FreeRDP Configuration Manual

Marc-André Moreau

Awake Coding Consulting Inc.

Contents

Chapter 1

Introduction

This document specifies various configuration procedures for common RDP deployment scenarios. These instructions should be used as a reference to help RDP developers configure a proper test setup to help them in their implementation.

1.1 Glossary

To be expanded.

1.2 References

To be expanded.

Chapter 2

Network Tracing

2.1 Introduction

Network tracing of RDP can be quite a challenge due to a number of factors such as encryption, compression, and the fact that these protocol features cannot always be disabled or worked around. One of the easiest way of decrypting RDP traffic is to configure the server with a self-signed certificate for which the private key is known, and then use this certificate with a network tracing tool to automatically decrypt the packets.

2.2 Certificate Generation

The following sections specify how to generate valid certificates that can be used with an RDP server.

2.2.1 MakeCert

MakeCert is a tool that is included with the Windows SDK or the Windows DDK that can generate certificates in the pfx file format.

If you have the Windows DDK installed, makecert.exe can be found at:

\WinDDK\\bin\\makecert.exe

If you have the Windows SDK installed, makecert.exe can be found at:

%programfiles%\Microsoft SDKs\Windows\\bin\makecert.exe

MakeCert is currently not distributed separately from the Windows DDK or the Windows SDK. Since it is a small and stand-alone tool, it can be easily copied

to another machine without the need for installing large software development packages. Keeping a copy for later use can therefore save a lot of time when configuring new machines.

To generate a self-signed certificate, invoke MakeCert with the following options:

makecert -r -pe -n "CN=%COMPUTERNAME%" -eku 1.3.6.1.5.5.7.3.1 -ss my -sr LocalMachine -sky exchange -sp "Microsoft RSA SChannel Cryptographic Provider" -sy 12

%COMPUTERNAME% expands to the current computer name, which is normally what you want. The name following "CN=" should be the common name of the certificate. Choose it wisely, because a certificate for which the common name attribute does not match the hostname that the client uses to connect is normally rejected.

MakeCert generates and import the certificate automatically, so do not expect to find a certificate file in the directory from which MakeCert has been executed. To get the certificate file, you will need to export it from the certificate store.

- Launch MMC as an elevated user (can be done from an Administrator command prompt)
- On the File menu, click Add/Remove Snap-in
- In the left pane, select Certificates, then click Add
- When prompted for user account type, select Computer account and click Next
- In the next dialog, leave Local computer as the computer to manage and click Finish
- Close the Add or Remove Snap-Ins dialog by clicking OK
- In the left pane, expand Certificates (Local Computer)
- Under Certificates (Local Computer), expand Personal and then select the Certificates directory
- In the right pane, you should find your newly generated self-signed certificate. Right-click on it, point to All Tasks, then click Export. The Certificate Export Wizard will appear.
- In the welcome screen, click Next
- In the Export Private Key screen, select Yes, export private key and click Next
- In the Export File Format screen, select Include all certificates in the certification path if possible and Export all extended properties, and click Next
- In the Password screen, enter a password which you will need to use when importing the certificate after it has been exported, and then click Next. The password is used to protect the private key. For testing purposes, you may want to use a simple dummy password such as "password".
- In the File to Export screen, specify a path and file name for the certificate to be exported. Click Next, and then Finish. A message box should

indicate that the certificate has been successfully exported.

2.2.2 OpenSSL

Create an OpenSSL extension file named “rdp.ext”

extensions = x509v3

[x509v3] keyUsage = keyEncipherment,dataEncipherment extendedKeyUsage = serverAuth

Create an OpenSSL config file named “rdp.cfg”:

[req] default_bits = 2048 distinguished_name = req_DN string_mask = nombstr

[req_DN] countryName = “1. Country Name (2 letter code)” countryName_default = CA countryName_min = 2 countryName_max = 2 stateOrProvinceName = “2. State or Province Name (full name)” stateOrProvinceName_default = Quebec localityName = “3. Locality Name (eg, city)” localityName_default = Montreal 0.organizationName = “4. Organization Name (eg, company)” 0.organizationName_default = Awake Coding Consulting Inc. organizationalUnitName = “5. Organization Unit Name (eg, section)” commonName = “6. Common Name (CA name or FQDN)” commonName_max = 64 commonName_default = awakecoding.com emailAddress = “7. Email Address (eg, name@FQDN)” emailAddress_max = 40 emailAddress_default = admin@awakecoding.com

Execute the following commands in the directory where rdp.ext and rdp.cfg are located:

openssl genrsa –out rdp.key 2048 openssl req -config rdp.cfg -new -key rdp.key -out rdp.csr openssl x509 -req -days 365 -extfile rdp.ext -signkey rdp.key -in rdp.csr -out rdp.crt openssl pkcs12 -export -inkey rdp.key -in rdp.crt -out rdp.pfx

2.3 Certificate Conversion

Convert from pfx to crt using OpenSSL:

openssl pkcs12 -in rdp.pfx -clcerts –nodes -out rdp.crt

Convert from crt to pfx using OpenSSL:

openssl pkcs12 -export –in rdp.crt -inkey rdp.key –nodes -out rdp.pfx

2.4 Certificate Installation

Import the certificate:

- Launch MMC as an elevated user (can be done from an Administrator command prompt)
- On the File menu, click Add/Remove Snap-in
- In the left pane, select Certificates, then click Add
- When prompted for user account type, select Computer account and click Next
- In the next dialog, leave Local computer as the computer to manage and click Finish
- Close the Add or Remove Snap-Ins dialog by clicking OK
- In the left pane, expand Certificates (Local Computer)
- Under Certificates (Local Computer), expand Personal
- Right-click Personal, point to All Tasks and click Import. The Certificate Import Wizard will appear.
- In the welcome screen, click Next
- In the File to Import screen, specify the path to certificate file to import, and click Next
- In the Password screen, enter the password that was used to export the certificate, select Mark this key as exportable, and click Next
- In the Certificate Store screen, select Place all certificates in the following store and select the Personal certificate store. Click Next and then Finish. A message box should indicate that the certificate has been successfully imported, and the certificate should now appear in the Personal certificate store.

2.4.1 Terminal Server

Windows Server 2008

Configure RDP server to use certificate: * Launch the Server Manager * In the left pane, expand Roles, Remote Desktop Services, and then select RD Session Host Configuration * In the middle pane, right-click the connection to configure, such as “RDP-Tcp” and select Properties. The Connection Properties dialog will appear. * In the General tab, click Select. A list of usable certificates will appear, select the appropriate one and click OK. * Click OK to apply the changes and close the Connection Properties dialog

Windows 7

Configure certificate permissions:

- Right-click on the certificate, point to All Tasks and click Manage Private Keys
- In the Permissions for private keys dialog, click Add

- In the Select Users or Groups dialog, type NETWORK SERVICE and click Check Names. Once the NETWORK SERVICE text is underlined, click OK
- In the Permissions for private keys dialog, click OK

Obtain certificate thumbprint:

- Double-click on the certificate. A Certificate dialog will appear.
- Select the Details tab, and select Thumbprint from the list of fields. Th thumbprint will be shown in the bottom text box as a series of hexadecimal numbers. Save the thumbprint for later as it is needed to configure the RDP server to use the certificae. The thumbprint should look like "a6 ff 13 00 b5 47 85 bf 48 3d 70 74 c8 aa 23 bb 3f 19 c1 71".

Configure RDP server to use certificate:

- Launch the Registry Editor (regedit.exe)
- In the directory structure, browse to the following key: [HKEY_LOCAL_MACHINE\System\CurrentCont Server\WinStations\RDP-Tcp]
- Right-click the RDP-Tcp key, point to New and click Binary Value. Name the new key SSLCertificateSHA1Hash
- Right-click the SSLCertificateSHA1Hash key and click Modify Binary Data. In the Edit Binary Data dialog, type the thumbprint of the certificate to be used by the RDP server. As it is particularly easy to make a mistake in this step, double-check that you have entered the thumbprint properly, and click OK

The RDP server should now be configured to use the new certificate.

2.4.2 TS Gateway

- Launch the Server Manager
- In the left pane, expand Roles, Remote Desktop Services and then RD Gateway Manager
- Under RD Gateway Manager, right-click the current server and click Properties to open the RD Gateway Server Properties dialog.
  - In the SSL Certificate tab, click Import Certificate to open the Import Certificate dialog.
  - From the list of certificates, select the one which you want to use, and click Import
  - Click OK to close the RD Gateway Server Properties dialog. A message box should inform you that the RD Gateway Server server needs to be restarted for the changes to take effect.

2.5 Protocol Configuration

Certain protocol features such as encryption and compression can make packet analysis harder.

2.5.1 TLS 1.0

Recent versions of Windows like Windows 8 will negotiate TLS 1.2 by default, a version of TLS which is not supported by Network Monitor. For easier packet decryption, it is recommended to force TLS 1.0 to be negotiated by disabling TLS 1.1 and TLS 1.2 on clients that support it.

Disabling TLS 1.1

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
1.1\Client] “Enabled”=dword:00000000 “DisabledByDefault”=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
1.1\Server] “Enabled”=dword:00000000 “DisabledByDefault”=dword:00000001

Disabling TLS 1.2

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
1.2\Client] “Enabled”=dword:00000000 “DisabledByDefault”=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
1.2\Server] “Enabled”=dword:00000000 “DisabledByDefault”=dword:00000001

2.5.2 Compression

To disable compression with mstsc, create a .rdp file and use the following option:

compression:i:0

With FreeRDP, simply do not turn on compression, or explicitly turn it off either with a .rdp file or with the –compression command-line option.

2.5.3 Network Level Authentication

To disable NLA with mstsc, create a .rdp file and use the following option:

enablecredsspsupport:i:0

To disable NLA with FreeRDP, you can use either the .rdp file or the –sec-nla command-line option.

2.6 Packet Capturing

There are two major packet capturing tools that can be used to capture RDP traffic: Network Monitor and Wireshark. The former has the advantage of being able to analyze a lot of the protocols of interest, but is not supported on non-Windows environments. The latter is open source and is supported on a wide variety of operating systems, but lacks good protocol analyzers for the vast majority of RDP.

2.6.1 Network Monitor

Installation

Download and install required tools:

- Network Monitor http://blogs.technet.com/b/netmon/
- NMParsers http://nmparsers.codeplex.com/
- NMDecrypt http://nmdecrypt.codeplex.com/

Change default parser profile:

- Launch Network Monitor
- On the Tools menu, click Options
- In the Parsers Profile tab, select Windows and click OK

Capturing

- Launch Network Monitor
- Click New Capture on the top menu bar
- Click Start on the top menu bar. This may take a few seconds, wait until the Stop button becomes enabled.
- Perform tasks generating network traffic of interest, and click Stop on the top menu bar

2.6.2 Wireshark

Installation

Download and install Wireshark (http://www.wireshark.org/) If you are using Linux, it packages should be available for all major distributions. If you choose to build Wireshark from source, make sure that you are building with SSL support.

Configuration

Configure SSL dissector:

- Launch Wireshark
- On the Edit menu, click Preferences
- In the left pane, expand Protocols and select SSL
- In the right pane, click Edit besides RSA keys list
- In the SSL Decrypt dialog, click New
- In the SSL Decrypt: New dialog, enter the following:
  - IP address of the RDP server
  - Port used by the RDP server
  - Protocol dissector to use with decrypted packets. When in doubt, use the data dissector.
  - Full path to the SSL private key file (.key extension)
  - Password used to protect the private key file, if there is one.
- Click OK to get back to the SSL Decrypt dialog, and click OK again

Capturing

Capture traffic:

- Launch Wireshark
- On the Capture menu, click Interfaces
- In the Capture Interfaces dialog, click Options besides the interface to capture from. If you do not know which interface to choose, it is normally the one with the highest amount of traffic as indicated in the Packets column.
- In the Capture Options dialog, type port 3389 in the Capture Filter field. The filter may be different depending on the port(s) used by the server. Filtering the capture is optional, but helps filtering out packets which are not of interest.
- Click Start
- Perform tasks generating network traffic of interest, and click Stop either from the top menu bar or on the Capture menu

Chapter 3

Users and Groups

3.1 Adding Users

3.1.1 Windows Server 2008

Local Users

- Launch the Server Manager
- In the left pane, expand Configuration and then Local Users and Groups
- Under Local Users and Groups, right-click Users and click New User. The New User dialog will appear.
  - Enter a username such as "jsmith" in the User name field
  - Enter a name such as "John Smith" in the Full name field
  - Enter a password such as "Password123!" in the Password and Confirm password fields
  - Unselect User must change password at next logon
  - Optionally select Password never expires (easier for testing)
  - Click Create to create the user
  - Click Close to close the dialog
- Under Local Users and Groups, click Users to show the list of users in the right pane
- In the right pane, right-click the user and then click Properties ("jsmith" from the previous example). The User Properties dialog will appear.
  - Under the Member Of tab, click Add. The Select Groups dialog will appear.
  - In the Enter the object names to select field, enter "Remote Desktop Users" and click Check Names. When the text becomes underlined, click OK.

- Click OK in the User Properties dialog to close it

Domain Users

- Launch the Server Manager
- In the left pane, expand Roles, Active Directory Domain Services, and then Active Directory Users and Computers.
- Under Active Directory Users and Computers, right-click a domain such as "lab1.awake.local", point to New and click User. The New Object – User dialog will appear. Complete the form and click Next:
  - First name: "John"
  - Last name: "Smith"
  - Full name: "John Smith"
  - User logon name: "jsmith"
  - User Logon name (pre-Windows 2000): "jsmith"
- In the Password and Confirm password fields, enter a password like "Password123!"
- Unselect User must change password at next logon, select Password never expires and then click Next
- Click Finish

Chapter 4

Active Directory

4.1 Server Configuration

4.1.1 Windows Server 2008

Installing the Active Directory Domain Services Role:

- Launch the Server Manager
- In the left pane, click Roles
- In the right pane, click Add Roles to launch the Add Roles wizard
- If the Before you begin page appears, click Next
- On the Server Roles page, select Active Directory Domain Services and click Next
- On the Introduction to Active Directory Domain Services page, click Next
- If prompted to add features required for the role, click Add Required Features
- On the Confirm Installation Selections page, click Install
- Wait for the Installation Results page to appear, click Close and reboot if necessary to complete the installation process.

Promoting the server to a domain controller:

- Click Start, click Run, type dcpromo and then click OK
- This starts the Active Directory Installation Wizard. Click Next
- On the Operating Systems Compatibility page, click Next
- On the Choose a Deployment Configuration, select Create a new domain in a new forest and click Next

- On the Name the Forest Root Domain page enter a FQDN such as "lab1.awake.local" and click Next. For testing purposes, avoid using a name which could potentially conflict with other existing names. Using the ".local" suffix is a good way to avoid conflicts.
- On the Set Forest Functional Level page, select the desired forest functional level from the list and then click Next. If you do not intend to have backwards compatibility in a particular lab environment, you may select the highest functional level, such as Windows Server 2008 R2.
- On the Add Domain Controller Options page, leave the DNS server option selected and click Next
- A dialog box will appear warning that a delegation for the DNS server cannot be created. Ignore this warning and click Yes.
- On the Location for Database, Log Files, and SYSVOL page, click Next
- On the Directory Services Restore Mode Administrator Password enter a password such as "Password123!" and then click Next
- On the Summary page, review the information and then click Next. Optionally, the summary information can be saved to a text file by clicking Export settings.
- Wait for installation to complete. You may select Reboot on completion, or click Finish manually later. In both cases, the server needs to be rebooted before continuing further.

Installing the Active Directory Certificate Services and DHCP Server roles:

- Launch the Server Manager
- In the left pane, click Roles
- In the right pane, click Add Roles to launch the Add Roles wizard
- If the Before you begin page appears, click Next
- On the Server Roles page, select Active Directory Certificate Services and DHCP Server and then click Next
- On the Introduction to DHCP Server page, click Next
- On the Select Network Connection Bindings page, the server's static IP address ("192.168.56.10") should be listed and selected by default. Click Next to continue
- On the Specify IPv4 DNS Server Settings page, enter the parent domain ("lab1.awake.local") and the preferred DNS server IPv4 address. By default this address is 127.0.0.1, but it needs to be changed to the current server's address ("192.168.56.10"). An alternate DNS server IPv4 address can also be entered. Click Next.
- On the Specify IPv4 WINS Server Settings page, select WINS is required for applications on this network and enter the current server's address ("192.168.56.10") in the Preferred WINS server IP address field. Click Next.
- On the Add or Edit DHCP Scopes page, click Add and enter the following information in the Add Scope dialog, click OK and then Next:

  - Scope name: “lab01” (or any descriptive name)
  - Starting IP address: 192.168.56.101
  - Ending IP address: 192.168.56.254
  - Subnet type: Wired (lease duration will be 8 days)
  - Leave Activate this scope selected
  - Subnet mask: 255.255.255.0
  - Default gateway (optional): 192.168.56.1
- On the Configure DHCPv6 Stateless Mode page, select Disable DHCPv6 stateless mode for this server and click Next
- On the Authorize DHCP Server page, select Use current credentials and click Next
- On the Introduction to Active Directory Certificate Services page, click Next
- On the Select Role Services page, select Certification Authority and click Next
- On the Specify Setup Type page, select Standalone and click Next
- On the Specify CA Type page, select Root CA and click Next
- On the Set Up Private Key page, select Create a new private key and click Next
- On the Configure Cryptography for CA, leave the default options and click Next
- On the Configure CA Name page, enter a common name for the CA and click Next. This name can be the same as the server name, but it is usually changed to clearly identify the name as being a certificate authority. In this case, we will use “LAB1-W2K8R2-CA”.
- On the Set Validity Period page, click Next
- On the Configure Certificate Database page, click Next
- On the Confirm Installation Selections page, click Install
- Wait for the Installation Results page to appear, click Close and reboot if necessary to complete the installation process.

Installing the WINS Server feature:

- Launch the Server Manager
- In the left pane, click Features
- In the right pane, click Add Features to launch the Add Features wizard
- In the Select Features page, select WINS Server and then click Next
- In the Confirm Installation Selections page, click Install
- Wait for the Installation Results page to appear, click Close and reboot if necessary to complete the installation process.

4.1.2 Windows Server 2012

Installing the Active Directory Domain Services Role:

- Launch the Server Manager
- At the top right, click Manage then click Add Roles and Features to launch the Add Roles and Features wizard
- If the Before you begin page appears, click Next
- On the Select installation type page, select Role-based or feature-based installation and click Next
- On the Select destination server page, leave the Select a server from the server pool option selected, select the current server from the Server Pool list, and then click Next
- On the Select server roles page, select Active Directory Domain Services. If prompted to add required features, click Add Features. Click Next to continue.
- On the Select features page, click Next
- On the Active Directory Domain Services page, click Next
- On the Confirm installation selections page, click Install
- Wait for the installation to complete and click Close

Promoting the server to a domain controller:

- Launch the Server Manager
- On the top right, click Notifications (flag icon) and then click Promote this server to a domain controller. This option is only shown after the installation of the Active Directory Domain Services role, and is a post-deployment configuration task. The Active Directory Domain Services Configuration wizard will appear.
- On the Deployment Configuration page, select Add a new forest and enter a FQDN for the domain in the Root domain name field such as "lab2.awake.local". Click Next to continue.
- On the Domain Controller Options page, select a Forest functional level and Domain functional level such as Windows Server 2008 R2. Ensure that the functional level you choose is compatible with the rest of your planned infrastructure. Leave the Domain Name System (DNS) server option selected. Enter a password in the Password and Confirm password fields, and then click Next.
- On the DNS Options page, there should be a warning saying that a delegation for the DNS server cannot be created. This warning can be safely ignored. Click Next to continue.
- On the Additional Options page, the NetBIOS domain name will be shown for verification. For instance, the corresponding NetBIOS name for the FQDN "lab2.awake.local" will be "LAB2". Click Next to continue.

- On the Paths page, click Next.
- On the Review Options page, click Next
- On the Prerequisites Check page, click Install
- Wait for the installation to complete. The server will restart automatically.

4.2 Client Configuration

4.2.1 Windows 7 and Windows Server 2008

Joining and existing domain:

- Right-click Computer and then click Properties
- Under Computer name, domain and workgroup settings click Change settings. The System Properties dialog will appear.
  - In the Computer Name tab, click Change. The Computer Name/Domain Changes will appear.
  - Under Member Of, select Domain, enter the domain name to join ("lab1.awake.local") and click OK
  - A password prompt will appear. Authenticate using an account with permission to join the domain, and click OK. A message box welcoming you to the domain should appear, click OK. Another message box will inform you that you must restart the computer, click OK again.
  - A dialog will then ask you to restart the computer now or later. In both cases, you need to restart the computer before going further.

4.2.2 Windows 8 and Windows Server 2012

Joining and existing domain:

- Open the System control panel page by pressing WinKey+X and clicking System in the menu that appears on the bottom left of the screen
- Under Computer name, domain and workgroup settings click Change settings. The System Properties dialog will appear.
  - In the Computer Name tab, click Change. The Computer Name/Domain Changes will appear.
- Under Member Of, select Domain, enter the domain name to join ("lab2.awake.local") and click OK
- A password prompt will appear. Authenticate using an account with permission to join the domain, and click OK. A message box welcoming you to the domain should appear, click OK. Another message box will inform you that you must restart the computer, click OK again.

- A dialog will then ask you to restart the computer now or later. In both cases, you need to restart the computer before going further.

Chapter 5

Remote Desktop Connection Broker

5.1 Server Configuration

5.1.1 Windows Server 2008

- Launch the Server Manager
- In the left pane, expand Roles, right-click Remote Desktop services and then click Add Role Services. The Add Role Services wizard will appear.
- On the Select Role Services page, select Remote Desktop Connection Broker and click Next
- On the Confirm Installation Selections page, click Install. Wait for the installation to complete and then click Close.

Chapter 6

Remote Desktop Web Access

6.1 Server Configuration

6.1.1 Windows Server 2008

- Launch the Server Manager
- In the left pane, expand Roles, right-click Remote Desktop services and then click Add Role Services. The Add Role Services wizard will appear.
- On the Select Role Services page, select Remote Desktop Web Access and click Next. You may be asked to install additional required services such as Web Server (IIS).
- On the Introduction to Web Server (IIS) page, click Next
- On the Select Role Services page, click Next
- On the Confirm Installation Selections page, click Install. Wait for the installation to complete and then click Close.

Chapter 7

Terminal Server Gateway

7.1 Server Configuration

7.1.1 Windows Server 2008

- Launch the Server Manager
- In the left pane, click Roles
- In the right pane, click Add Roles to launch the Add Roles wizard
- If the Before you begin page appears, click Next
- On the Server Roles page, select Remote Desktop Services and click Next
- On the Introduction to Remote Desktop Services page, click Next
- On the Select Role Services page, select Remote Desktop Session Host and Remote Desktop Gateway and then click Next
- On the Uninstall and Reinstall Applications for Compatibility page, click Next
- On the Specify Authentication Method for Remote Desktop Session Host, select either Require Network Level Authentication or Do not require Network Level Authentication and click Next
- On the Specify Licensing Mode page, select Configure later if you haven't installed licenses yet, otherwise select the appropriate mode between Per Device and Per User and click Next
- On the Select User Groups Allowed Access To This RD Session Host Server page, add the necessary user groups and click Next. Users from the Administrators group are allowed by default to connect using RDP.
- On the Configure Client Experience page, select the features to enable such as Audio and video playback, Audio recording redirection and Desktop composition and click Next. For testing purposes, enabling all features is a good idea.
- On the Choose and Server Authentication Certificate for SSL Encryption

page, either choose an existing certificate or select Create a self-signed certificate for SSL encryption and click Next. The SSL certificate for the Terminal Server Gateway is different from the SSL certificate used by the RDP server and can be changed later.

- On the Create Authorization Policies for RD Gateway page, select Now and click Next. The RD Gateway uses these policies to restrict both the users allowed to connect and the internal network resources that can be accessed.
- On the Select User Groups That Can Connect Through RD Gateway page, add necessary user groups and click Next
- In the Create an RD CAP for RD Gateway page, enter a name and select allowed authentication methods between Password and Smart card and click Next
- In the Create an RD RAP for RD Gateway page, enter a name and select Allow users to connect to any computer on the network and click Next. Alternatively, select Allow users to connect only to computers in the following group to restrict access to a limited set of computers in the internal network.
- On the Introduction to Network Policy and Access Services page, click Next
- On the Select Role Services page, leave Network Policy Server selected and click Next
- On the Introduction to Web Server (IIS) page, click Next
- On the Select Role Services page, leave default options selected and click Next
- On the Confirm Installation Selections page, click Install
- Wait for the Installation Results page to appear, click Close and reboot if necessary to complete the installation process.

7.2 Client Configuration

7.2.1 Windows 7

Ensure that both the client and the RD Gateway are on the same network, and that the client can connect to the server using its hostname, not its IP address. In this case, the server is called WIN20008R2SP1. The Administrator account is used for both authentication against the gateway and the remote desktop session host.

Configuring Remote Desktop Connection for RD Gateway connection:

- Launch Remote Desktop Connection (mstsc.exe)
- Enter WIN2008R2SP1 in the Computer field, and Administrator in the User name field

- Click Options at the bottom left of the Remote Desktop Connection window to expand advanced options
- In the Advanced tab, click Settings in the Connect from anywhere section. The RD Gateway Server Settings dialog will appear
  - Under Connection Settings, select Use these RD Gateway server settings. In the Server name field, enter WIN2008R2SP1 and select Ask for password (NTLM) as the Logon method. Unselect the Bypass RD Gateway server for local addresses option to ensure usage of the RD Gateway in a test environment.
  - Under Logon settings, select Use my RD Gateway credentials for the remote computer
  - Click OK to return to Remote Desktop Connection
- Click Connect
- In the Windows Security dialog, enter your credentials for the Administrator account. This dialog should say that the credentials will be used for a list of two computers, where one of them is listed as being an RD Gateway server.
- If you are using a self-signed certificate or an untrusted certificate, which is most likely the case in a test environment, a Remote Desktop Connection warning dialog will inform you that the identity of the RD Gateway cannot be verified. Do not click OK, since it will abort the connection sequence. The certificate needs to be saved and imported in the proper certificate store before we can successfully connect. Open the Certificate dialog by clicking View Certificate.
  - In the Details tab, click Copy to File to open the Certificate Export Wizard
    - In the Welcome to the Certificate Export Wizard page, click Next
    - In the Export File Format page, select DER encoded binary X.509 (CER) and click Next
    - In the File to Export page, specify a destination file name and path, such as gateway.cer in the Documents folder and click Next
    - In the Completing the Certificate Export Wizard page, click Finish to close the wizard
  - Close the Certificate dialog by clicking OK
- Close the Remote Desktop Connection warning dialog by clicking OK. The connection sequence will be aborted, but the RD Gateway certificate has been saved first. The certificate can now be imported in the Trusted Root Certification Authorities store for the client to accept identify the server on the next connection.

Installing RD Gateway certificate for trust:

- Double-click the RD Gateway certificate (gateway.cer in Documents from the previous steps). The Certificate dialog will appear.

- In the General tab, click Install Certificate. The Certificate Import wizard will appear.
  - In the Welcome to the Certificate Import Wizard page, click Next
  - In the Certificate Store page, select Place all certificates in the following store. Click Browse to open the Select Certificate Store dialog
    - Select Trusted Root Certification Authorities and click OK
  - Click Next, and then Finish in the Completing the Certificate Import Wizard page. A Security Warning dialog will appear asking to confirm the installation of the certificate, click Yes and then OK.
  - Click OK to close the Certificate dialog