Citrix NetScaler and Citrix XenDesktop 7 Deployment Guide
Table of contents

Executive summary and document overview 3

1. Introduction 3
   1.1 Overview summary 3

2. Architectural overview 4
   2.1 Physical view 4
   2.2 Logical view 5
   2.3 Target architecture 5

Cloud infrastructure 6

3. CloudStack management infrastructure setup 6
   3.1 Install Citrix XenDesktop 7 and supporting components 6
   3.2 Add DDCs to XenDesktop 10
   3.3 Install the Virtual Desktop Agent 12
   3.4 Create machine catalogs 14
   3.5 Create XenDesktop delivery groups 18
   3.6 Configure StoreFront 22
   3.7 Add StoreFront servers to deployment 26

Citrix NetScaler 28

4. NetScaler configuration 28
   4.1 Initial configuration 28
   4.2 Load balancing StoreFront—wizard 29
   4.3 Load balancing StoreFront—manual setup 38
   4.4 Load balancing DDCs 47
   4.5 Remote access with NetScaler Access Gateway—wizard 51
   4.6 Remote access with NetScaler Access Gateway—manual setup 57

5. Uncompromised monitoring 60
   5.1 NetScaler Insight Center configuration and screens 60

6. Considerations and troubleshooting 65

7. Tables and references 66
   7.1 Design decisions—overview 66
   7.1 Design decisions—zone architecture (Phoenix) 68
   7.2 Design decisions—networking 68

8. Conclusion 69
This guide demonstrates how to deploy Citrix NetScaler in conjunction with Citrix XenDesktop 7 with a focus on both simplicity in configuration and advanced features not easily delivered with other products.

Executive summary and document overview

1. Introduction

In this guide you’ll learn how to provision the XenDesktop 7 infrastructure, the NetScaler appliance and NetScaler Insight Center services to extend Citrix virtual desktop infrastructure and services to remote users in small to medium-size enterprises.

1.1 Overview summary

Best end user experience: With an integrated Citrix solution for remote and portable workstyles, end users enjoy a seamless experience resulting in fewer help desk calls and reduced training needs. Citrix Receiver client software is installed on the user device (iPhone, Android phone, thin client) to allow users, by way of the NetScaler appliance delivering high availability, scale and security, to access their desktops, applications and data through Citrix StoreFront. StoreFront, which ships with XenDesktop 7, authenticates users to XenDesktop sites and Citrix XenApp farms, enumerating and aggregating available desktops and applications into stores that users can access through Citrix Receiver or Receiver for Web. The StoreFront database records details of users’ application subscriptions to enable synchronization of those applications across all their devices. Benefits of the NetScaler/StoreFront solution include one-click configuration for user setup, local and remote access, automatically provisioned applications, self-service simplicity, a consistent user experience across any device and persistent access to applications and desktops.

End-to-end application visibility: New NetScaler 10.1 with HDX Insight seamlessly integrates with Desktop Director to provide a single location for management and monitoring of the XenApp and XenDesktop infrastructure. IT teams can drill down into network protocols (primarily ICA) through Desktop Director to troubleshoot individual user issues from a single console. The AppFlow capability of NetScaler allows you to export this data to third-party tools such as Splunk for in-depth correlation, analysis and reporting. The reports generated by NetScaler Insight Center, such as the applications and users consuming the most resources, can help IT determine peak usage and proactively allocate bandwidth accordingly. Response time measurements can help detect and resolve problems before a critical network or application failure occurs.

Enhanced security: By acting as a full proxy for ICA connections, NetScaler filters these connections before they hit the backend server, ensuring they are attack free. Proper integration with Secure Ticketing Authority (STA) prevents internal
user and server data, including IP address information, from leaking. SmartAccess allows you to control access to published XenApp virtual applications and XenDesktop virtual desktops on a server through the use of NetScaler Access Gateway session policies. NetScaler Access Gateway is a full-featured SSL VPN that is an integral component of NetScaler. It gives administrators granular, application-level control while empowering users with remote access to their virtual desktops from anywhere.

End-to-end support from a single vendor: Integration between NetScaler and IT Desktop Director provides a single console for troubleshooting end-user issues concerning the network and desktops. It also helps lower support and training costs (TCO) in the long run and enables IT teams to stay abreast of product roadmap updates. Choosing one vendor instead of multiple providers prevents finger pointing on integration issues.

2. Architectural overview

The environment described in this guide has been deployed on a single host, with internal networks configured to simulate an internal corporate network and a DMZ. The following diagrams illustrate the machines and network configuration in this deployment.

2.1 Physical view
2.2 Logical view

2.3 Target architecture

The following components have been installed on each of the machines:

1. Domain controller (DC)
   - Active Directory domain services
   - DNS
   - DHCP
   - Citrix License Server 11.11
2. Dynamic Delivery Controller 1 (DDC1)
   - XenDesktop 7
   - SQL Server Express 2012
3. Dynamic Delivery Controller 2 (DDC2)
   - XenDesktop 7
4. App/hosted shared desktops (APP)
   - XenDesktop 7 Virtual Desktop Agent (VDA)
5. Windows 8 VDI (XVDI)
   - XenDesktop 7 VDA
6. StoreFront 1 (SF1)
   - StoreFront 1.3
7. StoreFront 2 (SF2)
   - StoreFront 1.3
8. Client machine (client)
   - Citrix Receiver 3.4
Cloud infrastructure
3. XenDesktop 7 management infrastructure setup

This section defines the steps required to build the complete infrastructure.

3.1 Install Citrix XenDesktop 7 and supporting components

The XenDesktop 7 install process is a simple next/next/finish install. The services installed on each machine in this deployment are described in the previous section.

Once XenDesktop is installed, a site must be created. Click on Create a site in the studio mmc, and click Next on the introduction step. On the database configuration page, enter the details to connect to the SQL server. In this case, SQL Server Express has been installed on DDC1 and no database has been configured. As long as connectivity tests to the SQL Server pass, XenDesktop will create the database automatically. Enter whatever you want the database to be called in the database name field.
Click **Test** to confirm the database can be connected to.

Configure the license server and license for XenDesktop. In this deployment the license server has been installed on the domain controller, and we are using a trial license.
You may receive a certificate warning during this step if you do not have a computer certificate on the domain controller.

Enter the hypervisor information. XenDesktop must be able to create machines on the hypervisor, so root permission is required. Use the root account for Citrix XenServer.

Select the network on which you would like new machines to be created.
Select the storage location where the new devices will be placed.

Add App-V if necessary, as it was not configured as part of this deployment. Review the settings and click Finish. A new site will be created.
Some of the site configuration tests may fail. In this case the failed tests were SQL Server reference schema tests, which have no impact on the XenDesktop deployment.

3.2 Add DDCs to XenDesktop

If you are using SQL Server Express, you will have to start the browser on the SQL Server before you can add DDCs to the site, as without the browser remote machines cannot access the database.
From the studio MMC, click **Scale out your deployment** and input the address of the existing DDC in the deployment.

Click **Yes** to update the Citrix Studio database automatically.

Verify by navigating to **Desktop Studio, Configuration, Controllers** in the left panel. You should see both servers listed.
3.3 Install the Virtual Delivery Agent

The VDA must be installed on all machines that will deliver desktops or apps. Load the XenDesktop install media onto the target machines to launch the VDA installation.

Since we will be creating machines from this image with Machine Creation Services (MCS), we select the first option.
Add Citrix Receiver to the installation so that users can access applications from within hosted desktops.

Add both delivery controllers to the configuration. These must be FQDNs, so make sure that the machine is configured to use your DNS server and verify that the DNS entries are correct.
Leave the default features and firewall configuration unchanged and click **Install**. The machine will restart during installation. Verify that installation has completed successfully.

3.4 Create machine catalogs

From the studio MMC, click **Create Catalog**.
Click **Next** on the welcome screen.

Select the type of deployment. This will be a Windows Server OS catalog for hosting applications on RDS and hosted shared desktops.

Select **virtual machines** (VMs) or **physical hardware** and the image management you want to use. In this case we are managing virtual machines with MCS.
Select the snapshot of the master image to be used for image creation.

Select machine parameters for created VMs.
Specify the naming scheme and organizational unit (OU) for Active Directory accounts.

Add a scope if necessary. No scope was defined for machine catalogs in this deployment. Name the catalog and review the settings.
Studio will begin creating the machine catalog, and this will take a while.

3.5 Create XenDesktop delivery groups
Add some machines and click **Next**.

Add users.
Create profile definitions.

Add applications.
Add StoreFront access for application access within hosted shared desktops.

Repeat as necessary for all delivery groups.

At this point, XenDesktop and apps and desktops are configured. In the next section you’ll install StoreFront to test the configuration.
3.6 StoreFront configuration

Once StoreFront is installed, you must switch IIS to HTTPS before configuring StoreFront.

Go to IIS -> server certificates.

We will be using a domain certificate from the domain CA.

Import or create a web certificate for the URL that the clients will be using to access the environment. This certificate can be for the machine name. The URL that users will enter to access the environment will point to the load balancing server, so that server requires a matching certificate.

Edit the site bindings and add an HTTPS binding using the certificate just added to IIS.
Remove the HTTPS binding.

Launch StoreFront MMC.
Select **Create New Deployment**.

The Create New Deployment wizard will launch with HTTPS and the common name of the certificate as the base URL. This is the URL that users will enter to access the environment, and will eventually resolve to the Access Gateway IP address.

Name the store and click **Next**. Enter the delivery controllers. In this case, we want to load balance the delivery controllers with NetScaler, so each delivery controller entered here will be the load balancing vServer VIP, not the actual DDCs. Even if you have not configured load balancing yet, as we don’t, put in the IP of whatever the load balancing VIP will be when it is set up.
Access to the store typically does not need to be on SSL because it is completely internal traffic; however, SSL can be used if the DDCs and the load balancing vServer have certificates.

On the Remote Access page, select **No VPN tunnel** to specify the use of Access Gateway in ICA proxy mode. Click **Add**.

Add the two DDCs as Secure Ticket Authorities (STAs).
Click **Create** and Access Gateway will appear in the list of appliances.

Click **Create** and the store will be configured. The authentication, stores, Receiver for Web and Access Gateway should all be configured and visible from the StoreFront MMC.

### 3.7 Adding StoreFront servers to the deployment

To add servers to the existing StoreFront deployment, open the StoreFront MMC on the machine you wish to add and click **Join existing server group**.
The server will ask for the name and code of an authorizing server.

A code for authorizing a new server will be generated. Enter this code on the server you want to join the deployment.

The server will join the deployment. Click OK.
Citrix NetScaler

4. NetScaler configuration

4.1 Initial configuration

Once NetScaler is licensed, run the setup wizard to configure the IP address that will be used for communication with internal servers.

In this deployment we’ve chosen to skip the configuration wizard for load balancing XenApp and XenDesktop and perform these configurations manually instead. Once the initial setup wizard is complete, go to Network/IPs and confirm that the SNIP is set correctly.

Go to system/settings and configure basic features.
4.2 Load balancing StoreFront—wizard

From the navigation tree on the left, select Traffic Management and click on Load Balancing.

Click Load Balancing wizard.
Click **Next** on the **Introduction** screen.

Enter **SFService1** for the **Name** and click the **New** button.

Enter **SF1** for the server name, click **Domain Name** and enter **storefront1.xd.lab**. Then click **Create**.
Select SSL for the protocol.

Click the Add button to add in the first service.

Enter SFService2 for the name and click the New button.
Enter **SF2** for the server name, click **Domain Name** and enter **storefront2.xd.lab**. Then click **Create**.

Click the **Add** button to add in the second service.
Click **Next**.

Enter **StoreFrontLB** for the name and **172.16.1.156** for the IP address. Select **SSL** for the protocol.

Select both services and click **Add**.
Click **Next**.

Click **Finish** to complete the wizard. Then click **Exit**.

It is normal for the StoreFront virtual server to be in a down state at this point. We have created an SSL server but not added a certificate, causing the server to be in a down state. A certificate will be added next.
Under Load Balancing > Virtual Servers, double-click the new entry of SFVirtualServer that was created.

Click the **Method and Persistence** tab.

Ensure the method is set to **Least Connection**, persistence is set to **COOKIEINSERT** and time-out value is set to 0.

**NOTE:** This will result in fair-share load balancing between the two servers and ensure that open connections between clients persist to the same backend server. A time-out of 0 means that the session will only remain valid as long as the browser is open.
Click **OK**.

Click the **disk icon** towards the top right and then **Yes** to save the running state to disk.

Click **OK** on the confirmation.

Click the **SSL Settings** tab.
Click **WildcardCert** and click **Add**.

Click **OK**.
The **SFVirtualServer** should now show as Up.

![SFVirtualServer](image)

### 4.3 Load balancing StoreFront—manual setup

In this section we configure load balancing for the StoreFront servers. Go to load balancing/servers and click Add to add the two StoreFront servers.

![Create Server](image)
Repeat for SF2.

Both servers should be enabled in the list of servers.
Next create the SSL service on these servers. This will be the web traffic going to the StoreFront servers.

Repeat for SF2.
Verify that both services are up.

A load balancing virtual server can now be created to balance the two services created previously. This server must be an SSL server to load balance SSL services, meaning that it requires a certificate. Navigate to SSL certificates and import the certificate used for the Access Gateway URL.

Click on Manage Certificates/Keys/CSRs under SSL/Tools.

Select upload.
Upload the StoreFront certificate and any associated intermediate or root certificates.

In this case, the StoreFront certificate and the CA root certificate have been uploaded.
Navigate to **ssl/certificates** and click **Install**. Select the certificate for StoreFront.

Repeat for intermediate and root certificates.

Next select the **StoreFront certificate** and click **Link**. The root CA will be the only option for linking in this case. Click **OK**.
The certificate will now be available for use on the load balancing virtual server and Access Gateway.

Go to load balancing/virtual servers and click **Add**.

Switch the protocol to SSL and enter the IP address that the virtual server will use. This is the IP address that was entered into the StoreFront configuration as the hostname. Select both StoreFront services.
Change to the method and persistence tab and specify COOKIEINSERT persistence with a SOURCEIP backup.
Finally, under SSL settings, add the certificate for the server.

Verify that the server state is shown as **Up**.
4.4 Load balance DDCs

Next we need to configure load balancing for the DDCs. Go back to load balancing servers and add the first DDC server.
Repeat for DDC 2.

Configure Server

Server Name*  DDC 2

IP Address*  172.16.1.153

Translation IP Address

Translation Mask

Resolve Retry (secs)  5

Resolve Domain Immediately

Comments

Help  OK  Close
Next, create the services for XML traffic on the DDCs. In this deployment the XML service was left on port 80, the default. If the port was changed by the broker service, reflect that in the services created here.

Repeat for DDC 2.
Now, create the load balancing virtual server for the XML service. This is the IP address that was entered for the delivery controller in the StoreFront configuration.

Note: Persistence isn’t required for the DDC XML service.
4.5 Remote access with NetScaler Access Gateway – wizard

Log into the NetScaler GUI.


Click the Get Started button.
Enter **RemoteAccess** for the Name.

IP Address: **<<Public IP for access>>**

Click **Redirect requests from port 80 to secure port**.

Then click **Continue**.

From the Certificate drop-down menu, select the **public CA certificate for the NetScaler Access Gateway** and click **Continue**.

NOTE: This certificate needs to be issued from a public CA and must be previously installed on the NetScaler appliance.
Next is authentication. If you have previously configured LDAP authentication on NetScaler, select the available authentication and skip to the next step.

Under **Authentication Settings**, click the button for **Configure New** and enter the following details:

- **IP Address:** 172.16.1.200
- **Base DN:** `cn=Users, dc=xd, dc=lab`
- **Admin Base DN:** `cn=Administrator, cn=Users, dc=xd, dc=lab`
- **Password/Confirm Password:** Password1

Click **Continue**.
Enter the following details for Citrix Integration Settings:

**CloudGateway**
- Deployment Type: Windows Storefront
- StoreFront FQDN: storefront.xd.lab (FQDN of storefront load balancer)
- Receiver for Web Path: /Citrix/StoreWeb (url of receiver for web)
- PNAgent Path: /Citrix/PNAgent/config.xml
- Single Sign-on Domain: xd.lab
- STA URL: http://ddc1.training.lab
- Click **Done**.
Under **Configuration**, go to **Security > Access Gateway > Virtual Servers.**

Double-click the **RemoteAccess** entry.
Under **Published Applications** tab, click **Add** under Secure Ticket Authority.

Type in **http://ddc2.training.lab** and click **Create**.

Click **OK**.
Go to Traffic Management > Load Balancing > Virtual Servers.

Double-click the entry with the name that contains http_redirect. This was created as part of the wizard.
Click the Advanced tab and change the **Redirect URL** to be in the format `https://externally-accessible-FQDN` based on the IP address that was there.

### 4.6 Remote access with NetScaler Access Gateway – manual setup

Now that load balancing is configured, Access Gateway can be configured. In this deployment, a second subnet was configured to act as the “WAN.” This subnet contains only the Access Gateway VIP, a NetScaler SNIP and a client access machine. The subnet used is 172.16.2.x/24. First configure a SNIP on this subnet; in this guide 172.16.2.100 was used. Then go to **Access Gateways/virtual servers** and click **Add**.

Name the server using the common name of the certificate, give it a VIP and assign the StoreFront certificate and click **Create**.
We want Access Gateway to be able to authenticate users with Active Directory, so we added LDAP authentication to the system. Go to the system/authentication/ldap/servers tab and click Add. Fill in the domain controller information and click Create.

Now switch over to the Policies tab and click Add. Add the ns_true expression to the policy and click Create.
Now go back to the Access Gateway virtual server and switch to the authentication tab, and click Insert Policy. Select the policy we just created and click OK.

At this point we should be able to log into NetScaler Access Gateway.
You land on the NetScaler Access Gateway portal because there is no session policy defined to forward the session. That will be the next step. This step verifies that the certificate is valid and that the authentication works.

Back on the StoreFront Access Gateway virtual server, add the two DDs as STAs. Go to the Published Applications tab, and under Secure Ticket Authority enter http:// followed by the IP address of the servers. Once entered, each entry should appear up with an identifier listed.

Navigate to the Policies tab and click Insert Policy. Select New Policy. Name the policy. Next to Request Profile, select New.
Switch to the **Published Applications** tab and make the following changes:

1. Click the **Security** tab and set the **Default Authorization Action** to **ALLOW**.
Add the ns_true expression to the policy and click Create.

Now test it out....
You should be able to log in, be forwarded to Citrix Receiver, see applications and launch applications.

5. Uncompromised monitoring
NetScaler Insight Center is an industry-first application that consolidates end-to-end web application data with Citrix virtual desktop infrastructure performance data in one place for further detailed analysis. This section shows how to configure NetScaler Insight Center to monitor the XenDesktop 7 deployment.

5.1 NetScaler Insight Center configuration and screens
Log into the NetScaler Insight Center GUI, navigate to Configuration and under Inventory, click Add. Enter the IP, username and password of the NetScaler appliance from which you want to collect AppFlow data.
Click **Add**. Return to the **Inventory** screen, and the NetScaler appliance should be listed with its IP address and hostname.

Click on the IP address of the NetScaler appliance. All load balancing vServers, content switching vServers and NetScaler Access Gateway vServers should be shown on the **Applications List**.

Navigate to the IP address and service for which you want to enable AppFlow logging, right click and select **Enable AppFlow**.
You need to define an expression for the logging. This enables you to gather data only when a specific expression is true. To record all data from the vServer, enter **true** as the expression.

Click **OK**.

Now there should be a green check mark with **ENABLED** under the insight column header. In the screenshot below, AppFlow logging has been enabled for the StoreFront load balancing vServer.

NOTE: AppFlow logging must also be enabled on the NetScaler side to enable logging in Insight.
Repeat the process for any other load balancing vServers, then use the dropdown menu to switch to content switching vServers or VPN. The VPN category will list all NetScaler Access Gateway appliances. If the gateway runs in ICA proxy mode instead of VPN, check the **ICA** box when you complete the expression **true**.

Now navigate to the dashboard view and confirm that you can see the data gathered from NetScaler Access Gateway. In this example there is logging enabled on the StoreFront load balancing vServer, and several types of information are available, such as:

- **URLs**

![URLs](image)

- **Devices** (the NetScaler instances that are in use, by number of hits)

![Devices](image)
Clients (Infrastructure servers that NetScaler is contacting. 150,151 are StoreFront servers, 200 is DNS resolutions, etc.)

The HDX Insight portion of NetScaler Insight Center keeps detailed information about user ICA sessions. The following chart shows the average bandwidth, latency, RTT, etc., for a specific user.
Application launch history

Desktop performance and bandwidth

6. Considerations and troubleshooting

- The StoreFront servers on SSL are particularly sensitive to the persistence settings on the load balancer.
- In this deployment, modifications have been made to the host’s file on the StoreFront servers to resolve the FQDN of Access Gateway. These machines also had NetScaler Access Gateway set as their default to reach the IP on the external subnet.
7. Tables and references

7.1 Design decisions – overview

The best practice architecture uses two StoreFront servers and two DDCs for scale and availability. The two StoreFront servers are then configured behind a VIP on the load balancer. Users access the StoreFront service via the VIP. This provides increased availability to the control plane.

<table>
<thead>
<tr>
<th>Decision point</th>
<th>Design decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Servers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of management</td>
<td>1 (1 for virtual desktop infrastructure, 0 for storage, 0 for monitoring, 1 for</td>
<td>High availability</td>
</tr>
<tr>
<td>servers</td>
<td>load balancer management software)</td>
<td></td>
</tr>
<tr>
<td>Deployment location</td>
<td></td>
<td>You can easily add another set of management servers to the cluster without reconfiguring the entire infrastructure.</td>
</tr>
<tr>
<td>Deployment hypervisor</td>
<td>XenServer 6.0.2</td>
<td></td>
</tr>
<tr>
<td>Management server VM</td>
<td>CPU: 2 x vCPU, RAM: 40 GB, NIC: 2 1GbE NIC (Vlan 100), HDD: 100GB</td>
<td></td>
</tr>
</tbody>
</table>
### Decision point

<table>
<thead>
<tr>
<th>Decision point</th>
<th>Design decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring VM</td>
<td>NetScaler Insight Center 10.1. Storage: 120gB CPU: 2x vCPU RAM: 4gB</td>
<td></td>
</tr>
<tr>
<td>Operating system</td>
<td>RHEL 6 (64-bit)</td>
<td></td>
</tr>
</tbody>
</table>

### Management servers – load balancing

<table>
<thead>
<tr>
<th>Load balancing used</th>
<th>Load balancer</th>
<th>VIP (FQDN)</th>
<th>SSL encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>NetScaler SDX 11500, w/ 1 VPX instance</td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

### MySQL database

<table>
<thead>
<tr>
<th>Number of MySQL servers (VM)</th>
<th>Deployment hypervisor</th>
<th>Management server VM properties</th>
<th>Operating system</th>
<th>MySQL version</th>
<th>Replication</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>XenServer 6.0.2</td>
<td>CPU: 2 x vCPU RAM: 6 GB RAM NIC: 1 x NIC (vLAN 100) HDD: 100GB</td>
<td>RHEL 6 (64-bit)</td>
<td>MySQL 5.6</td>
<td>No Master: Slave:</td>
</tr>
</tbody>
</table>
7.1. Design – zone architecture (Phoenix)

We’ve labeled this deployment the Phoenix zone and it has 3 VLAN’s: Internal, DMZ, and Client. There’s also an L3 router and a couple L2 switches, all completely virtualized. This deployment highlights only one zone but each zone can be replicated using different IP subnets. Each zone can be clustered. The isolation between tenants is provided by switch-based security zones.

<table>
<thead>
<tr>
<th>Availability zone(s) – 1 (it is always recommended to go with two availability zones)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phoenix</td>
</tr>
<tr>
<td>Deployment location</td>
</tr>
<tr>
<td>Network mode</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>External DNS server(s)</td>
</tr>
<tr>
<td>Internal DNS server(s)</td>
</tr>
<tr>
<td>vLAN range</td>
</tr>
<tr>
<td>Guest CIDR</td>
</tr>
<tr>
<td>Public</td>
</tr>
<tr>
<td>Domain</td>
</tr>
</tbody>
</table>

7.2. Design decisions - networking

<table>
<thead>
<tr>
<th>Decision point</th>
<th>Design decision</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distribution switch</td>
<td>Cisco Nexus 7000</td>
<td></td>
</tr>
</tbody>
</table>

8. Conclusion

To conclude, it is quite apparent from this guide that the NetScaler ADC best optimizes your XenApp/XenDesktop deployment, as follows:

- Best end-user experience with the NetScaler ADC
- End-to-end application visibility with NetScaler Insight Center
- Enhanced security with the NetScaler ADC built-in firewall
- End-to-end support from a single vendor