame Details

```
IPv4.Address == 10.1.1.21
```

Frame Summary - // Show traffic To or From a specific IPv4 address: // 192.168.0.100 <-> ANY IPv4.Address == 10.1.1.21 // Show traffic between two IPv4 addresses. Both addre...

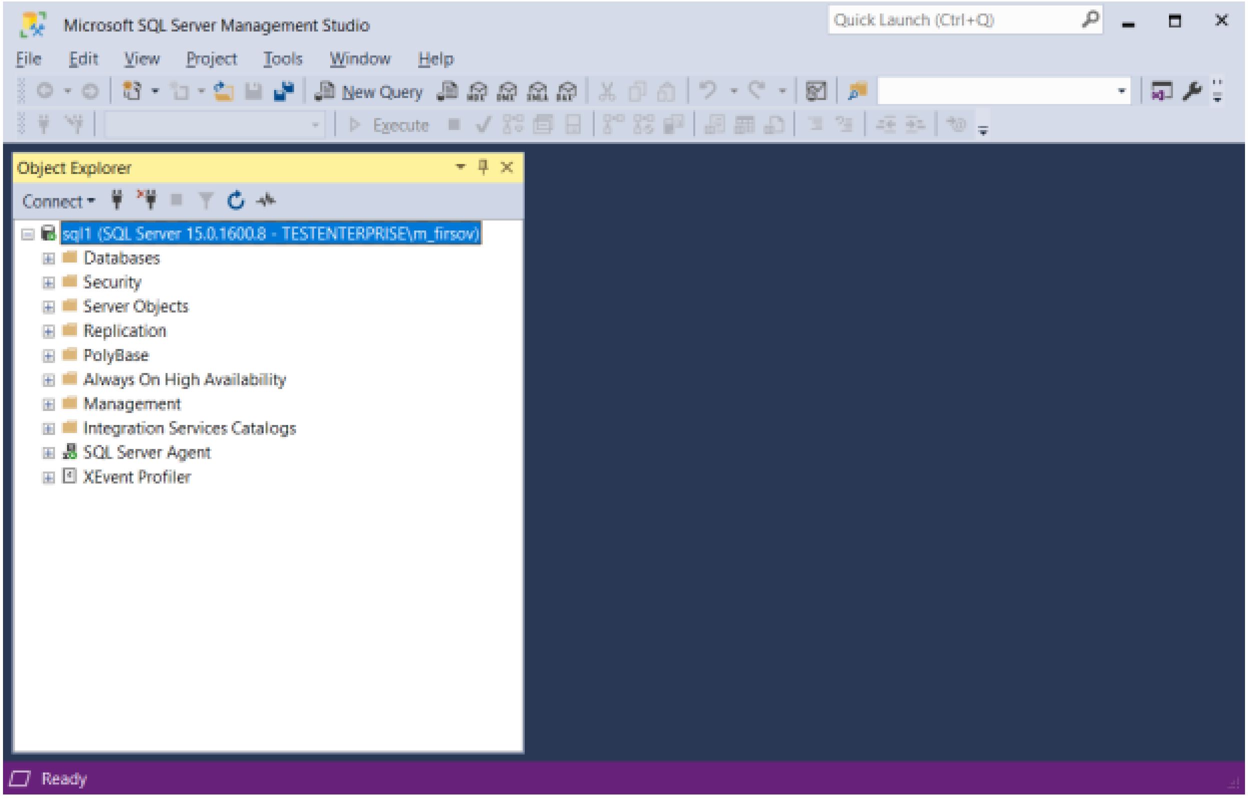
Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
11	8:07:12 AM 10/25/2019	0.9639322		10.1.1.51	sql1.TestENTERPRISE.net	ICMP	ICMP:Echo Request Message, From 10.1.1.51 To 10.1.1.2
12	8:07:12 AM 10/25/2019	0.9649076		10.1.1.51	sql1.TestENTERPRISE.net	AuthIP	AuthIP:version 1.0, Main Mode, Initiator, First Exchange w
13	8:07:12 AM 10/25/2019	0.9669314		sql1.TestENTERPRISE.net	10.1.1.51	AuthIP	AuthIP:version 1.0, Main Mode, responder, The responder
24	8:07:12 AM 10/25/2019	0.9745699		10.1.1.51	sql1.TestENTERPRISE.net	AuthIP	AuthIP:version 1.0, Main Mode, Initiator, Start a new auth
25	8:07:12 AM 10/25/2019	0.9745699		10.1.1.51	sql1.TestENTERPRISE.net	IPv4	IPv4:[Fragment, Offset = 1480] Src = 10.1.1.51, Dest = 1
28	8:07:12 AM 10/25/2019	0.9758642		sql1.TestENTERPRISE.net	10.1.1.51	AuthIP	AuthIP:version 1.0, Main Mode, responder, Authentication
83	8:07:12 AM 10/25/2019	1.1181298		10.1.1.51	sql1.TestENTERPRISE.net	AuthIP	AuthIP:version 1.0, Main Mode, Initiator, Payloads = HDR*
84	8:07:12 AM 10/25/2019	1.1193477		sql1.TestENTERPRISE.net	10.1.1.51	AuthIP	AuthIP:version 1.0, Main Mode, responder, Payloads = HD
85	8:07:12 AM 10/25/2019	1.1204917		10.1.1.51	sql1.TestENTERPRISE.net	AuthIP	AuthIP:version 1.0, Extended Mode, Initiator, Payloads = H
86	8:07:12 AM 10/25/2019	1.1210254		sql1.TestENTERPRISE.net	10.1.1.51	AuthIP	AuthIP:version 1.0, Extended Mode, responder, Payloads
87	8:07:12 AM 10/25/2019	1.1222655		10.1.1.51	sql1.TestENTERPRISE.net	AuthIP	AuthIP:version 1.0, Extended Mode, Initiator, Payloads = H
88	8:07:12 AM 10/25/2019	1.1222655		10.1.1.51	sql1.TestENTERPRISE.net	IPv4	IPv4:[Fragment, Offset = 1480] Src = 10.1.1.51, Dest = 1
89	8:07:12 AM 10/25/2019	1.1232560		sql1.TestENTERPRISE.net	10.1.1.51	AuthIP	AuthIP:version 1.0, Extended Mode, responder, Payloads
98	8:07:12 AM 10/25/2019	1.1286333		10.1.1.51	sql1.TestENTERPRISE.net	AuthIP	AuthIP:version 1.0, Extended Mode, Initiator, Payloads = H
99	8:07:12 AM 10/25/2019	1.1297355		sql1.TestENTERPRISE.net	10.1.1.51	AuthIP	AuthIP:version 1.0, Extended Mode, responder, Payloads
100	8:07:12 AM 10/25/2019	1.1300442		10.1.1.51	sql1.TestENTERPRISE.net	ICMP	ICMP:Echo Request Message, From 10.1.1.51 To 10.1.1.2
101	8:07:12 AM 10/25/2019	1.1305352		sql1.TestENTERPRISE.net	10.1.1.51	ICMP	ICMP:Echo Reply Message, From 10.1.1.21 To 10.1.1.51
106	8:07:13 AM 10/25/2019	1.9744085		10.1.1.51	sql1.TestENTERPRISE.net	ICMP	ICMP:Echo Request Message, From 10.1.1.51 To 10.1.1.2
107	8:07:13 AM 10/25/2019	1.9749354		sql1.TestENTERPRISE.net	10.1.1.51	ICMP	ICMP:Echo Reply Message, From 10.1.1.21 To 10.1.1.51
110	8:07:14 AM 10/25/2019	2.9899492		10.1.1.51	sql1.TestENTERPRISE.net	ICMP	ICMP:Echo Request Message, From 10.1.1.51 To 10.1.1.2
111	8:07:14 AM 10/25/2019	2.9905028		sql1.TestENTERPRISE.net	10.1.1.51	ICMP	ICMP:Echo Reply Message, From 10.1.1.21 To 10.1.1.51
113	8:07:15 AM 10/25/2019	4.0056414		10.1.1.51	sql1.TestENTERPRISE.net	ICMP	ICMP:Echo Request Message, From 10.1.1.51 To 10.1.1.2
114	8:07:15 AM 10/25/2019	4.0062844		sql1.TestENTERPRISE.net	10.1.1.51	ICMP	ICMP:Echo Reply Message, From 10.1.1.21 To 10.1.1.51

```
Frame: Number = 114, Captured Frame Length = 98, MediaType = ETHERNET
Ethernet: Etype = Internet IP (IPv4),DestinationAddress:[00-15-5D-00-48-00],SourceAddress:[00-15-5D-00-48-03]
Ipv4: Src = 10.1.1.21, Dest = 10.1.1.51, Next Protocol = ESP, Packet ID = 20365, Total IP Length = 84
Esp: Next Protocol = ICMP, SPI = 0x14698818, Seq = 0x4
Icmp: Echo Reply Message, From 10.1.1.21 To 10.1.1.51
```

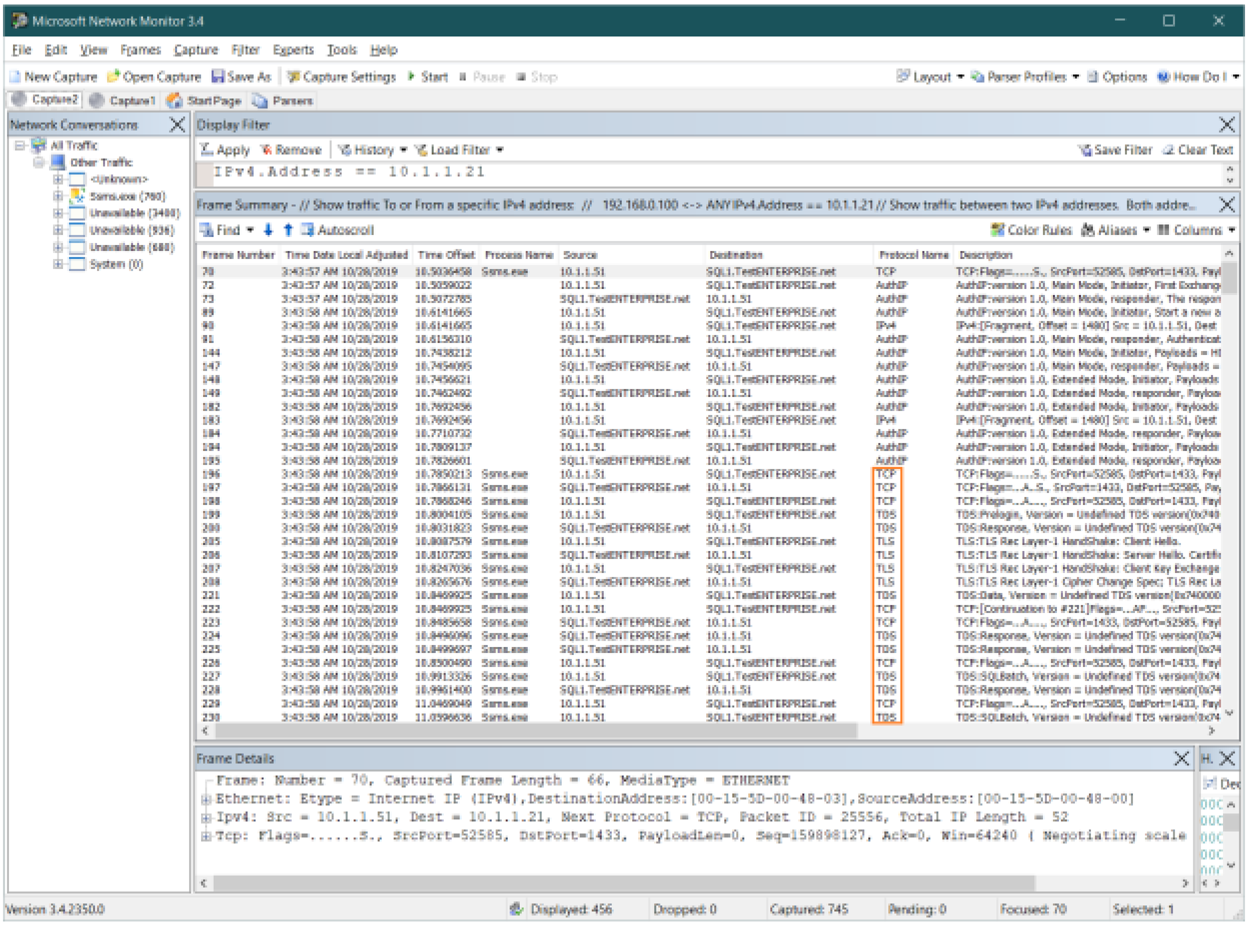
Version 3.4.2350.0 Displayed: 23 Dropped: 0 Captured: 122 Pending: 0 Focused: 114 Selected: 1

The result: ping succeeds as expected. Please note that the host with the connection security rule applied makes the second connection using AuthIP protocol right after the first unsuccessful echo request. After successful ipsec authentication we can see icmp request/reply packets.

2.2 Connecting to SQL1 in SSMS


Microsoft SQL Server Management Studio
Quick Launch (Ctrl+Q)
File Edit View Project Tools Window Help
New Query
Execute
Object Explorer
Connect
sql1 (SQL Server 15.0.1600.8 - TESTENTERPRISE\m_firsov)
Databases
Security
Server Objects
Replication
PolyBase
Always On High Availability
Management
Integration Services Catalogs
SQL Server Agent
XEvent Profiler
Ready

The trace:


Microsoft Network Monitor 3.4
File Edit View Frames Capture Filter Experts Tools Help
New Capture Open Capture Save As Capture Settings Start Pause Stop
Layout Parser Profiles Options How Do I
Capture2 Capture1 Start Page Parsers
Network Conversations
All Traffic
Other Traffic
<Unknown>
Ssms.exe (780)
Unavailable (3480)
Unavailable (936)
Unavailable (680)
System (0)
Display Filter
Apply Remove History Load Filter Save Filter Clear Text
Find Autoscroll Color Rules Aliases Columns
Frame Details
Version 3.4.2350.0
Displayed: 456 Dropped: 0 Captured: 745 Pending: 0 Focused: 70 Selected: 1

```
IPv4.Address == 10.1.1.21
```

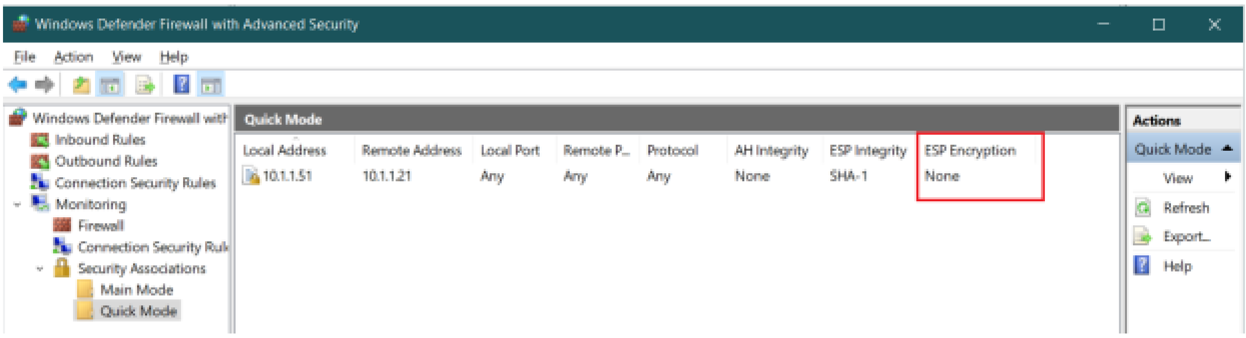
Frame Summary - // Show traffic To or From a specific IPv4 address: // 192.168.0.100 <-> ANY IPv4.Address == 10.1.1.21 // Show traffic between two IPv4 addresses. Both addre...

Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
70	3:43:57 AM 10/28/2019	10.5036458	Ssms.exe	10.1.1.51	SQL1.TestENTERPRISE.net	TCP	TCP:Flags=......S., SrcPort=52585, DstPort=1433, Payl
72	3:43:57 AM 10/28/2019	10.5059022		10.1.1.51	SQL1.TestENTERPRISE.net	AuthIP	AuthIP:version 1.0, Main Mode, Initiator, First Exchang
73	3:43:57 AM 10/28/2019	10.5072785		SQL1.TestENTERPRISE.net	10.1.1.51	AuthIP	AuthIP:version 1.0, Main Mode, responder, The respon
89	3:43:58 AM 10/28/2019	10.6141665		10.1.1.51	SQL1.TestENTERPRISE.net	AuthIP	AuthIP:version 1.0, Main Mode, Initiator, Start a new a
90	3:43:58 AM 10/28/2019	10.6141665		10.1.1.51	SQL1.TestENTERPRISE.net	IPv4	IPv4:[Fragment, Offset = 1480] Src = 10.1.1.51, Dest
91	3:43:58 AM 10/28/2019	10.6156310		SQL1.TestENTERPRISE.net	10.1.1.51	AuthIP	AuthIP:version 1.0, Main Mode, responder, Authenticat
144	3:43:58 AM 10/28/2019	10.7438212		10.1.1.51	SQL1.TestENTERPRISE.net	AuthIP	AuthIP:version 1.0, Main Mode, Initiator, Payloads = HI
147	3:43:58 AM 10/28/2019	10.7454095		SQL1.TestENTERPRISE.net	10.1.1.51	AuthIP	AuthIP:version 1.0, Main Mode, responder, Payloads =
148	3:43:58 AM 10/28/2019	10.7456621		10.1.1.51	SQL1.TestENTERPRISE.net	AuthIP	AuthIP:version 1.0, Extended Mode, Initiator, Payloads
149	3:43:58 AM 10/28/2019	10.7462492		SQL1.TestENTERPRISE.net	10.1.1.51	AuthIP	AuthIP:version 1.0, Extended Mode, responder, Payloa
182	3:43:58 AM 10/28/2019	10.7692456		10.1.1.51	SQL1.TestENTERPRISE.net	AuthIP	AuthIP:version 1.0, Extended Mode, Initiator, Payloads
183	3:43:58 AM 10/28/2019	10.7692456		10.1.1.51	SQL1.TestENTERPRISE.net	IPv4	IPv4:[Fragment, Offset = 1480] Src = 10.1.1.51, Dest
184	3:43:58 AM 10/28/2019	10.7710732		SQL1.TestENTERPRISE.net	10.1.1.51	AuthIP	AuthIP:version 1.0, Extended Mode, responder, Payloa
194	3:43:58 AM 10/28/2019	10.7809137		10.1.1.51	SQL1.TestENTERPRISE.net	AuthIP	AuthIP:version 1.0, Extended Mode, Initiator, Payloads
195	3:43:58 AM 10/28/2019	10.7826601		SQL1.TestENTERPRISE.net	10.1.1.51	AuthIP	AuthIP:version 1.0, Extended Mode, responder, Payloa
196	3:43:58 AM 10/28/2019	10.7850213	Ssms.exe	10.1.1.51	SQL1.TestENTERPRISE.net	TCP	TCP:Flags=......S., SrcPort=52585, DstPort=1433, Payl
197	3:43:58 AM 10/28/2019	10.7866131	Ssms.exe	SQL1.TestENTERPRISE.net	10.1.1.51	TCP	TCP:Flags=...A..S., SrcPort=1433, DstPort=52585, Pay
198	3:43:58 AM 10/28/2019	10.7868246	Ssms.exe	10.1.1.51	SQL1.TestENTERPRISE.net	TCP	TCP:Flags=...A...., SrcPort=52585, DstPort=1433, Payl
199	3:43:58 AM 10/28/2019	10.8004105	Ssms.exe	10.1.1.51	SQL1.TestENTERPRISE.net	TDS	TDS:Prelogin, Version = Undefined TDS version(0x740
200	3:43:58 AM 10/28/2019	10.8031823	Ssms.exe	SQL1.TestENTERPRISE.net	10.1.1.51	TDS	TDS:Response, Version = Undefined TDS version(0x74
205	3:43:58 AM 10/28/2019	10.8087579	Ssms.exe	10.1.1.51	SQL1.TestENTERPRISE.net	TLS	TLS:TLS Rec Layer-1 HandShake: Client Hello.
206	3:43:58 AM 10/28/2019	10.8107293	Ssms.exe	SQL1.TestENTERPRISE.net	10.1.1.51	TLS	TLS:TLS Rec Layer-1 HandShake: Server Hello. Certifi
207	3:43:58 AM 10/28/2019	10.8247036	Ssms.exe	10.1.1.51	SQL1.TestENTERPRISE.net	TLS	TLS:TLS Rec Layer-1 HandShake: Client Key Exchange
208	3:43:58 AM 10/28/2019	10.8265676	Ssms.exe	SQL1.TestENTERPRISE.net	10.1.1.51	TLS	TLS:TLS Rec Layer-1 Cipher Change Spec; TLS Rec La
221	3:43:58 AM 10/28/2019	10.8469925	Ssms.exe	10.1.1.51	SQL1.TestENTERPRISE.net	TDS	TDS:Data, Version = Undefined TDS version(0x740000
222	3:43:58 AM 10/28/2019	10.8469925	Ssms.exe	10.1.1.51	SQL1.TestENTERPRISE.net	TCP	TCP:[Continuation to #221]Flags=...AP..., SrcPort=525
223	3:43:58 AM 10/28/2019	10.8485658	Ssms.exe	SQL1.TestENTERPRISE.net	10.1.1.51	TCP	TCP:Flags=...A...., SrcPort=1433, DstPort=52585, Payl
224	3:43:58 AM 10/28/2019	10.8496096	Ssms.exe	SQL1.TestENTERPRISE.net	10.1.1.51	TDS	TDS:Response, Version = Undefined TDS version(0x74
225	3:43:58 AM 10/28/2019	10.8499697	Ssms.exe	SQL1.TestENTERPRISE.net	10.1.1.51	TDS	TDS:Response, Version = Undefined TDS version(0x74
226	3:43:58 AM 10/28/2019	10.8500490	Ssms.exe	10.1.1.51	SQL1.TestENTERPRISE.net	TCP	TCP:Flags=...A...., SrcPort=52585, DstPort=1433, Payl
227	3:43:58 AM 10/28/2019	10.9913326	Ssms.exe	10.1.1.51	SQL1.TestENTERPRISE.net	TDS	TDS:SQLBatch, Version = Undefined TDS version(0x74
228	3:43:58 AM 10/28/2019	10.9961400	Ssms.exe	SQL1.TestENTERPRISE.net	10.1.1.51	TDS	TDS:Response, Version = Undefined TDS version(0x74
229	3:43:58 AM 10/28/2019	11.0469049	Ssms.exe	10.1.1.51	SQL1.TestENTERPRISE.net	TCP	TCP:Flags=...A...., SrcPort=52585, DstPort=1433, Payl
230	3:43:58 AM 10/28/2019	11.0596636	Ssms.exe	10.1.1.51	SQL1.TestENTERPRISE.net	TDS	TDS:SQLBatch, Version = Undefined TDS version(0x74

```
 Frame: Number = 70, Captured Frame Length = 66, MediaType = ETHERNET
+Ethernet: Etype = Internet IP (IPv4),DestinationAddress:[00-15-5D-00-48-03],SourceAddress:[00-15-5D-00-48-00]
+Ipv4: Src = 10.1.1.51, Dest = 10.1.1.21, Next Protocol = TCP, Packet ID = 25556, Total IP Length = 52
+Tcp: Flags=......S., SrcPort=52585, DstPort=1433, PayloadLen=0, Seq=159898127, Ack=0, Win=64240 ( Negotiating scale
```

The result: connection succeeded – once ipsec authentication is completed SSMS establishes TDS session with the database server.

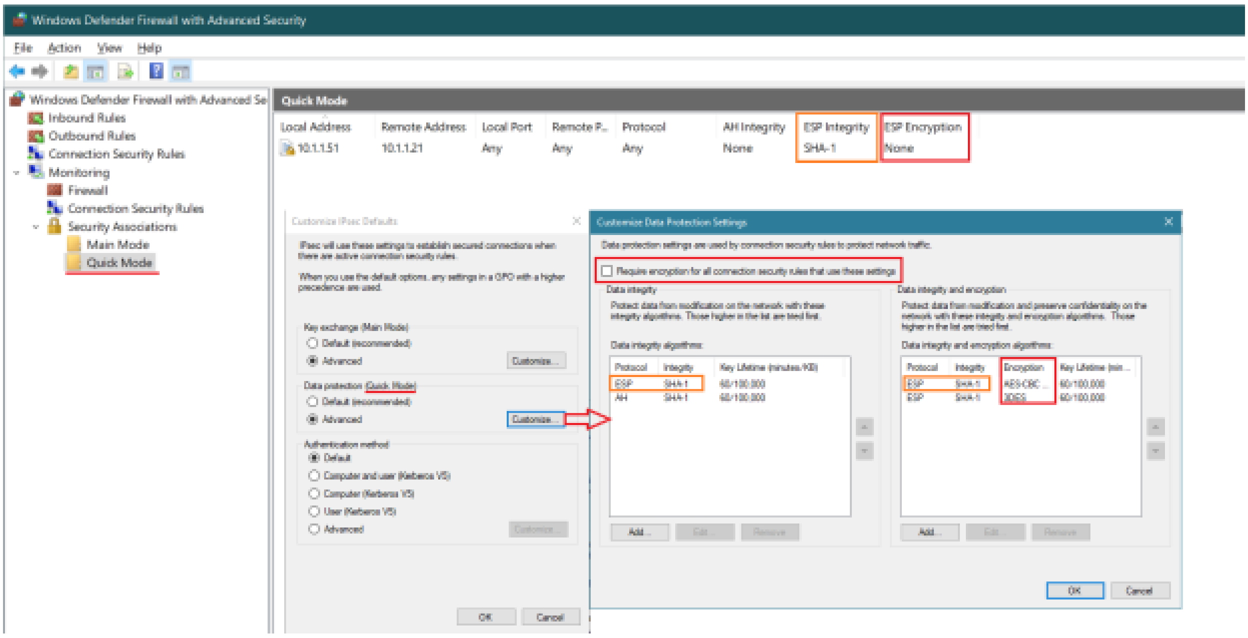
You may have already noted that both succeeded secure connections still display all their network-related information in the network parser – that's because by default no encryption is applied to the packets:



Quick Mode

Local Address	Remote Address	Local Port	Remote P...	Protocol	AH Integrity	ESP Integrity	ESP Encryption
10.1.1.51	10.1.1.21	Any	Any	Any	None	SHA-1	None

Here's how the default IPSec settings correlate with the connection security rules applied (I'll move on to the IPSec defaults right after this screenshot).



Quick Mode

Local Address	Remote Address	Local Port	Remote P...	Protocol	AH Integrity	ESP Integrity	ESP Encryption
10.1.1.51	10.1.1.21	Any	Any	Any	None	SHA-1	None

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

Customize Data Protection Settings

Data protection settings are used by connection security rules to protect network traffic.

□ Require encryption for all connection security rules that use these settings

Data integrity

Protect data from modification on the network with these integrity algorithms. Those higher in the list are tried first.

Data integrity algorithms:

Protocol	Integrity	Key Lifetime (minutes/KB)
ESP	SHA-1	60/100,000
AH	SHA-1	60/100,000

Data integrity and encryption

Protect data from modification and preserve confidentiality on the network with these integrity and encryption algorithms. Those higher in the list are tried first.

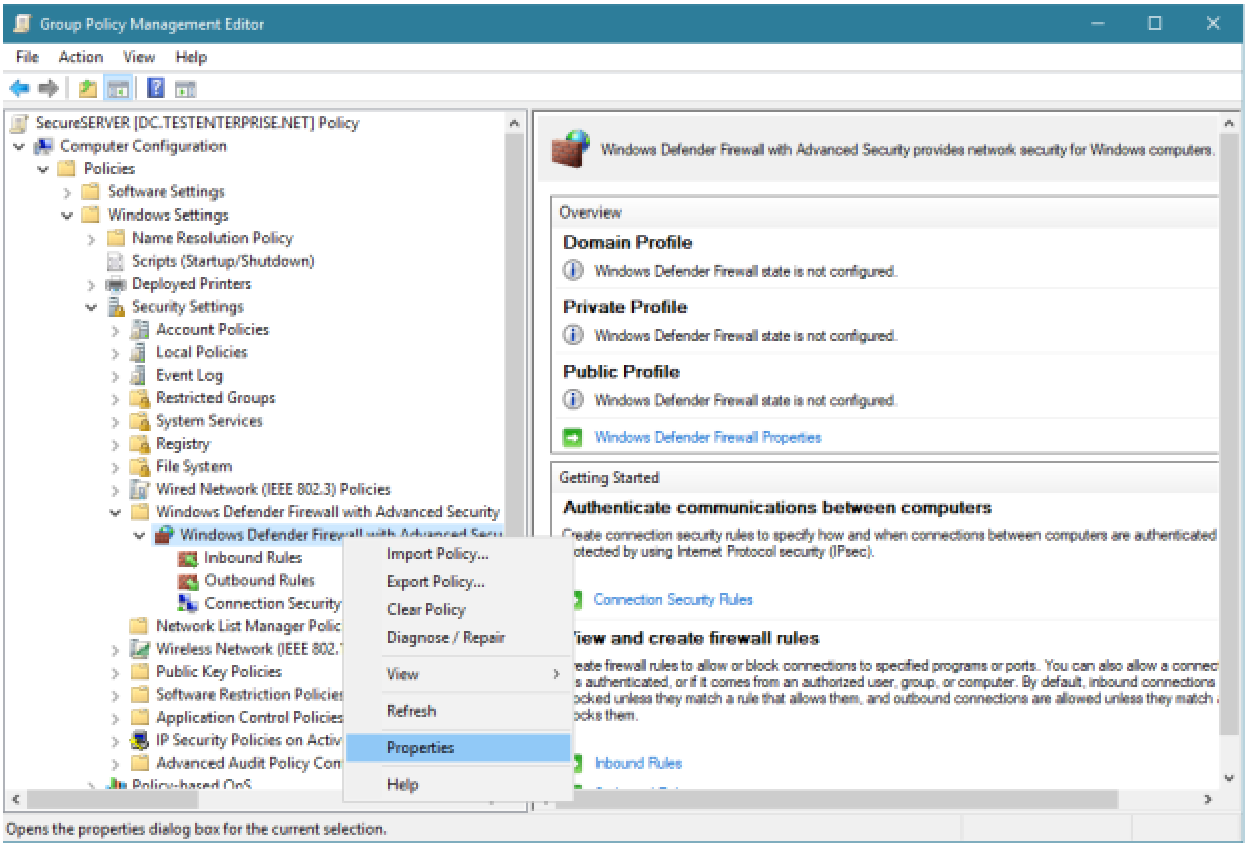
Data integrity and encryption algorithms:

Protocol	Integrity	Encryption	Key Lifetime (min...
ESP	SHA-1	AES-CBC ...	60/100,000
ESP	SHA-1	3DES	60/100,000

By default the "Require encryption…" checkbox is not checked so no encryption algorithms apply.

What if you want to disclose as little information as possible? It means ESP encryption must be enabled – this can be done either in the Windows Firewall's IPSec defaults – and thus all connections that satisfy the ipsec rules on this host will be encrypted – or create the main mode rules with different encryption settings using netsh advfirewall mainmode add rule command. In this article I will enable encryption using Windows Firewall.

You can enable encryption in any GPO – server, client, or both (the best option, I think) – for example, I'll edit the SecureSERVER gpo – navigate to Secure Settings\Windows Defender Firewall with Advanced Security, right-click it and select Properties:



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

Overview

Domain Profile

Windows Defender Firewall state is not configured.

Private Profile

Windows Defender Firewall state is not configured.

Public Profile

Windows Defender Firewall state is not configured.

Windows Defender Firewall Properties

Getting Started

Authenticate communications between computers

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

Connection Security Rules

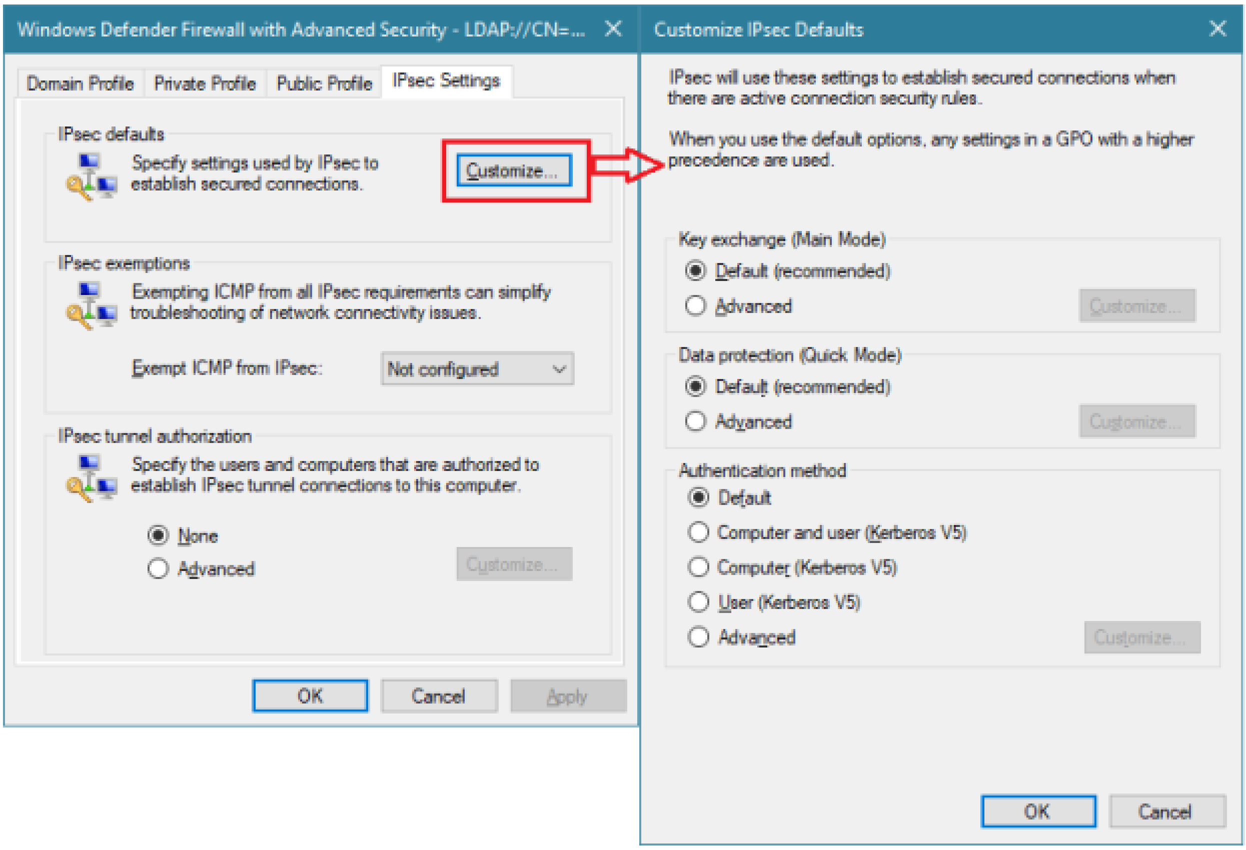
iew and create firewall rules

eate firewall rules to allow or block connections to specified programs or ports. You can also allow a connec s authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections ocked unless they match a rule that allows them, and outbound connections are allowed unless they match ocks them.

Inbound Rules

Opens the properties dialog box for the current selection.

Change to the IPsec Settings and click Customize in the **IPsec defaults** section:



IPsec defaults

Specify settings used by IPsec to establish secured connections.

IPsec exemptions

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

Exempt ICMP from IPsec: Not configured

IPsec tunnel authorization

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

● None
○ Advanced

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

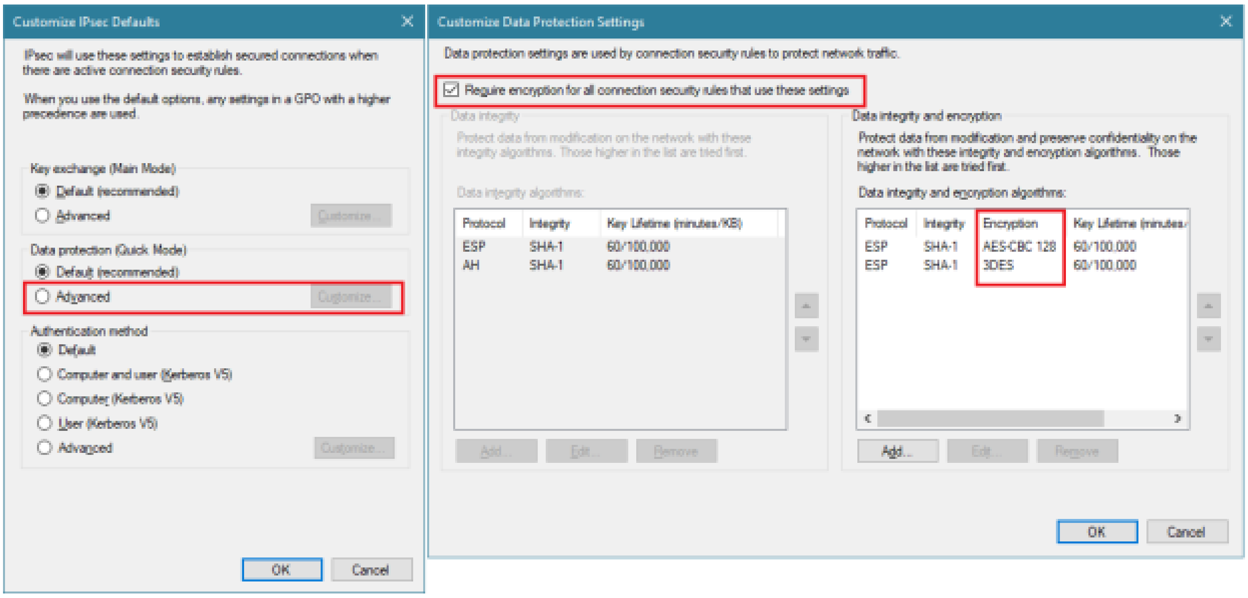
Data protection (Quick Mode)

● Default (recommended)
○ Advanced

Authentication method

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

It is the Quick Mode settings that define whether the encryption is enabled and if yes which encryption (as well as integrity) algorithms are to be used:



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

Customize Data Protection Settings

Data protection settings are used by connection security rules to protect network traffic.

☑ Require encryption for all connection security rules that use these settings

Data integrity

Protect data from modification on the network with these integrity algorithms. Those higher in the list are tried first.

Data integrity algorithms:

Protocol	Integrity	Key Lifetime (minutes/KB)
ESP	SHA-1	60/100,000
AH	SHA-1	60/100,000

Data integrity and encryption

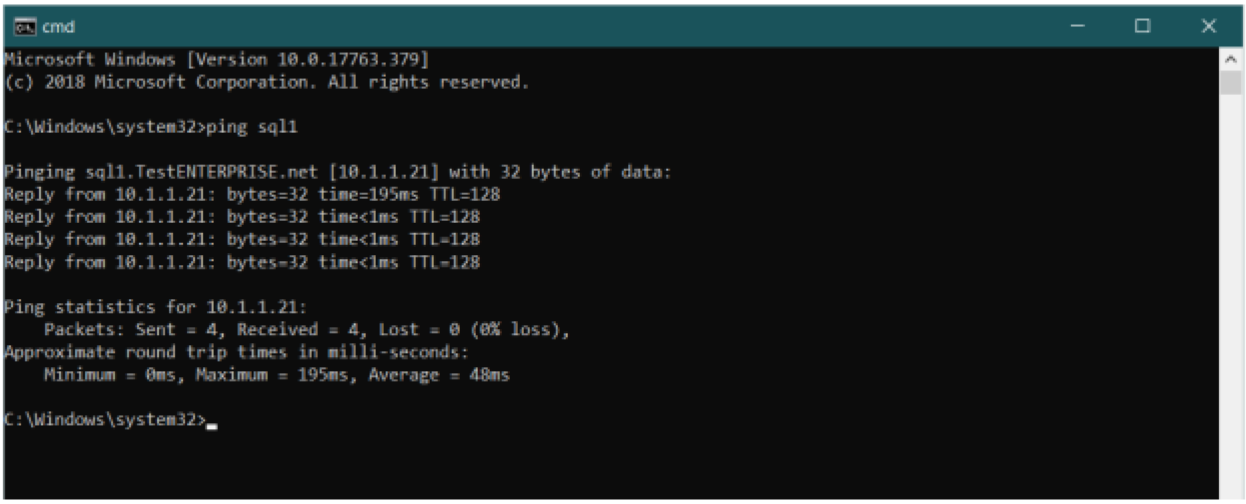
Protect data from modification and preserve confidentiality on the network with these integrity and encryption algorithms. Those higher in the list are tried first.

Data integrity and encryption algorithms:

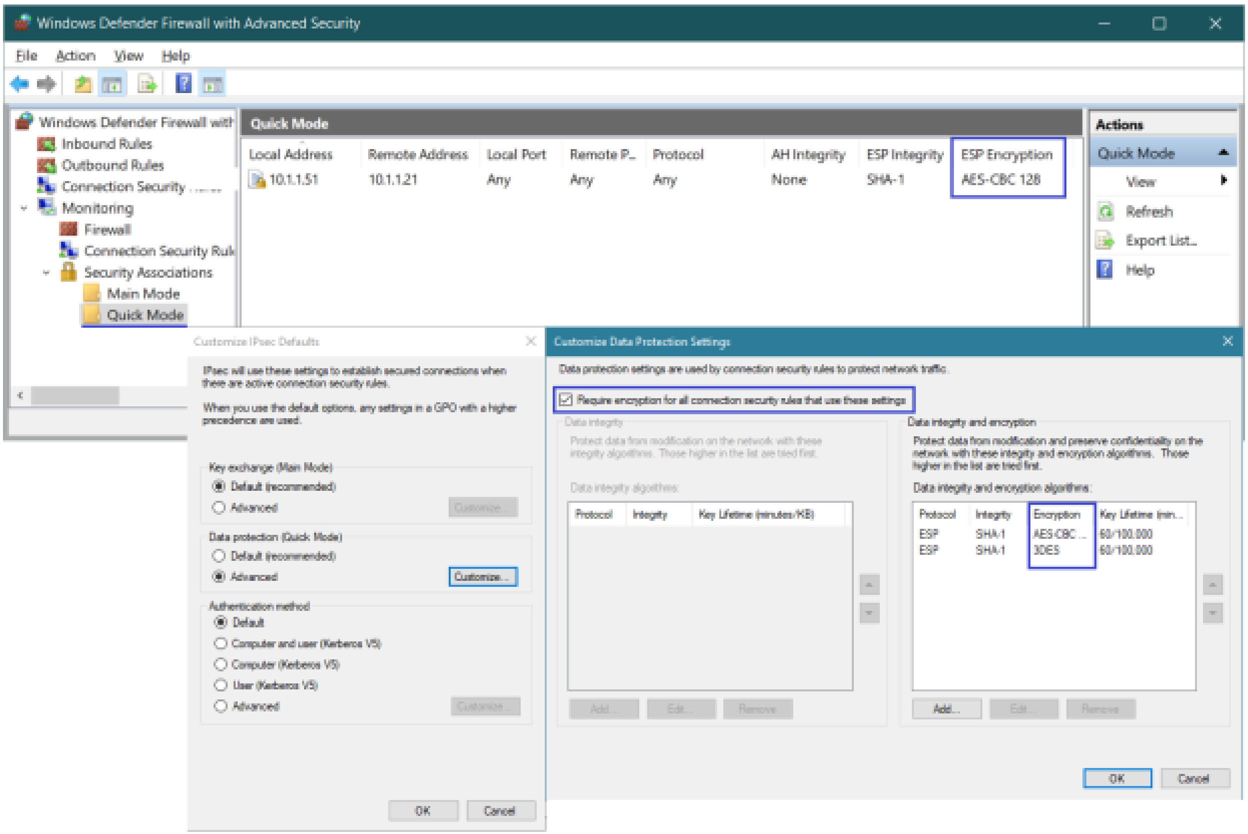
Protocol	Integrity	Encryption	Key Lifetime (minutes/
ESP	SHA-1	AES-CBC 128	60/100,000
ESP	SHA-1	3DES	60/100,000

After setting the Quick mode to the Advanced configuration depicted above we can repeat Test 2 (after gpupdate /force on SQL1, of course) and see how network connections will be displayed in Network Monitor with ESP in place:

2.1 Pinging SQL1 from Client1



```
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping sql1

Pinging sql1.TestENTERPRISE.net [10.1.1.21] with 32 bytes of data:
Reply from 10.1.1.21: bytes=32 time=195ms TTL=128
Reply from 10.1.1.21: bytes=32 time<1ms TTL=128
Reply from 10.1.1.21: bytes=32 time<1ms TTL=128
Reply from 10.1.1.21: bytes=32 time<1ms TTL=128

Ping statistics for 10.1.1.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 195ms, Average = 48ms

C:\Windows\system32>
```



Windows Defender Firewall with Advanced Security

Quick Mode

Local Address	Remote Address	Local Port	Remote P...	Protocol	AH Integrity	ESP Integrity	ESP Encryption
10.1.1.51	10.1.1.21	Any	Any	Any	None	SHA-1	AES-CBC 128

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

Customize Data Protection Settings

Data protection settings are used by connection security rules to protect network traffic.

☑ Require encryption for all connection security rules that use these settings

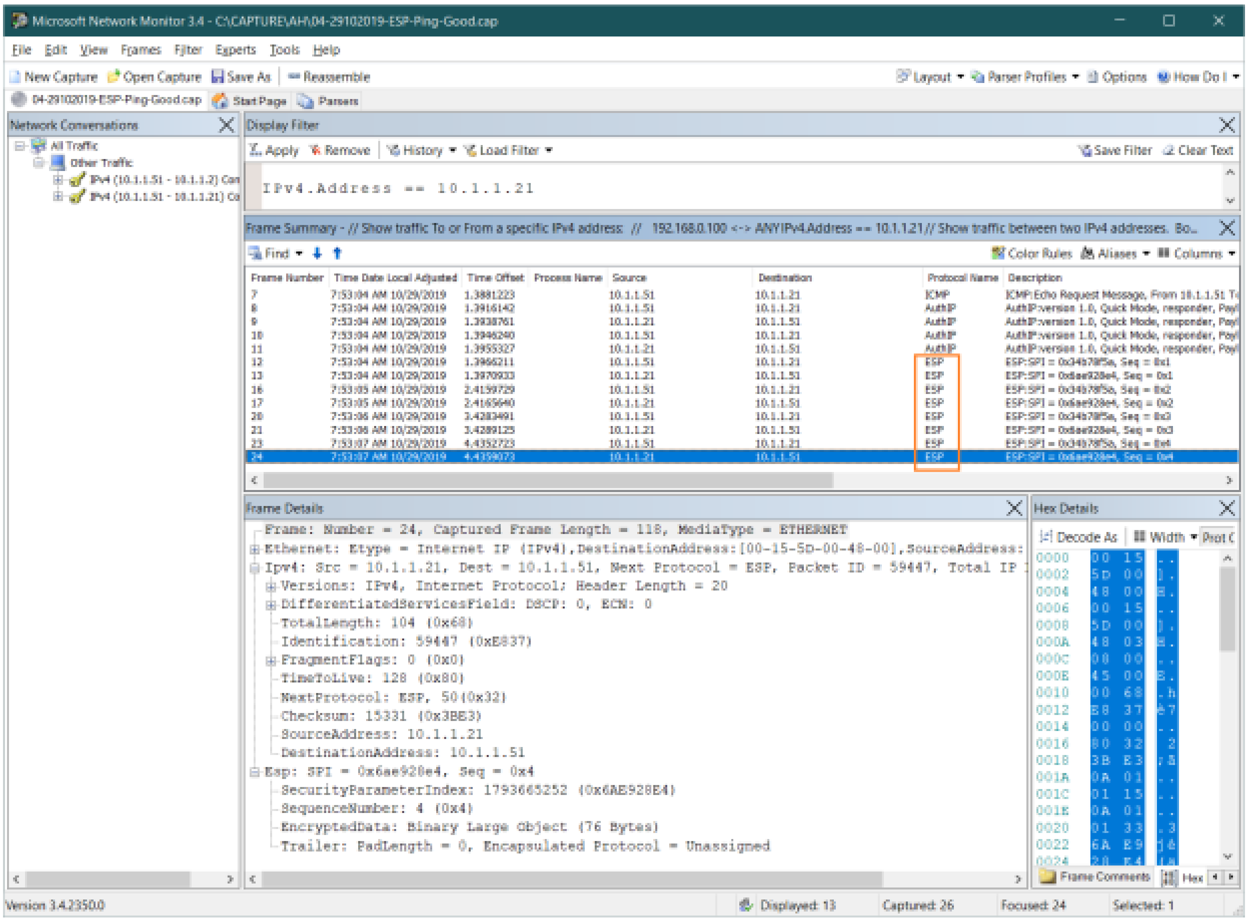
Data integrity and encryption

Protect data from modification and preserve confidentiality on the network with these integrity and encryption algorithms. Those higher in the list are tried first.

Data integrity and encryption algorithms:

Protocol	Integrity	Encryption	Key Lifetime (min...
ESP	SHA-1	AES-CBC ...	60/100,000
ESP	SHA-1	3DES	60/100,000

The trace:



Microsoft Network Monitor 3.4 - C:\CAPTURE\AH\04-29102019-ESP-Ping-Good.cap

Display Filter:

```
IPv4.Address == 10.1.1.21
```

Frame Summary - // Show traffic To or From a specific IPv4 address // 192.168.0.100 <-> ANYIPv4.Address == 10.1.1.21// Show traffic between two IPv4 addresses. Bo...

Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
7	7:53:04 AM 10/29/2019	1.3881223		10.1.1.51	10.1.1.21	ICMP	ICMP:Echo Request Message, From 10.1.1.51 T
8	7:53:04 AM 10/29/2019	1.3916142		10.1.1.51	10.1.1.21	AuthIP	AuthIP:version 1.0, Quick Mode, responder, Payl
9	7:53:04 AM 10/29/2019	1.3938761		10.1.1.21	10.1.1.51	AuthIP	AuthIP:version 1.0, Quick Mode, responder, Payl
10	7:53:04 AM 10/29/2019	1.3946240		10.1.1.51	10.1.1.21	AuthIP	AuthIP:version 1.0, Quick Mode, responder, Payl
11	7:53:04 AM 10/29/2019	1.3955327		10.1.1.21	10.1.1.51	AuthIP	AuthIP:version 1.0, Quick Mode, responder, Payl
12	7:53:04 AM 10/29/2019	1.3966211		10.1.1.51	10.1.1.21	ESP	ESP:SPI = 0x34b78f5a, Seq = 0x1
13	7:53:04 AM 10/29/2019	1.3970933		10.1.1.21	10.1.1.51	ESP	ESP:SPI = 0x6ae928e4, Seq = 0x1
16	7:53:05 AM 10/29/2019	2.4159729		10.1.1.51	10.1.1.21	ESP	ESP:SPI = 0x34b78f5a, Seq = 0x2
17	7:53:05 AM 10/29/2019	2.4165640		10.1.1.21	10.1.1.51	ESP	ESP:SPI = 0x6ae928e4, Seq = 0x2
20	7:53:06 AM 10/29/2019	3.4283491		10.1.1.51	10.1.1.21	ESP	ESP:SPI = 0x34b78f5a, Seq = 0x3
21	7:53:06 AM 10/29/2019	3.4289125		10.1.1.21	10.1.1.51	ESP	ESP:SPI = 0x6ae928e4, Seq = 0x3
23	7:53:07 AM 10/29/2019	4.4352723		10.1.1.51	10.1.1.21	ESP	ESP:SPI = 0x34b78f5a, Seq = 0x4
24	7:53:07 AM 10/29/2019	4.4359073		10.1.1.21	10.1.1.51	ESP	ESP:SPI = 0x6ae928e4, Seq = 0x4

Frame Details

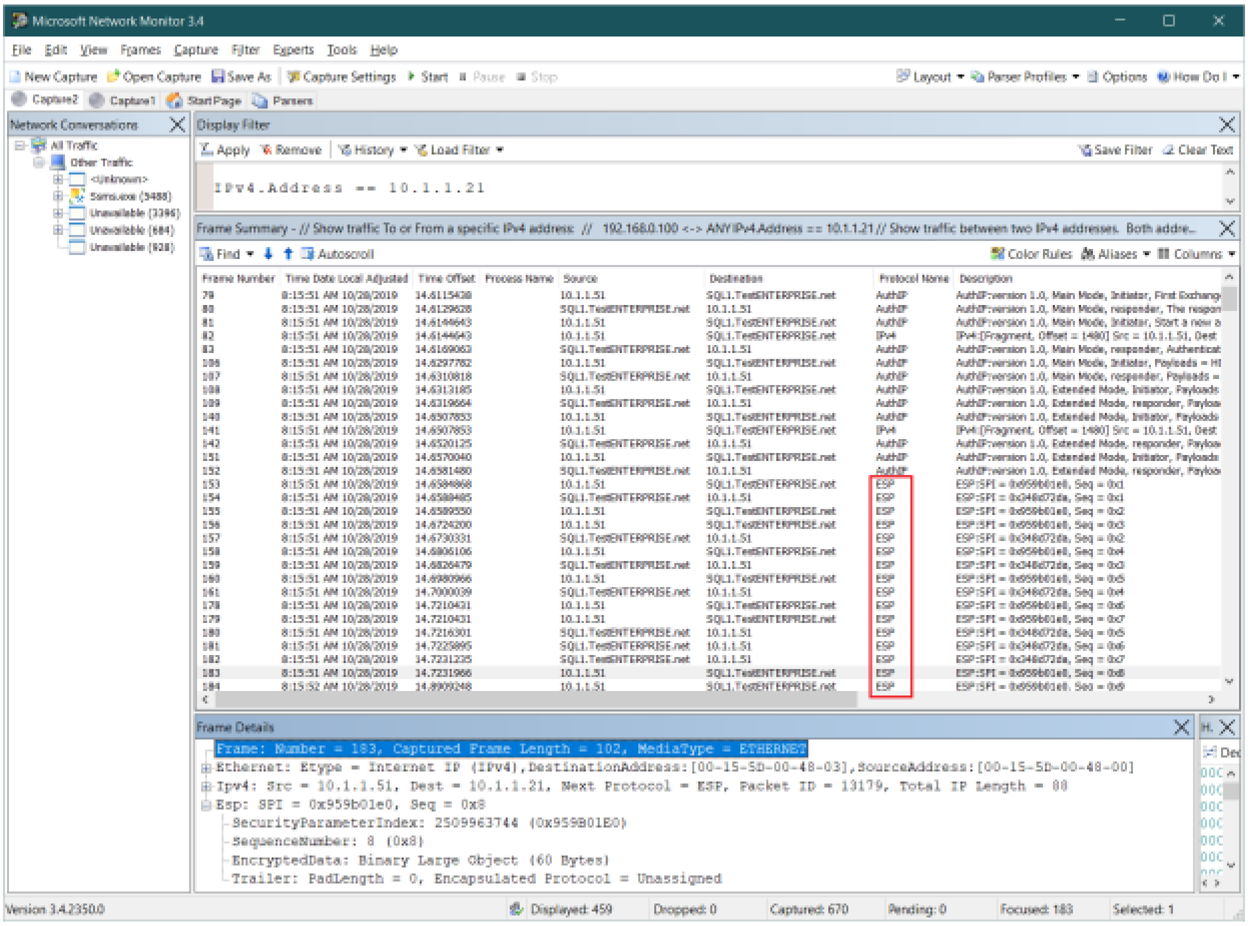
```
Frame: Number = 24, Captured Frame Length = 118, MediaType = ETHERNET
Ethernet: Etype = Internet IP (IPv4),DestinationAddress:[00-15-5D-00-48-00],SourceAddress:
Ipv4: Src = 10.1.1.21, Dest = 10.1.1.51, Next Protocol = ESP, Packet ID = 59447, Total IP
  Versions: IPv4, Internet Protocol; Header Length = 20
  DifferentiatedServicesField: DSCP: 0, ECN: 0
  TotalLength: 104 (0x68)
  Identification: 59447 (0xE837)
  FragmentFlags: 0 (0x0)
  TimeToLive: 128 (0x80)
  NextProtocol: ESP, 50(0x32)
  Checksum: 15331 (0x3BE3)
  SourceAddress: 10.1.1.21
  DestinationAddress: 10.1.1.51
Esp: SPI = 0x6ae928e4, Seq = 0x4
  SecurityParameterIndex: 1793665252 (0x6AE928E4)
  SequenceNumber: 4 (0x4)
  EncryptedData: Binary Large Object (76 Bytes)
  Trailer: PadLength = 0, Encapsulated Protocol = Unassigned
```

Hex Details

```
0000  00 15  ..
0002  5D 00  ].
0004  48 00  H.
0006  00 15  ..
0008  5D 00  ].
000A  48 03  H.
000C  00 00  ..
000E  45 00  E.
0010  00 68  .h
0012  E8 37  è7
0014  00 00  ..
0016  80 32   2
0018  3B E3  ;ã
001A  0A 01  ..
001C  01 15  ..
001E  0A 01  ..
0020  01 33  .3
0022  6A E9  jé
```

Version 3.4.2350.0 Displayed: 13 Captured: 26 Focused: 24 Selected: 1

2.2 Connecting to SQL1 in SSMS from Client1


Microsoft Network Monitor 3.4
File Edit View Frames Capture Filter Experts Tools Help
New Capture Open Capture Save As Capture Settings Start Pause Stop
Layout Parser Profiles Options How Do I
Capture2 Capture1 Start Page Parsers
Network Conversations
All Traffic
Other Traffic
<Unknown>
Svrnsi.exe (5488)
Unavailable (3396)
Unavailable (684)
Unavailable (828)
Display Filter
Apply Remove History Load Filter
Save Filter Clear Text
Find Autoscroll
Color Rules Aliases Columns
Frame Details
Version 3.4.2350.0

```
IPv4.Address == 10.1.1.21
```

Frame Summary - // Show traffic To or From a specific IPv4 address: // 192.168.0.100 <-> ANY IPv4.Address == 10.1.1.21 // Show traffic between two IPv4 addresses. Both addre...

Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
79	8:15:51 AM 10/28/2019	14.6115438		10.1.1.51	SQL1.TestENTERPRISE.net	AuthIP	AuthIP:version 1.0, Main Mode, Initiator, First Exchang
80	8:15:51 AM 10/28/2019	14.6129628		SQL1.TestENTERPRISE.net	10.1.1.51	AuthIP	AuthIP:version 1.0, Main Mode, responder, The respon
81	8:15:51 AM 10/28/2019	14.6144643		10.1.1.51	SQL1.TestENTERPRISE.net	AuthIP	AuthIP:version 1.0, Main Mode, Initiator, Start a new a
82	8:15:51 AM 10/28/2019	14.6144643		10.1.1.51	SQL1.TestENTERPRISE.net	IPv4	IPv4:[Fragment, Offset = 1480] Src = 10.1.1.51, Dest
83	8:15:51 AM 10/28/2019	14.6169063		SQL1.TestENTERPRISE.net	10.1.1.51	AuthIP	AuthIP:version 1.0, Main Mode, responder, Authenticat
106	8:15:51 AM 10/28/2019	14.6297782		10.1.1.51	SQL1.TestENTERPRISE.net	AuthIP	AuthIP:version 1.0, Main Mode, Initiator, Payloads = HI
107	8:15:51 AM 10/28/2019	14.6310818		SQL1.TestENTERPRISE.net	10.1.1.51	AuthIP	AuthIP:version 1.0, Main Mode, responder, Payloads =
108	8:15:51 AM 10/28/2019	14.6313185		10.1.1.51	SQL1.TestENTERPRISE.net	AuthIP	AuthIP:version 1.0, Extended Mode, Initiator, Payloads
109	8:15:51 AM 10/28/2019	14.6319664		SQL1.TestENTERPRISE.net	10.1.1.51	AuthIP	AuthIP:version 1.0, Extended Mode, responder, Payloa
140	8:15:51 AM 10/28/2019	14.6507853		10.1.1.51	SQL1.TestENTERPRISE.net	AuthIP	AuthIP:version 1.0, Extended Mode, Initiator, Payloads
141	8:15:51 AM 10/28/2019	14.6507853		10.1.1.51	SQL1.TestENTERPRISE.net	IPv4	IPv4:[Fragment, Offset = 1480] Src = 10.1.1.51, Dest
142	8:15:51 AM 10/28/2019	14.6520125		SQL1.TestENTERPRISE.net	10.1.1.51	AuthIP	AuthIP:version 1.0, Extended Mode, responder, Payloa
151	8:15:51 AM 10/28/2019	14.6570040		10.1.1.51	SQL1.TestENTERPRISE.net	AuthIP	AuthIP:version 1.0, Extended Mode, Initiator, Payloads
152	8:15:51 AM 10/28/2019	14.6581480		SQL1.TestENTERPRISE.net	10.1.1.51	AuthIP	AuthIP:version 1.0, Extended Mode, responder, Payloa
153	8:15:51 AM 10/28/2019	14.6584868		10.1.1.51	SQL1.TestENTERPRISE.net	ESP	ESP:SPI = 0x959b01e0, Seq = 0x1
154	8:15:51 AM 10/28/2019	14.6588485		SQL1.TestENTERPRISE.net	10.1.1.51	ESP	ESP:SPI = 0x348d72da, Seq = 0x1
155	8:15:51 AM 10/28/2019	14.6589550		10.1.1.51	SQL1.TestENTERPRISE.net	ESP	ESP:SPI = 0x959b01e0, Seq = 0x2
156	8:15:51 AM 10/28/2019	14.6724200		10.1.1.51	SQL1.TestENTERPRISE.net	ESP	ESP:SPI = 0x959b01e0, Seq = 0x3
157	8:15:51 AM 10/28/2019	14.6730331		SQL1.TestENTERPRISE.net	10.1.1.51	ESP	ESP:SPI = 0x348d72da, Seq = 0x2
158	8:15:51 AM 10/28/2019	14.6806106		10.1.1.51	SQL1.TestENTERPRISE.net	ESP	ESP:SPI = 0x959b01e0, Seq = 0x4
159	8:15:51 AM 10/28/2019	14.6826479		SQL1.TestENTERPRISE.net	10.1.1.51	ESP	ESP:SPI = 0x348d72da, Seq = 0x3
160	8:15:51 AM 10/28/2019	14.6980966		10.1.1.51	SQL1.TestENTERPRISE.net	ESP	ESP:SPI = 0x959b01e0, Seq = 0x5
161	8:15:51 AM 10/28/2019	14.7000039		SQL1.TestENTERPRISE.net	10.1.1.51	ESP	ESP:SPI = 0x348d72da, Seq = 0x4
178	8:15:51 AM 10/28/2019	14.7210431		10.1.1.51	SQL1.TestENTERPRISE.net	ESP	ESP:SPI = 0x959b01e0, Seq = 0x6
179	8:15:51 AM 10/28/2019	14.7210431		10.1.1.51	SQL1.TestENTERPRISE.net	ESP	ESP:SPI = 0x959b01e0, Seq = 0x7
180	8:15:51 AM 10/28/2019	14.7216301		SQL1.TestENTERPRISE.net	10.1.1.51	ESP	ESP:SPI = 0x348d72da, Seq = 0x5
181	8:15:51 AM 10/28/2019	14.7225895		SQL1.TestENTERPRISE.net	10.1.1.51	ESP	ESP:SPI = 0x348d72da, Seq = 0x6
182	8:15:51 AM 10/28/2019	14.7231225		SQL1.TestENTERPRISE.net	10.1.1.51	ESP	ESP:SPI = 0x348d72da, Seq = 0x7
183	8:15:51 AM 10/28/2019	14.7231966		10.1.1.51	SQL1.TestENTERPRISE.net	ESP	ESP:SPI = 0x959b01e0, Seq = 0x8
184	8:15:52 AM 10/28/2019	14.8909248		10.1.1.51	SQL1.TestENTERPRISE.net	ESP	ESP:SPI = 0x959b01e0, Seq = 0x9

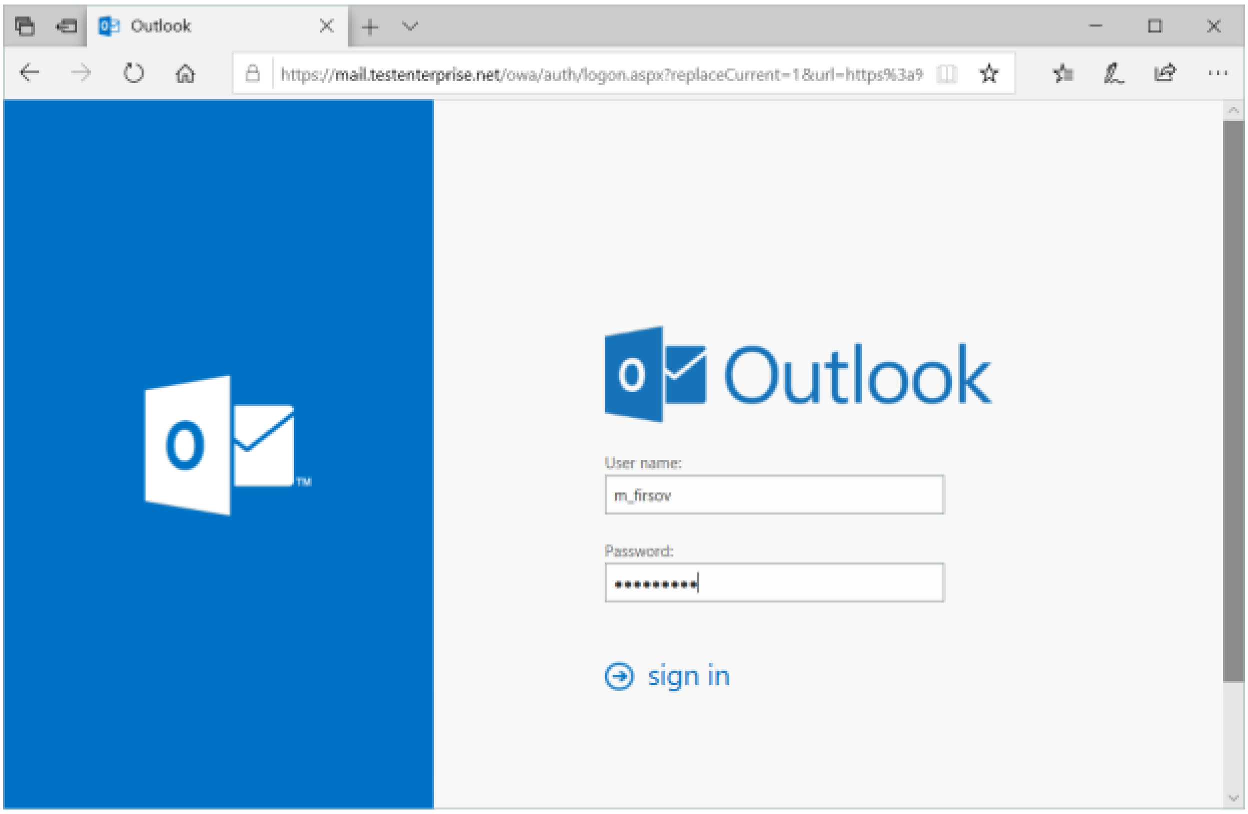
```
Frame: Number = 183, Captured Frame Length = 102, MediaType = ETHERNET
Ethernet: Etype = Internet IP (IPv4),DestinationAddress:[00-15-5D-00-48-03],SourceAddress:[00-15-5D-00-48-00]
Ipv4: Src = 10.1.1.51, Dest = 10.1.1.21, Next Protocol = ESP, Packet ID = 13179, Total IP Length = 88
Esp: SPI = 0x959b01e0, Seq = 0x8
  SecurityParameterIndex: 2509963744 (0x959B01E0)
  SequenceNumber: 8 (0x8)
  EncryptedData: Binary Large Object (60 Bytes)
  Trailer: PadLength = 0, Encapsulated Protocol = Unassigned
```

Displayed: 459 Dropped: 0 Captured: 670 Pending: 0 Focused: 183 Selected: 1

As you see enabling ESP encryption helps disclose only ip-related information, hiding the higher-level packet information from potential network sniffer user.

And the last test: how will the traffic from a secure client to a non-secure host look like?

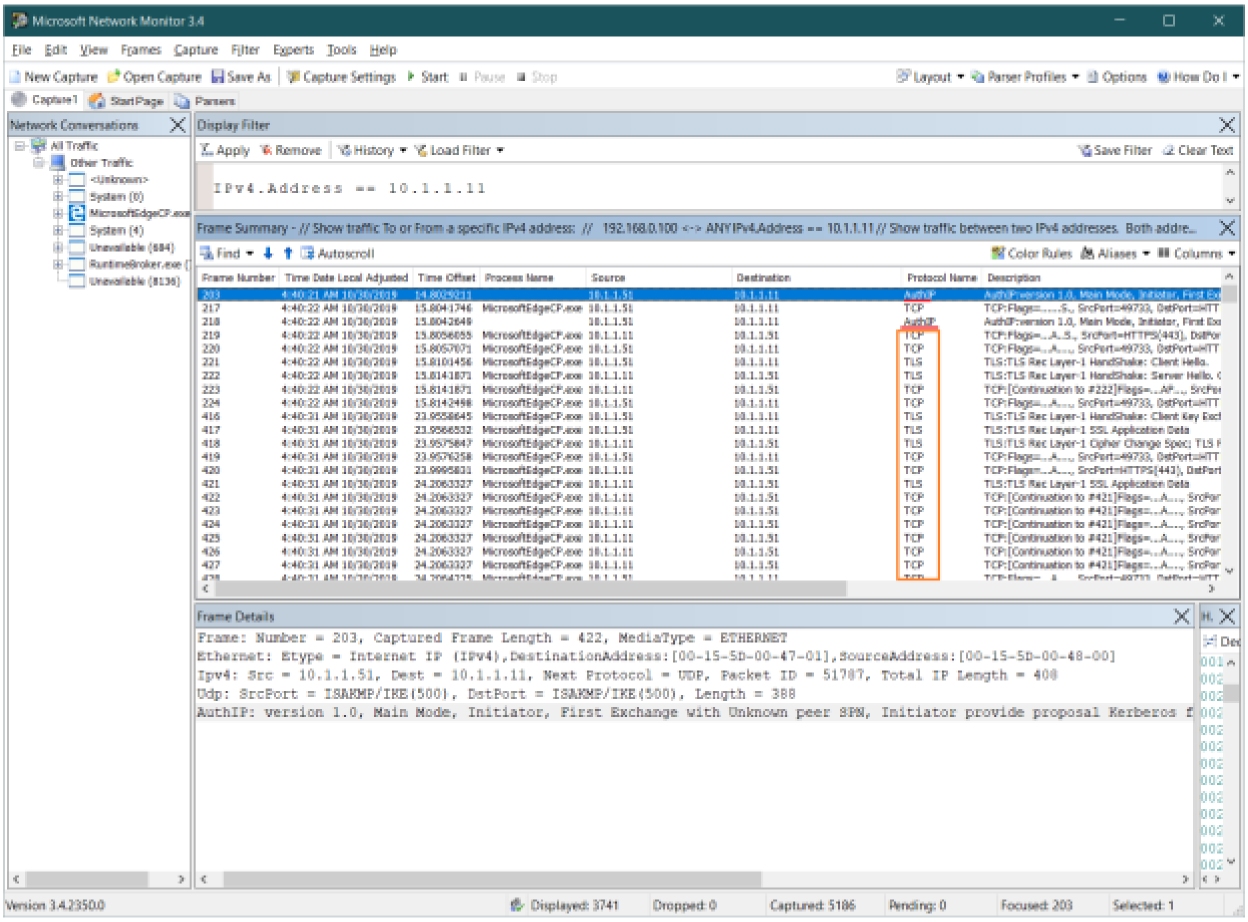
Test 3: Connecting to Exch1 from Client1


Outlook
https://mail.testenterprise.net/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a9
Outlook
sign in

User name: m_firsov

Password: ●●●●●●●●●

The trace:



```
IPv4.Address == 10.1.1.11
```

Frame Summary - // Show traffic To or From a specific IPv4 address: // 192.168.0.100 <-> ANYIPv4.Address == 10.1.1.11 // Show traffic between two IPv4 addresses. Both addre...

Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
203	4:40:21 AM 10/30/2019	14.8029211		10.1.1.51	10.1.1.11	AuthIP	AuthIP:version 1.0, Main Mode, Initiator, First Ex
217	4:40:22 AM 10/30/2019	15.8041746	MicrosoftEdgeCP.exe	10.1.1.51	10.1.1.11	TCP	TCP:Flags=......S., SrcPort=49733, DstPort=HTT
218	4:40:22 AM 10/30/2019	15.8042649		10.1.1.51	10.1.1.11	AuthIP	AuthIP:version 1.0, Main Mode, Initiator, First Ex
219	4:40:22 AM 10/30/2019	15.8056055	MicrosoftEdgeCP.exe	10.1.1.11	10.1.1.51	TCP	TCP:Flags=...A..S., SrcPort=HTTPS(443), DstPor
220	4:40:22 AM 10/30/2019	15.8057071	MicrosoftEdgeCP.exe	10.1.1.51	10.1.1.11	TCP	TCP:Flags=...A...., SrcPort=49733, DstPort=HTT
221	4:40:22 AM 10/30/2019	15.8101456	MicrosoftEdgeCP.exe	10.1.1.51	10.1.1.11	TLS	TLS:TLS Rec Layer-1 HandShake: Client Hello.
222	4:40:22 AM 10/30/2019	15.8141871	MicrosoftEdgeCP.exe	10.1.1.11	10.1.1.51	TLS	TLS:TLS Rec Layer-1 HandShake: Server Hello. (
223	4:40:22 AM 10/30/2019	15.8141871	MicrosoftEdgeCP.exe	10.1.1.11	10.1.1.51	TCP	TCP:[Continuation to #222]Flags=...AP..., SrcPor
224	4:40:22 AM 10/30/2019	15.8142498	MicrosoftEdgeCP.exe	10.1.1.51	10.1.1.11	TCP	TCP:Flags=...A...., SrcPort=49733, DstPort=HTT
416	4:40:31 AM 10/30/2019	23.9558645	MicrosoftEdgeCP.exe	10.1.1.51	10.1.1.11	TLS	TLS:TLS Rec Layer-1 HandShake: Client Key Exc
417	4:40:31 AM 10/30/2019	23.9566532	MicrosoftEdgeCP.exe	10.1.1.51	10.1.1.11	TLS	TLS:TLS Rec Layer-1 SSL Application Data
418	4:40:31 AM 10/30/2019	23.9575847	MicrosoftEdgeCP.exe	10.1.1.11	10.1.1.51	TLS	TLS:TLS Rec Layer-1 Cipher Change Spec; TLS F
419	4:40:31 AM 10/30/2019	23.9576258	MicrosoftEdgeCP.exe	10.1.1.51	10.1.1.11	TCP	TCP:Flags=...A...., SrcPort=49733, DstPort=HTT
420	4:40:31 AM 10/30/2019	23.9995831	MicrosoftEdgeCP.exe	10.1.1.11	10.1.1.51	TCP	TCP:Flags=...A...., SrcPort=HTTPS(443), DstPort
421	4:40:31 AM 10/30/2019	24.2063327	MicrosoftEdgeCP.exe	10.1.1.11	10.1.1.51	TLS	TLS:TLS Rec Layer-1 SSL Application Data
422	4:40:31 AM 10/30/2019	24.2063327	MicrosoftEdgeCP.exe	10.1.1.11	10.1.1.51	TCP	TCP:[Continuation to #421]Flags=...A...., SrcPor
423	4:40:31 AM 10/30/2019	24.2063327	MicrosoftEdgeCP.exe	10.1.1.11	10.1.1.51	TCP	TCP:[Continuation to #421]Flags=...A...., SrcPor
424	4:40:31 AM 10/30/2019	24.2063327	MicrosoftEdgeCP.exe	10.1.1.11	10.1.1.51	TCP	TCP:[Continuation to #421]Flags=...A...., SrcPor
425	4:40:31 AM 10/30/2019	24.2063327	MicrosoftEdgeCP.exe	10.1.1.11	10.1.1.51	TCP	TCP:[Continuation to #421]Flags=...A...., SrcPor
426	4:40:31 AM 10/30/2019	24.2063327	MicrosoftEdgeCP.exe	10.1.1.11	10.1.1.51	TCP	TCP:[Continuation to #421]Flags=...A...., SrcPor
427	4:40:31 AM 10/30/2019	24.2063327	MicrosoftEdgeCP.exe	10.1.1.11	10.1.1.51	TCP	TCP:[Continuation to #421]Flags=...A...., SrcPor

```
Frame: Number = 203, Captured Frame Length = 422, MediaType = ETHERNET
Ethernet: Etype = Internet IP (IPv4),DestinationAddress:[00-15-5D-00-47-01],SourceAddress:[00-15-5D-00-48-00]
Ipv4: Src = 10.1.1.51, Dest = 10.1.1.11, Next Protocol = UDP, Packet ID = 51787, Total IP Length = 408
Udp: SrcPort = ISAKMP/IKE(500), DstPort = ISAKMP/IKE(500), Length = 388
AuthIP: version 1.0, Main Mode, Initiator, First Exchange with Unknown peer SPN, Initiator provide proposal Kerberos f
```

Version 3.4.2350.0 Displayed: 3741 Dropped: 0 Captured: 5186 Pending: 0 Focused: 203 Selected: 1

The result: Client1 first tries authenticated connection and then falls back to the plain session.

In part 2 we’ll see how we can further restrict access to the secure servers.