Citrix XenApp 6.5 and XenDesktop 5.6 Security Standards and Deployment Scenarios

Supplementary scenarios

Overview

Citrix products offer the security specialist a wide range of features for securing Citrix XenApp and XenDesktop systems according to officially recognized standards.

Security standards as they apply to XenApp 6.5 and XenDesktop 5.6 are discussed here. These topics provide an overview of the standards that apply to XenApp and XenDesktop deployments and describe the issues involved in securing communications across a set of sample deployments. For more information about the details of the individual security features, refer to the relevant product or component documentation.

When deploying XenApp and XenDesktop within large organizations, particularly in government environments, security standards are an important consideration. For example, many government bodies in the United States and elsewhere specify a preference or requirement for applications to be compliant with Federal Information Processing Standards (FIPS) 140. These topics address common issues related to such environments.

These topics are designed for security specialists, systems integrators, and consultants, particularly those working with government organizations worldwide.

Supplementary Scenarios

To make a XenApp or XenDesktop deployment FIPS 140-compliant, you need to consider each communication channel within the installation. The following deployment samples show how users can connect to XenApp and XenDesktop servers with different configurations of components and firewalls. In particular, the samples provide general guidance on how to make each communication channel secure using TLS so that the system as a whole is FIPS 140-compliant.

This document provides guidance on the following supplementary deployment scenarios for XenDesktop 5.6 and XenApp 6.5:

Product	Deployment Scenario
XenApp	1. Direct internal access [LAN] 2. External remote access [via Internet]
XenDesktop	3. Direct internal access [LAN] 4. External remote access [via Internet]

This document does not replace the existing XenApp 6.5 Security Deployments: http://support.citrix.com/proddocs/topic/xenapp65-sec/ps-sec-deployment-samples-xa6.html.

These supplementary deployment scenarios utilize the following components:

SSL Relay is a Windows-based software component that is installed directly on the XenApp server or XenDesktop VDA. It provides the ability to secure data communications using the Transport Layer Security (TLS) protocol. TLS provides server authentication, encryption of the data stream, and message integrity checks. SSL Relay is used to encrypt and secure communication between:

- Citrix Receiver and XenApp and/or XenDesktop VDA
- Web Interface and XenApp
- NetScaler MPX appliance and XenApp and/or XenDesktop VDA

NetScaler MPX appliance, FIPS edition is a hardened, physical appliance that is traditionally deployed in the DMZ to provide secure remote access to XenDesktop and XenApp environments. It provides FIPS 140-2 Level 2 SSL encryption of traffic to encrypt and secure communication between:

- Citrix Receiver and the NetScaler MPX appliance
- NetScaler MPX appliance and XenApp and/or XenDesktop VDA and Web Interface

XenApp, XenDesktop, Web Interface and SSL Relay can be configured to use government approved cryptography to protect "sensitive but unclassified" data by using the applicable ciphersuites:

- RSA_WITH_3DES_EDE_CBC_SHA supports RSA key exchange and TripleDES encryption, as defined in Internet RFC 2246 (http://www.ietf.org/rfc/rfc2246.txt).
- RSA_WITH_AES_128_CBC_SHA supports RSA key exchange with Advanced Encryption Standard (AES) and 128-bit keys for TLS connections, as defined in FIPS 197 http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf and Internet RFC 3268 (http://www.ietf.org/rfc/rfc3268.txt). For more information about AES, see http://csrc.nist.gov/cryptval/des.htm.
- RSA_WITH_AES_256_CBC_SHA supports RSA key exchange with AES and 256-bit keys for TLS connections, as defined in FIPS 197 and RFC 3268.

NetScaler FIPS can be configured to use government approved cryptography to protect "sensitive but unclassified" data by using the applicable ciphersuites:

- Cipher Name: SSL3-DES-CBC3-SHA
  Description: SSLv3 Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
- Cipher Name: TLS1-AES-256-CBC-SHA
  Description: TLSv1 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
- Cipher Name: TLS1-AES-128-CBC-SHA
  Description: TLSv1 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1

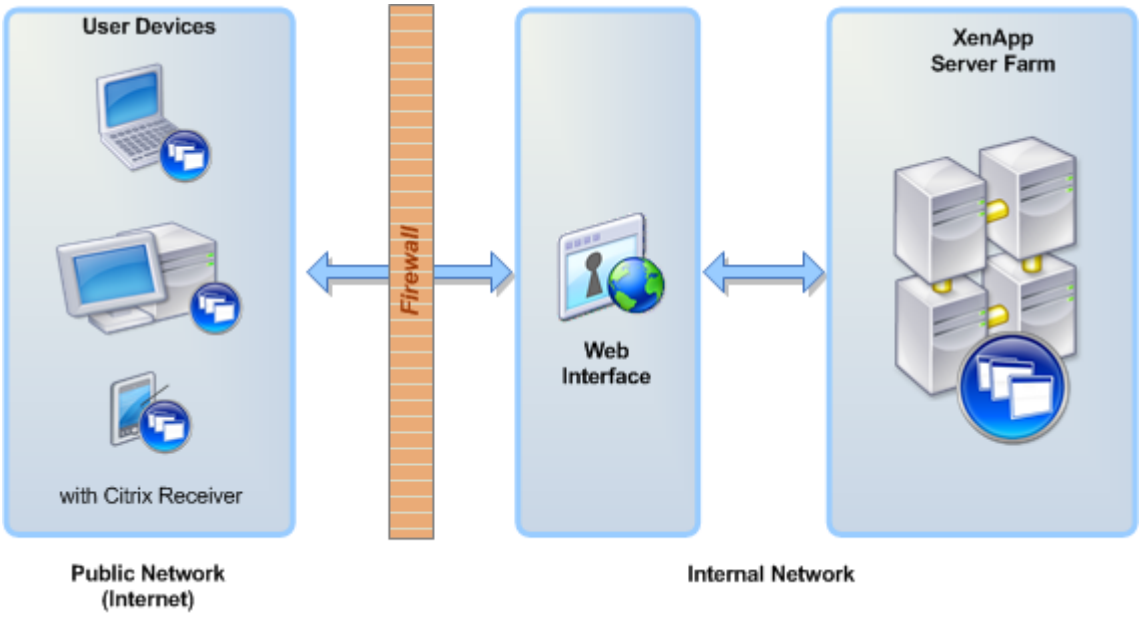
This list of approved ciphersuites is available on eDocs:
http://support.citrix.com/proddocs/topic/xenapp65-sec/ps-sec-government-ciphersuites.html

Support: For further information and support regarding these supplementary deployment scenarios:

a) Contact Technical Support if you have a valid Technical Support Contract (including TRM)
b) Contact your Partner if you do not have a support contract

XenApp using SSL Relay (Internal Network)

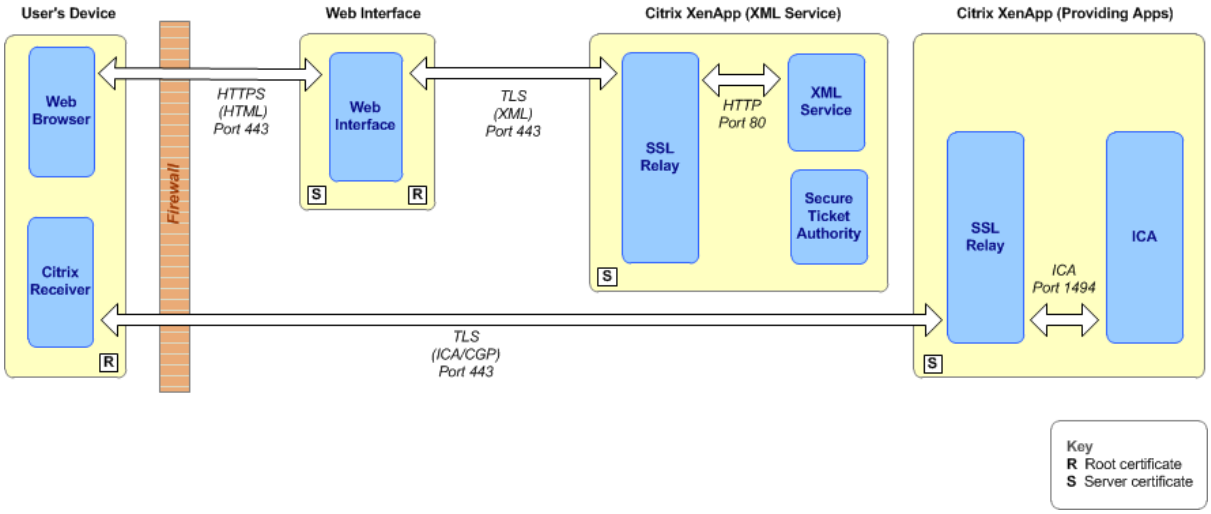
This deployment uses the SSL Relay to provide end-to-end TLS encryption between the XenApp server and Citrix Receiver running on the user devices.



The following table lists the components of the deployment and the operating systems required for the servers and client devices.

	Components	Operating System
XenApp Farm	XenApp 6.5 for Microsoft Windows Server 2008 R2 SSL Relay enabled Secure Ticket Authority installed on XenApp server	Windows Server 2008 R2
Web Server	Web Interface 5.4 for Internet Information Services	Windows Server 2008 R2 Windows Server 2008 Windows Server 2003 with Service Pack 2 .NET Framework 3.5 or 2.0 (IIS 6.0 only) Visual J#.NET 2.0 Second Edition
User Devices	Citrix Receiver for Windows 3.4 TLS-enabled Web browser	

This diagram shows a detailed view of the deployment including the components and certificates on each server, plus the communication and port settings.



Setting up the deployment comprises the following tasks:

- Configuration of the server running Web Interface
- Configuration of the servers running XenApp
- Clear the Web Interface Cache
- Configure the firewall settings

Configure security settings for the server running Web Interface

This procedure assumes Web Interface is already installed (on Microsoft Internet Information Services) and a XenApp Website is configured. For more information regarding installation and configuration of Web Interface, see *http://support.citrix.com/proddocs/topic/web-interface-impington/wi-install-web-interface-iis-task-gransden.html*

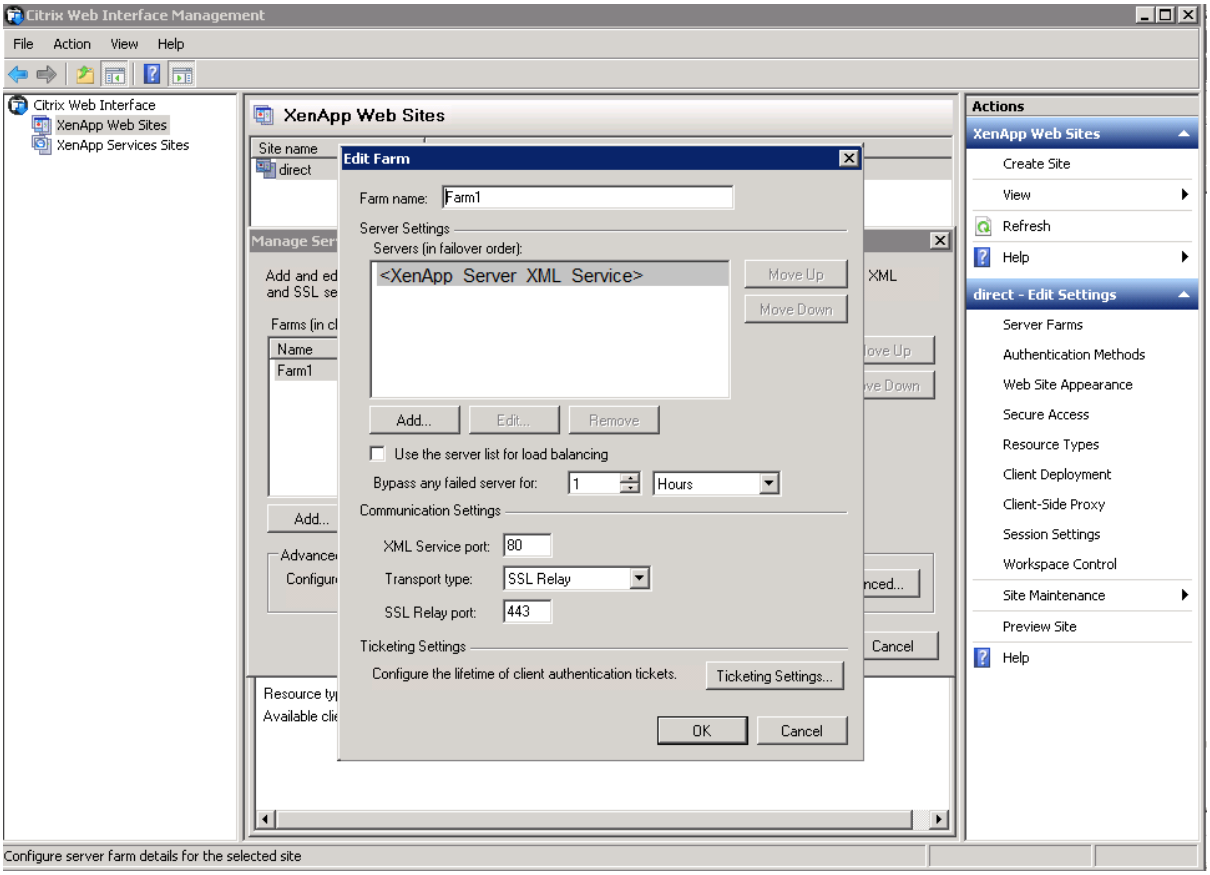
1. Ensure that a suitable server certificate is configured using IIS and HTTPS binding is configured.

2. If your deployment uses SHA-2, replace the netsslsdk.dll stored in '\inetpub\wwwroot\Citrix\<WI_site_name>\bin', with the .dll provided on the media (in the 'WI' folder).

3. Reset Microsoft Internet Information Services to load the new version of the netsslsdk.dll.

4. Using the Web Interface management console, ensure the server running XenApp (XML Service) is shown in the Server Farm list and the Communication Settings Transport Type is set to HTTPS or SSL Relay.

   For example, if using SSL Relay:

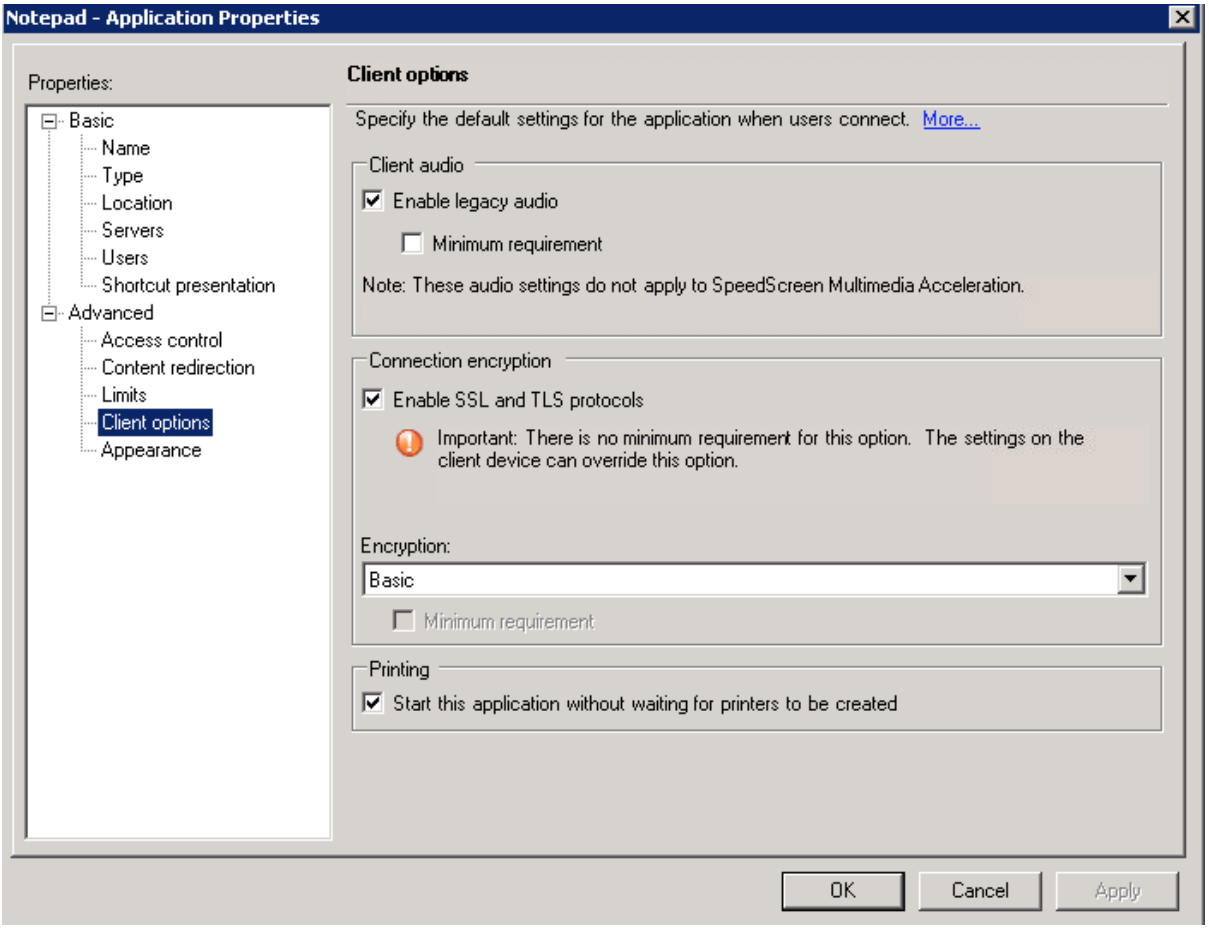


5. Ensure the server running Web Interface trusts the root certificate issued by the server running XenApp (XML Service).

Configure security settings on servers running the XenApp

1. Using the Citrix SSL Relays Configuration tool, ensure the SSL Relay is enabled and configured on all XenApp servers (including the XenApp server with the XML Service and XenApp server(s) hosting applications).

2. For all published applications, ensure connection encryption is enabled for SSL and TLS protocols:



Clear the Web Interface Cache

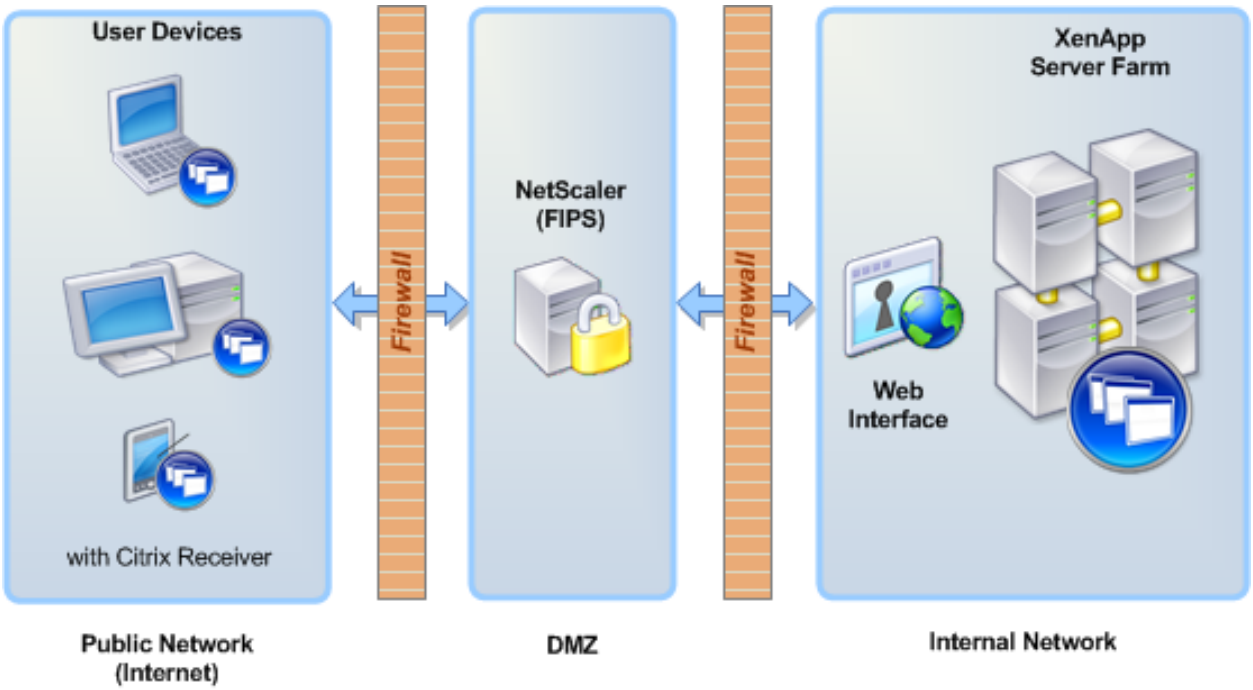
Restart Microsoft Internet Information Services on the server running Web Interface. This clears the published resources cache.

Configure the Firewall Settings

Lock down the firewall to allow localhost traffic only on ports 1494 and 2598.

XenApp using NetScaler (External Access)

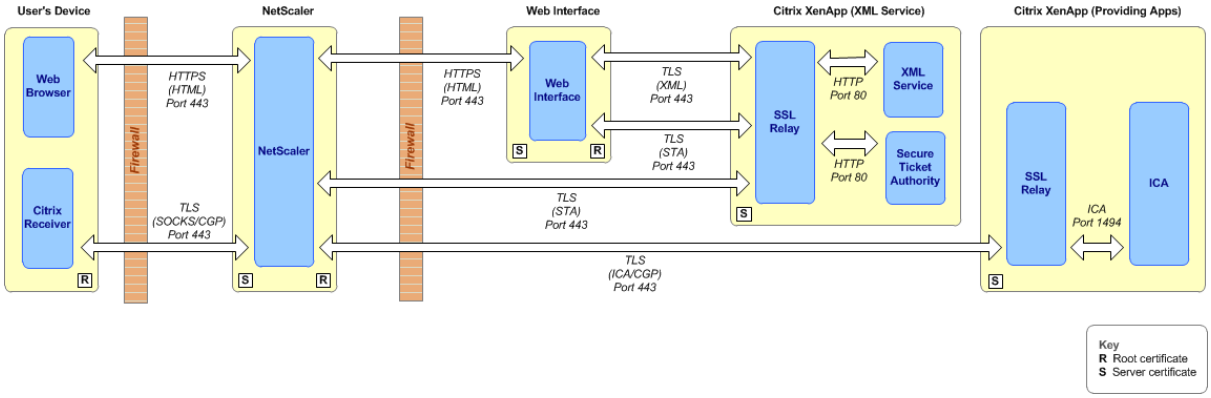
This deployment uses a Netscaler FIPS appliance to terminate the TLS connection from TLS enabled plug-ins (SSP and ICA engine) and forwards the traffic to the WI server using HTTPS and using TLS to SSL Relay (ICA connection).



The following table lists the components of the deployment and the operating systems required for the servers and client devices.

	Components	Operating System
XenApp Farm	XenApp 6.5 for Microsoft Windows Server 2008 R2 SSL Relay enabled Secure Ticket Authority installed on XenApp server	Windows Server 2008 R2
Web Server	Web Interface 5.4 for Internet Information Services	Windows Server 2008 R2 Windows Server 2008 Windows Server 2003 with Service Pack 2 .NET Framework 3.5 or 2.0 (IIS 6.0 only) Visual J#.NET 2.0 Second Edition
User Devices	Citrix Receiver for Windows 3.4 TLS-enabled Web browser	

This diagram shows a detailed view of the deployment including the components and certificates on each server, plus the communication and port settings.



Setting up this the deployment is same a setting up the XenApp using SSL Relay (Internal Network) deployment with the addition of configuration of NetScaler security settings.

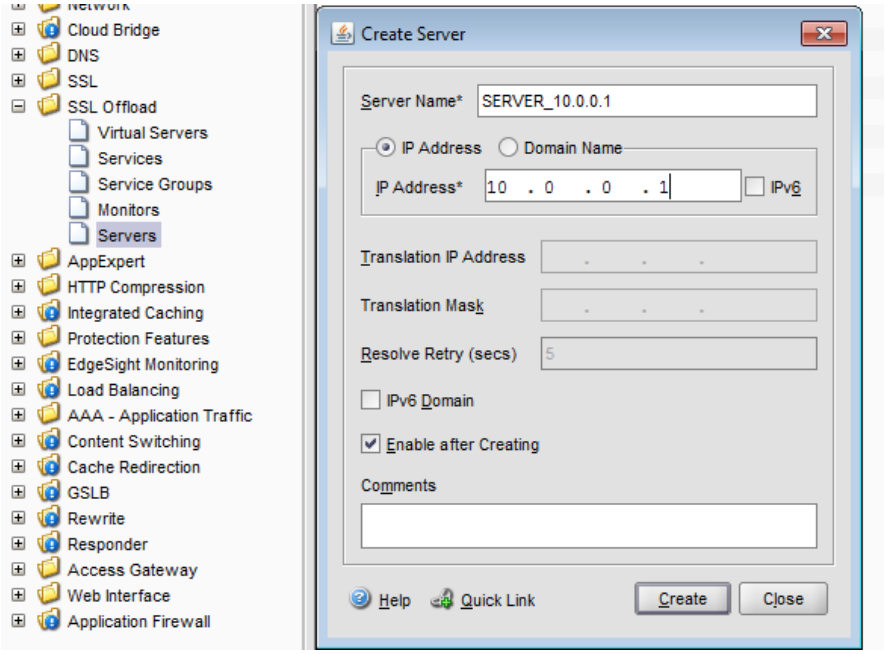
Configure NetScaler security settings

This procedure assumes the NetScaler appliance is already setup and configured for FIPS/TLS. For more information, see http://support.citrix.com/proddocs/topic/netscaler-getting-started-map-93/ns-instpk-install-ns-wrapper.html

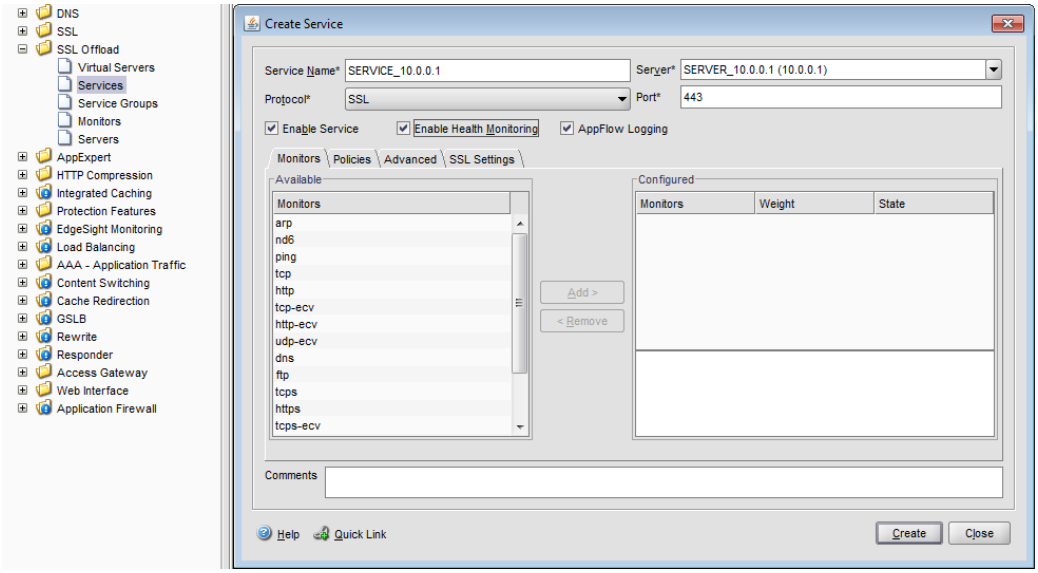
1. If you have previously configured Web Interface or STA sites on your NetScaler device, remove them from your NetScaler configuration. The details, if configured, are stored in Session Profile, Global Settings and Virtual Server Published Applications.

2. Create an SSL Offload Service for servers running Web Interface, STA and XenApp:

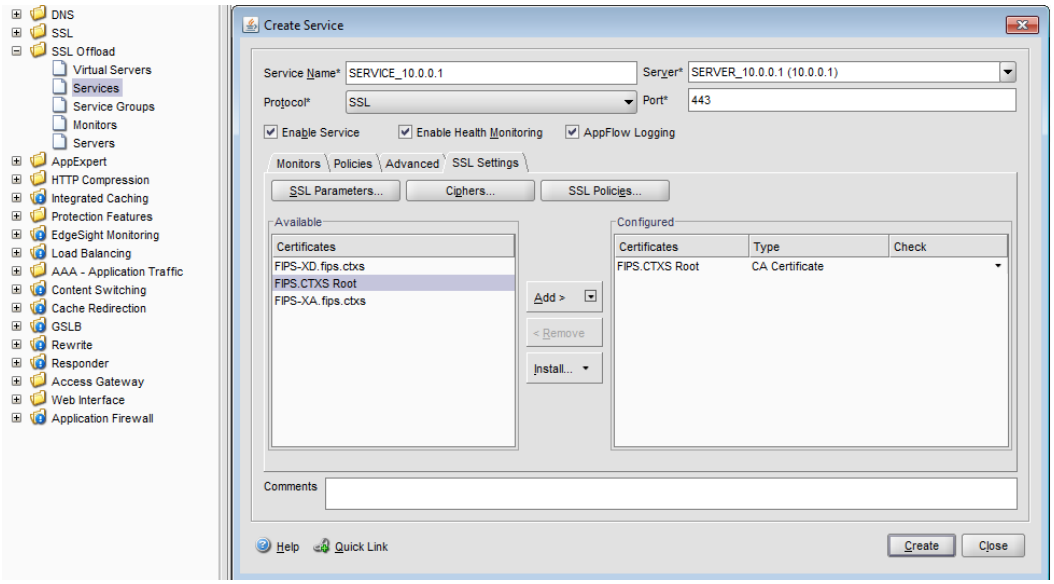
    a. Create an SSL Offload Server specifying the IP Address. For example, if using the NetScaler management tool:



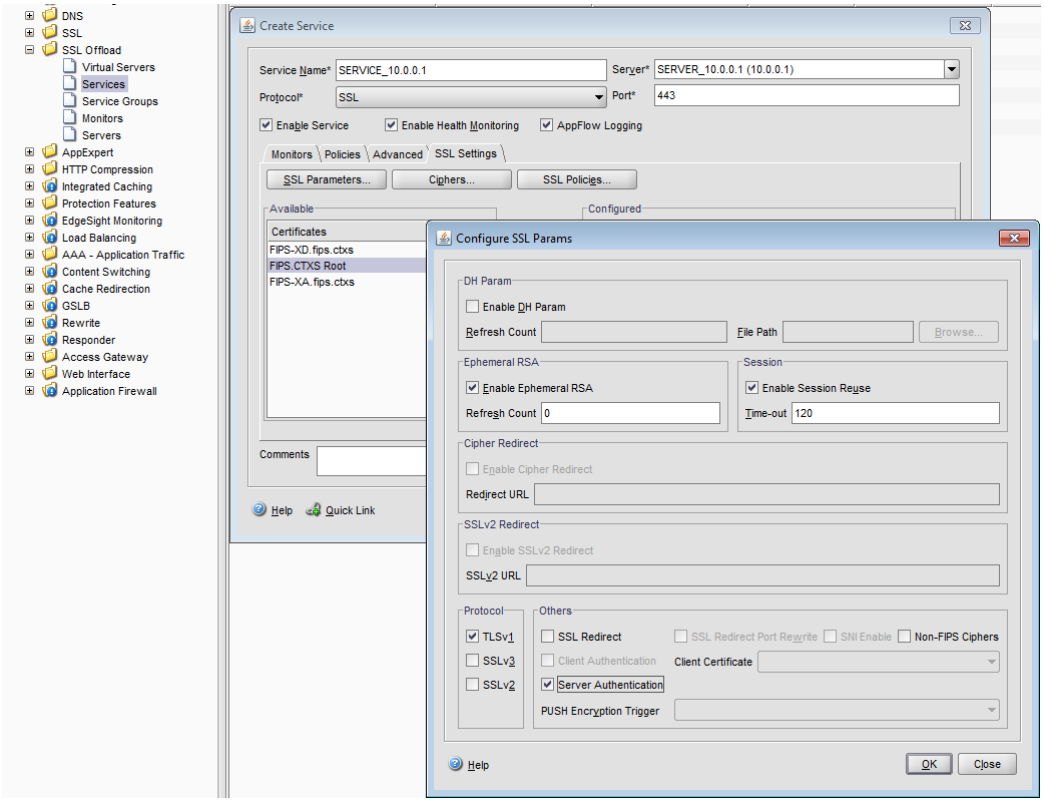
b. Create a Service. Specify the name of the SSL Upload Server and set Protocol ‘SSL’ and Port ‘443’. For example:



c. Select the SSL Settings tab and add the relevant root certificate as a CA. For example:



d. Configure the SSL Parameters to ensure the Protocol is set to TLS v1 only and Server Authentication. For example:

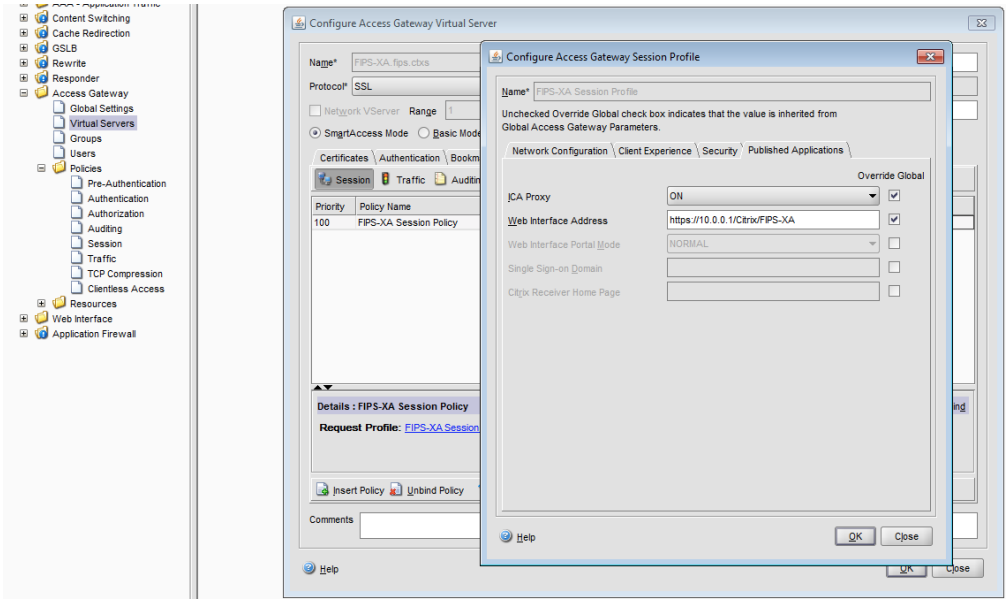


Note: You can perform steps a) to d) using the following NetScaler CLI commands:

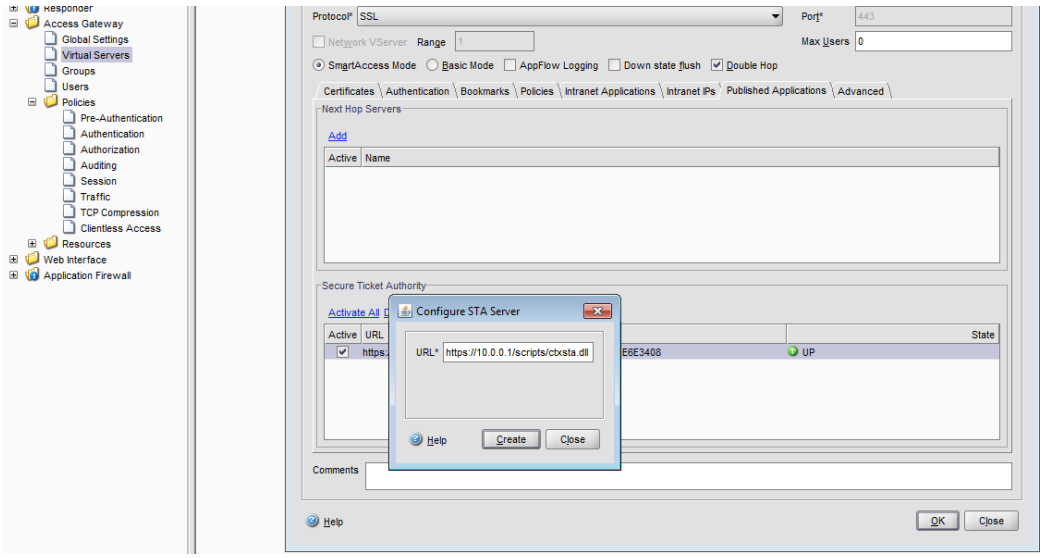
```
add server SERVER_10.0.0.1 10.0.0.1
add service SERVICE_10.0.0.1 SERVER_10.0.0.1 SSL 443
set ssl service SERVICE_10.0.0.1 -eRSA DISABLED -ssl3 DISABLED
-serverAuth ENABLED
bind ssl service SERVICE_10.0.0.1 -certkeyName "FIPS.CTXS Root"
-CA -ocspCheck Optional
```

where `"FIPS.CTXS Root"` is the name of the relevant root CA as configured in NetScaler.

3. Ensure the Access Gateway Session Profile 'Web Interface Address' is configured for 'https' using the relevant IP Address. For example:

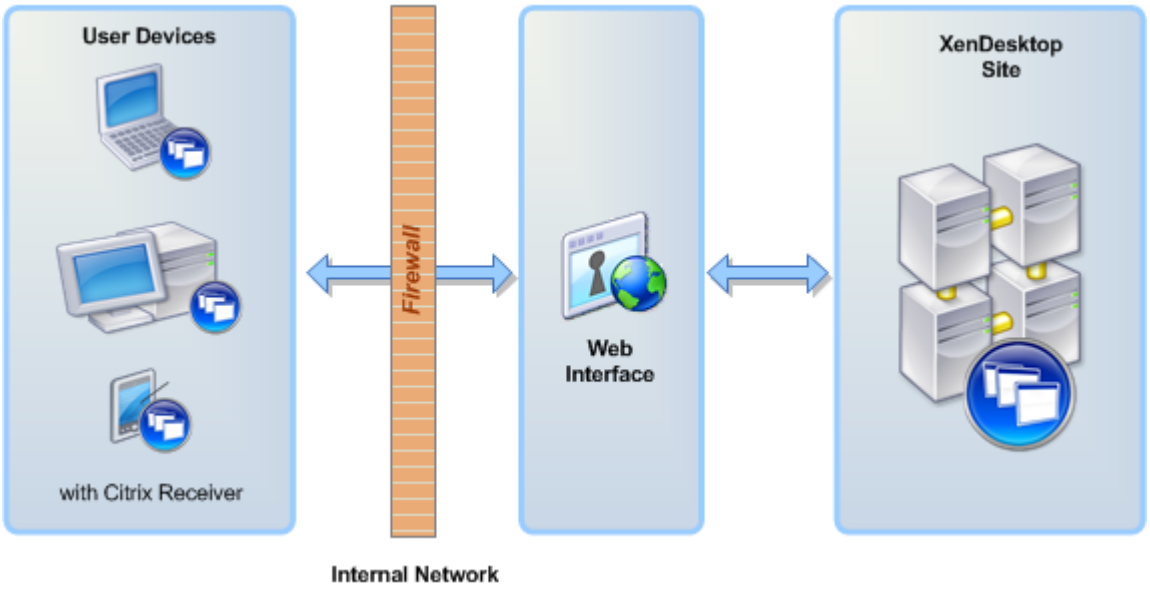


4. Ensure the URL for each STA is set for 'https' using the relevant IP Address. For example:



XenDesktop using SSL Relay (Internal Network)

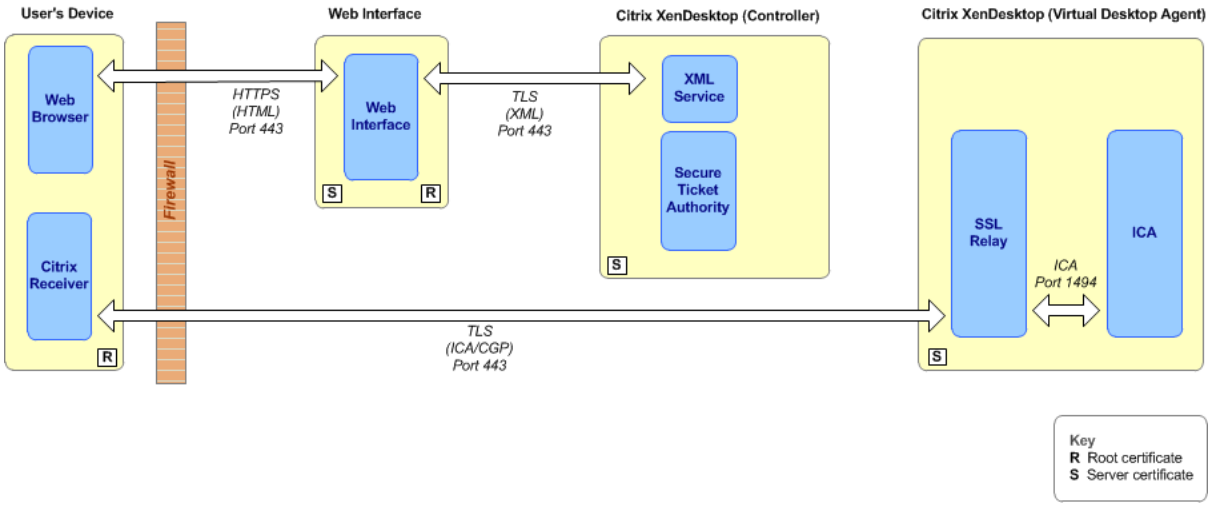
This deployment uses the SSL Relay (added to the XenDesktop VDA) to encrypt the ICA communication between XenDesktop and the Citrix Receiver. Also, all HTTP connections are secured using TLS.



The following table lists the components of the deployment and the operating systems required for the servers and client devices.

	Components	Operating System
XenDesktop Site	XenDesktop 5.6 SSL Relay Enabled Secure Ticket Authority is part of the XenDesktop Controller XenDesktop Workers	Windows Server 2008R2 Windows XP Windows 7 x86 Windows 7 x64
Web Server	Web Interface 5.4 for Internet Information Services	Windows Server 2008 R2 Windows Server 2008 Windows Server 2003 with Service Pack 2 .NET Framework 3.5 or 2.0 (IIS 6.0 only) Visual J#.NET 2.0 Second Edition
User Devices	Citrix Receiver for Windows 3.4 TLS-enabled Web browser	

This diagram shows a detailed view of the deployment including the components and certificates on each server, plus the communication and port settings.



Setting up the deployment comprises the following tasks:

- Configuration of the server running Web Interface
- Configuration of the server running the Virtual Desktop Agent
- Configuration of the server running the XenDesktop Controller
- Clear the Web Interface Cache
- Configure the firewall settings

Configure security settings for the server running Web Interface

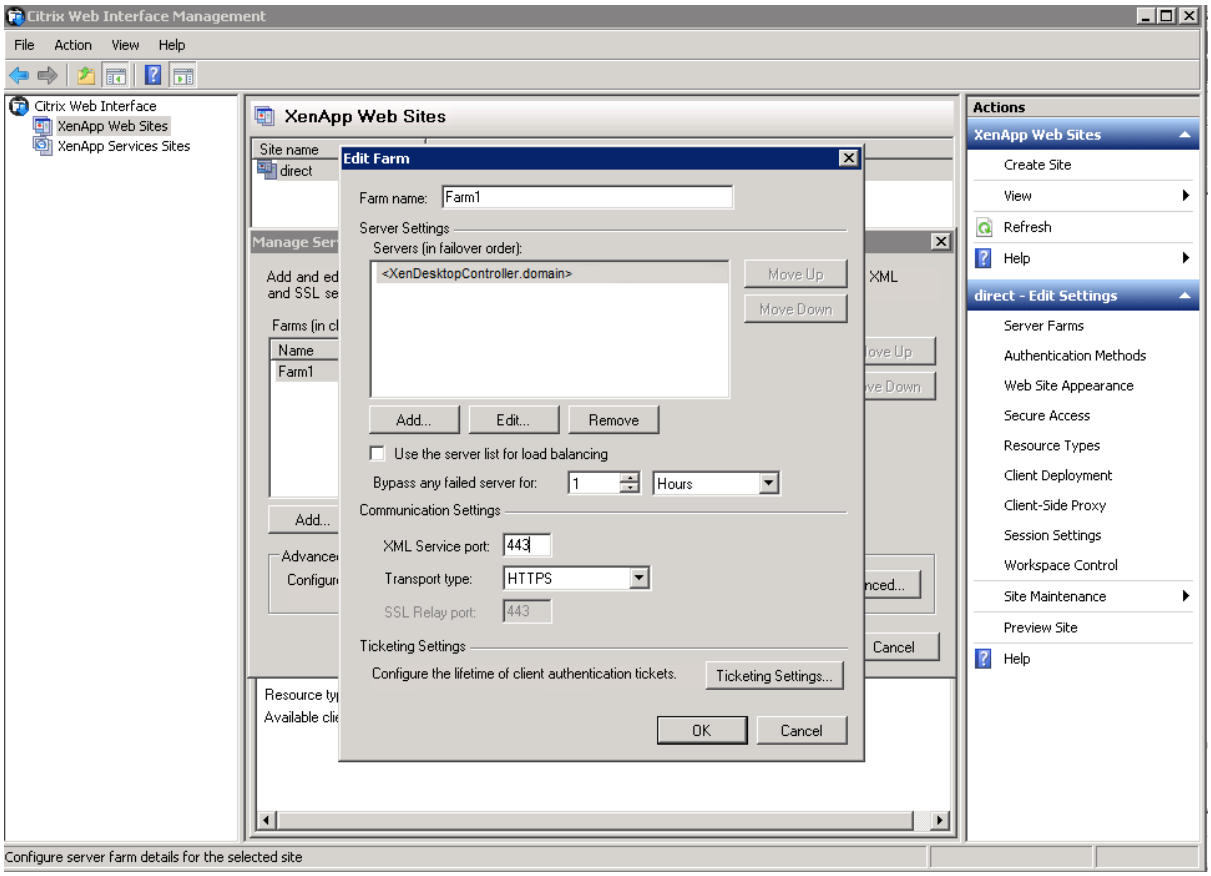
This procedure assumes Web Interface is already installed (on Microsoft Internet Information Services) and a XenApp Website is configured. For more information regarding installation and configuration of Web Interface, see *http://support.citrix.com/proddocs/topic/web-interface-impington/wi-install-web-interface-iis-task-gransden.html*

1. Ensure that a suitable server certificate is configured using IIS and HTTPS binding is configured.

2. If your deployment uses SHA-2, replace the netsslsdk.dll stored in '\inetpub\wwwroot\Citrix\<WI_site_name>\bin', with the .dll provided on the media (in the 'WI' folder).

3. Reset Microsoft Internet Information Services to load the new version of the netsslsdk.dll.

4. Using the Web Interface management console, check that the XenDesktop Controller is shown in the Server Farm list and the Communication Settings are set as follows:
   - XML Service port: 443
   - Transport type: HTTPS



5. Ensure the server running Web Interface trusts the root certificate issued by the server running the XenDesktop Controller.

Configure security settings on the server running the XenDesktop Virtual Desktop Agent

This procedure assumes the XenDesktop Virtual Desktop Agent is already installed. For more, see *http://support.citrix.com/proddocs/topic/xendesktop-ibi/cds-install-setup-ibi.html*

1. Install the following hotfixes (included on the media in folder 'VDA\x86' or 'VDA\x64'):

   - For 32-bit OS: XD560VDAWX86204.zip
   - For 64-bit OS: XD560VDAWX64204.zip

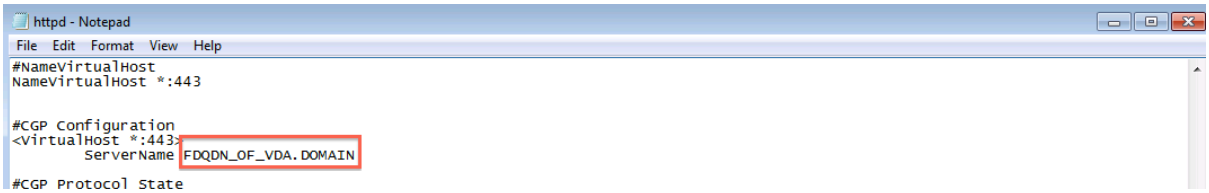
2. Create the server certificate for the VDA and install it in the Local Computer Certificate Store.

3. Extract the relevant XTE_VDA zip file (included on the media in the 'VDA' folder):

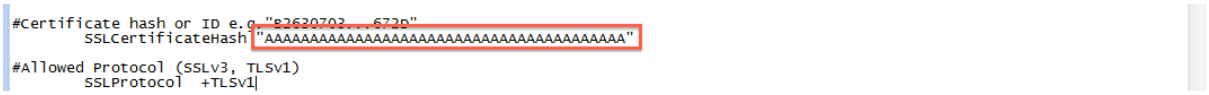
   - On 32-bit OS: Extract 'XTE_VDA_SSLRelay_x86.zip' to 'C:\Program Files\Citrix'
   - On 64-bit OS: Extract 'XTE_VDA_SSLRelay_x64.zip' to 'C:\Program Files (x86)\Citrix'

4. Open the file 'httd.conf' located in 'C:\Program Files\Citrix\XTE\conf\' or 'C:\Program Files (x86)\Citrix\xte\conf\'.

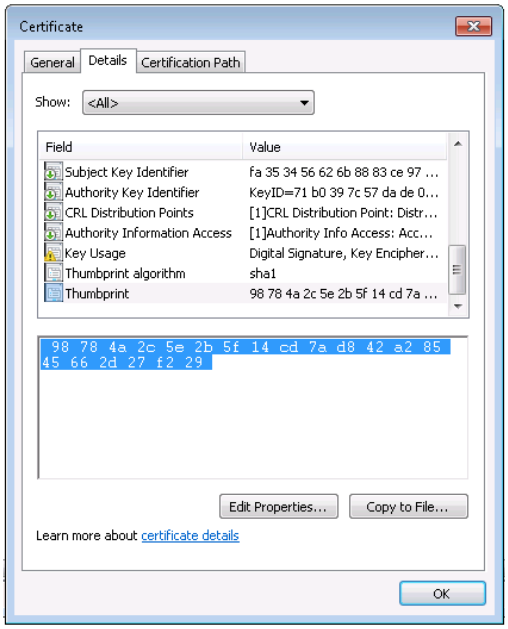
   a. Edit the Server Name to match the Fully Qualified Domain Name of the VDA in the format: <Name_of_VDA>.<domain> for example, 'vda_zyz.domain'.



   b. Edit 'SSLCertificationHash' to match the Certificate Thumbprint (without spaces) of the server certificate on the VDA.



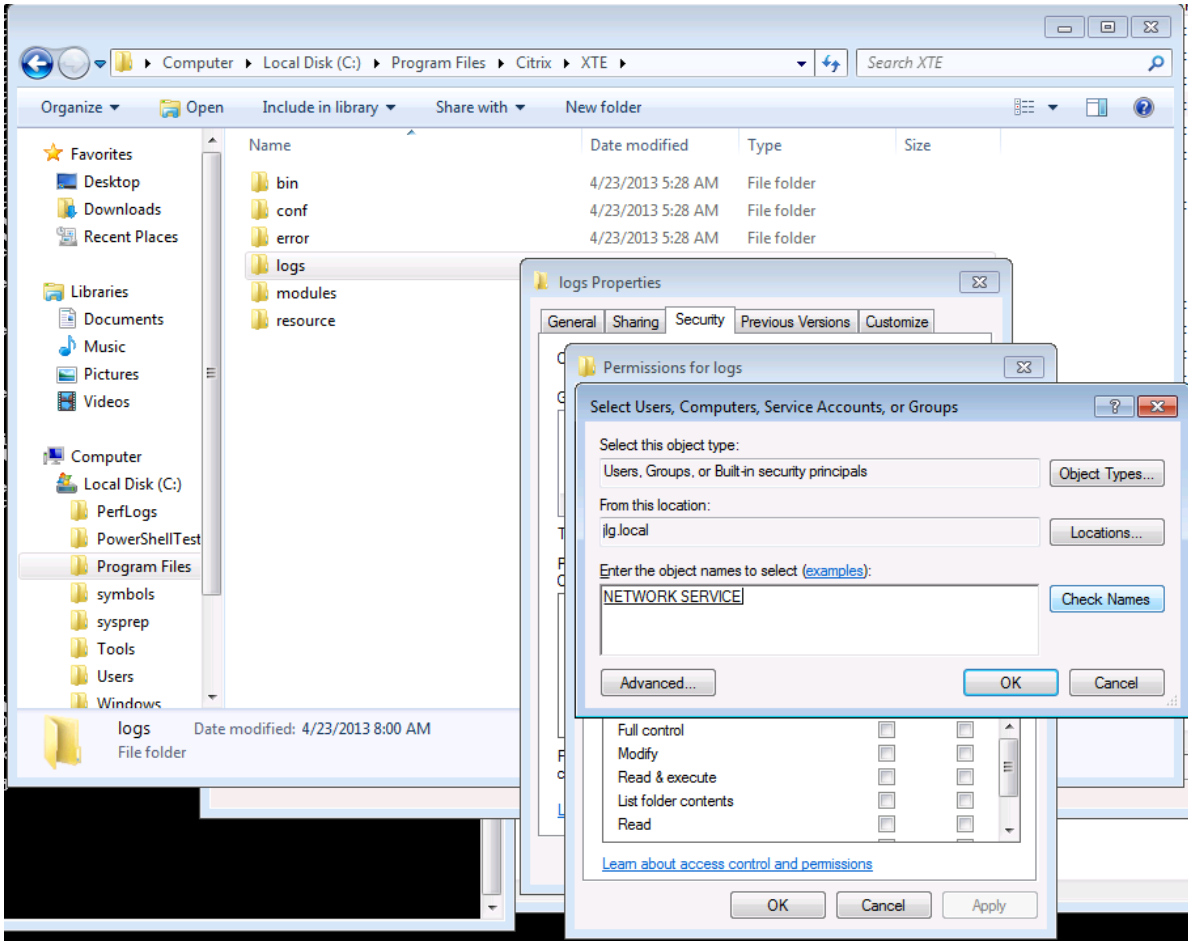
   For example: "98784a2c5e2b5f14cd7ad8428545662d27f229" for this certificate.

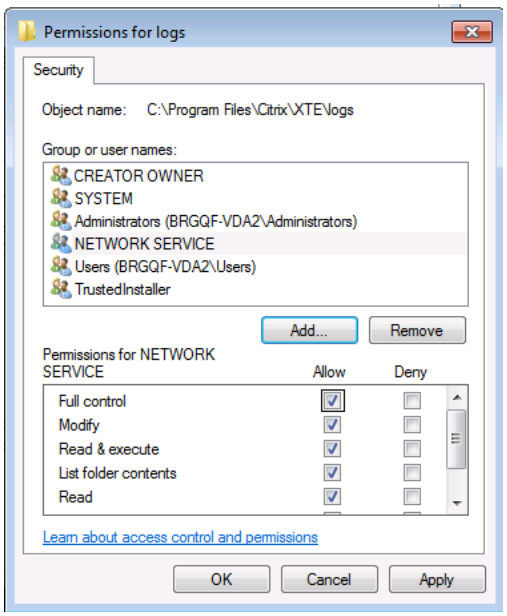


   Note: If you copy the content from the Certificate > Details screen above, ensure you do not copy the blank space at the beginning of the string as it is copied as a Unicode character. The SSL Relay is unable to read the file if it includes the Unicode character.

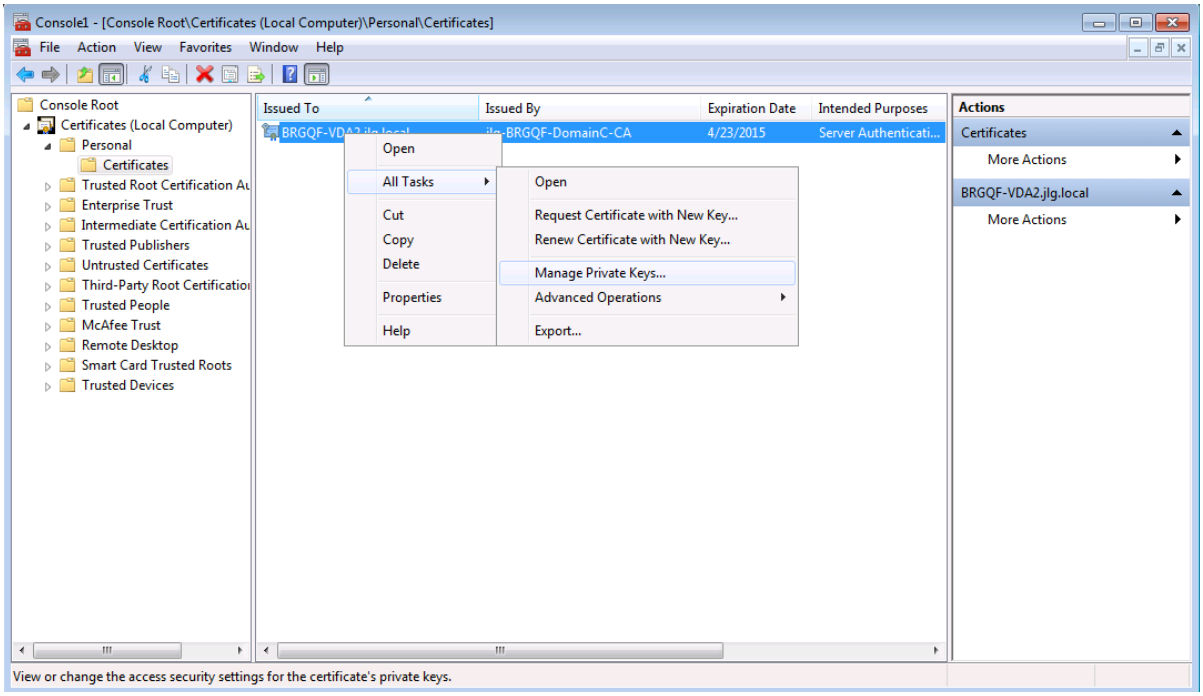
   c. Save the file.

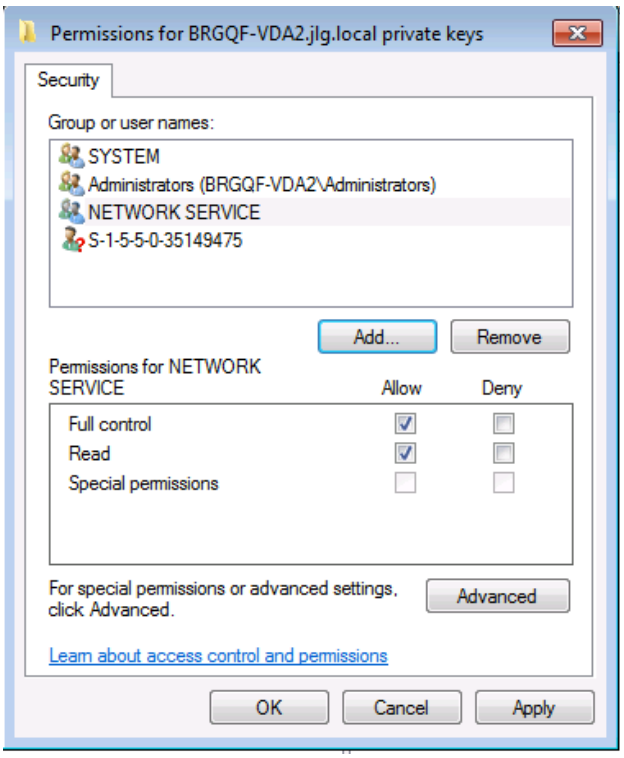
5. Allow the Network Service account full control of C:\Program Files\Citrix\XTE\logs.





6. Allow the Network Service account access to the certificate private key. For example, in Windows 7:





Note: On Windows XP a utility such as Microsoft Windows HTTP Services (WinHTTP) Certificate Configuration Tool, WinHttpCertCfg.exe, is required to install and configure client certificates ACLs.

7. As an Administrator (local or domain), start cmd.exe and run the following commands:
   a. On 32-bit OS:

```
sc create "CitrixSSLRelay" binpath= "\"C:\Program
Files\Citrix\XTE\bin\XTE.exe\" -k runservice -n \"Citrix SSL
Relay\" -f \"conf/httpd.conf\"" DisplayName= "Citrix SSL Relay"
start= auto obj= "NT AUTHORITY\NetworkService"
```

   b. On 64-bit OS:

```
sc create "CitrixSSLRelay" binpath= "\"C:\Program Files
(x86)\Citrix\XTE\bin\XTE.exe\" -k runservice -n \"Citrix SSL
Relay\" -f \"conf/httpd.conf\"" DisplayName= "Citrix SSL Relay"
start= auto obj= "NT AUTHORITY\NetworkService"
```

   c. On both 32-bit and 64-bit OS:

```
sc description "CitrixSSLRelay" "Services network requests for SSL
from Citrix components"
```

8. Using the registry file 'XTE_Parameters.reg' (included on the media in folder 'VDA\x86' or 'VDA\x64'), add the following registry key:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\CitrixSSLRelay\Parameters]
"ConfigArgs"=hex(7):00,00,00,00
```

9. Run the following command:

```
sc start "Citrix SSLRelay"
```

10. Ensure your firewall allows the Citrix Gateway Core Service to accept connections. You may be prompted by Windows Security Alert to allow the service on your firewall. If not, configure this manually.

11. Using the Services management console, ensure the Citrix SSL Relay Service is running.

12. Using the registry file (included on the media in folder 'VDA\x86' or 'VDA\x64') add the following registry key:

    - 'SslPortRegistryKey – x86.reg' (for 32-bit)

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy\Defaults\ICAPolicies]
"SslPort"=dword:000001bb
```

    - 'SslPortRegistryKey – x64.reg' (for 64-bit)

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\GroupPolicy\Defaults\ICAPolicies]
"SslPort"=dword:000001bb
```


13. Using the Services management console, restart the Citrix Desktop Server Service.

14. Log off the machine.

Configure the security settings on the server running the XenDesktop Controller

This procedure assumes the XenDesktop Controller is already installed and configured. For more information, see http://support.citrix.com/proddocs/topic/xendesktop-rho/cds-install-server-rho.html

1. Install the hotfixes included in the following zip file (included on the media in folder 'DDC\x86' or 'DDC\x64'):

   - For 32-bit OS: XD560_Controller_X86_HFs_5.zip
   - For 64-bit OS: XD560_Controller_X64_HFs_5.zip

2. Using Desktop Studio, select the PowerShell tab and click **Launch PowerShell**.

3. At the PowerShell command prompt, type:

```
Set-BrokerSite –DnsResolutionEnabled $true
```

4. Using the registry file 'HDXSSLEnable.reg' (included on the media in folder 'DDC\x86' or 'DDC\x64') add the following registry key:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer]
"HdxSslEnabled"=dword:00000001
```

5. Using the Services management console, restart the Citrix Broker Service.

Clear the Web Interface Cache

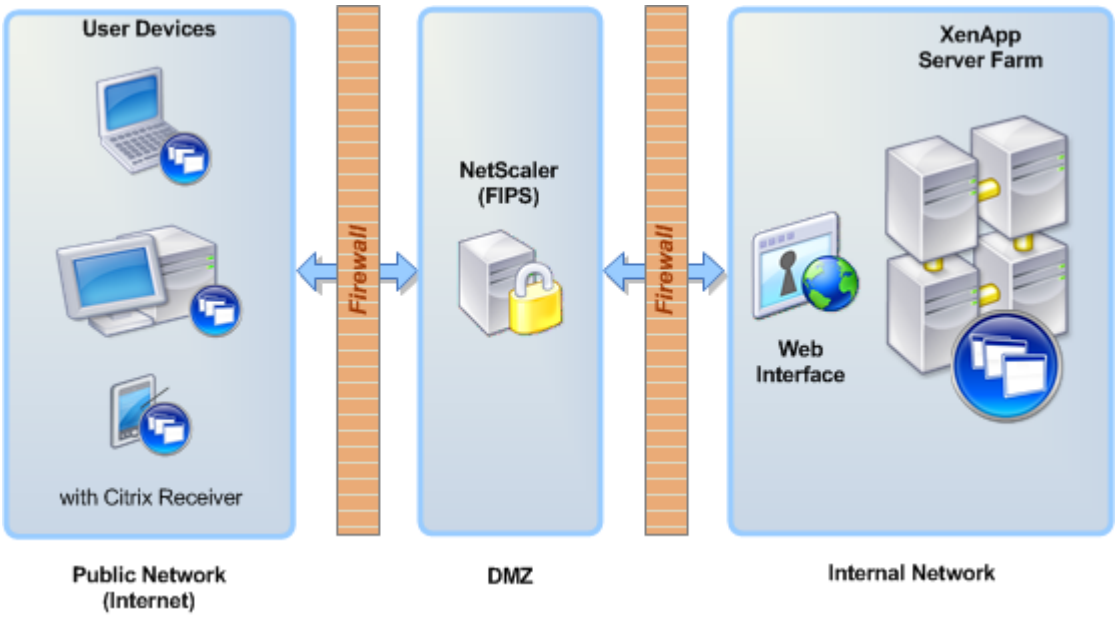
Restart Microsoft Internet Information Services on the server running Web Interface. This clears the published resources cache.

Configure the Firewall Settings

Lock down the firewall to allow localhost traffic only on ports 1494 and 2598.

XenDesktop using NetScaler (External Access)

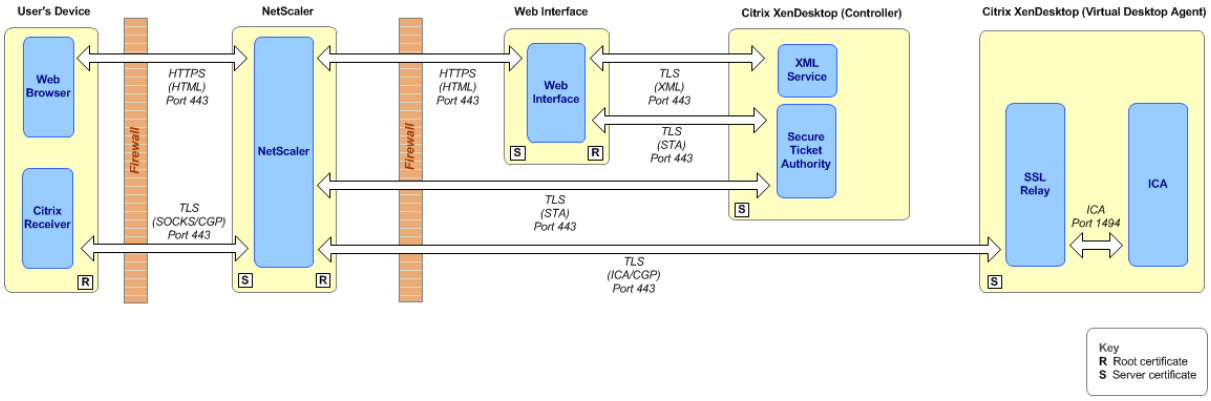
This deployment uses a Netscaler FIPS appliance to terminate the TLS connection from TLS enabled plug-ins (SSP and ICA engine) and forwards the traffic to the WI server using HTTPS and using TLS to SSL Relay (ICA connection).



This diagram shows a detailed view of the deployment including the components and certificates on each server, plus the communication and port settings.

	Components	Operating System
XenDesktop Site	XenDesktop 5.6 SSL Relay Enabled Secure Ticket Authority is part of the XenDesktop Controller XenDesktop Workers	Windows Server 2008R2 Windows XP Windows 7 x86 Windows 7 x64
Web Server	Web Interface 5.4 for Internet Information Services	Windows Server 2008 R2 Windows Server 2008 Windows Server 2003 with Service Pack 2 .NET Framework 3.5 or 2.0 (IIS 6.0 only) Visual J#.NET 2.0 Second Edition
User Devices	Citrix Receiver for Windows 3.4 TLS-enabled Web browser	

This diagram shows a detailed view of the deployment including where the components and certificates on each server, plus the communication and port settings.



Setting up this the deployment is same a setting up the XenDesktop using SSL Relay (Internal Network) deployment with the addition of configuration of NetScaler security settings.

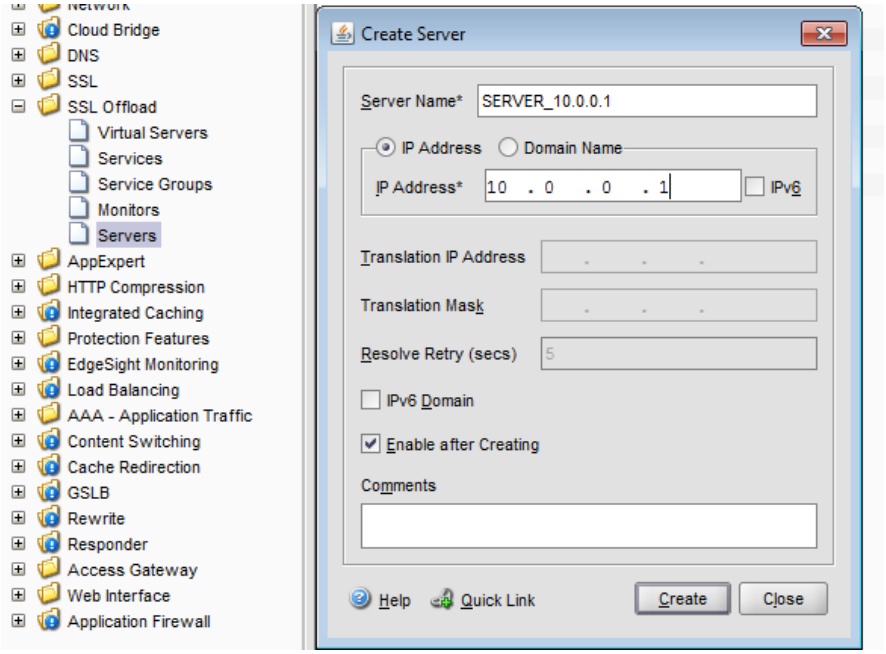
Configure NetScaler security settings

This procedure assumes the NetScaler appliance is already setup and configured for FIPS/TLS. For more information, see http://support.citrix.com/proddocs/topic/netscaler-getting-started-map-93/ns-instpk-install-ns-wrapper.html

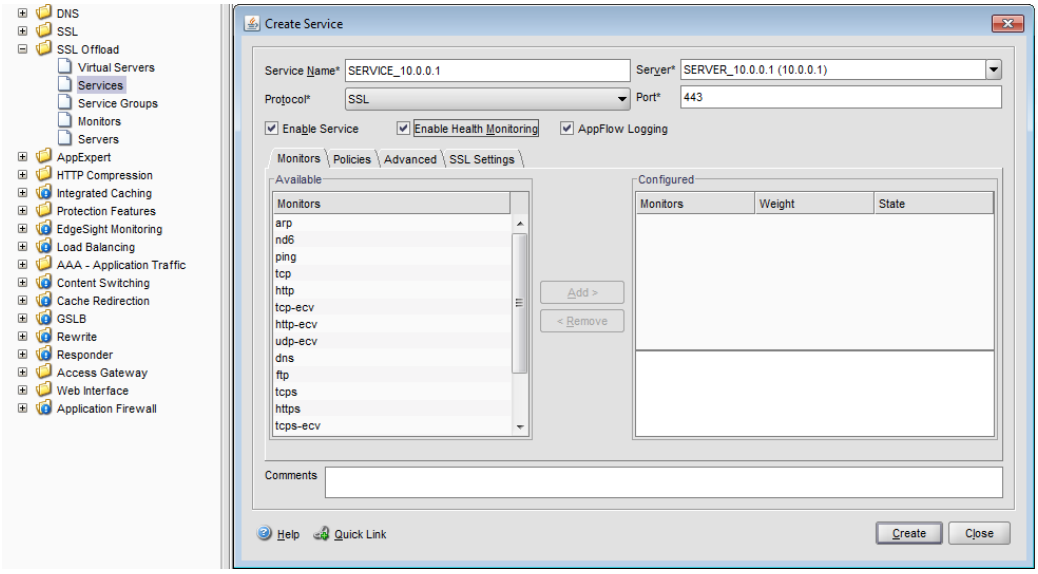
1. If you have previously configured Web Interface or STA site on your NetScaler device, remove them from your NetScaler configuration. The details, if configured, are stored in Session Profile, Global Settings and Virtual Server Published Applications.

2. Create an SSL Offload Service for servers running Web Interface, STA, XenDesktop Controller and each XenDesktop VDA:

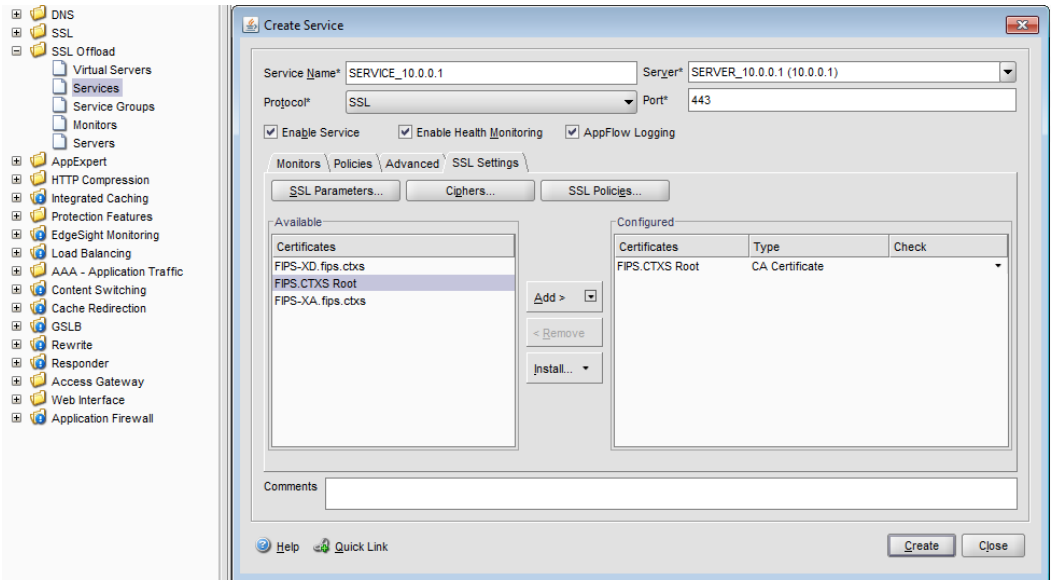
    a. Create an SSL Offload Server specifying the IP Address. For example, if using the NetScaler management tool:



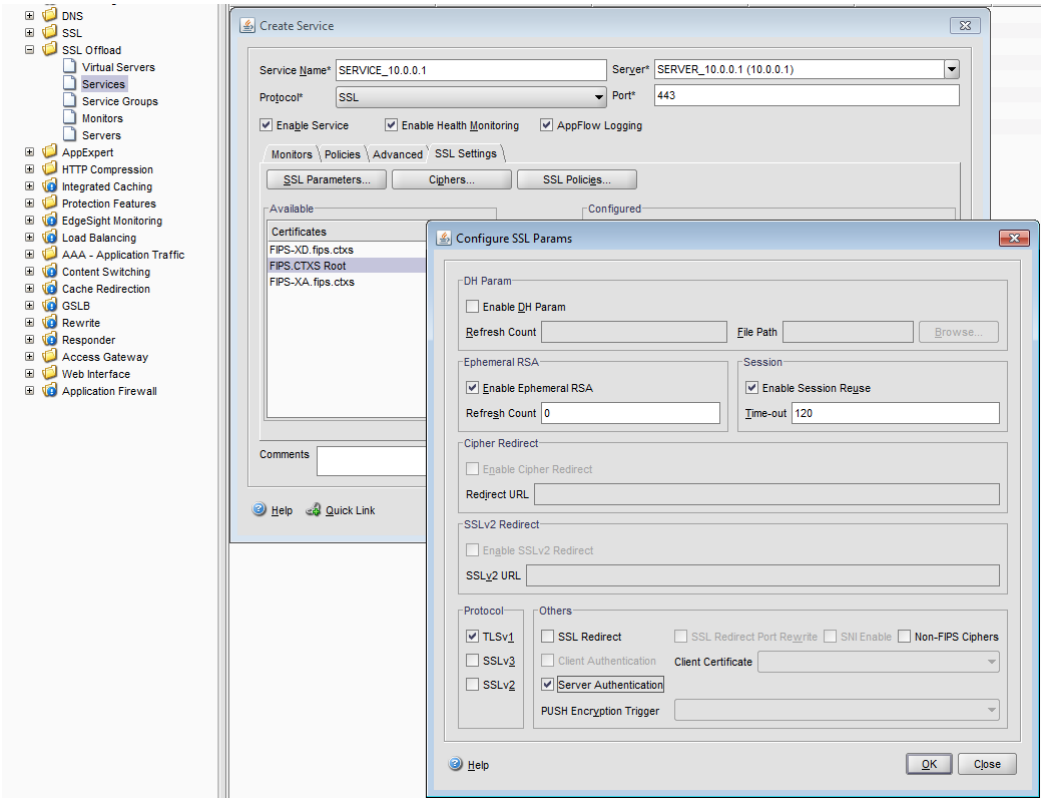
b. Create a Service. Specify the name of the SSL Upload Server and set Protocol ‘SSL’ and Port ‘443’. For example:



c. Select the SSL Settings tab and add the relevant root certificate as a CA. For example:



d. Configure the SSL Parameters to ensure the Protocol is set to TLS v1 only and Server Authentication. For example:

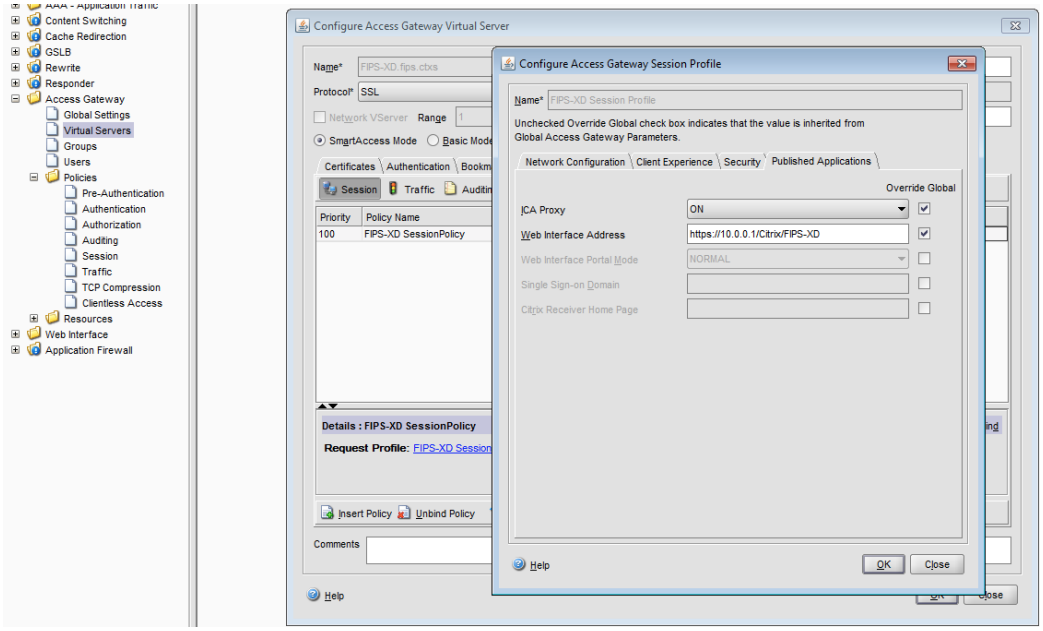


Note: You can perform steps a) to d) using the following NetScaler CLI commands:

```
add server SERVER_10.0.0.1 10.0.0.1
add service SERVICE_10.0.0.1 SERVER_10.0.0.1 SSL 443
set ssl service SERVICE_10.0.0.1 -eRSA DISABLED -ssl3 DISABLED
-serverAuth ENABLED
bind ssl service SERVICE_10.0.0.1 -certkeyName "FIPS.CTXS Root"
-CA -ocspCheck Optional
```

where `"FIPS.CTXS Root"` is the name of the relevant root CA as configured in NetScaler.

3. Ensure the Access Gateway Session Profile 'Web Interface Address' is configured for 'https' using the relevant IP Address. For example:



4. Ensure the URL for each STA is set for 'https' using the relevant IP Address. For example: