Implementing a Tachyon DMZ Server

Summary
The process for installing a Tachyon DMZ Server to support Internet-facing Tachyon clients.

Assumptions
The steps given on this page assume:

- Tachyon is already installed on the internal (corporate) network
- The Tachyon DMZ Server hosts only the Tachyon Switch and Background Channel components, and is installed in a DMZ
- If the Tachyon DMZ Server is domain-joined, it is either in the same domain in which the internal Tachyon Server resides, or there is a two-way trust between domains

In our example, the DMZ Server has only one Switch, and the internal Tachyon Server is a single-server configuration with Master and Response Stacks. If your system has different requirements please contact 1E for advice.

Tachyon client devices will be configured to swap between being on the internal network and being external to the network, and therefore will communicate with the internal Tachyon Server when connected internally and the external Tachyon DMZ Server when accessing externally (for example Internet). Tachyon client devices must have the appropriate certificates installed. Please refer to Requirements: Tachyon client certificates for more details.

Architecture
Enabling Tachyon to support devices that are external to your company network is done by slightly extending the default single-server architecture.

The Responses Stack handles communications between the Master Stack and the Tachyon clients. The Background Channel and Switches components handle the direct communication with the Tachyon clients, the Core processes the information in both directions between the Master Stack and the Switches.

To enable external Tachyon client devices to interact with Tachyon you need to put the Background Channel and at least one Switch into the DMZ.

Communications ports
The Tachyon communications ports between the Tachyon Master Server and the Tachyon DMZ Server must be opened, as illustrated in the picture shown opposite. Please refer to the Communication Ports page for more details.
Preparation

In the following summary and configuration steps, the following terminology is used:

- **Relevant internal servers**
  - Any internal server which hosts a Tachyon Server component which communicates with any DMZ Server
  - Typically this will include the servers which host the Coordinator, the Consumer API, and any Core bound to a DMZ switch that is registered in the dbo.SwitchToCoreApi table in the TachyonMaster database
  - The example diagrams and steps refer to only one internal server, but there may be separate servers for Master Stack (with Coordinator and Consumer API) and Response Stack (with Core).

- **DMZ Server**
  - Any server that has Tachyon Server components installed which is not on the internal network (that is, outside of the corporate network)
  - This includes a Tachyon DMZ Server (which has one or more Switches and a Background Channel)

You must ensure the following before installation of Tachyon on a DMZ Server.

- **The Tachyon Master Server** is installed and verified with internal Tachyon clients.
  - Please refer to Implementing Tachyon for more details
  - The documentation below assumes this has a Master Stack and Response Stack on the same server.
  - A Response Stack is required in order to provide the Core component that will be used by the remote DMZ Server. Internal clients are not required to use the Switch and Background Channel of this Response Stack.

- **The DMZ internal and external firewall** are configured correctly. Please refer to the Communication Ports page for more details.

- **The Tachyon DMZ Server** is provisioned. Although a DMZ Server does not have all Tachyon components, all prerequisites must be met in order for Tachyon Setup to run. In particular, the following must be prepared before installation. For more detail about each requirement, click on the relevant link.

- **Requirements: DNS Names (Preparation: DNS Names)**
  - The DMZ Server requires two DNS Names, even if the DMZ Server is configured with one network interface. **Two network interfaces** are required to prevent the same network interface being used for response traffic for both clients to server, and server to Core.
  - A **DMZ Server internal DNS Name** so that the internal Tachyon Server can connect to the DMZ Server. Documentation below assumes this DNS Name exists, but it can alternatively be the server’s hostname FQDN.
  - A **DMZ Server external DNS Name** so that Internet devices can connect to the DMZ Server, which is the name included in the Tachyon client configuration for Switch and Background Channel settings (IE Client configuration file). This DNS Name is not necessarily for the actual IP Address(es) of the external network interfaces if DMZ firewall, Network Address Translation (NAT) or other routing is employed.
  - Both DNS Names must be included in the Web server certificate. Please see Certificate requirements below for more information on certificate DNS Name requirements.
  - If DMZ Server is domain-joined, both DNS Names require an HTTP class Service Principal Name (SPN) registered on the DMZ Server's computer$ account. Please refer to Preparation: Service Principal Names for more details.

- **Requirements: Network interfaces (Preparation: Network interfaces)**
  - The DMZ Server should have an internal network interface, and an external network interface for each Switch, in order to keep Core and Switch traffic apart. This recommendation is for performance reasons when supporting over 500 devices.
  - If an internal interface is not used, then the external interface will use both DNS Names.
  - If using two interfaces...
    - the internal interface will use the internal DNS Name, and the external interface(s) will use the external DNS Name. This is the assumption made in the configuration steps below.
    - internal and external interfaces will typically be on different subnets.
    - ensure your network routing is configured to route outgoing traffic using the internal interface. You may need to configure a persistent route, for example using the same steps described in Preparation: Configuring a persistent route for SQL traffic.

- **Requirements: Tachyon Server Certificates (Preparation: Web server certificate)**
• Each DMZ Server requires its own web server certificate. Please see Certificate requirements below for more information.
• **Requirements: Windows Server roles and features (Preparation: Windows Server roles and features)**
  • IIS to host the Background Channel application.
  • Windows Authentication role if the server is domain joined and has a trust relationship with the domain that the Master Stack is configured to use.
• **Test devices** with the Tachyon client installed.
  • At least one connected to the internal network; another connected to the external network.

**Certificate requirements**

Tachyon Server certificate requirements are defined in Requirements: Tachyon Server certificates.

---

Each server that has Tachyon Server components installed requires its own Web Server certificate (except for a remote SQL Server). This certificate is also used by the Tachyon Switch and the Tachyon Coordinator. Therefore, a single-server installation requires only one Web Server certificate. This certificate must be provided prior to installation of Tachyon on the server.

**Certificate requirements for standard servers**

The Web Server certificate requires the minimum of the following:

1. Issued by a trusted Certificate Authority (CA)
   • The certificate for the Root CA in the Certification Path must exist in the Trusted Root CA store of the server
   • If the issuing CA is not the Root CA then the certificate for the issuing CA and any intermediate CA in the Certification Path must exist in the Intermediate CA store of the server
   • The above CA certificates must exist on the Tachyon Web Server and Windows client devices
   • Most organizations have automated distribution of these CA certificates to servers and clients, using Group Policy for example.
2. Has at least the following Key Usage:
   • Digital signature
   • Key encipherment
3. Has at least the following Enhanced Key Usages:
   • Server Authentication
4. Revocation information is included
   • References at least one CRL Distribution point that uses HTTP
5. Must have a private key available

- The default template **Web Server** available with a Microsoft PKI is suitable for requesting a Tachyon Web Server certificate.

- Tachyon systems that have DMZ Servers may have additional requirements, please refer to Implementing a Tachyon DMZ Server.

- Tachyon clients and Switches use OpenSSL and its validation process to verify certificates.
Web Server certificates used by a Tachyon Server must be issued with their fields set as follows:

<table>
<thead>
<tr>
<th>Fields</th>
<th>Example Option 3 type certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject Common Name Field (subject: commonName)</td>
<td>Subject can be any valid name, and is no longer mandatory as required by previous versions of Tachyon.</td>
</tr>
</tbody>
</table>
| Subject Alternative Name Extension (extensions: subjectAltName), type dnsName | The **Tachyon Server DNS Name FQDN** (DNS Alias) of the server. This is mandatory, same as required by previous versions of Tachyon.  
  Example: DNS Name=**TACHYON.ACME.LOCAL**  
  On a Master Stack, this is used by browsers, consumers, remote Tachyon Servers, and clients using ActiveEfficiency, Application Migration, or AppClarity Software Reclaimer.  
  On a Response Stack or DMZ Server, this is used by Tachyon clients. |
| Subject Alternative Name Extension (extensions: subjectAltName), type dnsName | An **Alternate DNS Name FQDN** (DNS Alias) of the server. This is a new requirement for Tachyon 5.0 and later.  
  Example: DNS Name=**TACHYONALT.ACME.LOCAL**  
  An **Alternate DNS Name** is required for any server hosting a Switch (Response Stack or DMZ Server) if the server has multiple IP Addresses. It is used for internal Tachyon communications between Switches and other Tachyon components.  
  An **Alternate DNS Name** is optional for a server hosting a Master Stack if you want an alternate DNS Name for clients using ActiveEfficiency, Application Migration, or AppClarity Software Reclaimer.  
  For more detail about setting up a DMZ Server, please refer to Implementing a Tachyon DMZ Server. |
Earlier versions of Tachyon required the certificate to have a CN and used SAN fields differently. If you are upgrading your Tachyon server from an earlier version it may still be using this type of certificate. When upgrading Tachyon, you can issue a replacement certificate, or continue using the old style certificate (because the new-style certificate requires only a SAN DNS Name that matches the DNS Alias, which are provided by the old style certificates).

<table>
<thead>
<tr>
<th>Fields</th>
<th>Example old Option 2 type certificate</th>
</tr>
</thead>
</table>
| Subject Common Name Field (subject: commonName) | The hostname FQDN of the server  
Example: **CN=ACME-TCN01.ACME.LOCAL**                                                                 |
| Subject Alternative Name Extension (extensions: subjectAltName), type dnsName | The DNS Alias FQDN of the server  
Example: **DNS Name=TACHYON.ACME.LOCAL**  

Add any additional DNS Names here.

---

**Example certificate request**

**Certificate Properties**

<table>
<thead>
<tr>
<th>Subject</th>
<th>General</th>
<th>Extensions</th>
<th>Private Key</th>
<th>Certification Authority</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

**Subject of certificate**

The user or computer that is receiving the certificate

**Subject name:**

Type: Common name  
Value: **CN=ACME-TCN01.ACME.LOCAL**

**Alternative name:**

Type: DNS  
Value: **DNS=TACHYON.ACME.LOCAL**

Add >< Remove

OK Cancel Apply
Option 2 type certificates required the CN to be the hostname FQDN, and the list of Subject Alternate Names (SAN) to contain the DNS Alias.

Also, prior to Tachyon 5.0 the certificate required its private key to be exportable.

Tachyon 5.0 and later is able to use this type of certificate when upgrading from an earlier version of Tachyon.

### Example of old Option 1 type certificate

<table>
<thead>
<tr>
<th>Fields</th>
<th>Example of old Option 1 type certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject Common Name Field (subject: commonName)</td>
<td>The DNS Alias FQDN of the server</td>
</tr>
<tr>
<td>Example: **CN=**TACHYON.ACME.LOCAL</td>
<td></td>
</tr>
<tr>
<td>Subject Alternative Name Extension</td>
<td>The DNS Alias FQDN of the server</td>
</tr>
<tr>
<td>(extensions: subjectAltName), type dnsName</td>
<td>Example: **DNS Name=**TACHYON.ACME.LOCAL</td>
</tr>
<tr>
<td></td>
<td>The hostname FQDN of the server</td>
</tr>
<tr>
<td></td>
<td>Example: **DNS Name=**ACME-TCN01.ACME.LOCAL</td>
</tr>
</tbody>
</table>
The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate
The user or computer that is receiving the certificate

Subject name:
Type: Common name
Value:

Add >
< Remove

Alternative name:
Type: DNS
Value:

Add >
< Remove

CN=TACHYON.ACME.LOCAL
DNS TACHYON.ACME.LOCAL ACME-TOND1.ACME.LOCAL
Tachyon DMZ Server installations have additional requirements for its certificates.

**Relevant internal servers**

<table>
<thead>
<tr>
<th>Type</th>
<th>Additional certificate requirements</th>
<th>Where used</th>
</tr>
</thead>
</table>

Option 1 type certificates required the CN to be the DNS Alias, and the list of Subject Alternate Names (SAN) to contain the hostname FQDN. Also, prior to Tachyon 5.0 the certificate required its private key to be exportable. Tachyon 5.0 and later is able to use this type of certificate when upgrading from an earlier version of Tachyon.
**Tachyon Server certificate**

The following applies to the **Tachyon Master Stack** and **Tachyon Response Stack** servers.

The **Certificate requirements for standard servers** require the **Tachyon Server DNS Name FQDN** and **hostname FQDN** to be present in the certificate. However, it has an *additional* requirement to separate communications between internal and external Switches:

- A **Subject Alternative Name** Extension (extensions:subjectAltName), of type **dnsName**, which must contain:
  - **Alternate DNS Name FQDN** - for example **tachyonalt.acme.local**

**Tachyon Consumer API client certificate**

The client certificate on the **Tachyon Master Stack server** has the following requirements:

1. Issued by a trusted Certificate Authority (CA)
   - The certificate for the Root CA in the Certification Path must exist in the Trusted Root CA store of the **Tachyon Master Stack server**
   - If the issuing CA is not the Root CA then the certificate for the issuing CA and any intermediate CA in the Certification Path must exist in the Intermediate CA store of the **Tachyon Master Stack server**
   - If the above CA certificates are different to those used by the **DMZ Server**, they will need to be exported and then imported on the **DMZ Server**
2. Has at least the following Enhanced Key Usage (EKU):
   - **Client Authentication** (OID 1.3.6.1.5.5.7.3.2)
3. Has a private key
4. Revocation information is included.
   - References at least one CRL Distribution point that uses HTTP.

**DMZ Server**

<table>
<thead>
<tr>
<th>Type</th>
<th>Additional certificate requirements</th>
<th>Where used</th>
</tr>
</thead>
</table>
| **DMZ Server certificate** | The **Certificate requirements for standard servers** are valid with regard to trust, usage, enhanced key usage, the private key, and revocation. However, as this is an externally reachable certificate, it is not recommended that the hostname FQDN is present in the certificate. As such, the certificate must meet the following requirements:  
  - A **Subject Alternative Name** Extension (extensions:subjectAltName), of type **dnsName**, which must contain:  
    - **DMZ Server external DNS Name FQDN** - in our example: **tachyon.acme.com**  
    - **DMZ Server internal DNS Name FQDN** - in our example **tachyondmz.acme.local**  
  Optionally, it may also contain a **Subject Common Name Field** (subject:commonName) that is unique within the organization that identifies the certificate (https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.6.5.pdf#page=54). | Used by the Switch(es) and Background Channel to secure communication to Internet-based Tachyon clients. |
The client certificate on the Tachyon DMZ Server has the following requirements:

1. Issued by a trusted Certificate Authority (CA)
   - The certificate for the Root CA in the Certification Path must exist in the Trusted Root CA store of the DMZ Server
   - If the issuing CA is not the Root CA then the certificate for the issuing CA and any intermediate CA in the Certification Path must exist in the Intermediate CA store of the DMZ Server
   - If the above CA certificates are different to those used by the Tachyon Response Stack, they will need to be exported and then imported on the Tachyon Response Stack server
2. Has at least the following Enhanced Key Usage (EKA)
   - Client Authentication (OID 1.3.6.1.5.5.7.3.2)
3. Has a private key
4. Revocation information is included.
   - References at least one CRL Distribution point that uses HTTP.
5. A Subject Alternative Name Extension (extensions:subjectAltName), of type dnsName, which must contain:
   - DMZ Server internal DNS Name FQDN - in our example tachyondmz.acme.local

If you wish, you can use the DMZ Server certificate as a client certificate, provided it also has EKA for Client Authentication (OID 1.3.6.1.5.5.7.3.2) as described above.

Certificate trust

The relevant internal servers must trust the DMZ Server certificate(s). In order to do so, ensure the DMZ Server certificate(s) issuing chain is imported into the Local Machine's Trusted Root Certification Authority or Intermediate Certification Authorities stores (as appropriate) on each relevant internal server.

The DMZ server must trust the relevant internal servers' certificate(s). In order to do so, ensure the relevant internal servers' certificate(s) issuing chain is imported into the Local Machine's Trusted Root Certification Authority and Intermediate Certification Authorities (as appropriate) stores on the DMZ Servers.

The DMZ server must also trust the Tachyon clients' certificates. In order to do so, ensure the relevant clients' certificate(s) issuing chain is imported into the Local Machine's Trusted Root Certification Authority and Intermediate Certification Authorities (as appropriate) stores on the DMZ Servers.

Please note that if any certification authority in this file have a HTTP CDP they must be reachable by the DMZ Server. Further information on this can be found in the note below.

If the certificates on the DMZ Server and the internal Tachyon servers are from different issuing CAs, then:

- Obtain the certificates (public keys only) for all the intermediate CAs, up to and including the Root CA of the internal Tachyon Server's Web Server Certificate, and add them to the corresponding CA stores on the DMZ Server. If you do not do this, the Switch on the DMZ Server will not be able to start because it won't be able to trust the Core API on the relevant internal server.

Similarly, if the certificates on the DMZ Server and client authentication certificates on external Tachyon clients are from different issuing CAs, then:

- Obtain the device's intermediate and root CA certificates, and add them to the corresponding CA stores on the DMZ Server.
- Windows devices will need the Tachyon DMZ Server's intermediate and root CA certificates to be added to their CA stores
- Non-windows devices will need the Tachyon DMZ Server's intermediate and root CA certificates to be added to their cacert.pem file

The installation process for a Tachyon DMZ Server

Overview

The process requires several manual steps before and after running Tachyon Setup, because the automated process is prevented by the DMZ Server not having access to the Tachyon Master database on the internal server. These steps include defining the cfgName used in the SwitchCommandLine for each Switch, which maps to a new row created in the SwitchConfiguration table in the Tachyon Master database. For more details about cfgName please refer to the Switch Command Lines page. In addition, the steps include increasing the level of security by changing the system so that all Switches connect to the Core API using HTTPS instead of HTTP (a remote Core is only accessible via HTTPS). The Background Channel is then initialized before finally carrying out verification steps to ensure everything is working.

One of the steps involves adding a new Background Channel. From that point onwards, you will not be able to update existing Background Channels until you have completed all steps. This means you cannot add or remove any instructions that use resources.
To illustrate the following detailed steps we use the ACME network with two servers.

**DNS Names**

Use the following table to help map the DNS Names used in your environment with the name used in the steps below.

<table>
<thead>
<tr>
<th>Server</th>
<th>DNS Name references</th>
<th>DNS Name examples</th>
<th>DNS Names used in your environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>The internal Tachyon Server</td>
<td>Tachyon Server hostname FQDN</td>
<td>ACME-TCNMST.acme.local</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tachyon Server DNS Name FQDN</td>
<td>tachyon.acme.local</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Alternate DNS Name FQDN</td>
<td>tachyonalt.acme.local</td>
<td></td>
</tr>
<tr>
<td>The external Tachyon DMZ Server</td>
<td>DMZ Server hostname FQDN</td>
<td>ACME-TCNDMZ</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DMZ Server internal DNS Name FQDN</td>
<td>tachyondmz.acme.local</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DMZ Server external DNS Name FQDN</td>
<td>tachyon.acme.com</td>
<td></td>
</tr>
</tbody>
</table>

**Detailed steps**

⚠️ Do all the steps if your DMZ Server is not domain-joined, or does not have a two-way trust between your internal domain and your DMZ domain.

Skip the highlighted steps if your DMZ server *is* domain joined and has a two-way trust between your internal domain and your DMZ domain.

<table>
<thead>
<tr>
<th>Location</th>
<th>Detailed steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Install the internal Tachyon Server, with Master and Response Stacks, and ensure it works by running the tests described in Verifyir</td>
</tr>
</tbody>
</table>
You must ensure the following before installation of Tachyon on a DMZ Server.

- The **Tachyon Master Server** is installed and verified with internal Tachyon clients.
- Please refer to Implementing Tachyon for more details.
- The documentation below assumes this has a Master Stack and Response Stack on the same server.
- A Response Stack is required in order to provide the Core component that will be used by the remote DMZ Server.
- The **DMZ internal and external firewall** are configured correctly. Please refer to the Communication Ports page for more details.
- The **Tachyon DMZ Server** is provisioned. Although a DMZ Server does not have all Tachyon components, all prerequisites on the relevant link.

**Requirements: DNS Names (Preparation: DNS Names)**
- A DMZ Server requires two DNS Names, even if the DMZ Server is configured with one network interface. The DMZ Server internal DNS Name so that the internal Tachyon Server can connect to the DMZ Server. Documenting DNS Names is for the actual IP Address(es) of the external network interfaces if DMZ firewall, Network Address Translation (NAT) or Both DNS Names must be included in the Web server certificate. Please see Certificate requirements below for more details.
- DMZ Server domain-joined, both DNS Names require an HTTP class Service Principal Name (SPN) registration.

**Requirements: Network interfaces (Preparation: Network interfaces)**
- The DMZ Server should have an internal network interface, and an external network interface for each Switch.
- If an internal interface is not used, then the external interface will use both DNS Names.
- If using two interfaces...
  - the internal interface will use the internal DNS Name, and the external interface(s) will use the external DNS Name.
  - ensure your network routing is configured to route outgoing traffic using the internal interface. You may need a persistent route.
- DMZ Server external DNS Name
- DMZ Server internal DNS Name

**Requirements: Windows Server roles and features**
- Each DMZ Server requires its own web server certificate. Please see Certificate requirements below for more information.
- Windows Authentication role if the server is domain joined and has a trust relationship with the domain that the Test devices are configured for.
- At least one connected to the internal network; another connected to the external network.

If the certificates on the DMZ Server and the internal Tachyon servers are from different issuing CAs, then:

- Obtain the certificates (public keys only) for all the intermediate CAs, up to and including the Root CA of the internal server. The Core API on the relevant internal server will not be able to start because it won't be able to trust the Core API on the relevant internal server.

Similarly, if the certificates on the DMZ Server and client authentication certificates on external Tachyon clients are from different CAs, then:

- Obtain the device's intermediate and root CA certificates, and add them to the corresponding CA stores on the Tachyon DMZ Server.
- Windows devices will need the Tachyon DMZ Server’s intermediate and root CA certificates to be added to their local certificates store.
- Non-windows devices will need the Tachyon DMZ Server’s intermediate and root CA certificates to be added to their local certificates store.

**Requirements: Tachyon Server Certificates**
- IIS to host the Background Channel application.
- Windows Authentication role if the server is domain joined and has a trust relationship with the domain that the Test devices are configured for.
- The DMZ Server requires two DNS Names, even if the DMZ Server is configured with one network interface.

**Requirements: Network interfaces**
- Each DMZ Server requires its own web server certificate. Please see Certificate requirements below for more information.
- Windows Authentication role if the server is domain joined and has a trust relationship with the domain that the Test devices are configured for.
- The DMZ Server requires two DNS Names, even if the DMZ Server is configured with one network interface.

**Requirements: DNS Names**
- A DMZ Server requires two DNS Names, even if the DMZ Server is configured with one network interface. The DMZ Server internal DNS Name so that the internal Tachyon Server can connect to the DMZ Server. Documenting DNS Names is for the actual IP Address(es) of the external network interfaces if DMZ firewall, Network Address Translation (NAT) or Both DNS Names must be included in the Web server certificate. Please see Certificate requirements below for more details.
- DMZ Server domain-joined, both DNS Names require an HTTP class Service Principal Name (SPN) registration.

**Requirements: Network interfaces**
- The DMZ Server should have an internal network interface, and an external network interface for each Switch.
- If an internal interface is not used, then the external interface will use both DNS Names.
- If using two interfaces...
  - the internal interface will use the internal DNS Name, and the external interface(s) will use the external DNS Name.
  - ensure your network routing is configured to route outgoing traffic using the internal interface. You may need a persistent route.
- DMZ Server external DNS Name
- DMZ Server internal DNS Name

**Requirements: Windows Server roles and features**
- Each DMZ Server requires its own web server certificate. Please see Certificate requirements below for more information.
- Windows Authentication role if the server is domain joined and has a trust relationship with the domain that the Test devices are configured for.
- The DMZ Server requires two DNS Names, even if the DMZ Server is configured with one network interface.

**Requirements: DNS Names**
- A DMZ Server requires two DNS Names, even if the DMZ Server is configured with one network interface. The DMZ Server internal DNS Name so that the internal Tachyon Server can connect to the DMZ Server. Documenting DNS Names is for the actual IP Address(es) of the external network interfaces if DMZ firewall, Network Address Translation (NAT) or Both DNS Names must be included in the Web server certificate. Please see Certificate requirements below for more details.
- DMZ Server domain-joined, both DNS Names require an HTTP class Service Principal Name (SPN) registration.

**Requirements: Network interfaces**
- The DMZ Server should have an internal network interface, and an external network interface for each Switch.
- If an internal interface is not used, then the external interface will use both DNS Names.
- If using two interfaces...
  - the internal interface will use the internal DNS Name, and the external interface(s) will use the external DNS Name.
  - ensure your network routing is configured to route outgoing traffic using the internal interface. You may need a persistent route.
- DMZ Server external DNS Name
- DMZ Server internal DNS Name
**On the internal Tachyon Server (Master Stack)**

Ensure the service account used by the Consumer API web application pool has read permission for the Tachyon Consumer API client certificate.

1. Start certlm.msc
2. Expand the Personal folder, and then select Certificates
3. Right-click on your Tachyon Consumer API client certificate and select All Tasks, then click Manage Private Keys
4. Click **Add**, and type in NT AUTHORITY\Network Service into the **Enter the object names to select** box
5. Click **OK**, and ensure the newly added Network Service has read permission
6. Click **OK**.
7. Remember this certificate's thumbprint (without hidden characters or spaces), it will used be in steps 7 and 15. For example: 545EF2AF74201A8CFAE0F0CEFE2D987237AEC176

On the internal Tachyon Server (Master Stack).

**In the TachyonMaster database, ensure the service account used by the Consumer API web application pool has read permission for: Tachyon Consumer API client certificate.**

**Network Service**

Start certlm.msc

Expand the Personal folder, and then select Certificates

Right-click on your Tachyon Consumer API client certificate and select All Tasks, then click Manage Private Keys

Click **Add**, and type in NT AUTHORITY\Network Service into the **Enter the object names to select** box

Click **OK**.

Remember the id of this row (normally 1)

**In the TachyonMaster database, modify the CoreApiConfiguration table to use the new HTTPS binding created in step 3.**

1. Change **BaseUrl** to point to the Core web application using the new HTTPS binding created in step 3. In our example this would be:
   - from `https://tachyon.acme.local:443/Core/`
   - to `https://tachyonalt.acme.local:443/Core/`
2. Remember the Id of this row (normally 1)

**In the TachyonMaster database, register each Switch planned for the DMZ Server, even though you have not yet installed the DMZ Server.**

1. For each Switch on the Tachyon DMZ Server, create a new row in the SwitchConfiguration table by copying the * (asterisk) row
   a. Remember the Id of each new row
   b. Change **Name** to `<SwitchHostname>-SWn` where SWn is the Switch suffix number 1 to 5. In our example this should be:
      - from * (asterisk)
      - to `ACME-TCNDMZ-SW1`
   c. Change **IpAddress** to the IP address of the external network interface on which this Switch should listen for connections from Clients. In our example this should be:
      - from
      - to `tachyon.acme.com`
   e. Change **InstructionsUrl** from `https://tachyon.acme.local:443/Consumer/Instructions` to `https://tachyonalt.acme.local:443/Consumer/Instructions`
   f. Do not change **SummaryUrl**

2. For each Switch on the Tachyon DMZ Server, create a new row in the SwitchToCoreApi table that maps the DMZ Switch to the internal servers.
   a. Change **InstrumentationUrl** to the hostname FQDN or alternate DNS Name of the internal server hosting the Tachyon Coordinator.
   c. Do not change **SummaryUrl**

If you leave this field set to its default value of NULL, it will cause each Switch to listen on all the addresses available to communicate with internal Tachyon servers as shown in the DNS Names picture above.
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 7 Internal TachyonMaster database. | In the TachyonMaster database, register the name of each new Background Channel.  
   1. For the Background Channel on the DMZ Server, create a new row in the BackgroundChannelApiConfiguration table:  
      - Set ResourceUrl as the DMZ Server internal DNS FQDN. In our example is: https://tachyondmz.acme.local:443/Core  
      - If you completed step 4 (for non-domain-joined) then set UseCertificateForAuthentication (default NULL) as the thumbprint of the Tachyon Consumer API client certificate  
   2. On the internal Tachyon Server (Response Stack), open a command prompt and ping the DMZ Server internal DNS Name FQDN to verify connectivity and collect the IP Address of the server.  
   3. If you have multiple switches, ensure you modify each SwitchCommandLine.n entry in the configuration file.  
   4. On the internal Tachyon Server (Response Stack), open the IIS Management Console, expand Sites and navigate to and expand the Tachyon website  
   5. Click on the Core application and double-click on IP Address and Domain Restrictions  
   6. Add the IP Address of the DMZ Server internal DNS Name to the IP Address and Domain Restrictions (including IPv6 address if used)  

   You only need to change the HTTPS FQDN in the -config setting for each existing Switch command-line. Do not change the IP Address and Domain Restrictions because the firewall is blocking ICMP.  

   If you have multiple switches, ensure you modify each SwitchCommandLine.n entry in the configuration file.  

   The command-line will include -IgnoreClientCerts if you unchecked Switches require client certificates to be presented.  

   Please refer to Implementation issues: IP address and domain restrictions for more details. This step is only required on the Core web application.  

   On the internal Tachyon Server (Response Stack) open a command prompt and ping the DMZ Server internal DNS Name FQDN because the firewall is blocking ICMP.  

| 9 Internal Tachyon Server (Response Stack). | On the internal Tachyon Server (Response Stack) that the DMZ Server will be communicating with, modify the IP Address and Domain Restrictions module in the Tachyon Core web application to enable the IP Address of the DMZ Server internal DNS Name FQDN. In our example this is https://tachyon.alt.acme.local:443/Core. This should prove that the name is resolved and provide the IP Address, even if you do not get a response.  

| 10 Internal Tachyon Server (Response Stack). | On the internal Tachyon Server (Response Stack), restart all Switches and confirm they are working.  
   1. Restart the 1E Tachyon Switch Host service  
   2. Ensure all internal Switches are running  
   3. In Tachyon Explorer, confirm that at least one internal Tachyon client is connected.  

| 11 Internal Tachyon Server (Master and Response Stacks) and internal Tachyon client(s). | Ensure that everything is still working by running the tests described in Verifying.  

| 12 DMZ Server. | On the Tachyon DMZ Server  
   On the Tachyon DMZ Server, run Tachyon Setup and complete the installation using the configuration option DMZ Server.  

If you are using internal and external network interfaces on the DMZ Server, then ensure you select an external interface IP Address for each Switch in the configuration.

### Switch configuration

This screen is only relevant if you selected one of the following configuration options:

- All components on a single server
- Tachyon Response Stack
- DMZ Server

This screen displays a list of IP Addresses that can be assigned to each Switch in your configuration. Tachyon Setup will need to confirm or change which IP Address is used by each Switch.

#### IPv6

The screen only displays a list of IPv4 IP Addresses available on the server. If you need to use IPv6 and have a functioning IPv6 network infrastructure, please contact 1E for further advice on how to use this screen.

Ideally to maximize the performance of Tachyon you should have the following configuration:

- You have enough Switches configured to support the selected number of devices - you can add additional Switches by clicking extra checkboxes, if you have enough IP Addresses configured
- One interface per Switch - interfaces may have more than one associated IP Address, so you'll need to check the MAC Addresses to make sure that the IP Addresses are on different interfaces
- An additional interface if you have a remote SQL Server, necessary to separate incoming and outgoing response traffic

However, in a lab or other environment which has less than 500 devices, you can have all components using a single IP Address.

If you have a local installation of SQL Server, then **Used for SQL** will show **No** for all IP Addresses, and you can select whichever IP Address you wish to for each Switch.

If you are using a remote SQL Server, then **Used for SQL** will show **Yes** for the IP Address which the validation process used to validate the connection to the SQL Server you selected for the Responses database. If this is not the same interface used for SQL, you will need to configure the persistent route, and restart Tachyon Setup.

For an installation with multiple Switches, aside from each selected IP Address, all Switches will have an identical configuration.

Click **Validate** to check that your selection conforms to the best practice rules for configuring switches.

Once the selection has been validated, click **Next** to continue.
The workflow in **Tachyon Setup** has not yet been optimized for installing just the Switch and Background Channel components:

- In the **Database servers** screen - options on this screen are greyed out - configuration settings are not required.
- In the **Website configuration** screen - specify the **HTTPS Host Header** as the **Internal DNS Name of the DMZ Server**.

You will manually add the binding for the client (external) DNS Name in the next step.

<table>
<thead>
<tr>
<th>Step</th>
<th>DMZ Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>After installation, on the Tachyon DMZ Server, add an additional HTTPS binding for external client devices to use.</td>
</tr>
</tbody>
</table>
|      | 1. On the Tachyon DMZ Server, open **IIS Management Console**  
|      | 2. Expand **Sites** and navigate to and expand the **Tachyon** website  
|      | 3. Under the Edit Site actions, click on **Bindings...**  
|      | 4. Click **Add...**  
|      | 5. Select type **https**  
|      | 6. Set the **Host name** to the **DMZ Server external DNS FQDN**. In our example this would be: **tachyon.acme.com**  
|      | 7. Enable **Require Server Name Indication**  
|      | 8. Select the **SSL certificate** to be the DMZ Server certificate (described above, in **DMZ Server certificate**)  
|      | 9. Click **OK** to save, and **Close** |
| 14   | Allow the internal Master Stack server to use domain credentials to access the DMZ Server's Background Channel. |
|      | **Only do this step if the DMZ Server is domain joined and there is two-way trust between your internal domain and your DMZ.** |
|      | On the DMZ Server, configure **AllowedUsers** on the Background Channel web application. |
|      | 1. Expand **Sites** then navigate to and expand the **Tachyon** website  
|      | 2. Click on **Background** and double-click on the **Application Settings** icon  
|      | 3. In the **Application Settings** view, double-click on the **AllowedUsers** value  
|      | 4. In the **Edit** dialog, append to the list the domain computer account of the internal Tachyon Server, and click **OK**. In our example this would be:  
|      | - from **NT AUTHORITY\Network Service;ACME\ACME-TCNDMZ$**  
|      | - to **NT AUTHORITY\Network Service;ACME\ACME-TCNDMZ$;ACME\ACME-TCNMST$** |
| 15   | Allow the internal Master Stack server to use certificates to access the DMZ Server's Background Channel. You will use the thumbprint from step 4. |
|      | On the DMZ Server, configure **AllowedUsers** on the Background Channel web application. |
|      | 1. Expand **Sites** then navigate to and expand the **Tachyon** website  
|      | 2. Click on **Background** and double-click on the **Application Settings** icon  
|      | 3. In the **Application Settings** view, double-click on the **AllowedUsers** value  
|      | 4. In the **Edit** dialog, append to the list the **Tachyon Consumer API client certificate** thumbprint from step 4, and click **OK**. In our example this would be:  
|      | - from **NT AUTHORITY\Network Service;545EF2AF74201A8CFACE0F0CEFE2D987237AE176**  
|      | - to **NT AUTHORITY\Network Service;545EF2AF74201A8CFACE0F0CEFE2D987237AE176** |
| 16   | Enable **Require client authentication** on the Background Channel web application. |
|      | This step changes SSL Settings for the parent, and the next step will change the same setting for specific child directories. |
|      | 1. On the Tachyon DMZ Server, open **IIS Management Console**  
|      | 2. Expand **Sites** and navigate to and expand the **Tachyon** website  
|      | 3. Click on **Background** and double-click on the **SSL Settings** feature  
|      | 4. Ensure the **Require SSL** box is checked and that the **Require** radio button is selected  
<p>|      | 5. In the <strong>Actions</strong> pane, click <strong>Apply</strong> |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| **17** | DMZ Server  
Only when not domain-joined, or is untrusted.  
Skip this step if domain-joined and trusted.  
For the Background Channel web application, enable **Ignore client authentication** on virtual directories: Content, Installers, PolicyDocuments, Updates:  
1. On the Tachyon DMZ Server, open IIS Management Console  
2. Expand the Tachyon website, and expand Background application  
3. Repeat the following steps for each of the virtual directories: Content, Installers, PolicyDocuments and Updates:  
   a. Double-click on the **SSL Settings** feature  
   b. Ensure the **Require SSL** box is checked and that the **Ignore** radio button is selected  
   c. In the **Actions** pane, click **Apply**  
   ![Do not change any settings for the bin directory.](image)

| **18** | DMZ Server  
Only when not domain-joined, or is untrusted.  
Skip this step if domain-joined and trusted.  
Increase the **uploadReadAheadSize** setting for the Background Channel.  
On a DMZ Server that is not domain-joined, Background Channel requires this to support certificate authentication, which is not required for a domain-joined server which uses Windows Integrated Authentication:  
1. On the Tachyon DMZ Server, open IIS Management Console  
2. Expand Sites and navigate to and expand the Tachyon website  
3. Click on **Background** and double-click on the **Configuration Editor** icon  
4. In the **Section** drop-down, select system.web/httpRuntime and make a note of maxRequestLength value (the default is 262144)  
5. In the **Section** drop-down, select system.webServer/serverRuntime and change the **uploadReadAheadSize** setting from the default of 49152 to (this is maxRequestLength in bytes = 262144 x 1024)  
6. In the **Actions** pane, click **Apply**

| **19** | DMZ Server  
Only when not domain-joined, or is untrusted.  
Skip this step if domain-joined and trusted.  
Create a Policy virtual directory for the Background Channel:  
1. On the Tachyon DMZ Server, open IIS Management Console  
2. Expand Sites and navigate to and click on the Tachyon website  
3. Right click on **Background** and select **Add Virtual Directory**...  
4. Set the **Alias** to Policy and the **Physical Path** to the Background Channel folder, by default this is C:\ProgramData\1E\Tachyon\PolicyDocuments  
5. Click **OK**  
6. Click on the newly created **Policy** virtual directory in the **Connections** pane  
7. Double-click on the **SSL Settings** icon  
8. Ensure **Require SSL** is checked and that the **Ignore** radio button is selected under **Client certificates**

| **20** | DMZ Server.  
Perform an **IIS Reset** on the DMZ Server. |
21 **DMZ Server.**

Modify the Switch host configuration file on the Tachyon DMZ Server to use the HTTPS binding set up in step 3.

On the Tachyon DMZ Server, in the Tachyon installation directory Switch folder, modify the `Tachyon.Switch.Host.exe.config` file:

2. Modify the `CoreUrl` key to use HTTPS with the new HTTPS binding created for the Response Stack in step 3. In our example this would be:
   ```xml
   from <add key="CoreUrl" value="https://tachyondmz.acme.local:443/Core"/>
   to <add key="CoreUrl" value="https://tachyonalt.acme.local:443/Core"/>
   ```
   
   **Important:** Before editing, the values for CoreURL and SwitchCommandLine may include a FQDN such as .acme.local and .acme.com.

3. For each external Switch, modify its `SwitchCommandLine` to change the `-config` to use HTTPS and the new HTTPS binding.
   ```xml
   from <add key="SwitchCommandLine.1" value="-cfgName=ACME-TCNDMZ-SW1 -config=https://tachyondmz.acme.local:443/Core"/>
   to <add key="SwitchCommandLine.1" value="-cfgName=ACME-TCNDMZ-SW1 -config=https://tachyonalt.acme.local:443/Core"/>
   ```
   
   **Important:** If SwitchCommandLine.n is commented out in the XML file, uncomment it and fill-in the content by copying from SwitchHost.log. You must add the `-IgnoreClientCerts` if you unchecked Switches require client certificates to be present.

4. Repeat the above step for each additional Switch.

22 **DMZ Server.**

Restart the **Tachyon Switch Host** service on the DMZ Server, and then ensure all DMZ Switches are running.

Review the `Switch.Host.log` files.

23 **Internal Tachyon Server (Response Stack) and DMZ Server.**

Copy existing Background Channel content from the internal Tachyon Server to the Tachyon DMZ Server:

1. On the DMZ Server, verify that NETWORK SERVICE has modify rights on the %PROGRAMDATA%1E folder, and this is in-lined.
2. Copy the content (minus the web.config file) from each of the following directories from the internal Tachyon Server (Response Stack) and DMZ Server:
   - %PROGRAMDATA%1E\Tachyon\Content
   - %PROGRAMDATA%1E\Tachyon\PolicyDocuments
   - %PROGRAMDATA%1E\Tachyon\Updates

   **Important:** Only the initial copy of content is required. From this point on, the Consumer API will maintain the content of the Background Channel. PolicyDocuments can be omitted. When you click on the **Deploy** button in Guaranteed State (in step 27), then all policies will be deployed. If any source directory is empty then it means you have not tested that feature when verifying the internal Tachyon system.

24 **Internal Tachyon Portal, Tachyon Server (Response Stack) and DMZ Server.**

Verify that the internal Tachyon Server can upload content to the Background Channel on the Tachyon DMZ Server:

1. Connect to the Tachyon website and open the Settings application and navigate to Instruction sets.
2. Delete the **Verification** instructions.
3. Verify that %PROGRAMDATA%1E\Tachyon\Content\1E-TachyonPlatform-VerificationStage2 is removed from the internal Tachyon Portal.
4. Upload the Verification Instructions.
5. Verify that %PROGRAMDATA%1E\Tachyon\Content\1E-TachyonPlatform-VerificationStage2 is re-created on the internal Tachyon Portal.

25 **DMZ Server and external Tachyon client(s).**

Verify an external Tachyon client can connect to the Tachyon DMZ Server Switch.

Change the Tachyon client configuration (1E Client configuration file) to point at both the internal Tachyon Server and the Tachyon for only the Tachyon DMZ Server.

1. Edit the %PROGRAMFILES%1E\Client\1E.Client.conf file
2. Modify the Switch configuration property.
   - In our example this would be: `Switch=tachyon.acme.local:4000;tachyon.acme.com:4000`
3. Modify the BackgroundChannelUrl configuration property.
   - In our example this would be: `BackgroundChannelURL=https://tachyon.acme.local:443/Backgroundhttps://tachyon.acme.com:4000`.
4. Ensure the test device is connected to the external network and not the internal network, then review the 1E.Client.log to confirm the external test device is online.
<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
</table>
| **26** | **Internal Tachyon Portal and external Tachyon client(s).** | **Run** verification steps **to verify an external Tachyon client can download content from the Tachyon DMZ Server Background Channel.**  
1. Browse to the Tachyon website and open the Explorer application  
2. Run the verification stage 1 and 2 and confirm a successful response is received from the external Tachyon client  

---

| **27** | **Internal Tachyon Portal and external Tachyon client(s).** | **Verify the external client can receive Policy updates.**  
1. Open the Guaranteed State application in a browser  
2. Click **Administration**, then click **Policies**  
3. Select an existing enabled policy that will affect the Tachyon client and then click **Disable**  
4. Click **Deploy**  
5. Check the 1E Client log on the external Tachyon client to verify that it has successfully received a message to fetch new policy.

---

iadYou do not need any policies defined in Guaranteed State for this step to take effect. Pressing **Deploy** will create an empty  

---