SOPHOS
Cybersecurity evolved.

ZTNA 的六大优势

相比远程访问 VPN

Sophos 白皮书。2021 年 10 月

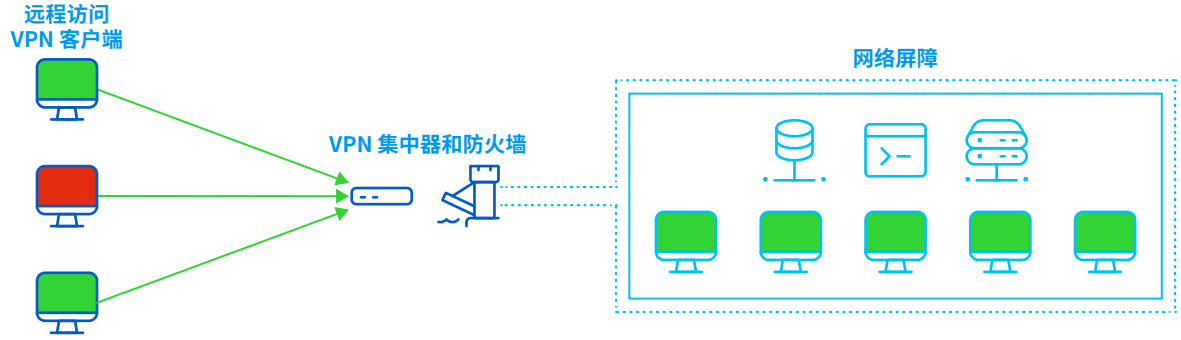
远程访问 VPN 一直以来为我们带来了很好的服务，但最近远程办公数量的增加，将这一正在过时的技术的局限性推上风口浪尖。一些企业继续挖掘 VPN 的最后潜力，许多企业则在寻找更好的替代手段 – 能够解决远程访问 VPN 面临挑战的技术。一些企业已经开始全面拥抱下一代远程访问技术：ZTNA，即零信任网络访问。相比传统远程访问 VPN，ZTNA 具有更好的安全性，更加精细的控制，更高可见性，以及透明的用户体验。

在这篇 ZTNA 买家指南中，我们将探讨传统远程访问 VPN 的局限性和挑战，零信任网络访问具备的优势，并总结寻找新的 ZTNA 解决方案时应关注的关键功能。

远程访问 VPN 面临的挑战

数十年来，远程访问 VPN 一直是大多数网络的基础，提供远程访问网络系统和资源的安全方法。但是，时代已经发生变革，企业网络变得像中世纪堡垒 – 厚实的堡垒外墙和护城河在内部网络资源周围建立起一道安全可靠的屏障。VPN 相当于为授权用户提供一个安全门房以进入安全屏障，但进入后，用户可以完全访问屏障内的所有内容。

传统远程访问 VPN



当然，网络也发生了巨大的变化，分布式程度比以往更高。应用程序和数据现在位于云端，用户远程办公，攻击者和黑客不断寻找网络漏洞进行攻击。

在任何现代环境中采取基于传统 VPN (IPSec/SSL) 的远程访问解决方案可能非常痛苦，必须应对 IP 管理、流量流动和路由、防火墙访问规则以及客户端和证书部署与配置。超出几个节点和数是个用户就会将这变为不必要的全职工作 - 仅仅保持运行。如果这还不够，监控安全无疑是噩梦。

总的来说，传统远程访问 VPN 有许多不必要的局限性和挑战：

1. **绝对信任** – 远程访问 VPN 能够带您穿过屏障进入企业网络，就像真的在公司一样，但此时，您受到绝对信任，获得企业网络资源的广泛访问权，带来不必要的巨大安全风险。
2. **潜在威胁媒介** – 远程访问不了解用于连接企业网络的设备状态，有可能形成威胁从被攻破设备进入网络的渠道。
3. **回传效率低** – 远程访问提供网络上的单个存在点，可能需要通过远程访问 VPN 通道从多个位置、数据中心或应用程序回传流量。
4. **缺乏可见性** – 远程访问 VPN 不了解流量和使用模式，要实现用户活动和应用程序使用的可见性更加困难。
5. **用户体验** – 远程访问 VPN 客户端以用户体验差，增加延迟或负面影响性能，连接问题，成为帮助台负担而闻名。
6. **管理、部署和注册** – 远程访问 VPN 客户端难以设置、部署和注册新用户，停用离开的用户。难以在防火墙或网关侧管理 VPN，尤其对于多个节点、防火墙访问规则、IP 管理和流量流动与路由。很快变为一份全职工作。

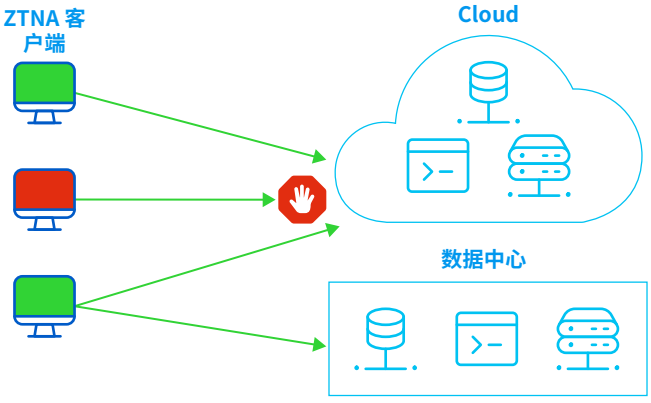
ZTNA 是什么，工作方式是什么

ZTNA 即零信任网络访问从一开始就设计旨在解决远程访问 VPN 的挑战和局限性，为用户提供随时随地安全连接工作所需的应用程序和数据的更好解决方案，仅此而已。ZTNA 与远程访问 VPN 存在很多根本性区别。

顾名思义，ZTNA 基于零信任原则 – 即，不信任一切，检验一切。零信任基本消除旧城堡外墙和护城河屏障概念，让所有用户、所有设备、所有联网应用程序获得自己的屏障，只有验证凭据、检验设备运行状况和检查访问政策后才能相互连接。这样极大提高安全性、分区和控制。

ZTNA 工作方式的另一个重要区别在于用户并不是在具有完全活动自由的网络上，而是为获得授权访问的应用程序（仅此而已），在用户与特定网关之间建立各个通道，明显提高微分区的安全性。这给安全性、控制、可见性、效率和性能带来很多好处。例如，远程访问 VPN 不提供用户访问的应用程序的任何信息，而 ZTNA 可以提供所有应用程序的实时状态和活动，在确定潜在问题和执行许可审计方面具有重要意义。ZTNA 带来的更多微分区确保设备或用户访问不会在网络资源之间横向移动。每个用户、设备和应用程序或资源拥有自己的安全屏障，不再有绝对信任概念。

零信任网络访问



ZTNA 本质上更加动态和透明，在后台运行，无需用户进行初始身份验证以外的其他交互。这种体验非常平滑流畅，用户甚至不会意识到通过安全加密通道连接应用程序。

ZTNA 的优势

零信任网络访问具有许多方面的巨大优势，但主要因为以下一个或多个原因而采用：

- **在家办公：**ZTNA 解决方案更方便管理在家办公员工的远程访问权。更方便更灵活部署和注册，将 VPN 的全职工作变为资源强度更小的工作。对于远程办公员工更透明更简单。
- **应用程序微分区：**ZTNA 解决方案通过微分区，将设备运行状况集成到访问政策，持续身份验证，消除 VPN 的绝对信任和横向移动问题，极大提高应用程序安全性。
- **阻止勒索软件：**ZTNA 解决方案消除勒索软件和其他网络渗透攻击的一个常见攻击渠道。ZTNA 用户不再“位于网络上”，可能通过 VPN 获得立足点的威胁对于 ZTNA 手足无措。
- **快速推出新应用程序和用户：**ZTNA 在用户来来往往的快速多变环境中实现更好的安全性和更大灵活性。快速推出新应用程序，轻松注册或停用用户与设备，获取应用程序状态和使用的信息。

总的来说，ZTNA 相比传统远程访问 VPN 解决方案的优势包括：

1. **零信任** – ZTNA 基于零信任原则，即“不信任一切，检验一切”。这样可以像自己的屏障一样有效对待每个用户和设备，不断评估和验证身份与运行状况，获得企业应用程序和数据的访问权，从而明显改善安全性和微分区。用户只能访问其政策明确允许定义的应用程序和数据，减少横向移动以及相关风险。
2. **设备运行状况** – ZTNA 将设备合规性和运行状况集成在访问政策中，不允许不合规、感染或受威胁系统访问企业应用程序和数据，消除这一重要威胁渠道，减少数据失窃或外泄的风险。
3. **在任何地方办公** – ZTNA 是跨网络的，可从任何网络良好安全工作，无论是家中、酒店、咖啡店还是办公室网络。连接管理安全透明，与用户和设备所在位置无关，无论用户在哪里办公，都能带来无缝体验。
4. **更透明** – ZTNA 在需要时自动建立背后的按需安全连接，提供流畅无缝的最终用户体验。大多数用户甚至不会意识到 ZTNA 解决方案帮助保护了他们的数据。
5. **更好的可见性** – ZTNA 可以提供应用程序活动的更高可见性，对于监测应用程序状态、容量规划、许可管理和审计非常重要。
6. **更容易管理** - ZTNA 解决方案往往更精简更洁净，因此更容易部署和管理。在用户来来往往的快速多变环境中更加灵活 - 使日常管理成为一个快速轻松的工作，而不是全职工作。

买家指南：需要考虑 ZTNA 解决方案的哪些方面

查看客户端、网关和标识提供机构的支持平台列表，比较不同供应商的 ZTNA 解决方案时，务必考虑以下重要功能：

云交付云管理

云管理提供巨大的优势，能够即可上线并运行，减少管理基础设施，部署和注册，支持在任何地方访问。云管理的一个重要优势是能够即可登录并开始，无需添加额外管理服务器或基础设施。云管理还支持在任何设备从任何位置即时安全访问，支持您需要的工作方式。方便世界各地的新用户注册。

与其他网络安全解决方案集成

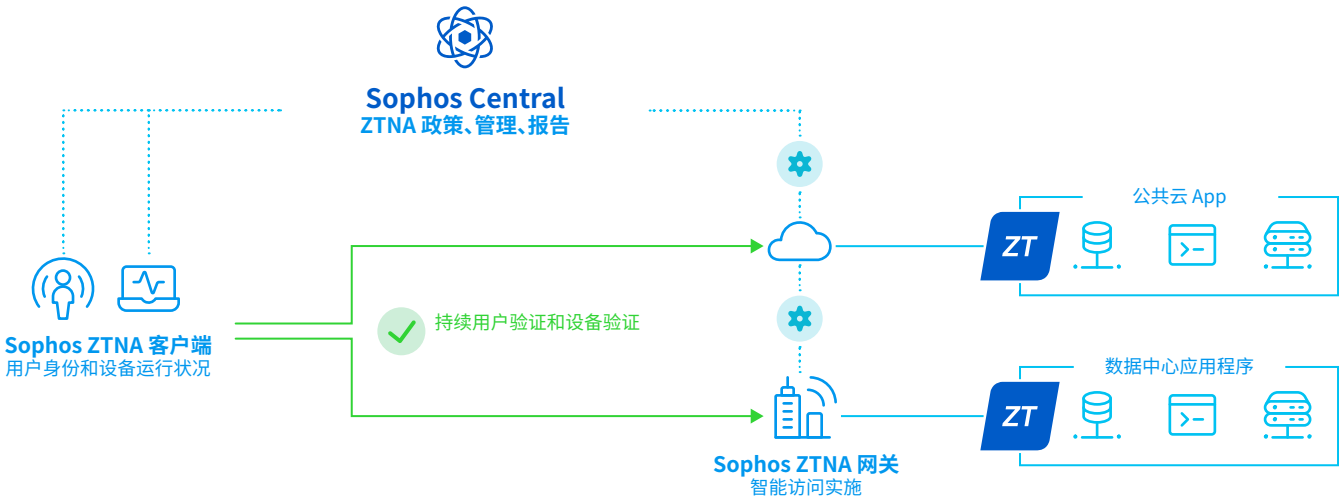
大多数 ZTNA 解决方案作为单独产品时非常完美，但与其他网络安全产品（如防火墙和端点）紧密集成的解决方案具有显著优势。常见的集成云管理控制台可以让您或您的团队发挥成倍的力量。使用一个面板在一个位置管理所有 IT 安全，包括 ZTNA，可以缩短培训时间，降低日常管理开销。还可以提供各个 IT 安全产品的独有信息，尤其是共享遥测信息的情况下，显著提升安全性，在被攻破设备或威胁进入网络时实时应对。它们可以合作即时应对攻击或威胁，阻止其横向移动、传播或盗窃数据。

用户和管理体验

确保您考虑的解决方案提供出色的最终用户体验，简化管理工作。现在随着越来越多用户从世界各地远程办公，注册和高效设备设置对于让新用户尽快发挥生产力至关重要。务必注意 ZTNA 代理的部署方式，以及将新用户添加到政策的容易程度。还确保您投入的解决方案提供平滑流畅的最终用户体验，带来您需要的可见性，如应用程序活动实时信息，帮助您主动识别峰值负荷、容量、许可使用甚至应用程序问题。

Sophos ZTNA

Sophos ZTNA 从一开始设计旨在实现简单、集成、安全的零信任网络访问。Sophos ZTNA 采用云交付和云管理，集成在全球最受信任的网络安全云管理和报告平台 Sophos Central 中。从 Sophos Central 不仅可以管理 ZTNA，还可以管理 Sophos Firewall、端点、服务器防护、移动设备、云安全、电子邮件防护等。



Sophos ZTNA 独有紧密集成 Sophos Firewall 和 Sophos Intercept X 端点，能够发挥 Synchronized Security 和 Security Heartbeat 在防火墙、设备、ZTNA 和 Sophos Central 之间共享设备运行状况，自动应对威胁或不合规设备的优势。自动限制访问，隔离被攻破的系统，直到清理完成。

Sophos 客户对全集成 Sophos 网络安全解决方案节省大量时间的优势表示认同，称使用 Sophos 产品套件，从 Sophos Central 管理，利用 Synchronized Security 自动识别和应对威胁后，IT 团队仿佛人手扩充了一倍。Sophos ZTNA 当然也可配合任何其他厂商的安全产品工作，但配合其他 Sophos 生态体系效果更佳，带来可见性、防护和响应方面的切实现实优势。