### **最终版SOP：在Windows VPS上部署PWA应用的权威指南**

#### **一、 目标与核心思路**

* **最终目标：** 在一台Windows VPS服务器上，成功部署一个Node.js编写的PWA（渐进式网络应用），并使其能通过自定义的 https:// 域名（例如 https://menu.teaforia.in）被用户正常访问和安装。
* **核心思路：** 根据服务器的网络环境和安全策略，我们提供两种经过验证的、可靠的解决方案。
  1. **方案一：Cloudflare Tunnel (推荐，无需开放端口)**
     + **适用场景：** 服务器处于有严格防火墙限制（如无法联系Azure管理员开放端口）、或追求最高安全性的环境中。
     + **工作原理：** 通过在服务器上安装一个轻量级的cloudflared服务，主动与Cloudflare的全球网络建立一个安全的出站连接隧道。所有外部请求都将通过这个隧道被安全地路由到服务器内部的Node.js应用，**完美绕过所有入站防火墙限制**。
  2. **方案二：IIS反向代理 + Certify The Web (传统，需开放443端口)**
     + **适用场景：** 您拥有服务器网络环境的完全控制权，能够开放公网的443端口（例如，您是Azure门户的管理员）。
     + **工作原理：** 采用经典的Web服务器架构。IIS作为反向代理，负责处理所有来自公网的HTTPS请求，然后将解密后的流量转发给在后台运行的Node.js应用。使用Certify The Web工具以图形化的方式，轻松地为IIS自动获取和管理SSL证书。

#### **二、 前置准备**

在开始之前，请确保您已具备以下条件：

1. **一个Cloudflare账户：** 并且您的域名（例如 teaforia.in）已经添加到该账户中，由Cloudflare进行DNS解析。
2. **一台Windows VPS服务器：** 您拥有该服务器的管理员权限。
3. **一个正在运行的Node.js应用：** 您的PWA应用已经可以在服务器上通过 node app.js 或类似命令启动，并在一个指定的内部端口上监听（例如 localhost:3001）。为了保证生产环境的稳定，强烈建议使用进程守护管理器如 pm2 来运行您的应用。

### **方案一：Cloudflare Tunnel (推荐，无需开放端口)**

此方案安全性最高，且配置过程不依赖于服务器的入站防火墙策略。

#### **第一部分：在Cloudflare上创建和配置隧道**

**步骤 1：进入Cloudflare Zero Trust仪表板**

1. 登录Cloudflare官网。
2. 在主页左侧导航栏，点击 **“Zero Trust”**。
3. 如果首次进入，根据提示选择并确认免费计划。

**步骤 2：创建新隧道**

1. 在Zero Trust仪表板的左侧导航栏，点击 **Access > Tunnels**。
2. 点击蓝色的 **“Create a tunnel” (创建隧道)** 按钮。
3. 在“Select your tunnel type”页面，点击 **“Select Cloudflare”**。
4. 在“Name your tunnel”页面，为您的隧道起一个容易识别的名字（例如 menu.teaforia.in），然后点击 **“Save tunnel” (保存隧道)**。

**步骤 3：在Windows VPS上安装隧道连接器**

1. 保存隧道后，您会进入“Install and run connectors”页面。
2. **切换到您的Windows VPS远程桌面**。
3. 在服务器上，以**管理员身份**打开 **Windows PowerShell**。
4. 回到Cloudflare的网页，在第4点下方，有一个灰色背景的命令框，内容是 cloudflared.exe service install ey...。点击命令框右侧的**复制图标**，将整条命令完整复制。
5. 将这条命令**粘贴**到PowerShell窗口中，然后按**回车**执行。
6. 等待命令执行成功。然后回到Cloudflare网页，您会看到下方的“Connectors”区域出现一个新的连接，并且状态显示为绿色的 **“Healthy” (健康)** 或 **“Connected” (已连接)**。

**步骤 4：配置路由规则（关联域名与应用）**

1. 在Cloudflare的连接器状态页面，点击右下角的 **“Next” (下一步)** 按钮。
2. 您会进入“Route Traffic”页面。在这里，我们需要将公共域名指向服务器内部的应用。
3. **配置公共主机名 (Public Hostname):**
   * **Subdomain (子域名):** 输入 menu。
   * **Domain (域名):** 从下拉菜单中选择 teaforia.in。
   * **Path (路径):** **保持留空**。
4. **配置服务 (Service):**
   * **Type (类型):** 从下拉菜单中选择 HTTP。
   * **URL (地址):** 输入 localhost:3001 (或者您Node.js应用实际监听的内部地址和端口)。
5. 点击 **“Complete setup” (完成设置)** 或 **“Save hostname” (保存主机名)**。

**步骤 5：处理DNS冲突（如果发生）**

* 如果在上一步保存时，系统提示 Error: An A, AAAA, or CNAME record with that host already exists.，这说明您之前为 menu.teaforia.in 设置的DNS记录还存在。
* **解决方案：**
  1. 回到Cloudflare主控制台的 **DNS > Records** 页面。
  2. 找到类型为 A、名称为 menu 的那条旧记录。
  3. 点击“编辑”，然后将其**删除**。
  4. 返回隧道的配置页面，再次点击“Complete setup”。

### **方案二：IIS反向代理 + Certify The Web (传统，需开放443端口)**

此方案采用经典Web服务器架构，**前提是您必须有权限开放服务器的443端口**。

#### **第一部分：在Azure/VPS防火墙中开放443端口**

这是此方案**最关键的前置条件**。您必须联系您的VPS提供商，或登录Azure门户，为您的服务器IP (4.188.76.209) 添加一条**入站安全规则**，**允许 TCP 协议的 443 端口**的流量。如果此步无法完成，请直接使用方案一。

#### **第二部分：在服务器上配置IIS和证书**

**步骤 1：安装IIS及所需模块**

1. 在服务器管理器中，通过“添加角色和功能”安装 **“Web 服务器(IIS)”** 角色。
2. 手动下载并安装以下两个模块：
   * **URL Rewrite Module:** [官方下载页面](https://www.iis.net/downloads/microsoft/url-rewrite)
   * **Application Request Routing (ARR):** [官方下载页面](https://www.iis.net/downloads/microsoft/application-request-routing)

**步骤 2：使用Certify The Web获取证书**

1. 从官网 certifytheweb.com 下载并安装**社区版**。
2. 首次运行时，根据提示注册您的联系人邮箱。
3. 点击 **“New Certificate” (新建证书)**。
4. **选择网站：** 在 Select Site 下拉菜单中，选择您在IIS中为 menu.teaforia.in 创建的站点（如果还没有，请先在IIS中创建一个指向空文件夹的临时站点）。
5. **配置授权：**
   * 点击右侧的 **Authorization** 标签。
   * **Challenge Type:** 选择 dns-01。
   * **DNS Update Method:** 选择 Cloudflare DNS。
   * **Credentials:** 点击 New，在弹出窗口中粘贴您的 **Cloudflare API 令牌** 和 **Zone ID**，然后保存。
6. **请求证书：** 点击右下角的 **Request Certificate** 按钮。程序会自动完成验证、获取和安装证书到IIS，并创建好443端口的HTTPS绑定。

#### **第三部分：配置IIS反向代理**

1. 进入您IIS网站的物理根目录（例如 C:\temp-site）。
2. 创建一个名为 web.config 的文件。
3. 将以下XML内容完整复制并粘贴到文件中：  
   <?xml version="1.0" encoding="UTF-8"?>  
   <configuration>  
    <system.webServer>  
    <rewrite>  
    <rules>  
    <rule name="ReverseProxyToNode" stopProcessing="true">  
    <match url="(.\*)" />  
    <action type="Rewrite" url="http://localhost:3001/{R:1}" />  
    </rule>  
    </rules>  
    </rewrite>  
    </system.webServer>  
   </configuration>
4. 保存文件。IIS会自动加载此配置。

#### **最终验证 (适用于任一方案)**

1. **确认Node.js应用运行：** 确保您服务器上的PWA应用正在通过 pm2 或其他方式稳定运行。
2. **访问您的域名：** 在您的本地电脑或手机上，打开浏览器，访问 https://menu.teaforia.in。
3. **检查结果：**
   * 您的PWA应用应该能被成功加载。
   * 浏览器地址栏应该显示一个**安全锁标志**，表示HTTPS已生效。
   * PWA的“添加到主屏幕”或安装提示应该能正常出现。

至此，您已掌握了两种在高限制环境下部署PWA应用的强大方案。