## File Services on Windows Core

From the command prompt, run **oclist.exe | more** (this will pause the output at the end of the first page, waiting for a keystroke to continue to the next page). On the first page, you will see the entry "Not Installed:CoreFileServer". Hit the "q" key.

To install file services and the FSRM, type in the following command:

**Dism.exe /Online /Enable-Feature /FeatureName:CoreFileServer /FeatureName:NetFx2-ServerCore /FeatureName:FSRM-Infrastructure-Core**

or (the below commands do the same thing)[[1]](#footnote-1)

**start /w ocsetup.exe CoreFileServer**

**start /w ocsetup.exe NetFx2-ServerCore**

**start /w ocsetup.exe FSRM-Infrastructure-Core**

This will take a while to run and it will not give you any information on how the install is progressing.

Once you are back at the command prompt, you will need to open the firewall ports for remote management of file services. Enter the following command on BOTH the core server and your Windows management workstation. Note: the command must be run from an administrative command prompt on the management computer ( Administrative command prompt is obtained by going to **Start 🡪 All Programs 🡪 Accessories**, right-click on **Command Prompt** and select **Run as administrator**).

**netsh advfirewall firewall set rule group="Remote Volume Management" new enable=yes**

The following command needs to be executed on the Core server only:

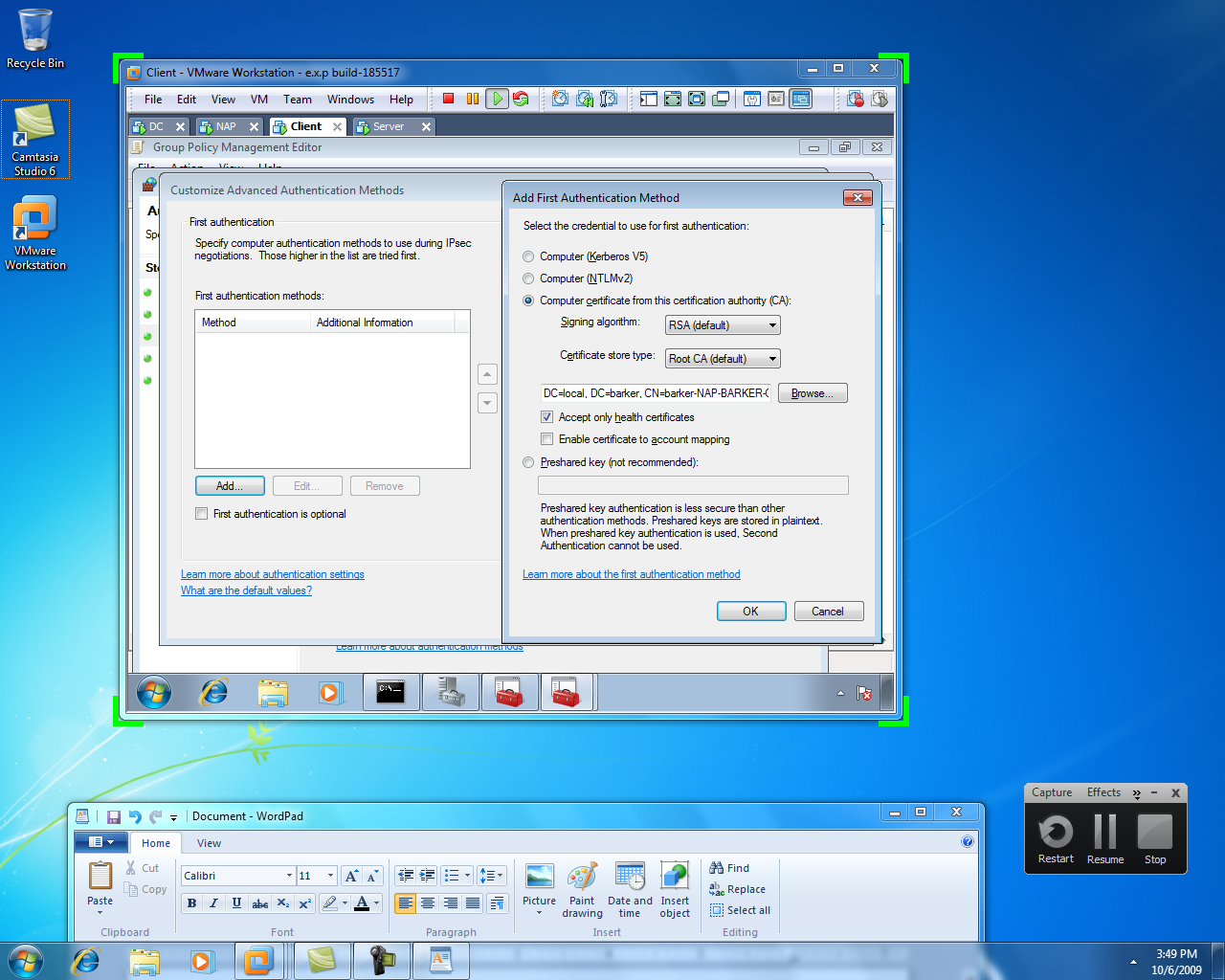
**netsh advfirewall firewall set rule group="Remote File Server Resource Manager Management" new enable=yes**

Once the firewall is configured you can remotely create shares and manage them.

1. Make the Core file server, NAP server and Domain Controller a member of the **NAP exempted computers** group. Windows 2008 servers must be made a member of this group because Windows 2008 server has no SHA(System Health Agent is part of Security Center).
2. Create two groups – one named **Boundary Network**, the other named S**ecure Network**. Put the domain controller and NAP server in the boundary group. Put the file server and client computer (Windows 7 computer) in the secure group.
3. Reboot the domain controller and then reboot all other computers.
4. Verify a NAP health certificate gets installed (use the certificates MMC to remotely look at the computers personal certificates

## Boundary Network configuration

1. Configure an IPSEC policy for the boundary network group named NAP Boundary. Make sure to remove Authenticated Users from Security filtering and add the Boundary Computers group.
   1. Open GPMC.msc and expand **Forest 🡪 Domains 🡪 <your domain>**
   2. Right-click on the Domain name and select **Create a GPO in this domain, and Link it Here. . .**. Name the policy **NAP Boundary**
   3. The GPO will appear under the domain name on the navigation pane on the left.
   4. Click on the **NAP Boundary GPO**. In the details pane you will see a security filtering section.
   5. In the Security Filtering section, click on **Authenticated Users** then click on the **Remove** button. Click on OK when asked to remove the delegated privilege.
   6. Click on the **Add…** button
   7. Type in **Boundary network** and click on **OK**.
   8. Right-click on the policy and select **Edit**.
   9. Expand **Computer Configuration 🡪 Policies 🡪 Windows Settings 🡪 Security Settings 🡪 Windows Firewall with Advanced Security**. Click on **Windows Firewall with Advanced Security (LDAP)**. Click on **Windows Firewall** **Properties** in the details pane.
      1. On the **Domain Profile** tab, click on the drop-down next to **Firewall state:** Select **On (Recommended)**
         1. Next to **Inbound Connections**: click on the drop-down and select **Block (default)**
         2. Next to **Outbound connections:** click on the drop-down box and select **Allow (Default)**.
      2. On the **Private Profile** tab, click on the drop-down next to **Firewall state:** Select **On (Recommended)**
         1. Next to **Inbound Connections**: click on the drop-down and select **Block (default)**
         2. Next to **Outbound connections:** click on the drop-down box and select **Allow (Default)**.
      3. On the **Public Profile** tab, click on the drop-down next to **Firewall state:** Select **On (Recommended)**
         1. Next to **Inbound Connections**: click on the drop-down and select **Block (default)**
         2. Next to **Outbound connections:** click on the drop-down box and select **Allow (Default)**.
   10. Expand **Windows Firewall with Advanced Security 🡪 Connection Security Rules**.
   11. Right-click on the details pane of connecting security rules and select **New Rule**.
   12. Verify that **Isolation** is selected and click on **Next**. Verify that **Request Authentication for Inbound and Outbound Connections** is selected and click on **Next**. On the Authentication method page, click on **Advanced** then click on the **Customize…** button.
       1. Under **First authentication methods** click on Add.
       2. Click on the radio button next to **Computer certificate from this certification authority (CA):**  Click on the **Browse…** button and find the certificate authority you created (hint – your last name). Select it and click on **OK**.
       3. Click on the check box next to **Accept only health certificates** to select it.

****

**Configuring Certificate authentication for the connection method**

* + 1. Click on **OK**. Click on **OK** again.
  1. Click on **Next**.
  2. On the Profile page, leave all profiles checked (**Domain, Private, Public**). Click on **Next**.
  3. In the Name page, type in **Boundary Rule**. Click on Finish.
  4. Close GPMC. Run **gpupdate /force** on the NAP and DC servers.

NOTE: At this point, the NAP and DC servers will start communicating with IPSEC using certificate authentication. The client computer and core file server won’t, because they don’t have a policy for IPSEC.

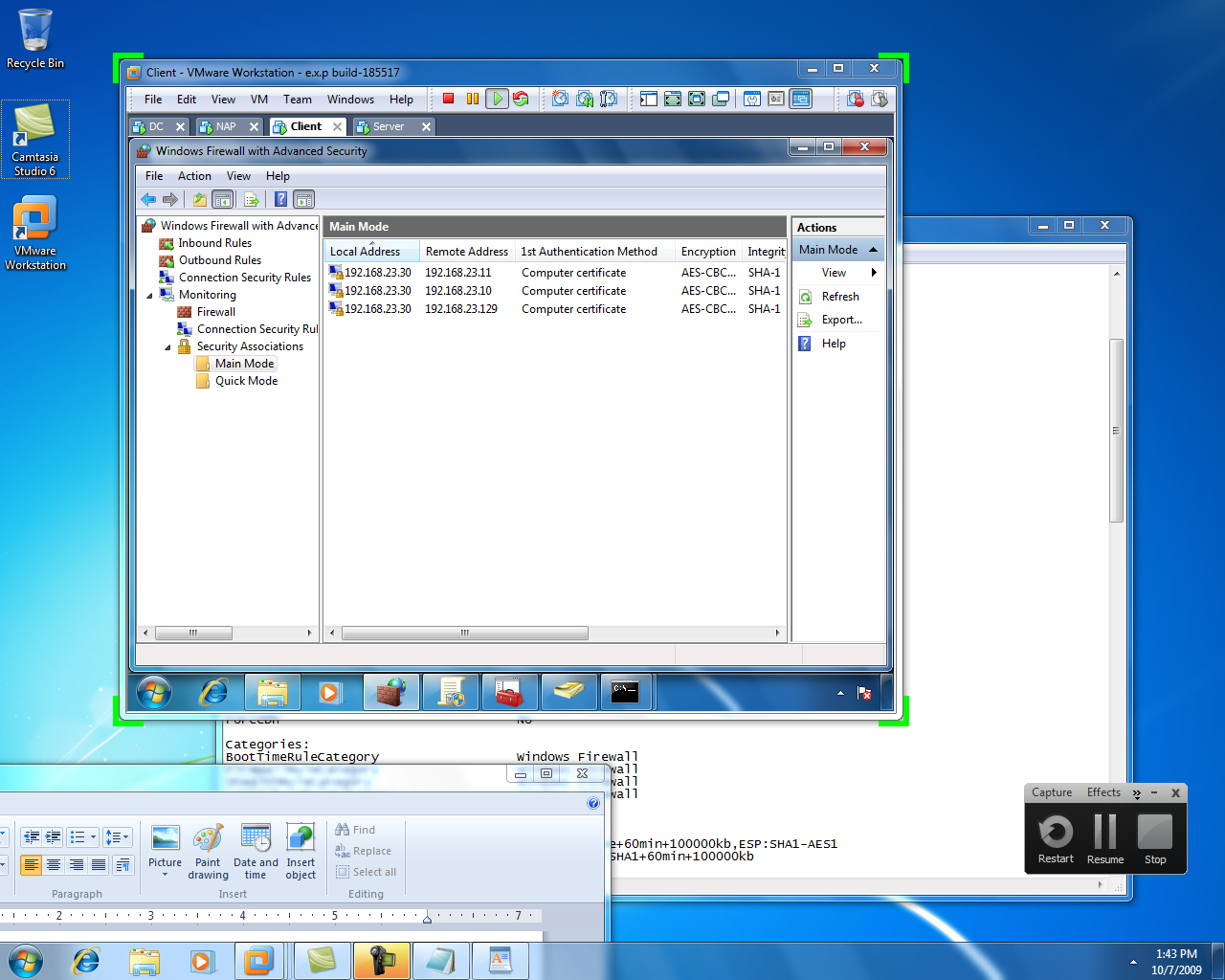
## Secure Network Configuration

1. Configure an IPSEC policy for the **Secure Network** group named **NAP Secure**. Make sure to remove **Authenticated Users** from Security Filtering and add the **Secure Network** group.
   1. Open GPMC.msc and expand **Forest 🡪 Domains 🡪 <your domain>**
   2. Right-click on the Domain name and select **Create and Link GPO Here. . .**. Name the policy **NAP Secure**
   3. Right-click on the policy and select **Edit**.
   4. Expand **Computer Configuration 🡪 Policies 🡪 Windows Settings 🡪 Security Settings 🡪 Windows Firewall with Advanced Security**. Click on **Windows Firewall with Advanced Security (LDAP)**. Click on **Windows Firewall** **Properties** in the details pane.
      1. On the **Domain Profile** tab, click on the drop-down next to **Firewall state:** Select **On (Recommended)**
         1. Next to **Inbound Connections**: click on the drop-down and select **Block (default)**
         2. Next to **Outbound connections:** click on the drop-down box and select **Allow (Default)**.
      2. On the **Private Profile** tab, click on the drop-down next to **Firewall state:** Select **On (Recommended)**
         1. Next to **Inbound Connections**: click on the drop-down and select **Block (default)**
         2. Next to **Outbound connections:** click on the drop-down box and select **Allow (Default)**.
      3. On the **Public Profile** tab, click on the drop-down next to **Firewall state:** Select **On (Recommended)**
         1. Next to **Inbound Connections**: click on the drop-down and select **Block (default)**
         2. Next to **Outbound connections:** click on the drop-down box and select **Allow (Default)**.
   5. Expand **Windows Firewall with Advanced Security 🡪 Connection Security Rules**.
   6. Right-click on the details pane of **Connection Security Rules** and select **New Rule**.
   7. Verify that **Isolation** is selected and click on **Next**. Verify that **Require Authentication for Inbound Connections and Request Authentication for Outbound Connections** is selected and click on **Next**. On the Authentication method page, click on **Advanced** then click on the **Customize…** button.
      1. Under **First authentication methods** click on Add.
      2. Click on the radio button next to **Computer certificate from this certification authority (CA):**  Click on the **Browse…** button and find the certificate authority you created (hint – your last name). Select it and click on **OK**.
      3. Click on the check box next to **Accept only health certificates** to select it.
      4. Click on **OK**. Click on **OK** again.
   8. Click on **Next**.
   9. On the Profile page, leave all profiles checked (**Domain, Private, Public**). Click on **Next**.
   10. In the Name page, type in **Secure Only Rule**. Click on **Finish**.
   11. Close GPMC. Run **gpupdate /force** on the NAP and DC servers.

## Test configuration

Try to connect from the client PC to the NAP server, file server and Domain controller – an easy way to do this is by using Server Manager to connect to the servers. Check to make sure security associations are being created. Also make sure you can access shares on the file server.

1. Open Windows Firewall with Advanced Security (**Start** 🡪 **Administrative Tools** 🡪 **Windows Firewall with Advanced Security**).
2. Expand **Monitoring 🡪 Security associations 🡪 Main Mode**. You should see several entries in the main pane.

****

**Looking at Security associations (note authentication method – Computer certificate)**

For windows core, use the following command to show the same information. (You can run the same command from Windows 7, but it has to be done from an administrative command prompt):

**Netsh advfirewall monitor show mmsa**

**C:\Windows\system32>netsh advfirewall monitor show mmsa**

**Main Mode SA at 10/07/2009 13:09:57**

**----------------------------------------------------------------------**

**Local IP Address: 192.168.23.30**

**Remote IP Address: 192.168.23.129**

**Auth1: ComputerCert**

**Auth2: None**

**MM Offer: None-AES128-SHA1**

**Cookie Pair: 9940712d72b914a2:9e1c3674e5a673ed**

**Health Cert: Yes**

**Main Mode SA at 10/07/2009 13:09:57**

**----------------------------------------------------------------------**

**Local IP Address: 192.168.23.30**

**Remote IP Address: 192.168.23.10**

**Auth1: ComputerCert**

**Auth2: None**

**MM Offer: None-AES128-SHA1**

**Cookie Pair: 6df23b3fbd8e4996:9054274dbf43ceee**

**Health Cert: Yes**

**Main Mode SA at 10/07/2009 13:09:57**

**----------------------------------------------------------------------**

**Local IP Address: 192.168.23.30**

**Remote IP Address: 192.168.23.11**

**Auth1: ComputerCert**

**Auth2: None**

**MM Offer: None-AES128-SHA1**

**Cookie Pair: d8b88f0e2f6c7e1a:343258010d1925c6**

**Health Cert: Yes**

**Ok.**

**Looking at Security associations from command line (note authentication method – Computer certificate)**

More Commands: (at an administrative command prompt). For a more detailed list see: <http://technet.microsoft.com/en-us/library/cc725926%28WS.10%29.aspx>

Show Security associations and other IPSEC details

1. **Netsh advfirewall monitor show consec**

**C:\Windows\system32>netsh advfirewall monitor show consec**

**Global Settings:**

**----------------------------------------------------------------------**

**IPsec:**

**StrongCRLCheck 0:Disabled**

**SAIdleTimeMin 5min**

**DefaultExemptions NeighborDiscovery,DHCP**

**IPsecThroughNAT Never**

**AuthzUserGrp None**

**AuthzComputerGrp None**

**StatefulFTP Enable**

**StatefulPPTP Enable**

**Main Mode:**

**KeyLifetime 480min,0sess**

**SecMethods DHGroup2-AES128-SHA1,DHGroup2-3DES-SHA1**

**ForceDH No**

**Categories:**

**BootTimeRuleCategory Windows Firewall**

**FirewallRuleCategory Windows Firewall**

**StealthRuleCategory Windows Firewall**

**ConSecRuleRuleCategory Windows Firewall**

**Quick Mode:**

**QuickModeSecMethods ESP:SHA1-None+60min+100000kb,ESP:SHA1-AES1**

**28+60min+100000kb,ESP:SHA1-3DES+60min+100000kb,AH:SHA1+60min+100000kb**

**QuickModePFS None**

**Security Associations:**

**Main Mode SA at 10/07/2009 13:09:49**

**----------------------------------------------------------------------**

**Local IP Address: 192.168.23.30**

**Remote IP Address: 192.168.23.129**

**Auth1: ComputerCert**

**Auth2: None**

**MM Offer: None-AES128-SHA1**

**Cookie Pair: 9940712d72b914a2:9e1c3674e5a673ed**

**Health Cert: Yes**

**Main Mode SA at 10/07/2009 13:09:49**

**----------------------------------------------------------------------**

**Local IP Address: 192.168.23.30**

**Remote IP Address: 192.168.23.10**

**Auth1: ComputerCert**

**Auth2: None**

**MM Offer: None-AES128-SHA1**

**Cookie Pair: 6df23b3fbd8e4996:9054274dbf43ceee**

**Health Cert: Yes**

**Main Mode SA at 10/07/2009 13:09:49**

**----------------------------------------------------------------------**

**Local IP Address: 192.168.23.30**

**Remote IP Address: 192.168.23.11**

**Auth1: ComputerCert**

**Auth2: None**

**MM Offer: None-AES128-SHA1**

**Cookie Pair: d8b88f0e2f6c7e1a:343258010d1925c6**

**Health Cert: Yes**

**Quick Mode SA at 10/07/2009 13:09:49**

**----------------------------------------------------------------------**

**Local IP Address: 192.168.23.30**

**Remote IP Address: 192.168.23.10**

**Local Port: Any**

**Remote Port: Any**

**Protocol: Any**

**Direction: Both**

**QM Offer: ESP:SHA1-None+60min+100000kb**

**PFS: None**

**Quick Mode SA at 10/07/2009 13:09:49**

**----------------------------------------------------------------------**

**Local IP Address: 192.168.23.30**

**Remote IP Address: 192.168.23.129**

**Local Port: Any**

**Remote Port: Any**

**Protocol: Any**

**Direction: Both**

**QM Offer: ESP:SHA1-None+60min+100000kb**

**PFS: None**

**IPsec Statistics**

**----------------**

**Active Assoc : 3**

**Offload SAs : 0**

**Pending Key : 0**

**Key Adds : 12**

**Key Deletes : 9**

**ReKeys : 0**

**Active Tunnels : 0**

**Bad SPI Pkts : 0**

**Pkts not Decrypted : 0**

**Pkts not Authenticated : 0**

**Pkts with Replay Detection : 0**

**Confidential Bytes Sent : 0**

**Confidential Bytes Received : 0**

**Authenticated Bytes Sent : 352,176**

**Authenticated Bytes Received: 656,804**

**Transport Bytes Sent : 352,176**

**Transport Bytes Received : 656,804**

**Bytes Sent In Tunnels : 0**

**Bytes Received In Tunnels : 0**

**Offloaded Bytes Sent : 0**

**Offloaded Bytes Received : 0**

**Ok.**

**C:\Windows\system32>**

1. Using 'dism /online /enable-feature' instead of OCSetup gives you the option of looking at log files detailing any install issues. the log file can viewed using notepad: notepad.exe C:\windows\logs\dism\dism.log REF: <http://code.msdn.microsoft.com/r2core/Wiki/Print.aspx?title=Home&version=13&action=Print> [↑](#footnote-ref-1)