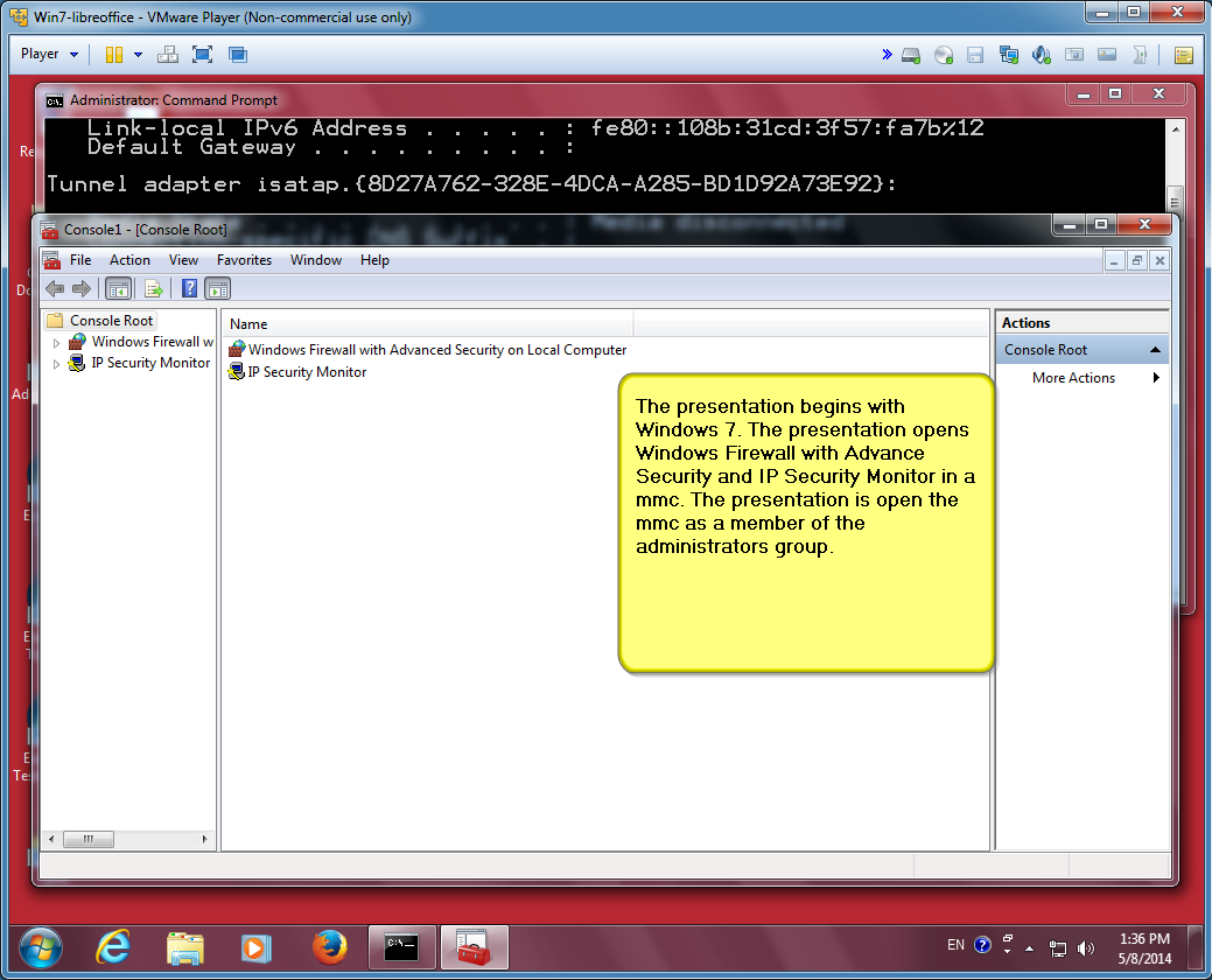
Windows simple IPsec setup for IPv6

The presentation uses the Windows Firewall with Advance Security to configure a simple IPv6 IPsec network. One system is a Windows 7 system. The other system is Windows 8.0 system. Both machines are on a private IPv6 network.

The primary reference is http://technet.microsoft.com/en-us/library/cc732283%28v=ws.10%29.aspx

Preuss
5/8/2014

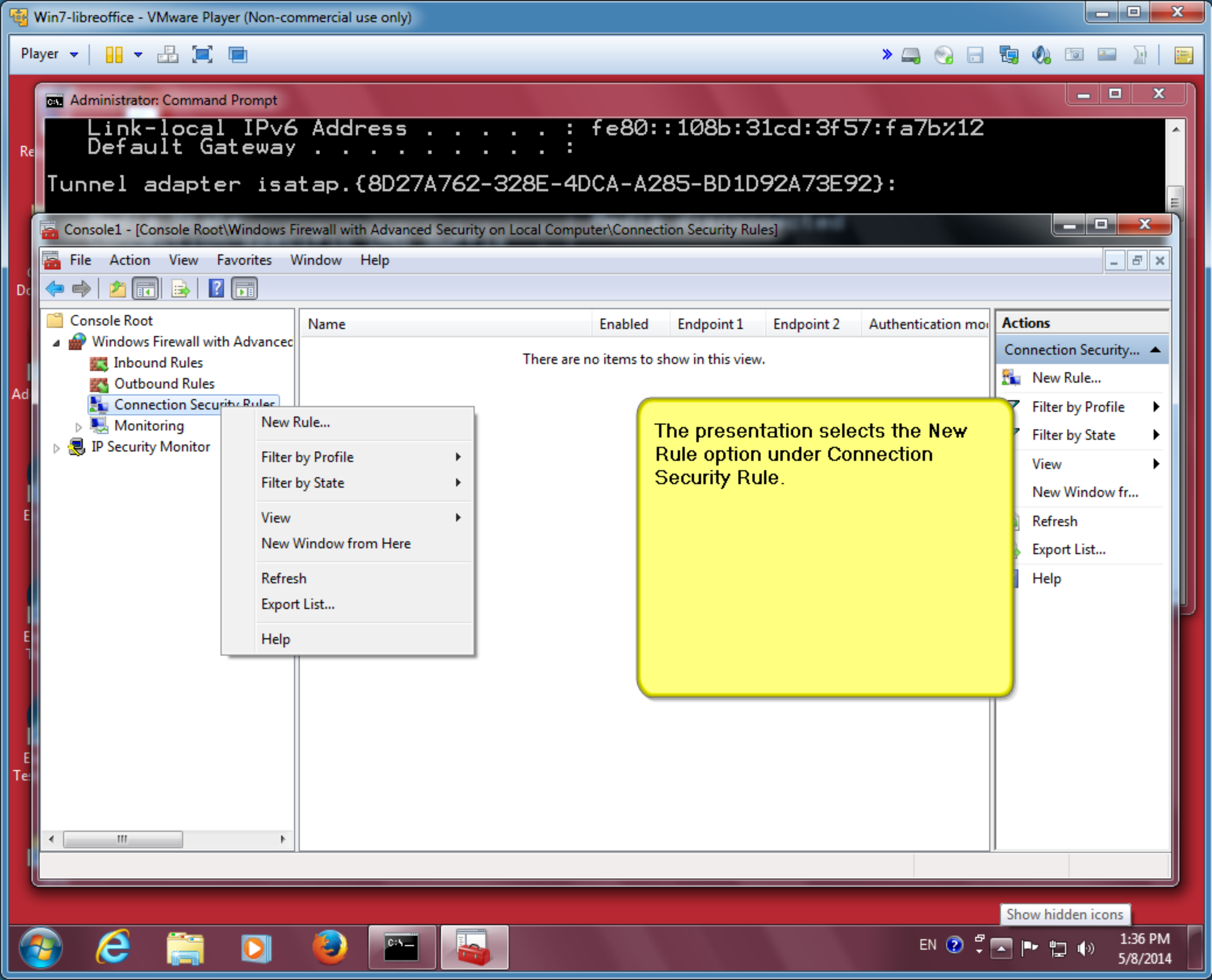


```
   Link-local IPv6 Address . . . . . : fe80::108b:31cd:3f57:fa7b%12
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{8D27A762-328E-4DCA-A285-BD1D92A73E92}:
```

Windows Firewall with Advanced Security on Local Computer

IP Security Monitor

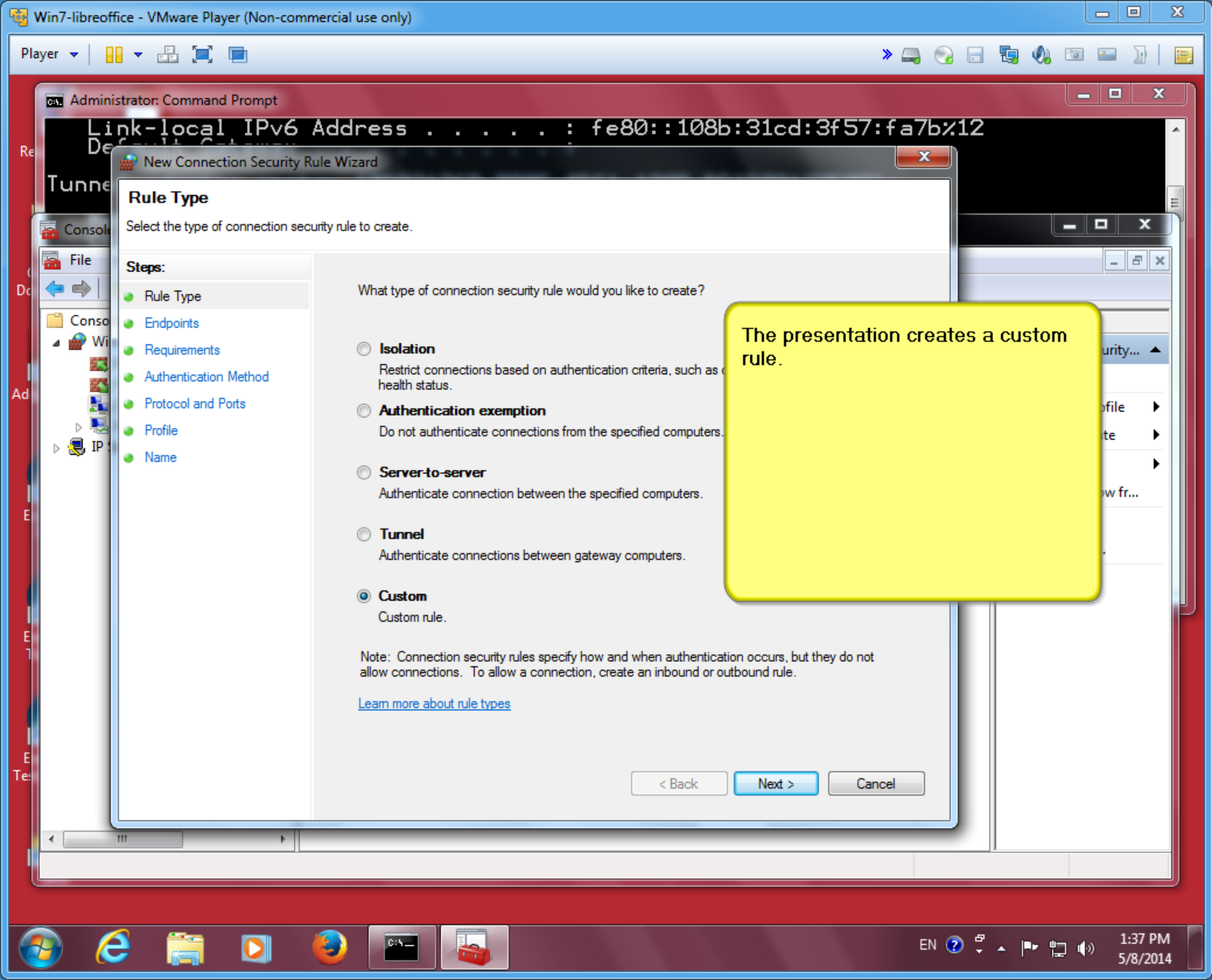
The presentation begins with Windows 7. The presentation opens Windows Firewall with Advance Security and IP Security Monitor in a mmc. The presentation is open the mmc as a member of the administrators group.



Win7-libreoffice - VMware Player (Non-commercial use only)
Player
Administrator: Command Prompt

```
   Link-local IPv6 Address . . . . . : fe80::108b:31cd:3f57:fa7b%12
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{8D27A762-328E-4DCA-A285-BD1D92A73E92}:
```

The presentation selects the New Rule option under Connection Security Rule.



Win7-libreoffice - VMware Player (Non-commercial use only)
Player
Administrator: Command Prompt

```
   Link-local IPv6 Address . . . . . : fe80::108b:31cd:3f57:fa7b%12
   De
Tunne
```

New Connection Security Rule Wizard

Rule Type

Select the type of connection security rule to create.

Steps:
Rule Type
Endpoints
Requirements
Authentication Method
Protocol and Ports
Profile
Name

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

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

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

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

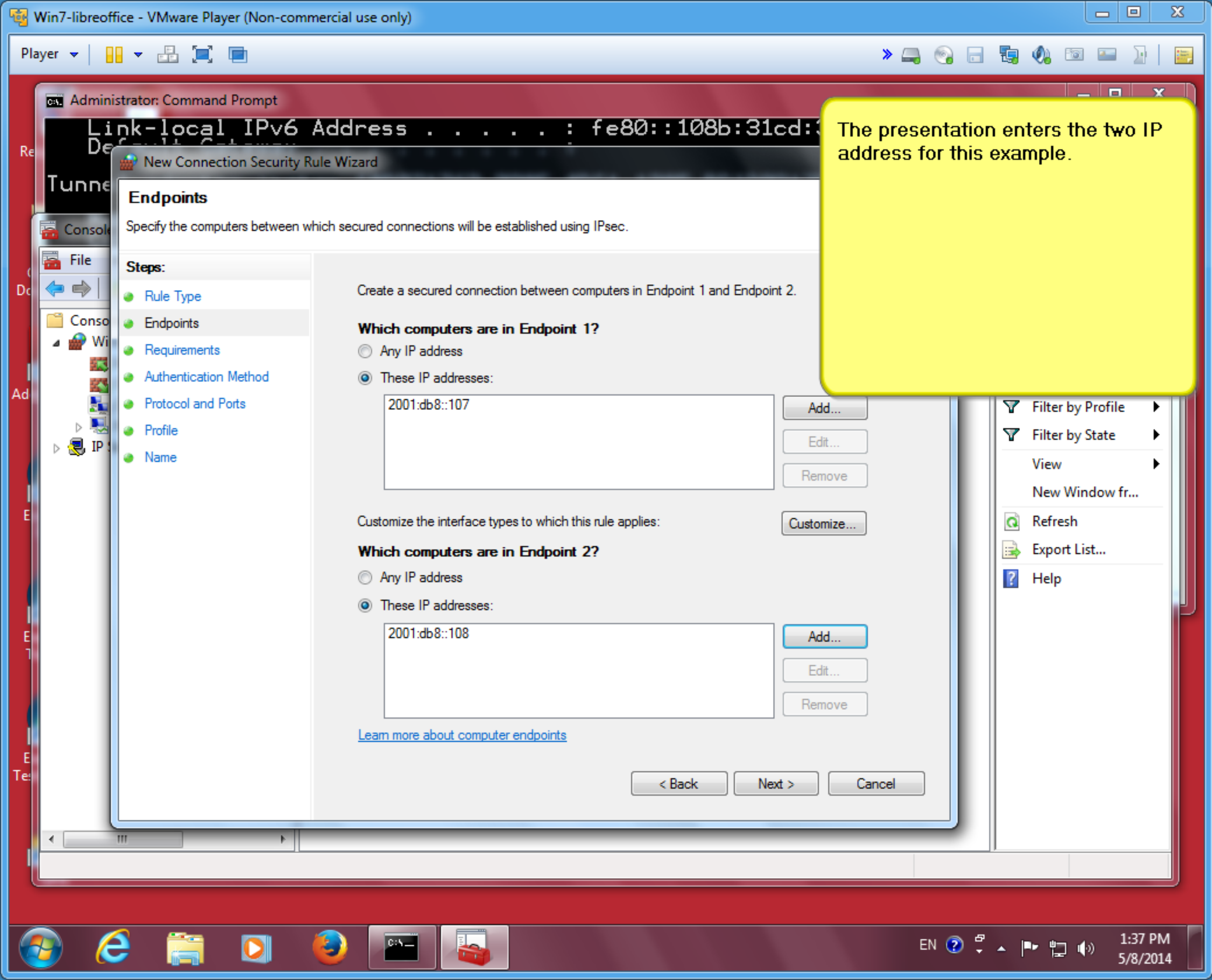
○ **Tunnel**
Authenticate connections between gateway computers.

● **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.

Learn more about rule types

The presentation creates a custom rule.



Win7-libreoffice - VMware Player (Non-commercial use only)
Player
Administrator: Command Prompt
Link-local IPv6 Address . . . . . : fe80::108b:31cd:3
Tunne
Console
File
Wi
IP
Filter by Profile
Filter by State
View
New Window fr...
Refresh
Export List...
Help
EN
1:37 PM
5/8/2014

The presentation enters the two IP address for this example.

New Connection Security Rule Wizard

Endpoints

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

Steps:

- Rule Type
- Endpoints
- Requirements
- Authentication Method
- Protocol and Ports
- Profile
- Name

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

Which computers are in Endpoint 1?

○ Any IP address

● These IP addresses:

2001:db8::107

Add... Edit... Remove

Customize the interface types to which this rule applies: Customize...

Which computers are in Endpoint 2?

○ Any IP address

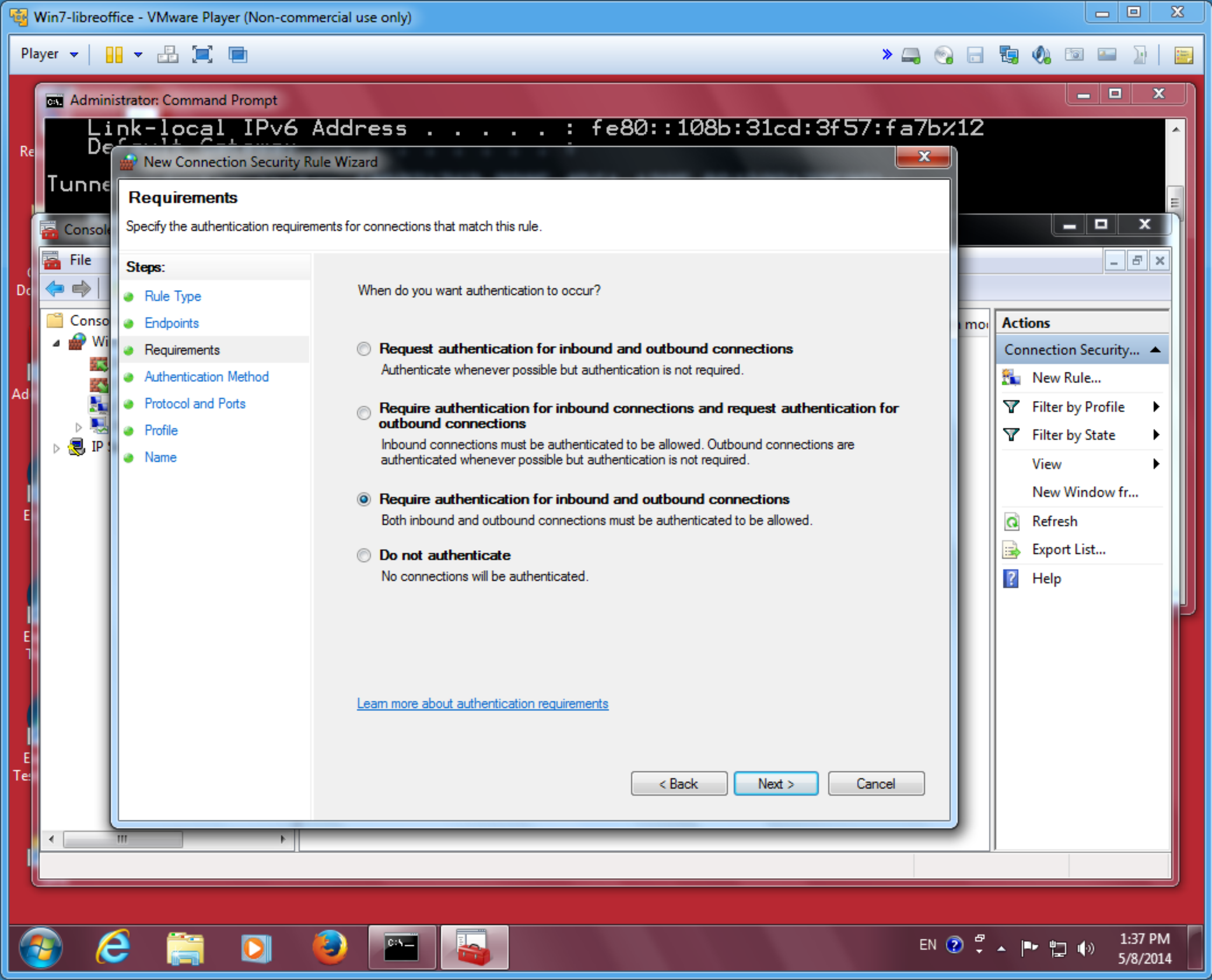
● These IP addresses:

2001:db8::108

Add... Edit... Remove

Learn more about computer endpoints

< Back Next > Cancel



```
   Link-local IPv6 Address . . . . . : fe80::108b:31cd:3f57:fa7b%12
```

New Connection Security Rule Wizard

Requirements

Specify the authentication requirements for connections that match this rule.

Steps:

- Rule Type
- Endpoints
- Requirements
- Authentication Method
- Protocol and Ports
- Profile
- Name

When do you want authentication to occur?

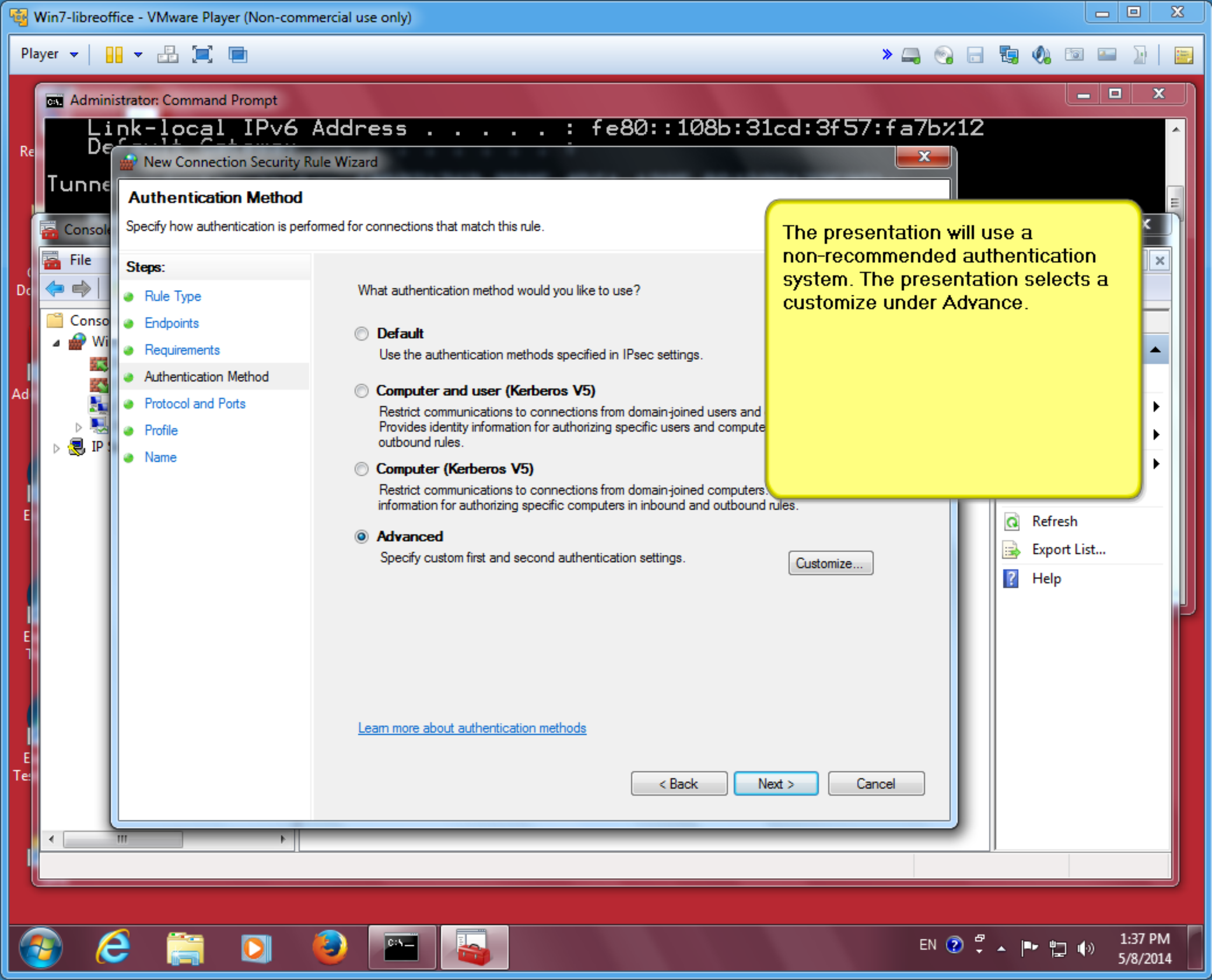
○ **Request authentication for inbound and outbound connections**
Authenticate whenever possible but authentication is not required.

○ **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.

○ **Do not authenticate**
No connections will be authenticated.

Learn more about authentication requirements



Win7-libreoffice - VMware Player (Non-commercial use only)

Administrator: Command Prompt

```
   Link-local IPv6 Address . . . . . : fe80::108b:31cd:3f57:fa7b%12
   De
Tunne
```

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
- Protocol and Ports
- 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
Provides identity information for authorizing specific users and compute
outbound rules.

○ **Computer (Kerberos V5)**

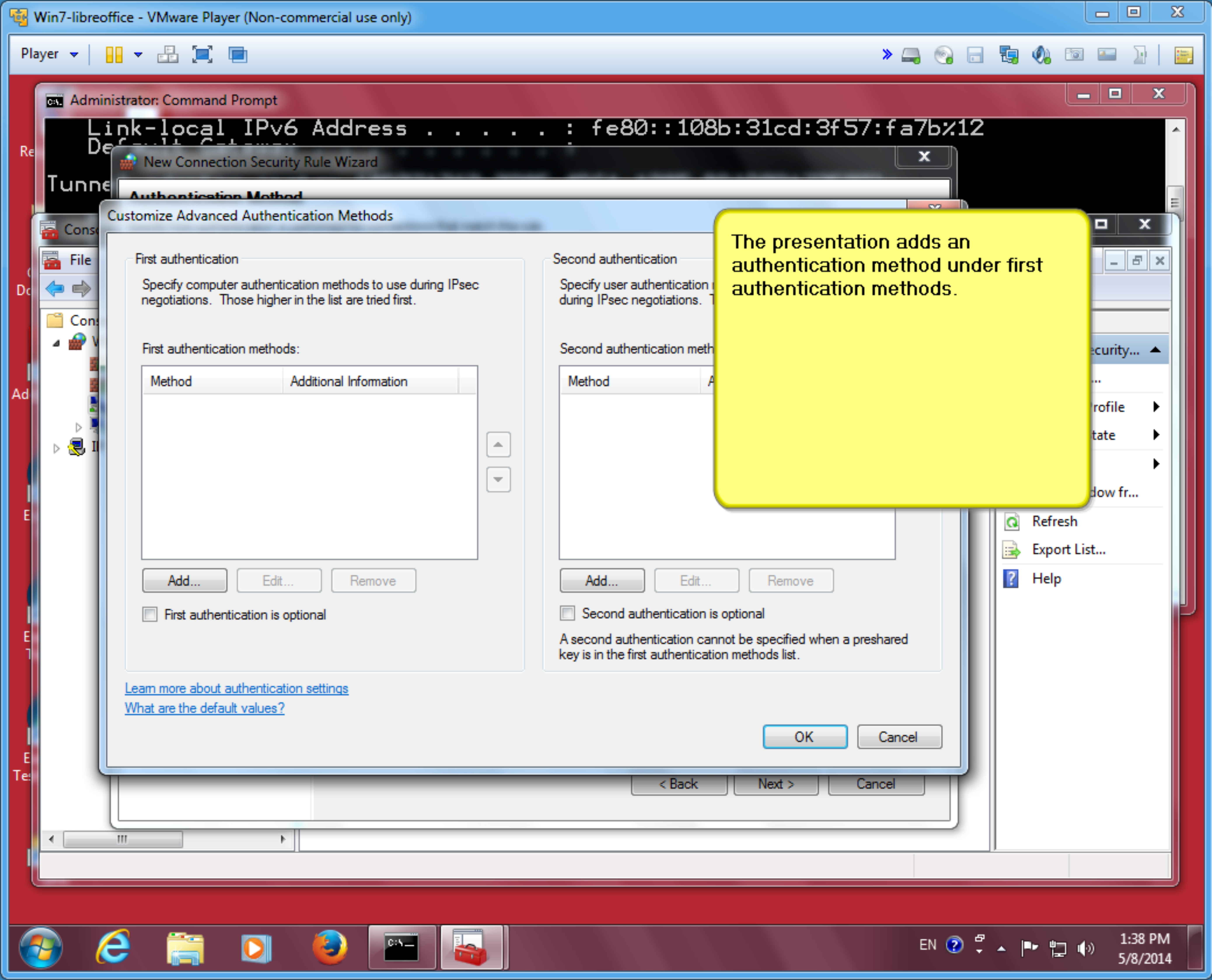
Restrict communications to connections from domain-joined computers.
information for authorizing specific computers in inbound and outbound rules.

● **Advanced**

Specify custom first and second authentication settings.

Learn more about authentication methods

The presentation will use a non-recommended authentication system. The presentation selects a customize under Advance.


Win7-libreoffice - VMware Player (Non-commercial use only)
Player
Administrator: Command Prompt
New Connection Security Rule Wizard
Authentication Method
< Back
Next >
Cancel
Refresh
Export List...
Help
EN
1:38 PM
5/8/2014

```
Link-local IPv6 Address . . . . . : fe80::108b:31cd:3f57:fa7b%12
```

The presentation adds an authentication method under first authentication methods.

Customize Advanced Authentication Methods

First authentication

Specify computer authentication methods to use during IPsec negotiations. Those higher in the list are tried first.

First authentication methods:

Method	Additional Information

Add... Edit... Remove

□ First authentication is optional

Second authentication

Specify user authentication during IPsec negotiations.

Second authentication meth

Method

Add... Edit... Remove

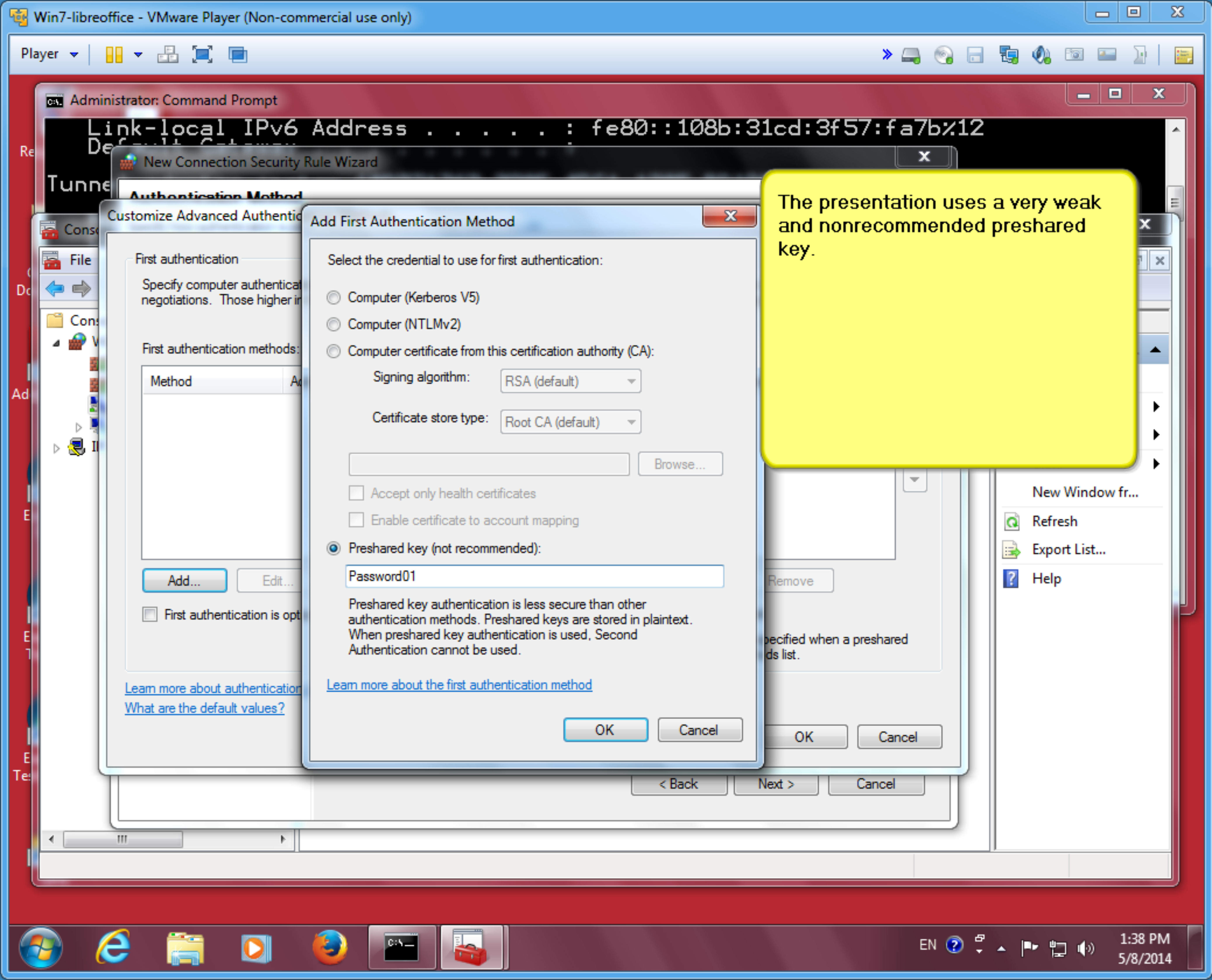
□ Second authentication is optional

A second authentication cannot be specified when a preshared key is in the first authentication methods list.

Learn more about authentication settings

What are the default values?

OK Cancel



The presentation uses a very weak and nonrecommended preshared key.

Win7-libreoffice - VMware Player (Non-commercial use only)

Administrator: Command Prompt

```
   Link-local IPv6 Address . . . . . : fe80::108b:31cd:3f57:fa7b%12
```

New Connection Security Rule Wizard

Authentication Method

Customize Advanced Authentic

First authentication

Specify computer authenticat negotiations. Those higher ir

First authentication methods:

Method	A

Add... Edit... Remove

□ First authentication is opt

pecified when a preshared ds list.

Learn more about authenticatio

What are the default values?

OK Cancel

< Back Next > Cancel

Add First Authentication Method

Select the credential to use for first authentication:

○ Computer (Kerberos V5)

○ Computer (NTLMv2)

○ Computer certificate from this certification authority (CA):

Signing algorithm: RSA (default)

Certificate store type: Root CA (default)

Browse...

□ Accept only health certificates

□ Enable certificate to account mapping

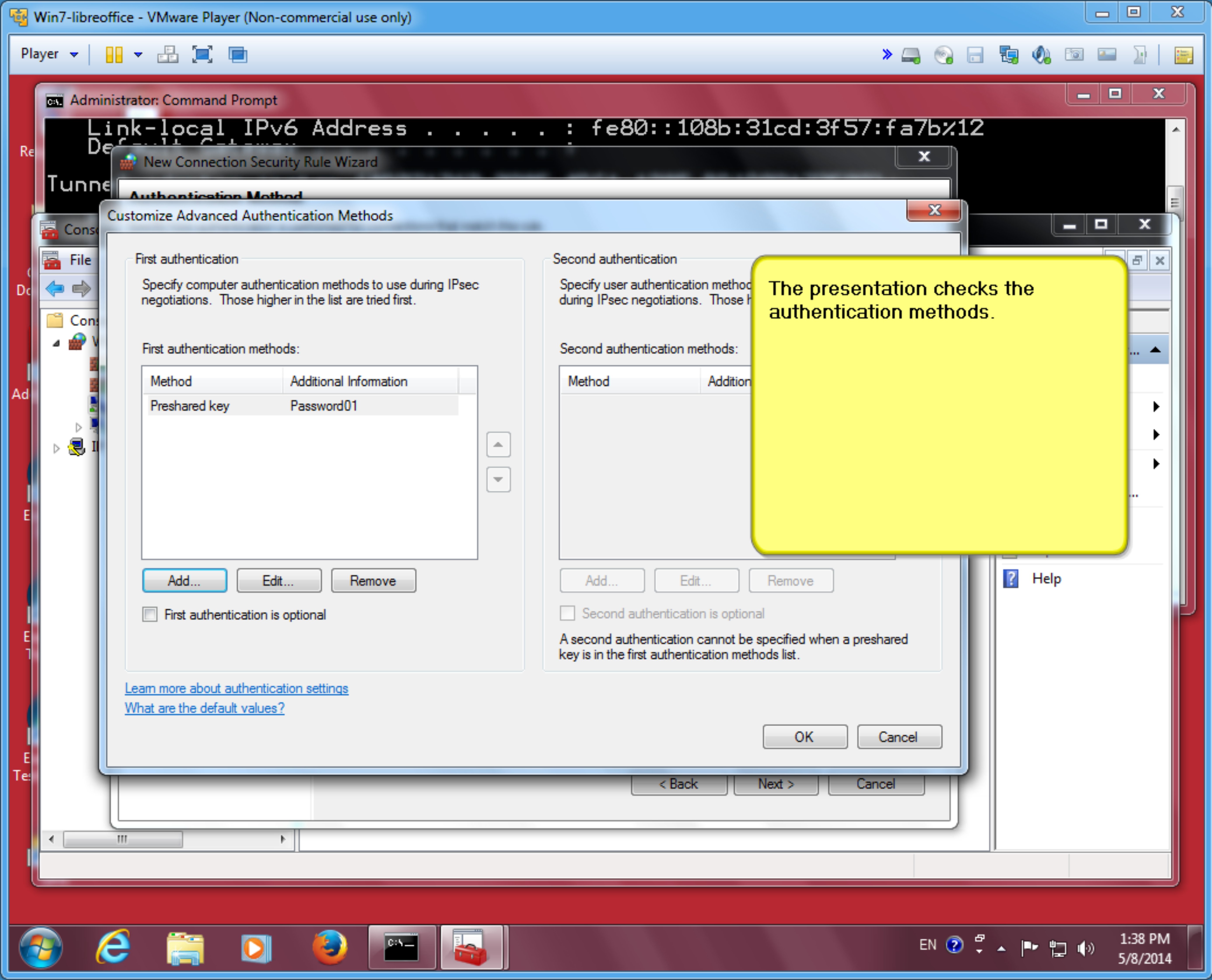
● Preshared key (not recommended):

Password01

Preshared key authentication is less secure than other authentication methods. Preshared keys are stored in plaintext. When preshared key authentication is used, Second Authentication cannot be used.

Learn more about the first authentication method

OK Cancel


Win7-libreoffice - VMware Player (Non-commercial use only)
Player
Administrator: Command Prompt
New Connection Security Rule Wizard
Authentication Method
Customize Advanced Authentication Methods
File
Help
&lt; Back
Next &gt;
Cancel
EN
1:38 PM
5/8/2014

```
Link-local IPv6 Address . . . . . : fe80::108b:31cd:3f57:fa7b%12
```

The presentation checks the authentication methods.

First authentication

Specify computer authentication methods to use during IPsec negotiations. Those higher in the list are tried first.

First authentication methods:

Method	Additional Information
Preshared key	Password01

□ First authentication is optional

Second authentication

Specify user authentication methoc during IPsec negotiations. Those h

Second authentication methods:

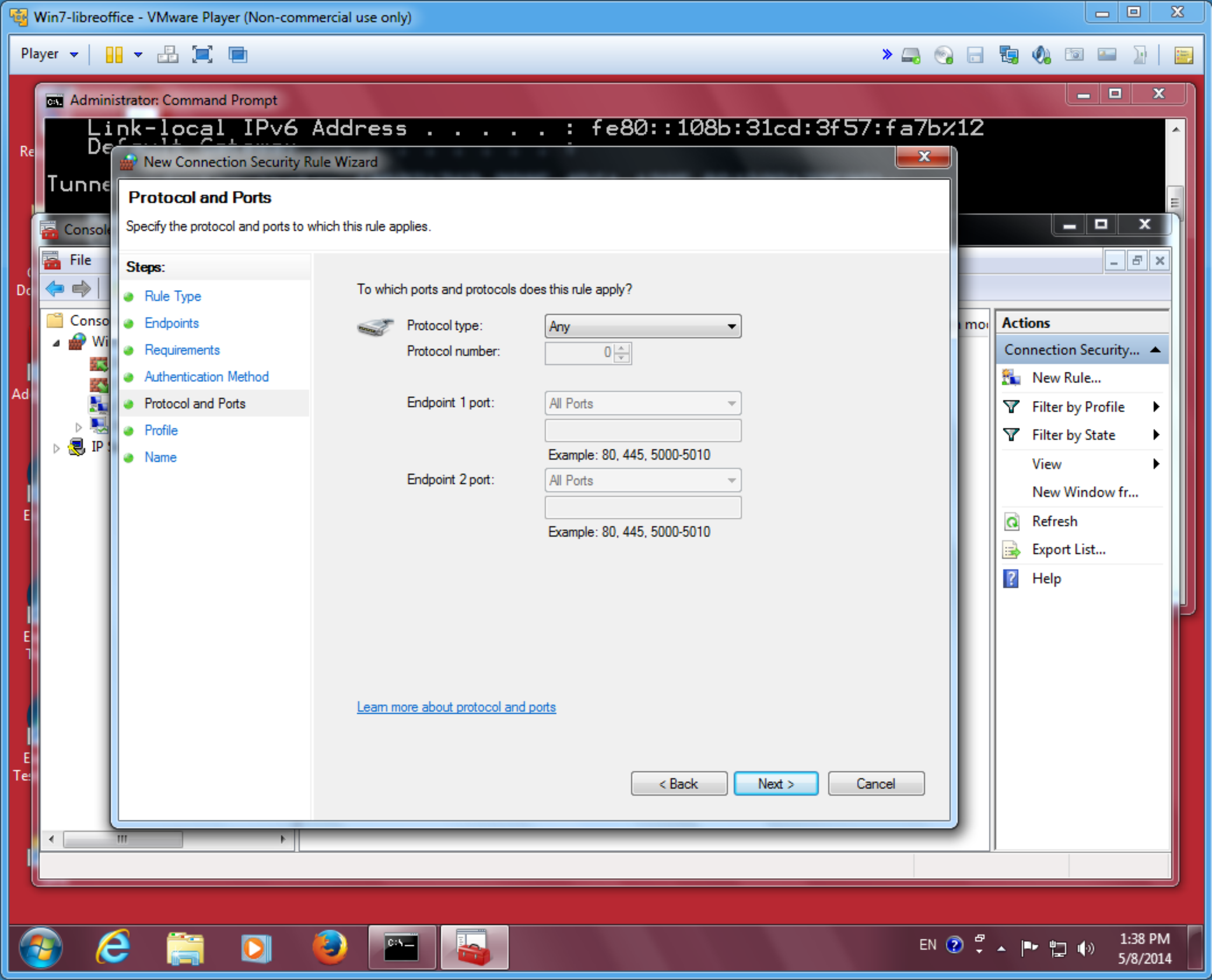
Method	Addition

□ Second authentication is optional

A second authentication cannot be specified when a preshared key is in the first authentication methods list.

Learn more about authentication settings

What are the default values?



```
   Link-local IPv6 Address . . . . . : fe80::108b:31cd:3f57:fa7b%12
```

New Connection Security Rule Wizard

Protocol and Ports

Specify the protocol and ports to which this rule applies.

Steps:

- Rule Type
- Endpoints
- Requirements
- Authentication Method
- Protocol and Ports
- Profile
- Name

To which ports and protocols does this rule apply?

Protocol type: Any

Protocol number: 0

Endpoint 1 port: All Ports

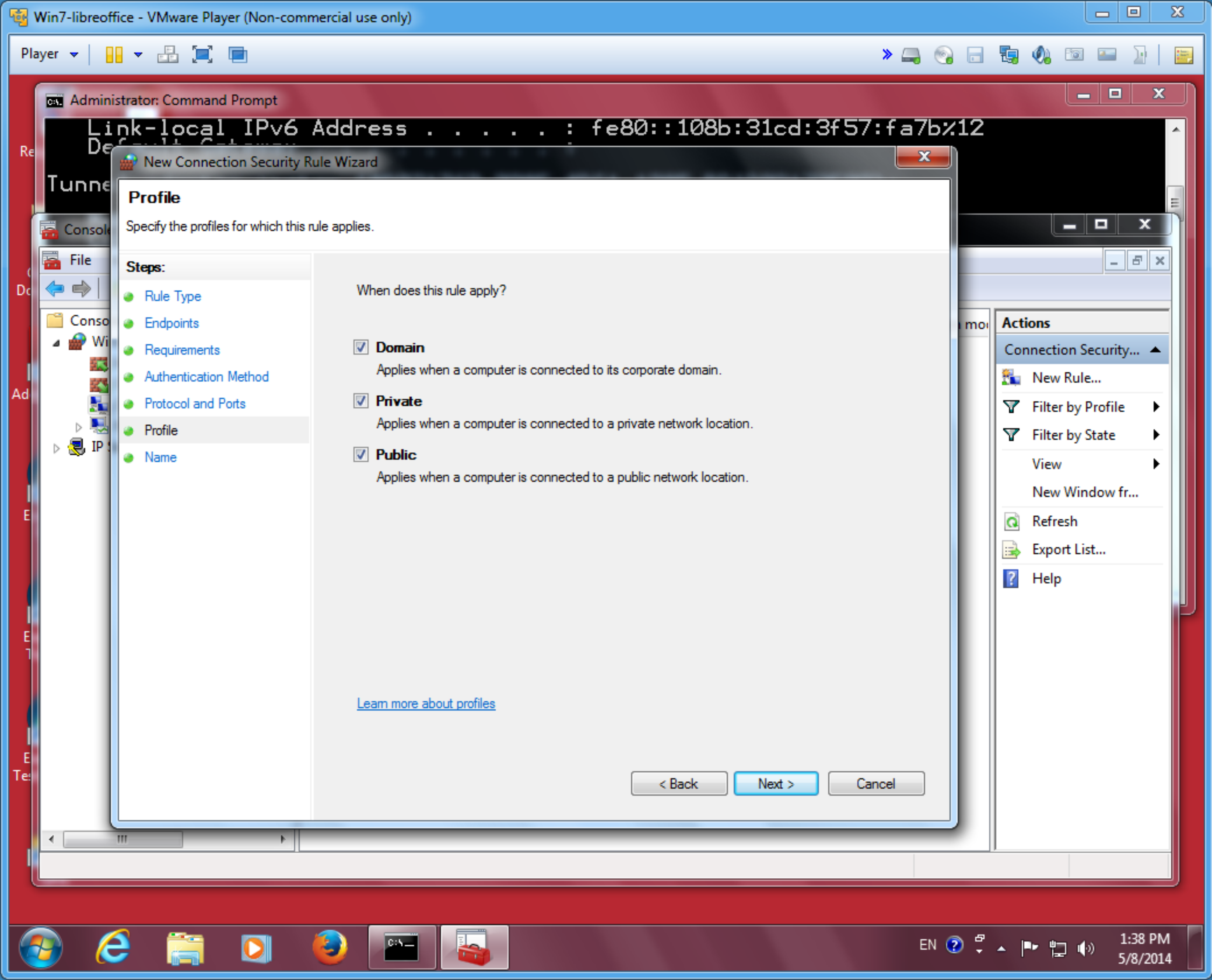
Example: 80, 445, 5000-5010

Endpoint 2 port: All Ports

Example: 80, 445, 5000-5010

Learn more about protocol and ports

< Back | Next > | Cancel



```
Link-local IPv6 Address . . . . . : fe80::108b:31cd:3f57:fa7b%12
```

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.

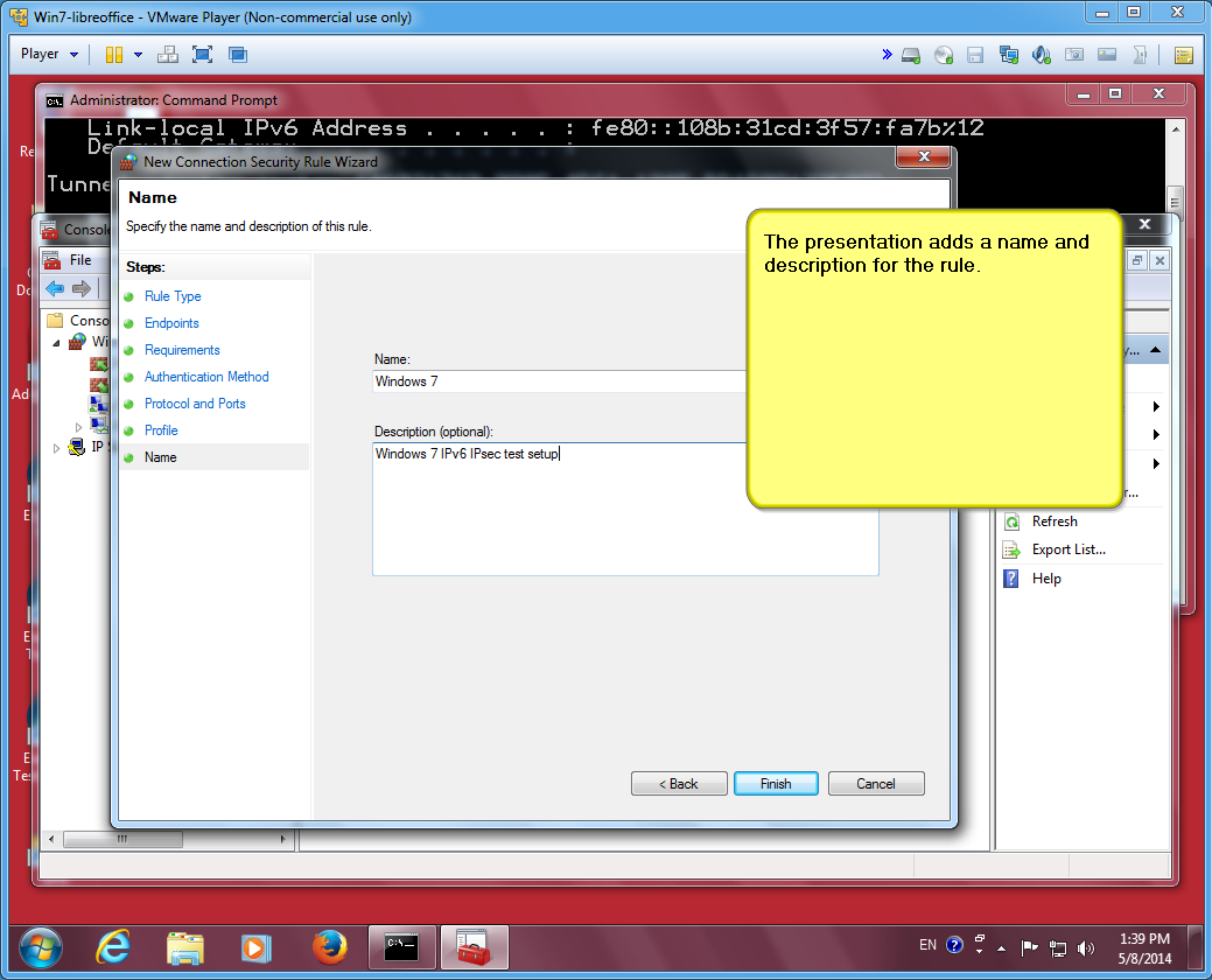
☑ **Private**

Applies when a computer is connected to a private network location.

☑ **Public**

Applies when a computer is connected to a public network location.

Learn more about profiles



Win7-libreoffice - VMware Player (Non-commercial use only)
Player
Administrator: Command Prompt
New Connection Security Rule Wizard
Console
File
Refresh
Export List...
Help
< Back
Finish
Cancel
EN
1:39 PM
5/8/2014

```
   Link-local IPv6 Address . . . . . : fe80::108b:31cd:3f57:fa7b%12
```

The presentation adds a name and description for the rule.

Name

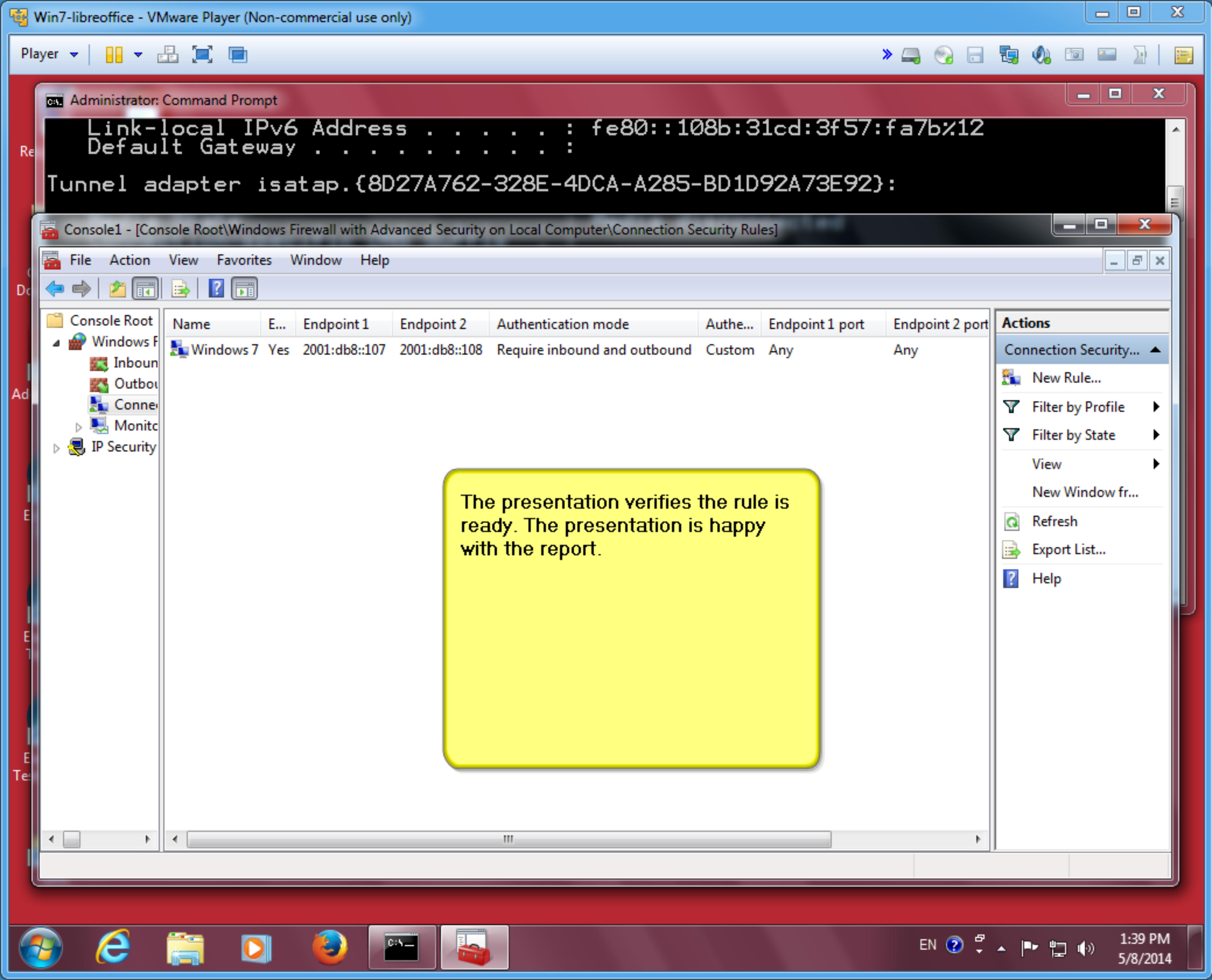
Specify the name and description of this rule.

Steps:

- Rule Type
- Endpoints
- Requirements
- Authentication Method
- Protocol and Ports
- Profile
- Name

Name: Windows 7

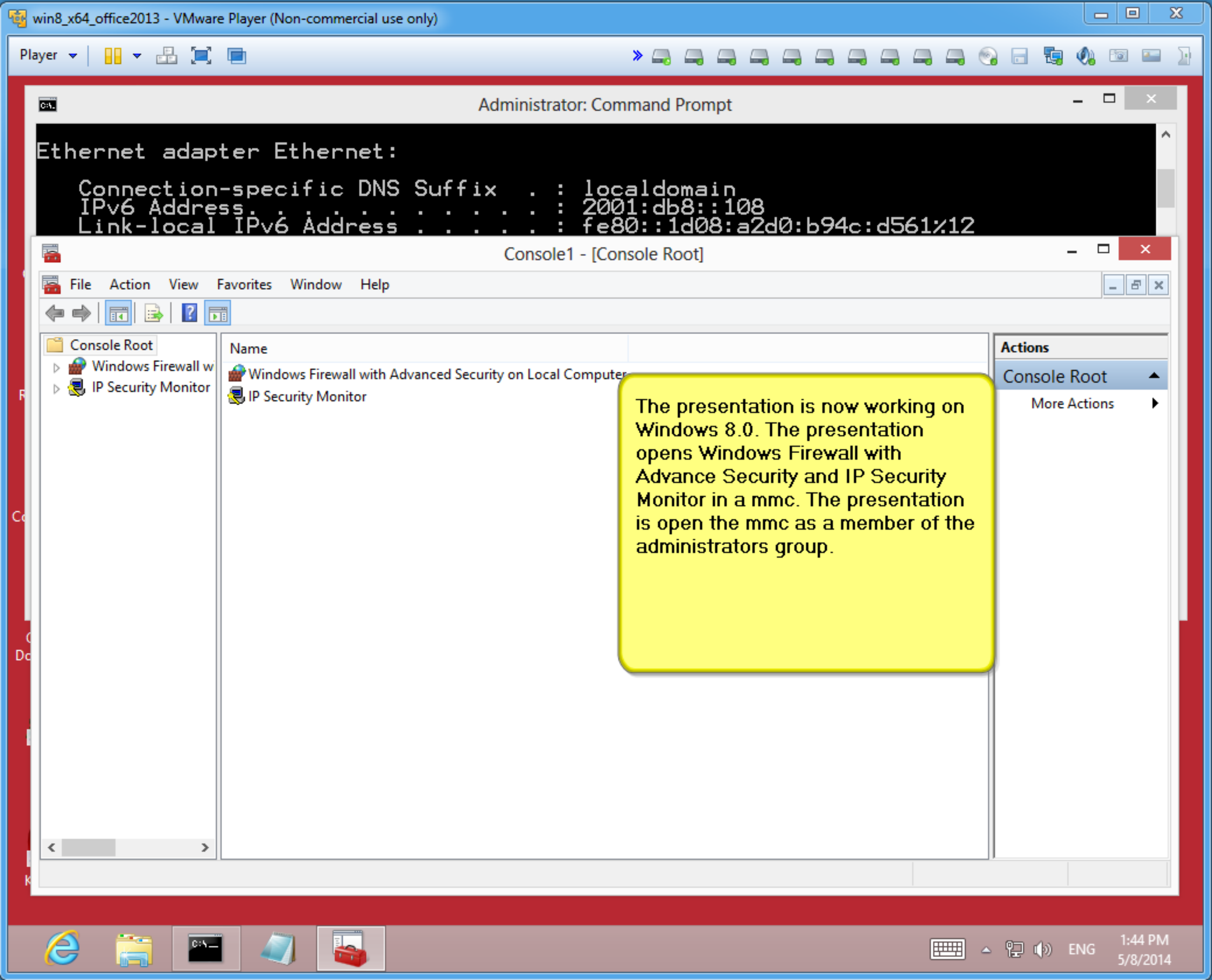
Description (optional): Windows 7 IPv6 IPsec test setup



```
   Link-local IPv6 Address . . . . . : fe80::108b:31cd:3f57:fa7b%12
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{8D27A762-328E-4DCA-A285-BD1D92A73E92}:
```

Name	E...	Endpoint 1	Endpoint 2	Authentication mode	Authe...	Endpoint 1 port	Endpoint 2 port
Windows 7	Yes	2001:db8::107	2001:db8::108	Require inbound and outbound	Custom	Any	Any

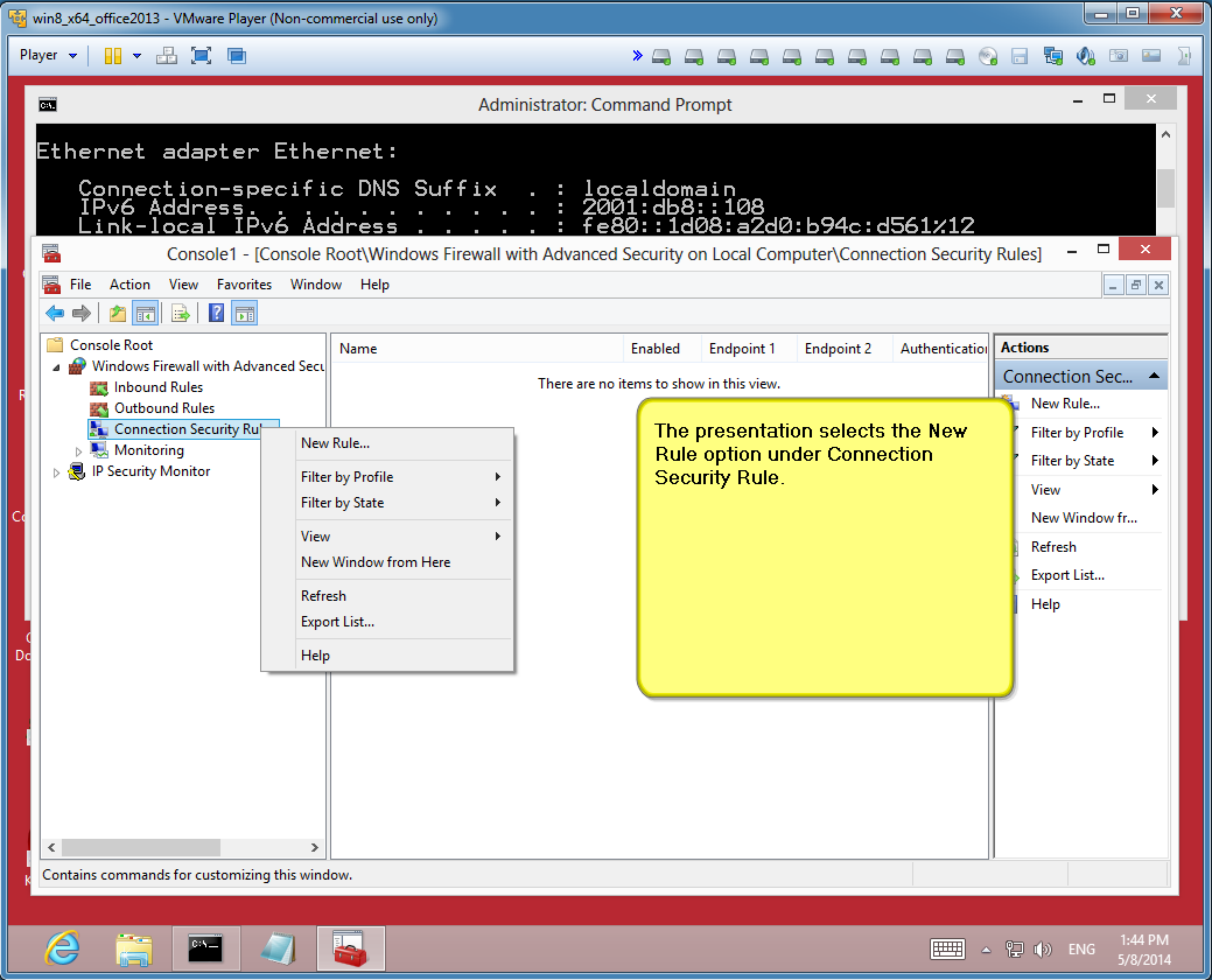
The presentation verifies the rule is ready. The presentation is happy with the report.



win8_x64_office2013 - VMware Player (Non-commercial use only)
Player
Administrator: Command Prompt
Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
Console Root
Windows Firewall w
IP Security Monitor
Name
Windows Firewall with Advanced Security on Local Computer
IP Security Monitor
Actions
Console Root
More Actions
ENG
1:44 PM
5/8/2014

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : localdomain
   IPv6 Address. . . . . . . . . . . : 2001:db8::108
   Link-local IPv6 Address . . . . . : fe80::1d08:a2d0:b94c:d561%12
```

The presentation is now working on Windows 8.0. The presentation opens Windows Firewall with Advance Security and IP Security Monitor in a mmc. The presentation is open the mmc as a member of the administrators group.

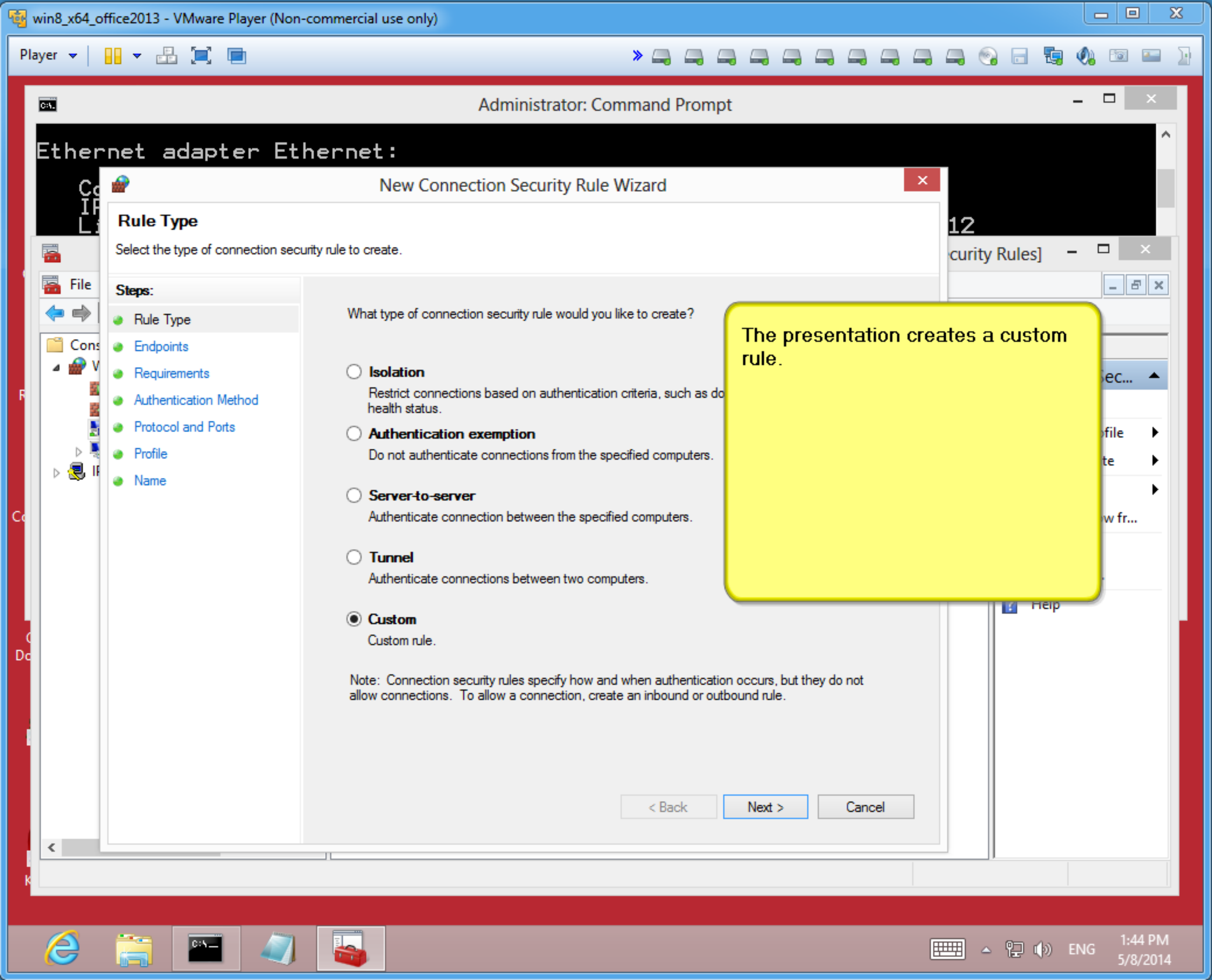


```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : localdomain
   IPv6 Address. . . . . . . . . . . : 2001:db8::108
   Link-local IPv6 Address . . . . . : fe80::1d08:a2d0:b94c:d561%12
```

There are no items to show in this view.

The presentation selects the New Rule option under Connection Security Rule.

Contains commands for customizing this window.


win8_x64_office2013 - VMware Player (Non-commercial use only)
Player
Administrator: Command Prompt
Ethernet adapter Ethernet:
File
New Connection Security Rule Wizard
< Back
Next >
Cancel
Help
1:44 PM
5/8/2014
ENG

Rule Type

Select the type of connection security rule to create.

Steps:

- Rule Type
- Endpoints
- Requirements
- Authentication Method
- Protocol and Ports
- Profile
- Name

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

○ **Isolation**
Restrict connections based on authentication criteria, such as do
health status.

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

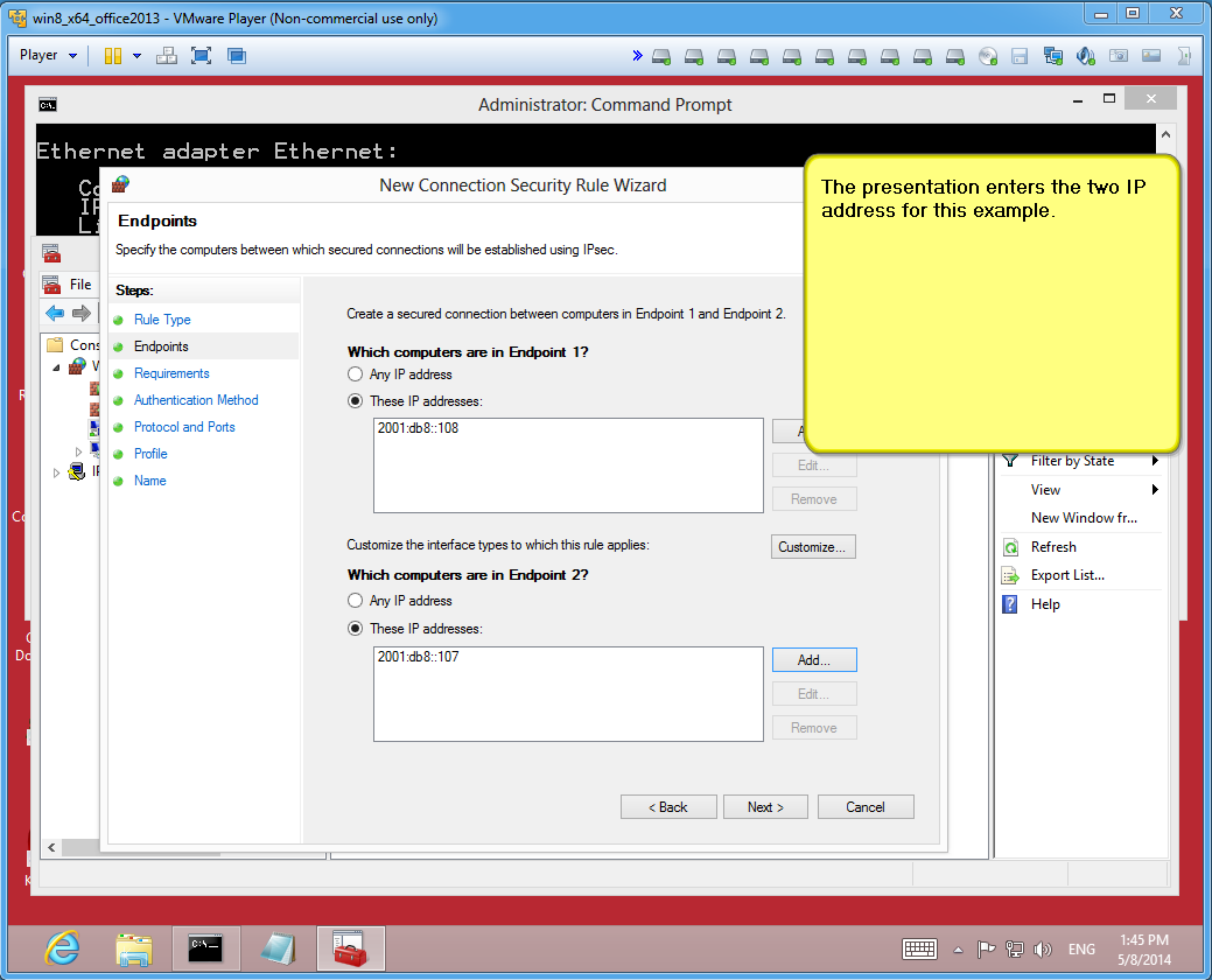
○ **Server-to-server**
Authenticate connection between the specified computers.

○ **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.

The presentation creates a custom rule.


win8_x64_office2013 - VMware Player (Non-commercial use only)
Player
Administrator: Command Prompt
Ethernet adapter Ethernet:
File
Filter by State
View
New Window fr...
Refresh
Export List...
Help
ENG
1:45 PM
5/8/2014

The presentation enters the two IP address for this example.

New Connection Security Rule Wizard

Endpoints

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

Steps:

- Rule Type
- Endpoints
- Requirements
- Authentication Method
- Protocol and Ports
- Profile
- Name

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

Which computers are in Endpoint 1?

○ Any IP address

● These IP addresses:

2001:db8::108

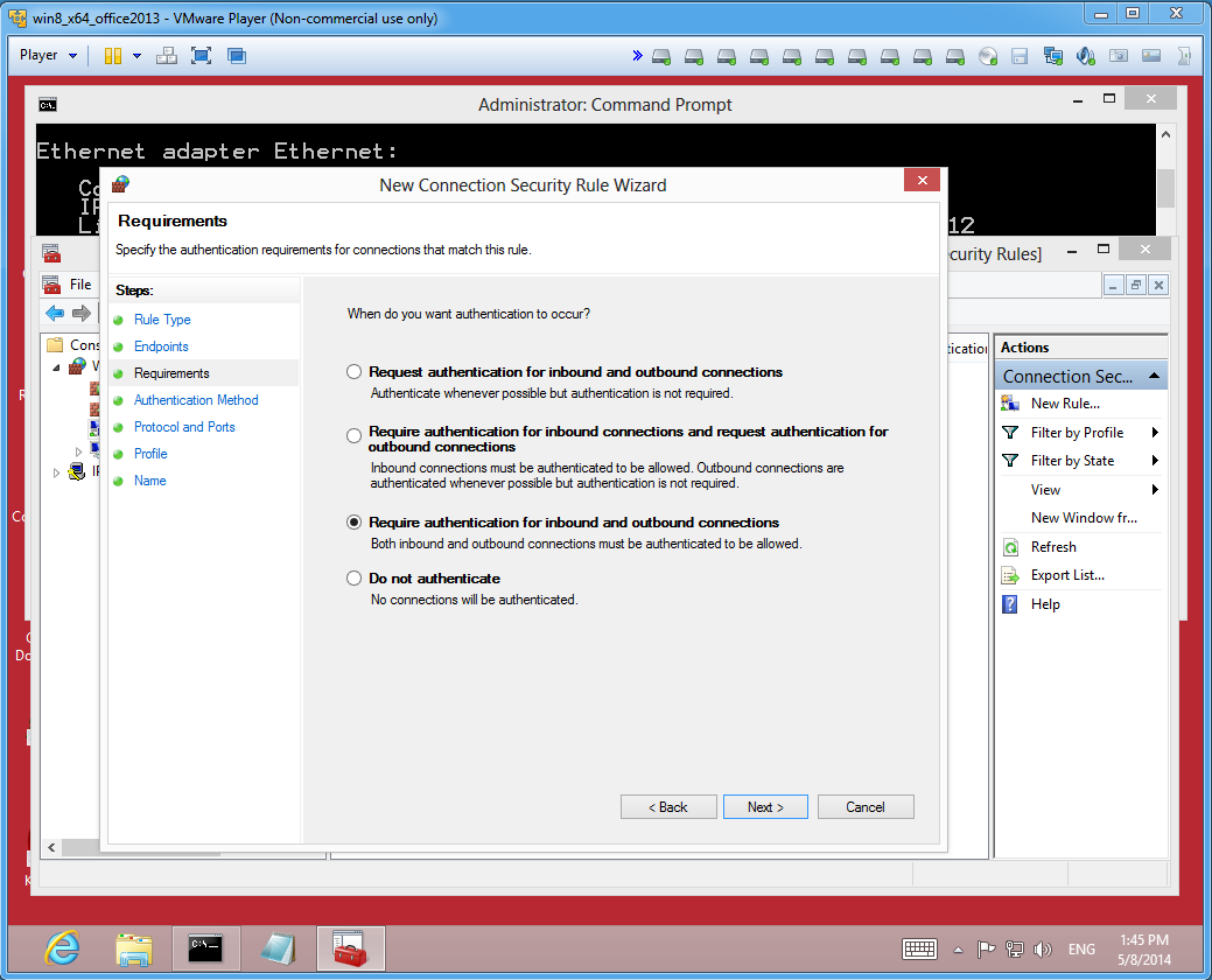
Customize the interface types to which this rule applies:

Which computers are in Endpoint 2?

○ Any IP address

● These IP addresses:

2001:db8::107



New Connection Security Rule Wizard

Requirements

Specify the authentication requirements for connections that match this rule.

Steps:

- Rule Type
- Endpoints
- Requirements
- Authentication Method
- Protocol and Ports
- Profile
- Name

When do you want authentication to occur?

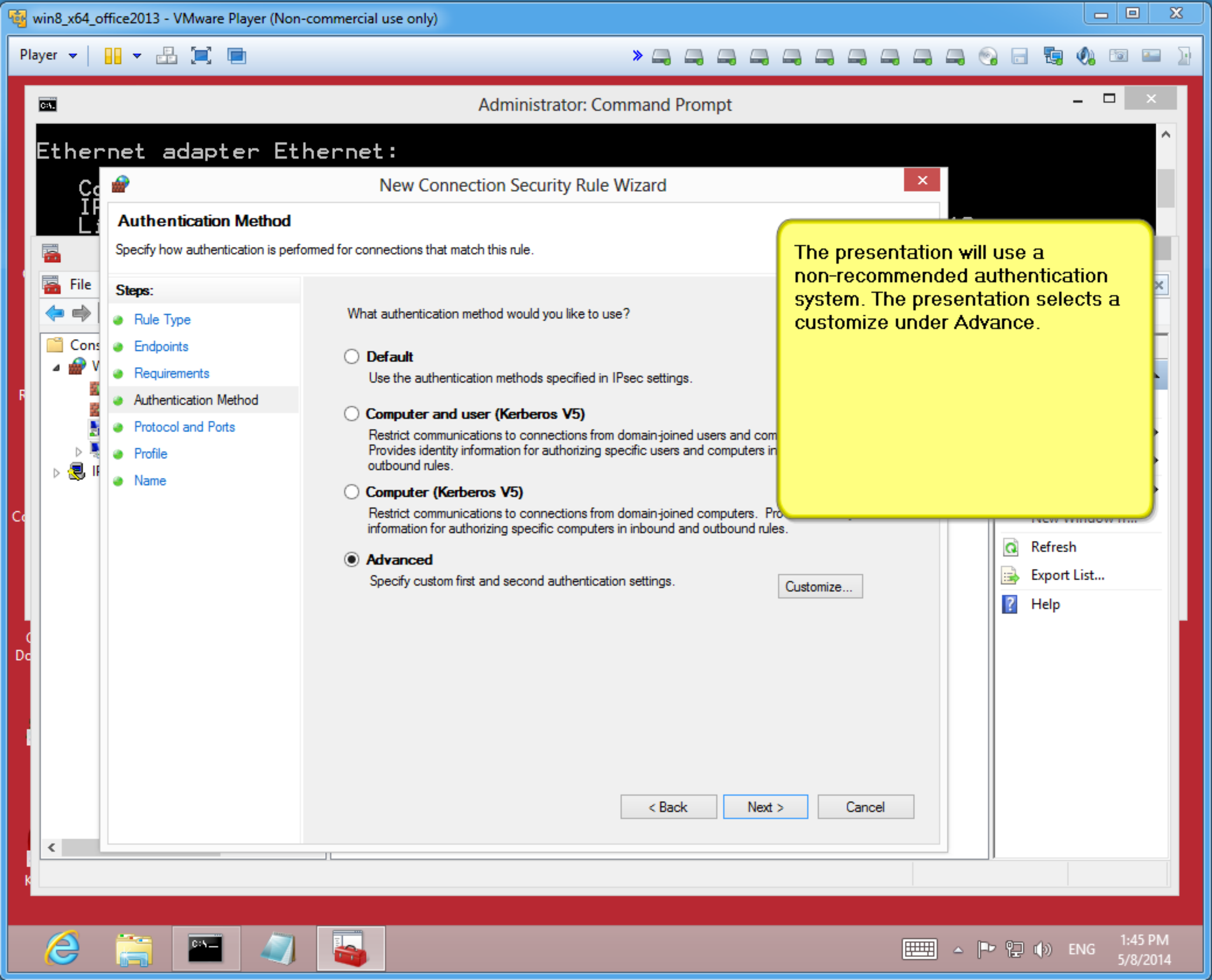
○ **Request authentication for inbound and outbound connections**
Authenticate whenever possible but authentication is not required.

○ **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.

○ **Do not authenticate**
No connections will be authenticated.

< Back | Next > | Cancel


win8_x64_office2013 - VMware Player (Non-commercial use only)
Player
Administrator: Command Prompt
File
Refresh
Export List...
Help
1:45 PM
5/8/2014
ENG

```
Ethernet adapter Ethernet:
```

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
- Protocol and Ports
- 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 com
Provides identity information for authorizing specific users and computers in
outbound rules.

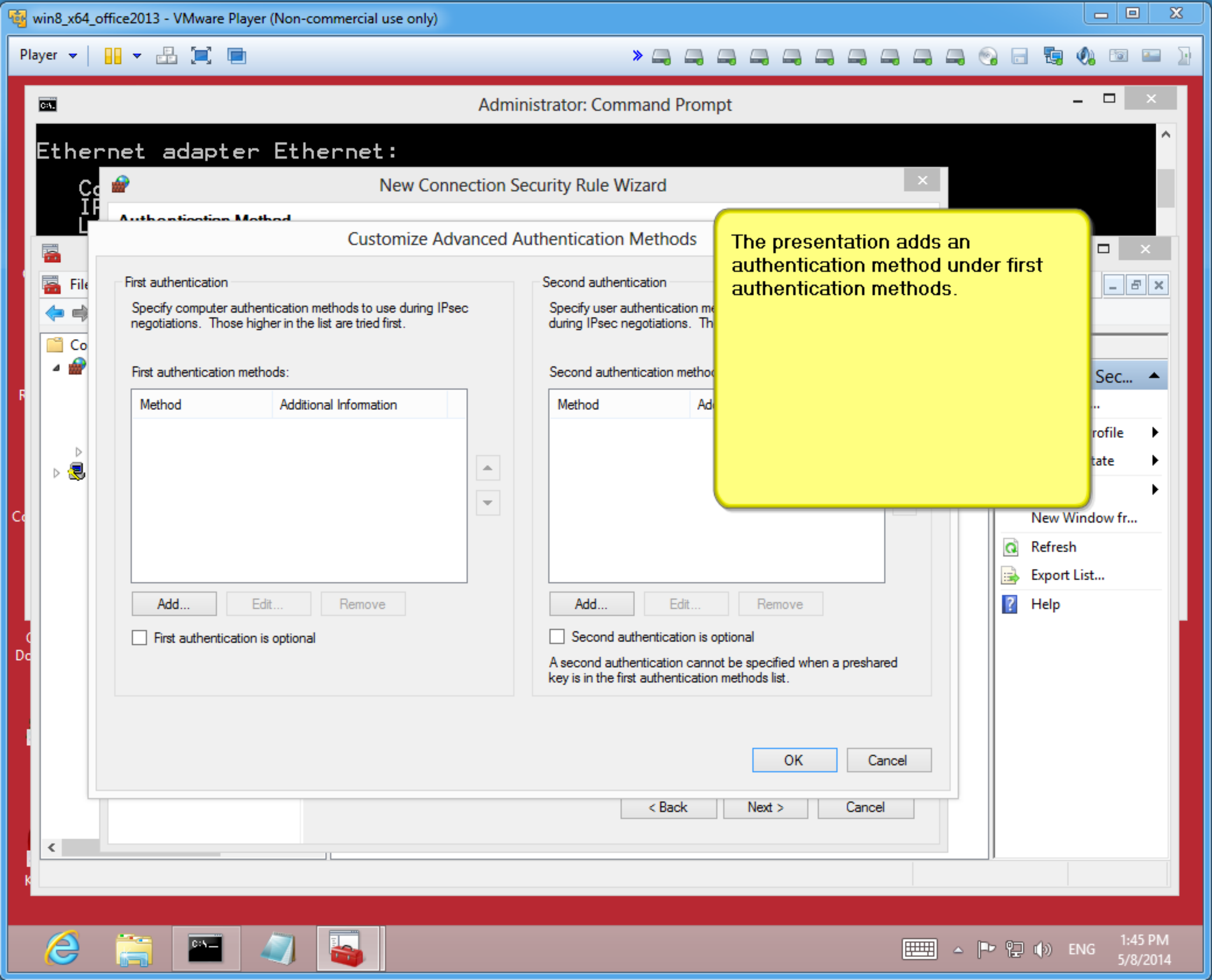
○ **Computer (Kerberos V5)**

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

● **Advanced**

Specify custom first and second authentication settings.

The presentation will use a non-recommended authentication system. The presentation selects a customize under Advance.


win8_x64_office2013 - VMware Player (Non-commercial use only)
Player
Administrator: Command Prompt
New Connection Security Rule Wizard
Sec...
rofile
tate
New Window fr...
Refresh
Export List...
Help
< Back
Next >
Cancel
ENG
1:45 PM
5/8/2014

The presentation adds an authentication method under first authentication methods.

```
Ethernet adapter Ethernet:

   Co
   IP
   L
```

Authentication Method

Customize Advanced Authentication Methods

First authentication

Specify computer authentication methods to use during IPsec negotiations. Those higher in the list are tried first.

First authentication methods:

Method	Additional Information

□ First authentication is optional

Second authentication

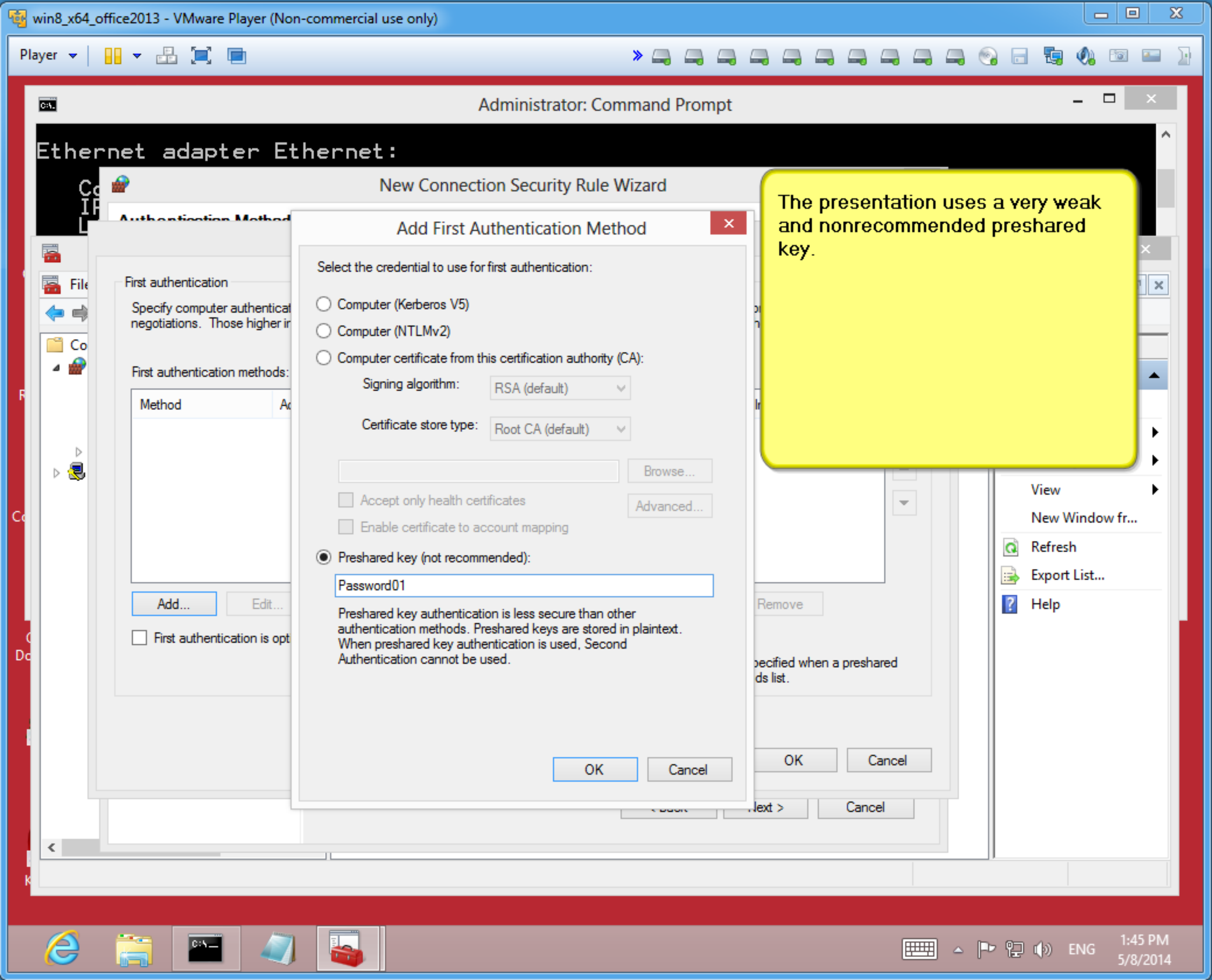
Specify user authentication me
during IPsec negotiations. Th

Second authentication metho

Method	Ad

□ Second authentication is optional

A second authentication cannot be specified when a preshared key is in the first authentication methods list.



The presentation uses a very weak and nonrecommended preshared key.

Add First Authentication Method

Select the credential to use for first authentication:

○ Computer (Kerberos V5)

○ Computer (NTLMv2)

○ Computer certificate from this certification authority (CA):

Signing algorithm: RSA (default)

Certificate store type: Root CA (default)

□ Accept only health certificates

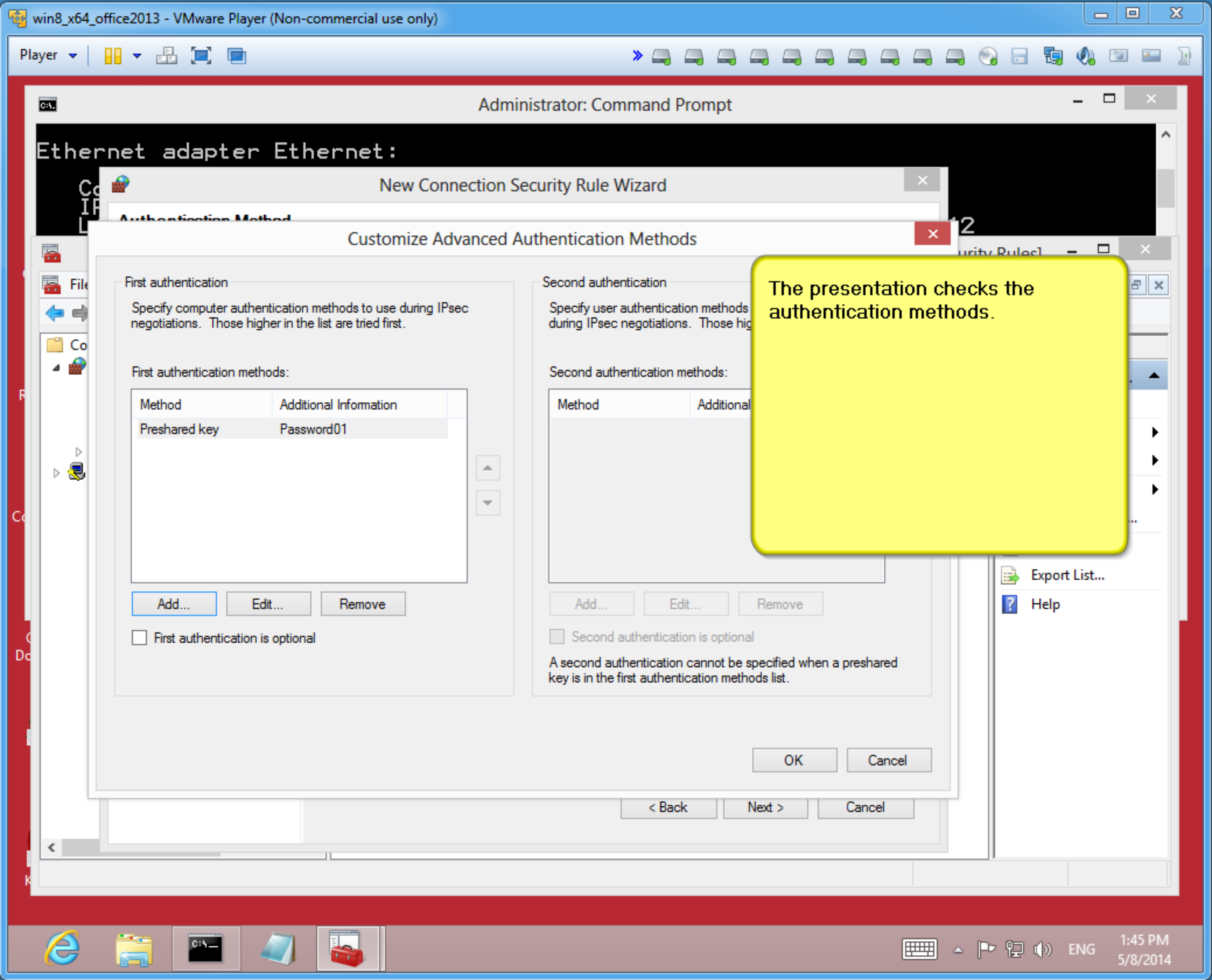
□ Enable certificate to account mapping

● Preshared key (not recommended):

Password01

Preshared key authentication is less secure than other authentication methods. Preshared keys are stored in plaintext. When preshared key authentication is used, Second Authentication cannot be used.

win8_x64_office2013 - VMware Player (Non-commercial use only)
Player
Administrator: Command Prompt
Ethernet adapter Ethernet:
New Connection Security Rule Wizard
First authentication
First authentication methods:
Method
Add...
Edit...
Remove
First authentication is opt
Browse...
Advanced...
OK
Cancel
< Back
Next >
View
New Window fr...
Refresh
Export List...
Help
ENG
1:45 PM
5/8/2014



win8_x64_office2013 - VMware Player (Non-commercial use only)
Player
Administrator: Command Prompt
Ethernet adapter Ethernet:
New Connection Security Rule Wizard
Authentication Method
Customize Advanced Authentication Methods
Export List...
Help
< Back
Next >
Cancel
ENG
1:45 PM
5/8/2014

The presentation checks the authentication methods.

First authentication

Specify computer authentication methods to use during IPsec negotiations. Those higher in the list are tried first.

First authentication methods:

Method	Additional Information
Preshared key	Password01

□ First authentication is optional

Second authentication

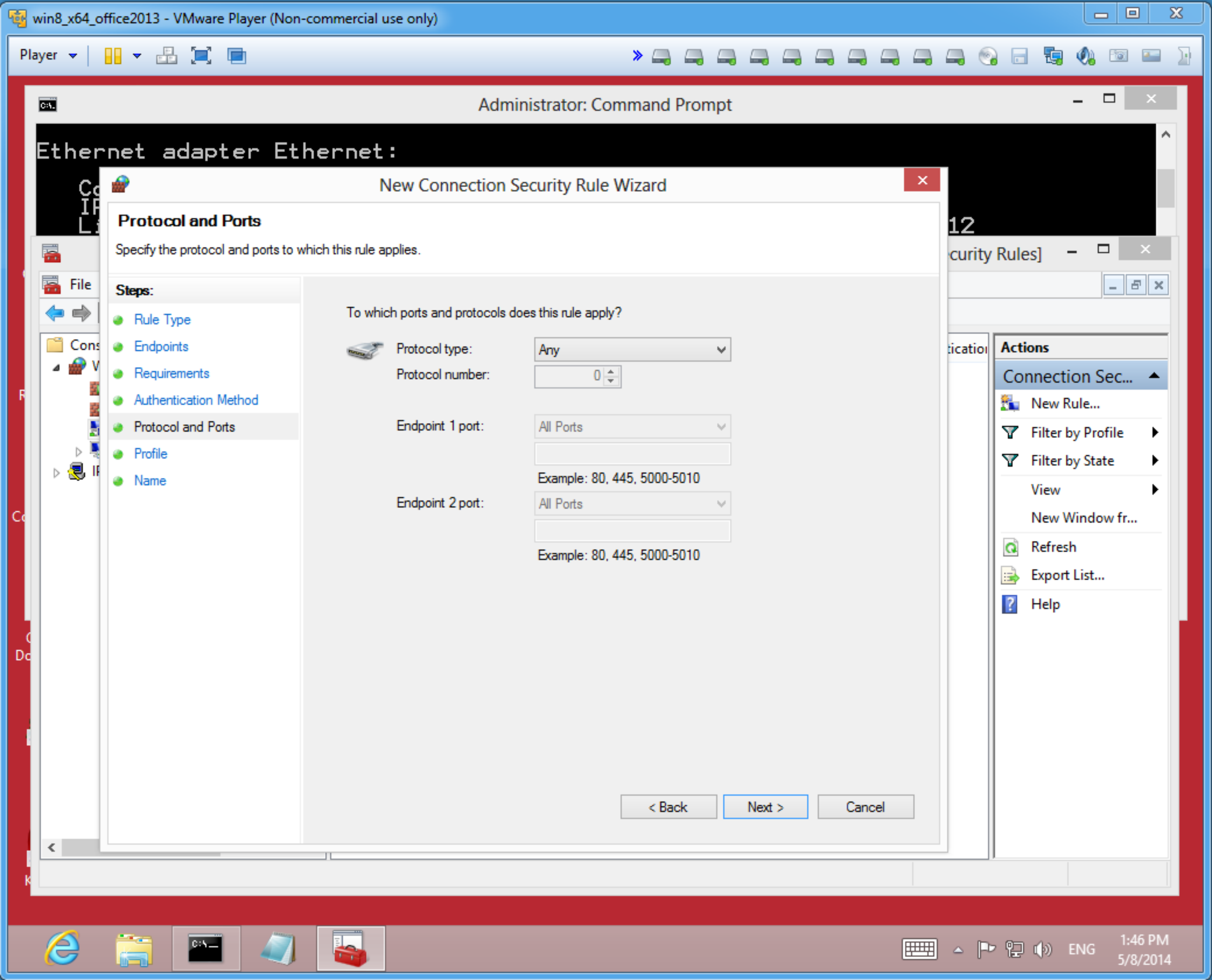
Specify user authentication methods during IPsec negotiations. Those hig

Second authentication methods:

Method	Additional

□ Second authentication is optional

A second authentication cannot be specified when a preshared key is in the first authentication methods list.



```
Ethernet adapter Ethernet:

   Co
   IP
   Li                                                        12
```

New Connection Security Rule Wizard

Protocol and Ports

Specify the protocol and ports to which this rule applies.

Steps:

- Rule Type
- Endpoints
- Requirements
- Authentication Method
- Protocol and Ports
- Profile
- Name

To which ports and protocols does this rule apply?

Protocol type: Any

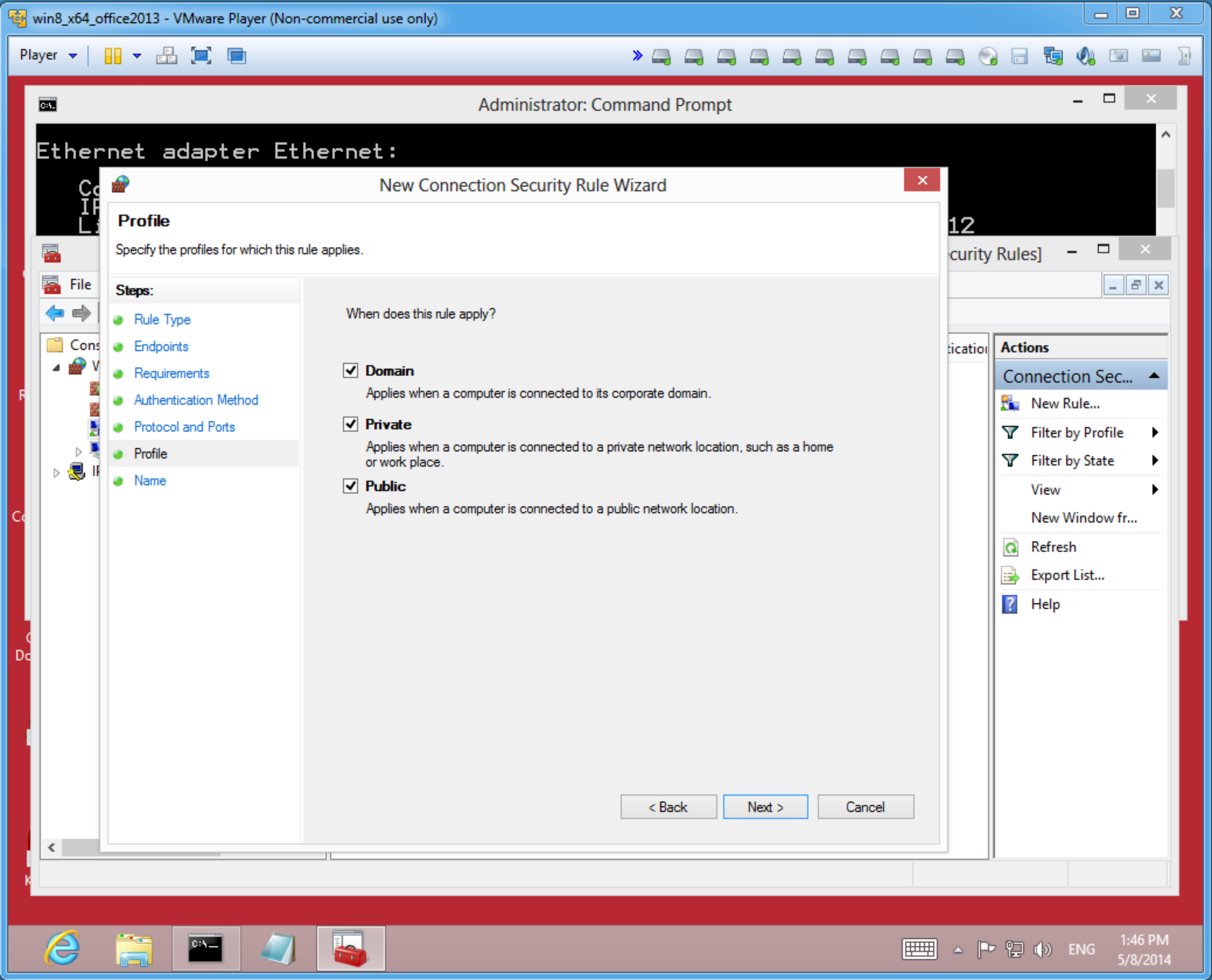
Protocol number: 0

Endpoint 1 port: All Ports

Example: 80, 445, 5000-5010

Endpoint 2 port: All Ports

Example: 80, 445, 5000-5010



```
Ethernet adapter Ethernet:
```

New Connection Security Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Endpoints
- Requirements
- Authentication Method
- Protocol and Ports
- Profile
- Name

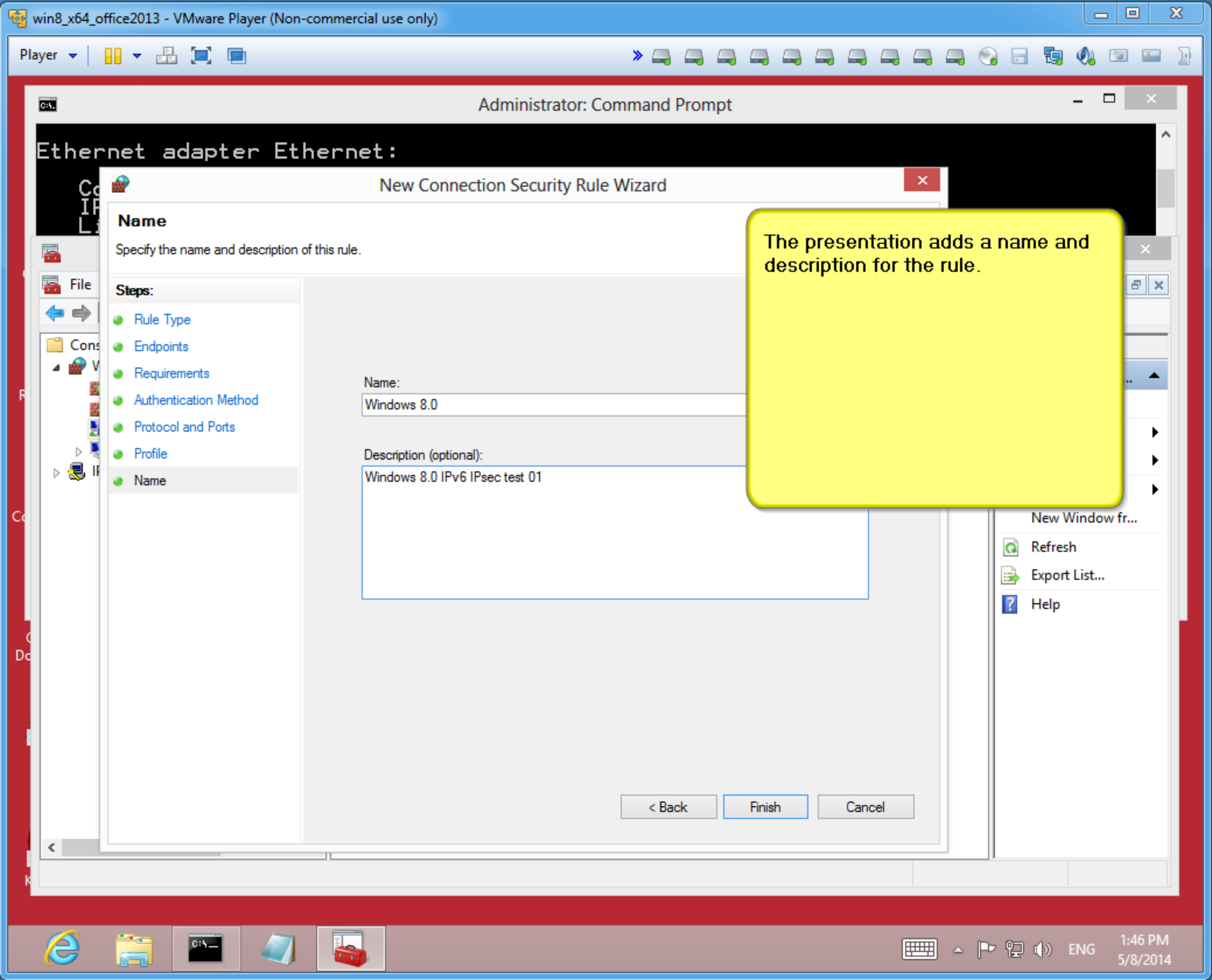
When does this rule apply?

☑ **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



The presentation adds a name and description for the rule.

win8_x64_office2013 - VMware Player (Non-commercial use only)

Administrator: Command Prompt

```
Ethernet adapter Ethernet:
```

New Connection Security Rule Wizard

Name

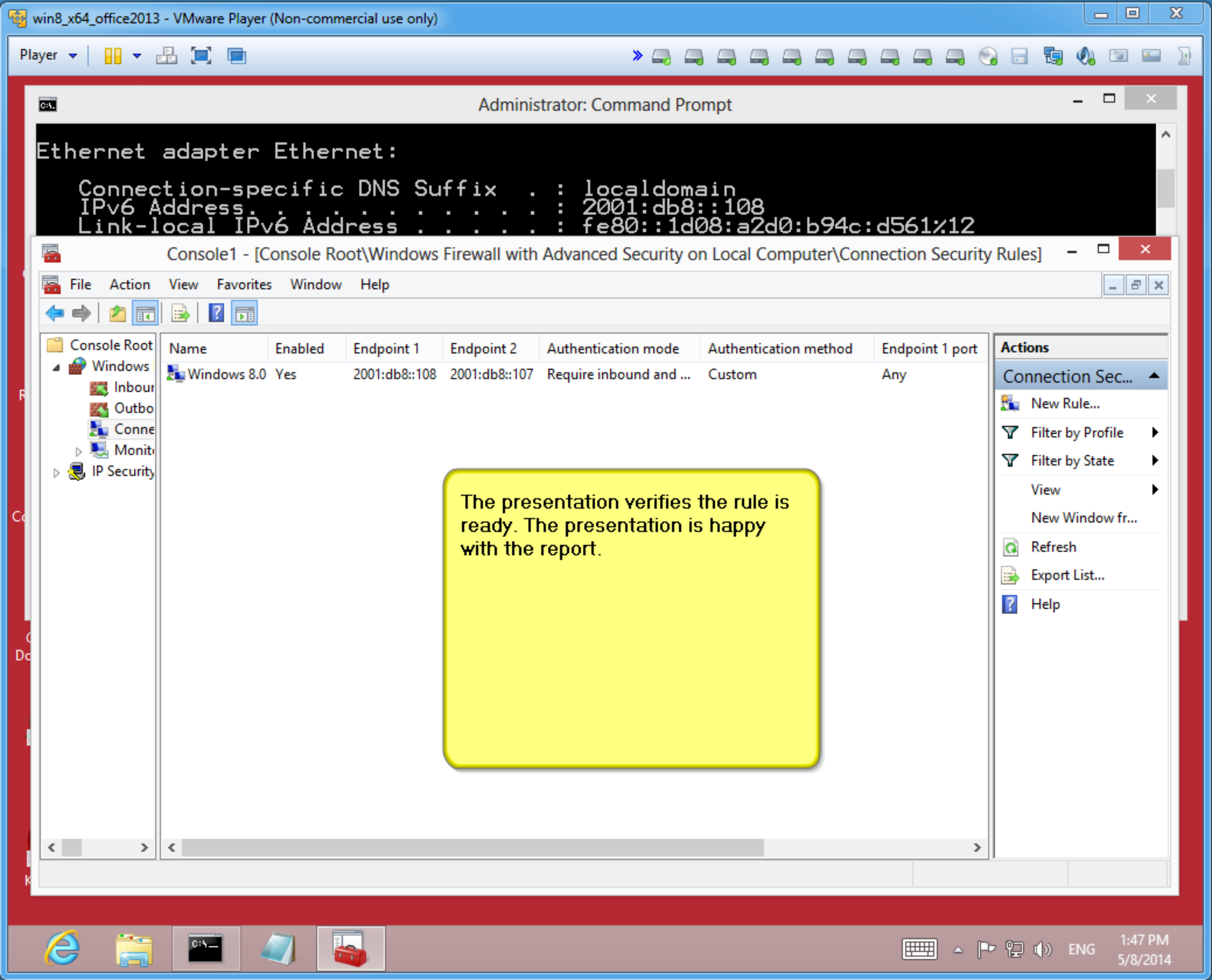
Specify the name and description of this rule.

Steps:

- Rule Type
- Endpoints
- Requirements
- Authentication Method
- Protocol and Ports
- Profile
- Name

Name: Windows 8.0

Description (optional): Windows 8.0 IPv6 IPsec test 01



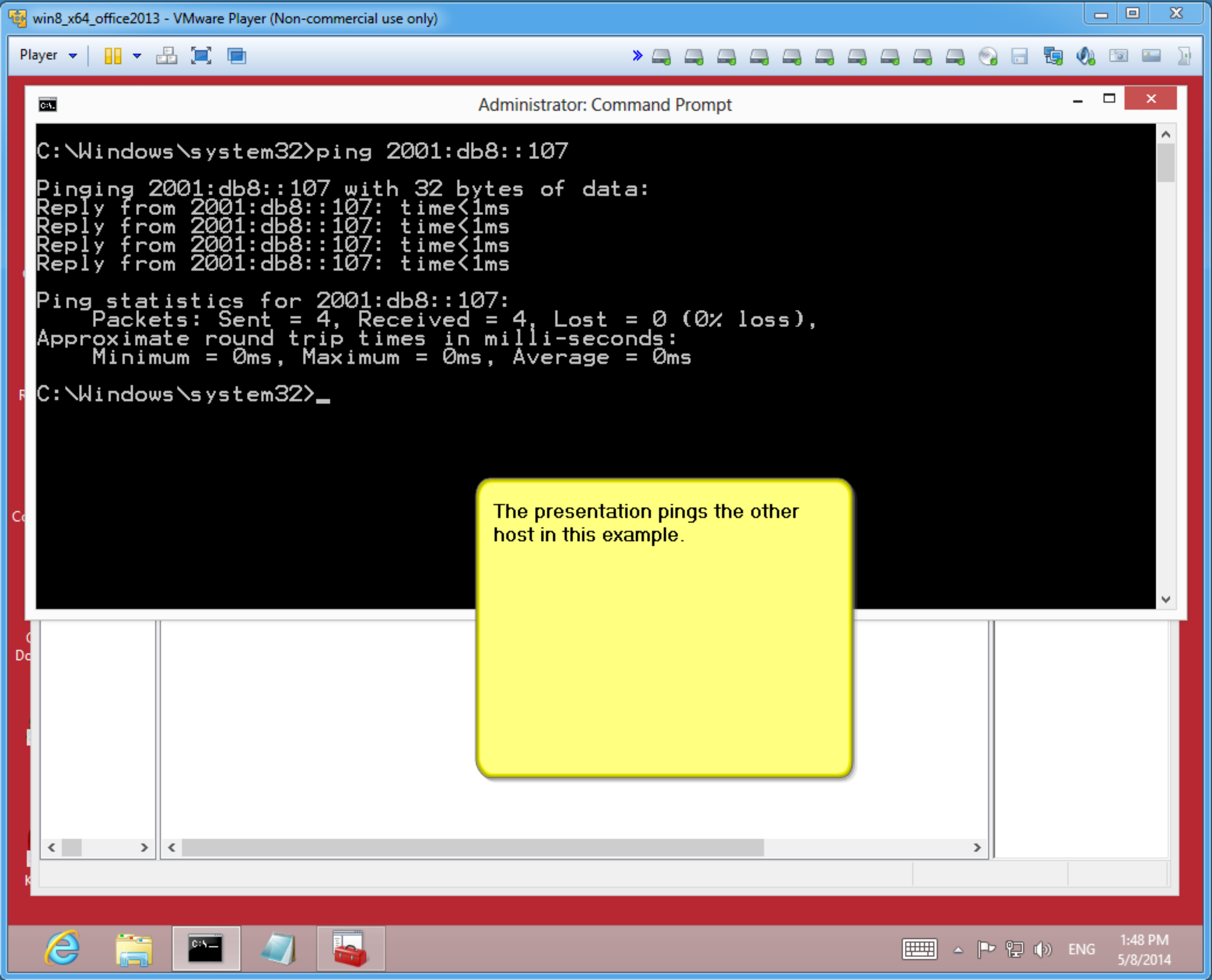
win8_x64_office2013 - VMware Player (Non-commercial use only)
Player
Administrator: Command Prompt

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : localdomain
   IPv6 Address. . . . . . . . . . . : 2001:db8::108
   Link-local IPv6 Address . . . . . : fe80::1d08:a2d0:b94c:d561%12
```

Console1 - [Console Root\Windows Firewall with Advanced Security on Local Computer\Connection Security Rules]
File
Action
View
Favorites
Window
Help
Console Root
Windows
Inbour
Outbo
Conne
Monit
IP Security

Name	Enabled	Endpoint 1	Endpoint 2	Authentication mode	Authentication method	Endpoint 1 port
Windows 8.0	Yes	2001:db8::108	2001:db8::107	Require inbound and ...	Custom	Any

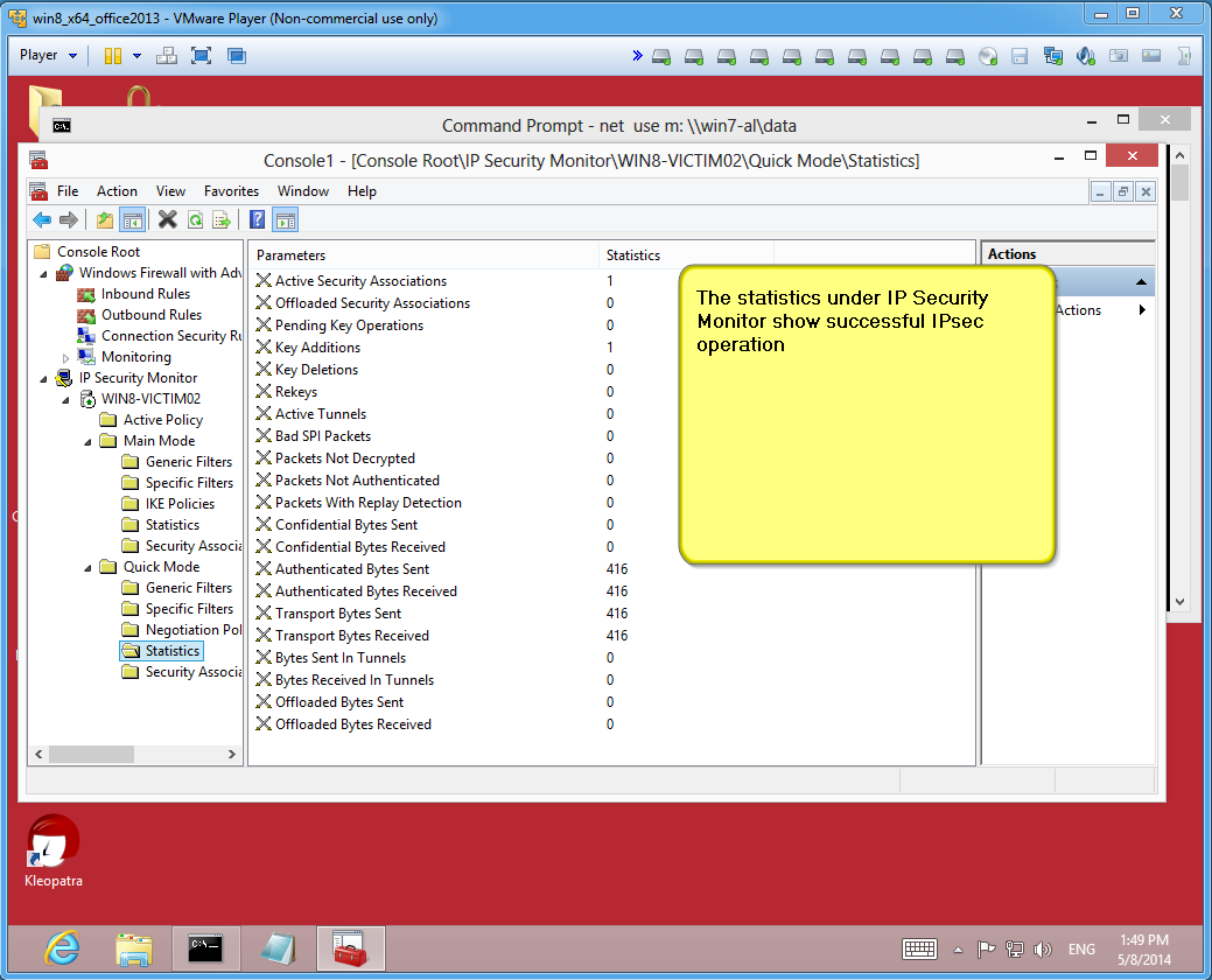
The presentation verifies the rule is ready. The presentation is happy with the report.



win8_x64_office2013 - VMware Player (Non-commercial use only)
Player
Administrator: Command Prompt
ENG
1:48 PM
5/8/2014

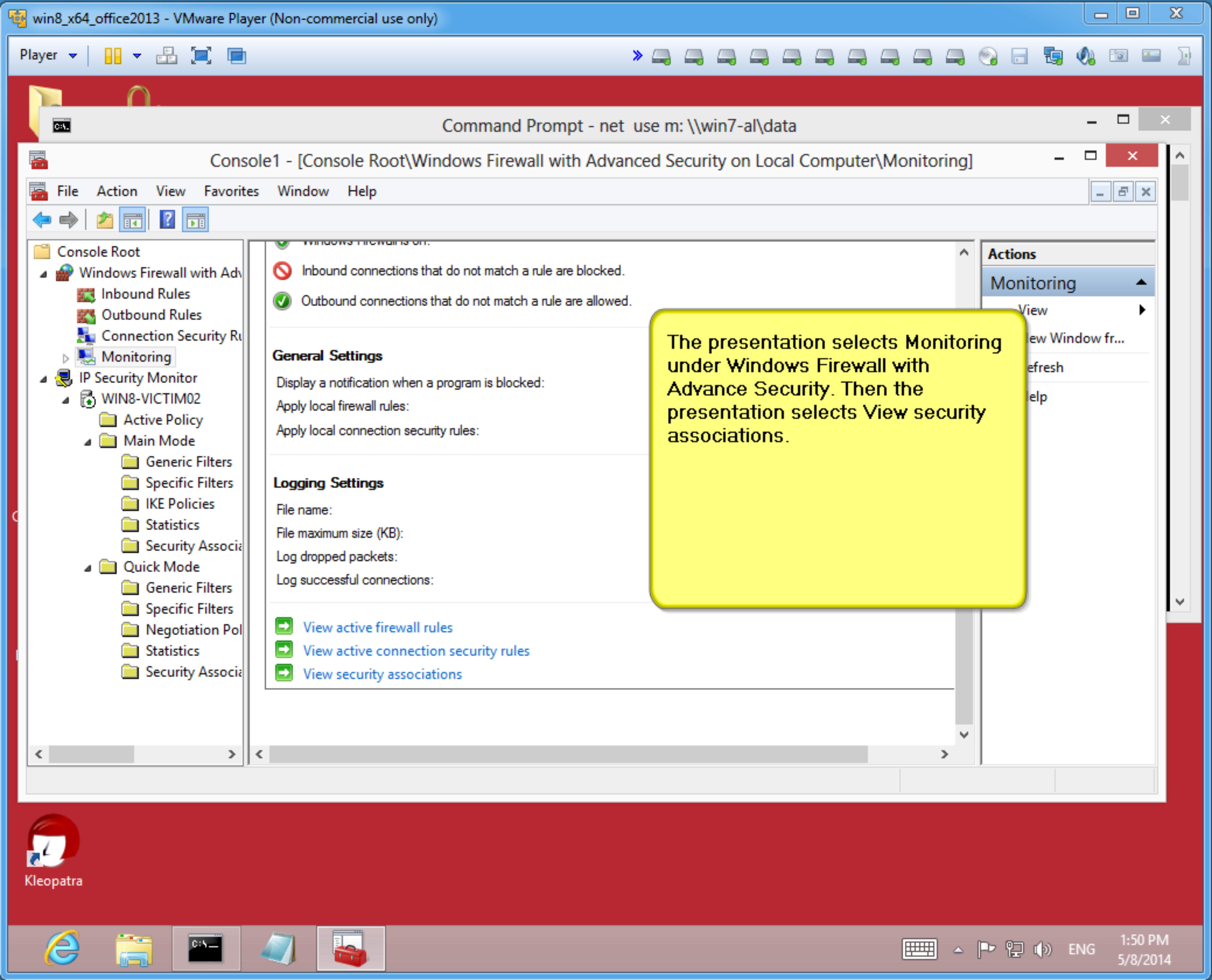
```
C:\Windows\system32>ping 2001:db8::107

Pinging 2001:db8::107 with 32 bytes of data:
Reply from 2001:db8::107: time<1ms
Reply from 2001:db8::107: time<1ms
Reply from 2001:db8::107: time<1ms
Reply from 2001:db8::107: time<1ms

Ping statistics for 2001:db8::107:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Windows\system32>_
```

The presentation pings the other host in this example.



Parameters	Statistics
Active Security Associations	1
Offloaded Security Associations	0
Pending Key Operations	0
Key Additions	1
Key Deletions	0
Rekeys	0
Active Tunnels	0
Bad SPI Packets	0
Packets Not Decrypted	0
Packets Not Authenticated	0
Packets With Replay Detection	0
Confidential Bytes Sent	0
Confidential Bytes Received	0
Authenticated Bytes Sent	416
Authenticated Bytes Received	416
Transport Bytes Sent	416
Transport Bytes Received	416
Bytes Sent In Tunnels	0
Bytes Received In Tunnels	0
Offloaded Bytes Sent	0
Offloaded Bytes Received	0

The statistics under IP Security Monitor show successful IPsec operation



Windows Firewall is on.

Inbound connections that do not match a rule are blocked.

Outbound connections that do not match a rule are allowed.

General Settings

Display a notification when a program is blocked:

Apply local firewall rules:

Apply local connection security rules:

Logging Settings

File name:

File maximum size (KB):

Log dropped packets:

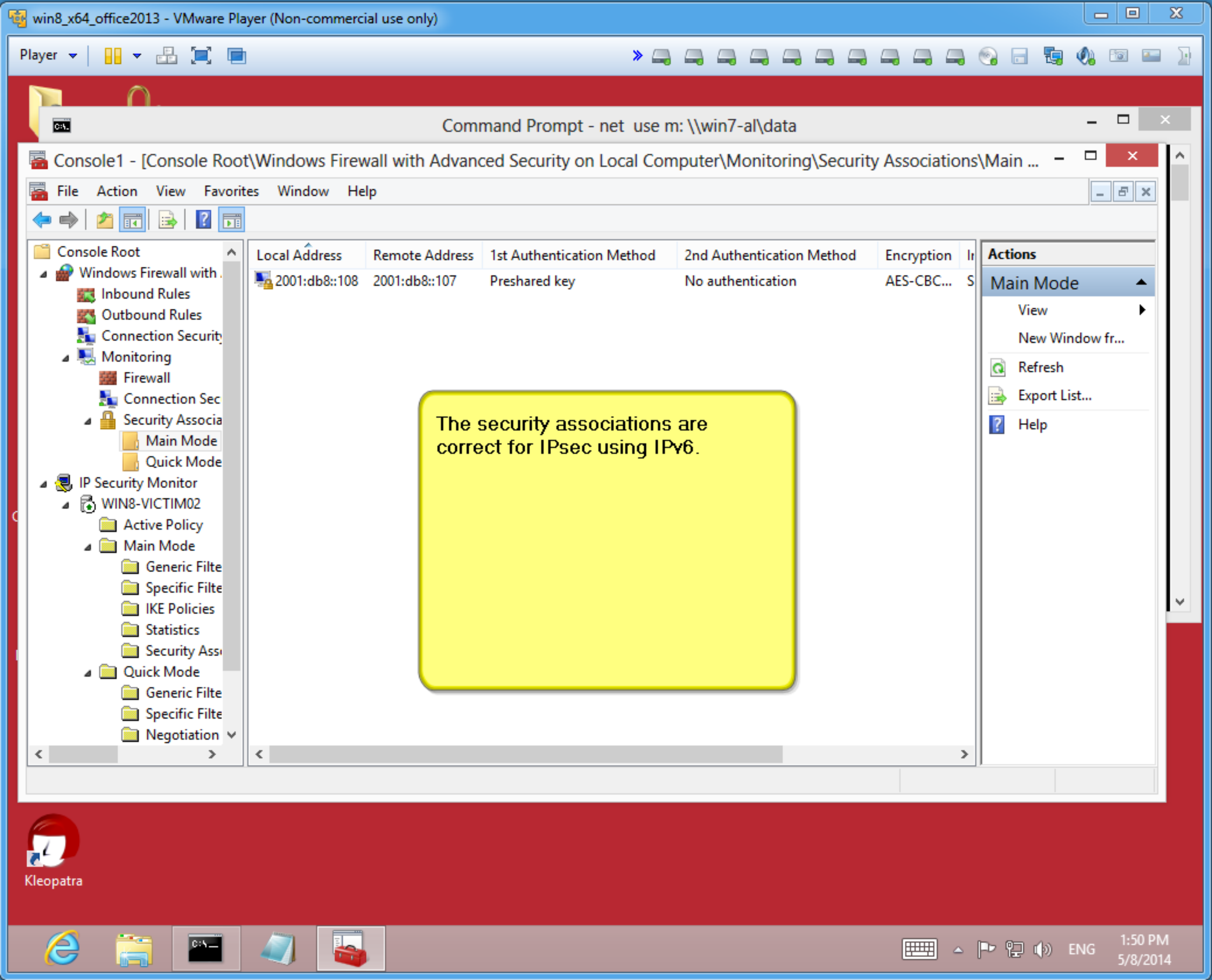
Log successful connections:

View active firewall rules

View active connection security rules

View security associations

The presentation selects Monitoring under Windows Firewall with Advance Security. Then the presentation selects View security associations.



Local Address	Remote Address	1st Authentication Method	2nd Authentication Method	Encryption	Ir
2001:db8::108	2001:db8::107	Preshared key	No authentication	AES-CBC...	S

The security associations are correct for IPsec using IPv6.