AhnLab

安全月刊

2021.03 Vol.100

远程办公安全

远程办公的普遍以及对安全的需求不断增加

远程办公带来的风险以及解决方案，AhnLab 告诉你答案！

在上一期的AhnLab安全月刊《2021年，AhnLab关注客户与云》中，我们提到了远程办公（Work From Home: WFH）和安全问题是数字化新常态之一。随着新冠病毒的影响，无接触（Untact）趋势加速发展，工作环境密度较高的公司的职员对远程办公需求不断增加。并且，在变化的环境中保护企业资产的安全方案的必要性也随之日益凸显。

那么，在远程办公环境中如何构建安全呢？在本文中， AhnLab将告诉你对这个常见但并非简单的问题的答案。

由于远程办公在疏忽于安全控制的外部执行，因此始终存在着诸如信息泄露之类安全风险。更具体地，可以以如下3个方面来说明远程办公时存在的安全风险。首先，由于外部终端相对而言缺乏物理控制，因此在丢失或被盗时存在数据泄露的风险。通过公用的有线和无线网络访问内部网也是一种安全威胁。最后，在对内部资源的远程访问方面也存在未经授权的访问等安全问题。

如此，在远程办公的环境中通过各种途径引入威胁，并且由于未应用更新而导致的应用程序的漏洞增加，以及感染新·变种恶意代码的风险也在增加。从企业的角度来看，对终端的管理负担自然不可避免地加重。

如果攻击者利用这些漏洞成功进行攻击，企业不仅会泄露信息，还会受到系统破坏、业务中断等严重的打击。从长远的角度来看，品牌形象也会随之下降。因此，无论在访问工作系统之前还是之后，都必须始终加强安全。

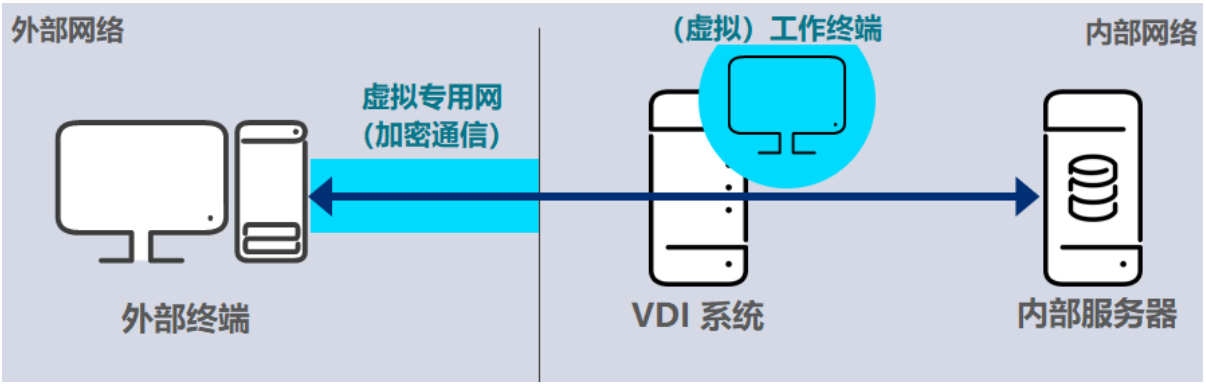
远程办公时的远程访问类型

远程访问内部网络的方式分为“间接访问”和“直接访问”。这可以根据远程业务的特性和公司内部环境进行选择。接下来简单介绍这两种访问方式的定义和特征。

间接访问方式

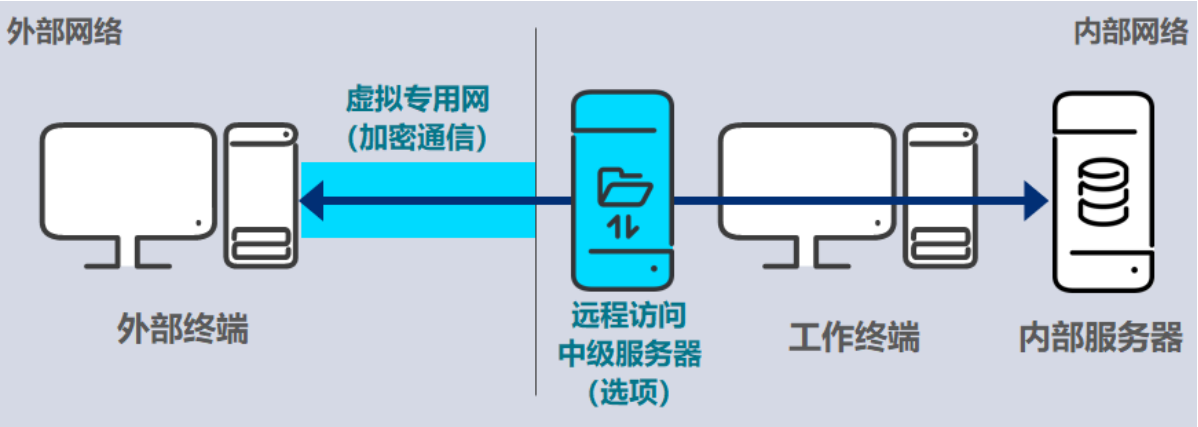
首先，间接访问是指通过公司内部的业务终端从外部终端连接到内部网络。根据虚拟桌面（VDI）或远程访问程序的使用，它又分为两种方式。

VDI方式是通过VDI的虚拟业务终端从外部终端连接到内部网络。VDI可位于公司内部的公共网络或业务网络，并且还可以使用基于互联网云的DaaS(Desktop as a Service)等VDI服务。在虚拟业务终端上处理业务，而不是外部终端，并且外部终端上只显示虚拟桌面的图像。



【图 1】基于虚拟桌面（VDI）方式的结构图

通过远程访问程序的连接方式是使用远程访问程序从外部终端连接到业务终端。外部终端和业务终端之间可以直接访问或通过另外的远程访问中继服务器连接。与VDI不同，它的特点访问实际工作的终端而不是虚拟终端来处理业务。

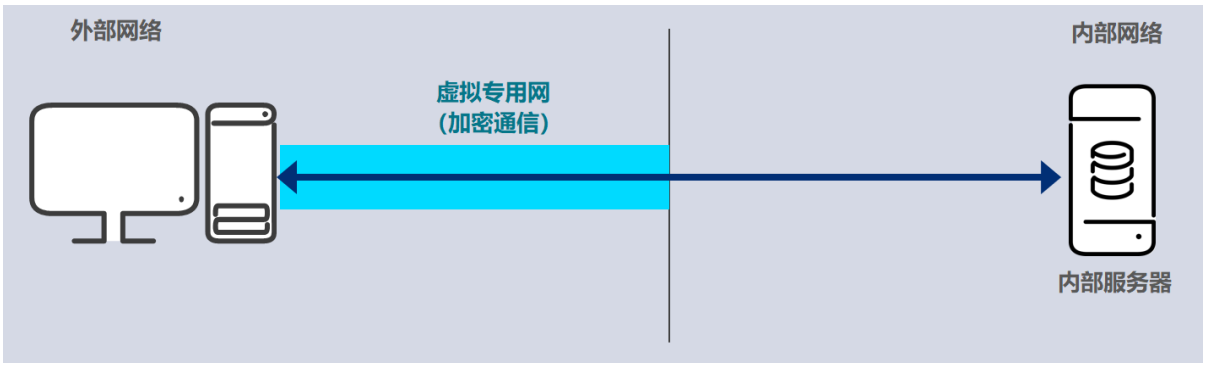


【图 2】远程访问程序方式的结构图

直接访问方式

直接访问是外部终端机不通过内部业务终端而直接访问内部服务器。在外部终端上处理业务时，业务数据直接储存在外部终端中，因此要格外注意信息泄露等安全事故。

※ 对于直接访问的外部终端，请使用公司可以强制执行安全控制的公司发给的终端机，不推荐使用个人终端机。



【图 3】直接访问方式的结构图

AhnLab 构建安全的远程办公环境的方案

AhnLab提供对直接和间接访问的安全方案。安全流程从满足各安全要求的现有方式（例如，安装防病毒软件、建立APT防御措施以及使用安全的操作系统）向实现统一管理的方向发展。

尤其是，基于AhnLab的下一代网络安全解决方案“AhnLab TrusGuard”和“EPP Security Assessment（ESA）”之间的联动，加强了远程办公环境的安全性。运行TrusGuard VPN客户端时，允许已通过ESA安全预检查的外部终端建立VPN连接，并为预检查结果较脆弱的外部终端提供了解决安全漏洞的方案。

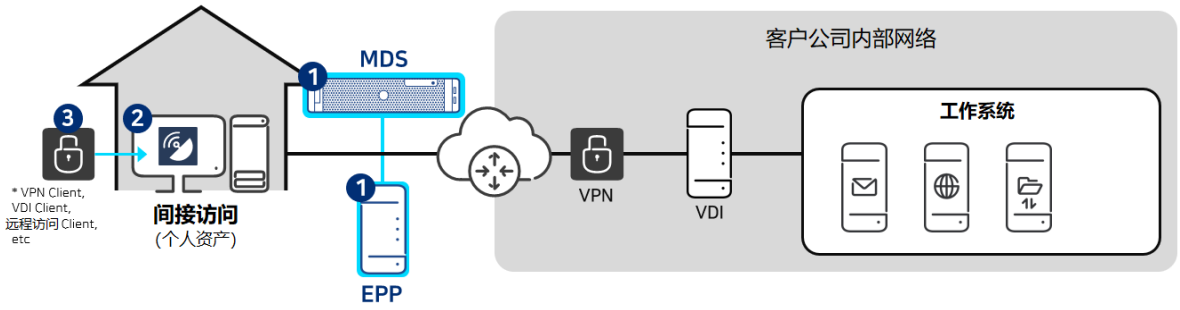
AhnLab提供的间接访问安全方案

AhnLab支持两种用于间接访问的安全方案。方案由三个步骤组成，其中第一步和第二步的内容相同。

第一步，在外部网络中构建AhnLab Endpoint Protection Platform（EPP）以管理间接访问终端，并构建MDS服务器。然后设置V3、EPP、ESA和EPP Patch Management（EPM）的策略。随后，准备用于管理间接访问终端的统一Agent。安装VPN客户端时，必须统一安装Agent。第二步就是安装统一Agent。统一Agent包括EPP Agent、V3、ESA、EPM和MDS Agent。
在随后的第三步中，预检查分为两种方法，分别在客户端和服务器中进行。

方案1：Client to ESA的联动结构

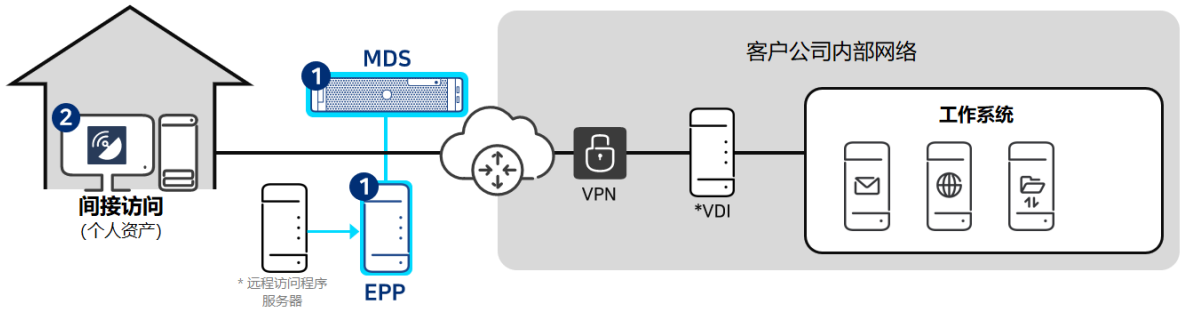
这是一种对间接访问的客户端（VPN、VDI、远程连接程序等）进行预检查后允许访问的方式，并且需要联动才能实现此目的。在这种情况下，在客户端需要确认最新的ESA检查分数，客户企业必须自行开发联动并应用，AhnLab则提供用于ESA联动的API。如果最新检查分数较低，则VPN连接被阻止。



【图 4】间接访问 - Client to ESA联动配置概念图

方案2：Server to EPP联动结构

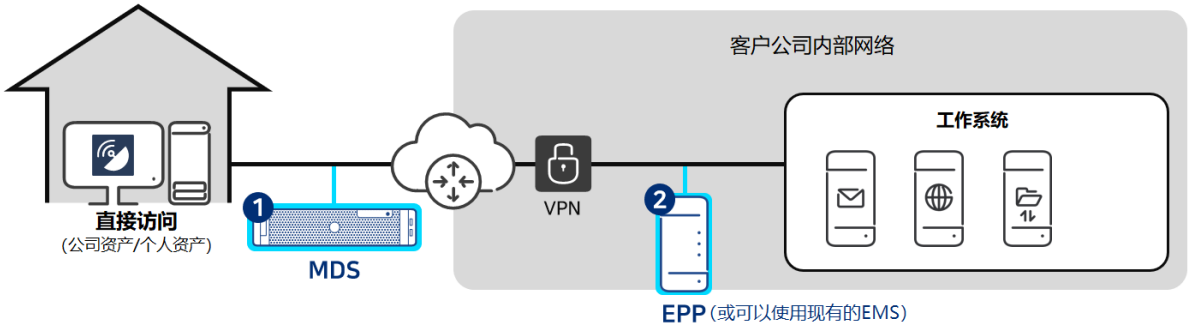
间接访问的服务器（远程访问程序服务器、VDI服务器等）在进行预检查后允许访问，并且需要联动。在这种情况下，间接访问程序服务器确认存储在EPP中的终端的最新ESA检查分数。同样，间接访问程序企业必须自行开发联动并应用，AhnLab则提供用于EPP联动的API。如果最新检查分数较低，则远程访问程序连接被阻止。



【图 5】间接访问 - Server to EPP联动配置概念图

AhnLab提供的直接访问安全方案

直接访问的安全方案包括两个步骤，其流程与间接访问大同小异。第一步，在内部网络中构建用于直接访问终端管理的EPP，并构建MDS服务器。对于EPP，也可以使用现有的EMS。随后，在设置V3、ESA、EPM策略之后，准备统一Agent。第二步，同样安装由EPP Agent、V3、ESA、EPM、MDS Agent组成的统一Agent，并且在安装VPN客户端时，必须统一安装它们。



【图 6】直接访问安全方案的概念图

远程办公的安全，答案在于平台

AhnLab拥有广范的安全产品组合，通过解决方案之间的集成和链接来提供平台形式的安全能力。每个解决方案都不是独自运行，而是协同运行以构建大框架的安全流程。对于远程办公的安全，也同样以端点安全平台“AhnLab EPP”为中心，每个解决方案根据情况和步骤来发挥适当的性能。

以下总结了远程办公时的安全注意事项和AhnLab的整体响应方案。

访问方式	区分	响应方案	产品
共同 (间接&直接)	安装防病毒软件	安装 V3，并通过 EPP 管理 V3	EPP，V3
	建立 APT 防御措施	通过 MDS 应用 APT 防御措施	MDS
	使用安全的操作系统	通过 ESA 检查操作系统的安全	EPP，ESA
	必须应用已知安全补丁	通过 ESA 检查安全补丁的应用状态和采取措施 通过 EPM 检查安全补丁应用和通过 EPP 管理补丁	- EPP - ESA，EPM
	设置登录密码	通过 ESA 检查屏幕保护程序的设置和采取措施	ESA， EPM
	设置屏幕保护程序	通过 ESA 进行本地安全策略检查和采取措施	EPP，ESA
	远程访问时，预检查安全措施	通过 ESA 预检查信息保护基本控制措施	EPP，ESA
间接 (远程访问程序，VDI)	连接到内部网络时，阻止互联网连接	通过 V3 脱机防火墙功能阻止互联网连接	EPP，V3
直接	始终阻止互联网连接	通过 V3 防火墙功能始终阻止互联网连接	EPP，V3

【表 1】远程办公时的安全注意事项和AhnLab的响应方案

今后，远程办公可能将变得越来越普遍。我们希望各位读者能够熟知必须的安全注意事项，并通过构建响应流程以有效保护您的业务资产。

AhnLab

安全月刊

https:// cn.ahnlab.com

https://global.ahnlab.com

https://www.ahnlab.com

关于AhnLab

Ahnlab的尖端技术和服务不断满足当今世界日新月异的安全需求，
确保我们客户的业务连续性，并致力于为所有客户打造一个安全的计算环境。
我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、
移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。
AhnLab已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

AhnLab

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室
电话：+86 10 8260 0932（北京） / +86 21 6095 6780（上海） | cn.sales@ahnlab.com