何为零信任架构?
如何实现?

Alcatel·Lucent Enterprise

电子书
零信任架构

目录

何为零信任架构?.....3

了解宏隔离和微隔离.....5

为什么既需要宏隔离，又需要微隔离.....6

如何实现.....7

方法论.....7

其他注意事项.....11

为何选择 ALE?.....11

已知的事实.....12

何为零信任架构?

零信任架构（ZTA）是什么意思？零信任架构就是，每个用户和设备在被允许访问数据之前都必须经过身份验证和授权。这是一种“不信任任何人、需要验证所有内容”的策略。

在此，打一个比喻对理解会有所帮助。

如果我们将传统的安全视为保护村庄的堡垒，就需要在村庄（即企业）周围构建堡垒墙（又称为防火墙）。任何来自堡垒外部的内容都是不受信任且需审查的，但堡垒内部的任何内容都默认被信任和被允许。这种信任边界既是物理的也是隐性的，取决于您在堡垒的哪一侧，因为只要您在墙的“正确”一侧，就无需进一步的检查。如果我们从企业网络的角度考虑这种方法，可能就会有一些基本的划分，如 VLAN、SSID、子网或连接到防火墙的接口，但这种划分是静态的，更多地与网络可扩展性和可管理性挂钩，而不是与安全性挂钩。

然而今天，由于一些原因，防火墙（堡垒）方法本身变得不那么有效。首先是移动性。当用户连接到企业外部的其他网络，这可能会带来威胁。其次，访客不一定值得信任。有人会说，即使是员工（堡垒内的人）也不应该被盲目信任。第三，接入到网络的物联网设备越来越多。这些设备会带来更高的安全风险，因为它们可能没有得到 IT 部门的批准和管理，而且通常缺乏安全能力。使用传统的“堡垒/村庄”（“防火墙/企业”方法），如果某个用户或设备被入侵，几乎没有什么可以阻止威胁蔓延到其他用户和设备。一旦进入内部就可以自由活动了。

在堡垒的比喻中，如果唯一保护村庄不受入侵者入侵的是城墙，那么当他们学会如何爬上堡垒的城墙时，就会进行大屠杀。

问题是，我们能做些什么？让我们从“不信任任何人”或“零信任”的方法来考虑这个问题。

在零信任状态下，任何用户或设备都不受信任。无论他们是在企业内还是在企业外，都要接受同样的检查。没有信任内部用户这种说法。每次访问都要经过验证和授权。

在堡垒的比喻中，意味着除了保护村庄免受外部威胁的堡垒外，每栋房子和每栋建筑都有自己的安全措施来保护村庄免受居住在堡垒内的邪恶分子的威胁。对于企业来说，软件定义的微隔离更精细化。在堡垒和建筑物周边的安全之上，我们还有私人保镖如影随形。无论我们走到哪里，都需要出示通行证。在企业网络中，这种信任边界是模糊的、分布式的且可移动的。它没有绑定到特定的位置、交换机端口 VLAN，而是取决于身份、设备、情况、一天中的时间以及其他因素。它是由软件定义的，可以动态调整。采用这种方法，就需要对组件进行管理，并且应该能够根据需要做出反应和重新配置，以应对威胁或对工作流程的变化。

了解宏隔离和微隔离

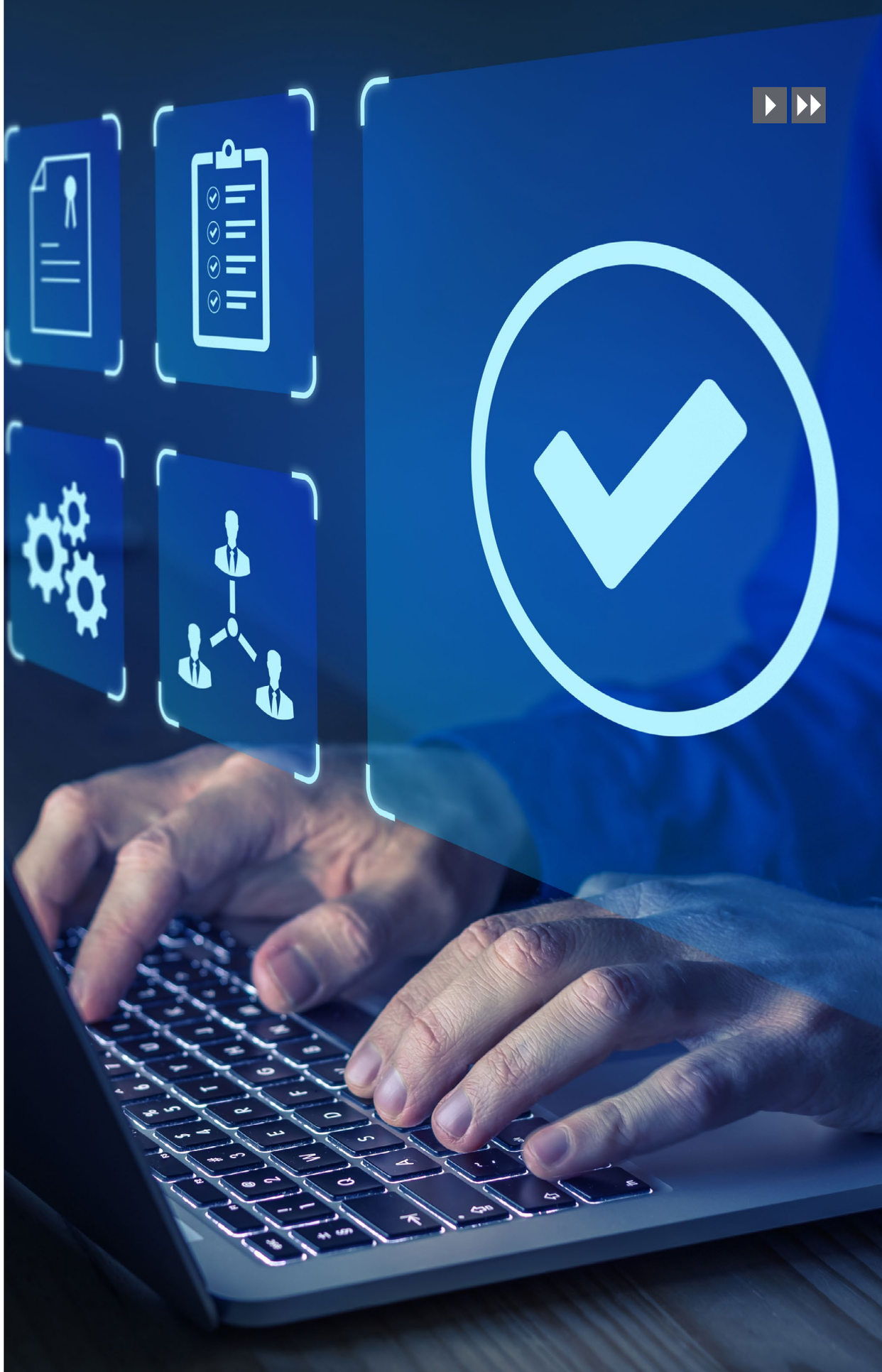
在零信任架构中有两种隔离方式，即宏隔离和微隔离。按照我们的比喻，堡垒墙是宏隔离，私人保安是微隔离。

在**宏隔离**中，物理网络被划分为不同的逻辑网段。这些网段既可以是 VLAN，也可以是 VLAN 和 VRF 的组合，当谈到最短路径桥接（SPB）、MPLS，甚至 VXLAN 或 GRE 隧道时，它们还可以是 VPN 。不同网段的用户或设备之间的通信流量均由防火墙控制。所有企业都以某种方式或形式使用隔离，但并非总是出于安全原因。通常，这种隔离是出于可扩展性、管理或组织上的原因。如果两个设备映射到的 VLAN 不同，但它们可以不通过防火墙进行通信，则它们位于相同的宏隔离上。在逻辑上与 PC 隔离的独立 VLAN 和 VRF 上运行 IP 电话就是这种隔离的一个典型示例。

问题是，如何将用户或设备映射到这些网段？虽然它可以静态完成（例如通过交换机端口或 SSID），但这确实是一种过时的方式。太过于死板，对移动用户来说不是个好选择。理想的情况是，应该有一个软件定义的身份验证系统，以便当用户或设备连接并进行身份验证时为其分配一个配置文件。无论物理位置、交换机端口或 SSID 如何，配置文件将为用户或设备提供正确的网段。

虽然宏隔离确实有安全优势，但在许多情况下，进行宏隔离是出于组织或管理的原因。例如，摄像头和门锁由门禁安全团队控制，而恒温器则由维护团队控制。

微隔离更精细化。并非所有用户都一样，也并非所有用户都有合法权限访问所有资源。相同的配置文件将用户映射到同一个网段，但它也还包括一组策略，可以实现对用户/设备权限进行更精细化的控制，不同的角色（如人力资源和财务）有不同的权限。这称为**基于角色的访问**，与**最小权限原则**直接关联。因此，即使摄像头和门锁都在同一网段，它们也不需要使用相同的资源。摄像头需要与录像机通信，门锁需要与其服务器通信。摄像头无需与门锁通信，就像门锁无需与其他门锁通信一样。这些精细控制权限是通过策略实现的，策略是配置文件的一部分，并在身份验证后动态应用于设备。



微隔离需要由软件定义，原因有几个。用户和物联网设备都不是静态的，他们可以移动、连接和断开，策略不能绑定到某个位置或端口。事实上，微隔离配置需要结合多种因素的组合进行动态的配置，包括但不限于用户或设备的身份、一天中的时间、位置等。

综上所述，不同网段之间的通信由防火墙控制时就是宏隔离。同一网段内的通信由与设备或用户角色相关联的网络访问控制（NAC）策略控制时就是微隔离。

为什么既需要宏隔离，又需要微隔离

如果只使用一种类型的隔离，会发生什么情况?

先来看看只使用宏隔离的情况。如果仅使用宏隔离，防火墙就会成为瓶颈，因为所有流量都需要通过防火墙进行身份验证和授权。这可能会导致性能问题。您可以在分布层部署更多的防火墙，但这可能代价高昂，并且不一定能提高性能，因为防火墙不是线速的。此外，需要多个策略执行点和多个位置来保持策略的更新，管理起来非常麻烦。

仅使用微隔离也是有问题的。如果仅通过 NAC 策略执行策略，这些策略列表将变得非常冗长且复杂，可能耗尽设备容量限值。

最重要的是，最好在这两种隔离方式之间取得平衡。 用防火墙控制不同网段之间的流量（南北流量），用 NAC 策略控制某个网段内的流量（东西流量）。

将这两种隔离方式结合，您可以应对从一个安全段溢出到另一个安全段的安全威胁，以及在同一网段中横向移动的安全威胁。更具体来说，微隔离可以阻止成功入侵摄像头的攻击者利用漏洞作为破坏门锁等其他资源的支点。

目标是对每个连接进行身份验证，并为每个用户或设备分配权限。这意味着使用隔离来防止威胁通过横向移动传播，并对任何不符合要求的用户或设备进行持续监控和隔离。

如何实现

在新建项目的情况下，使用微隔离从头开始构建零信任架构相对容易。但是，在改造项目的情况下，使用微隔离改造网络可能会导致用户、设备和应用程序由于身份验证失败或策略不完整而被挡在网络之外。企业很难甚至不太可能在一个升级周期内一次性完成迁移。

在改建项目中，会有一段非零信任和零信任架构并存的时期，一次在一层或一个位置进行迁移。重要的是要确保部署的基础架构设施及其部署方式是灵活的，能够在其他基础架构设施就绪时以零信任或微隔离模式运行。也就是说，基础架构设施将需要与现有和未来的组件进行互操作。

方法论

实现零信任架构有五个步骤——监控、验证和评估、计划、模拟和执行。

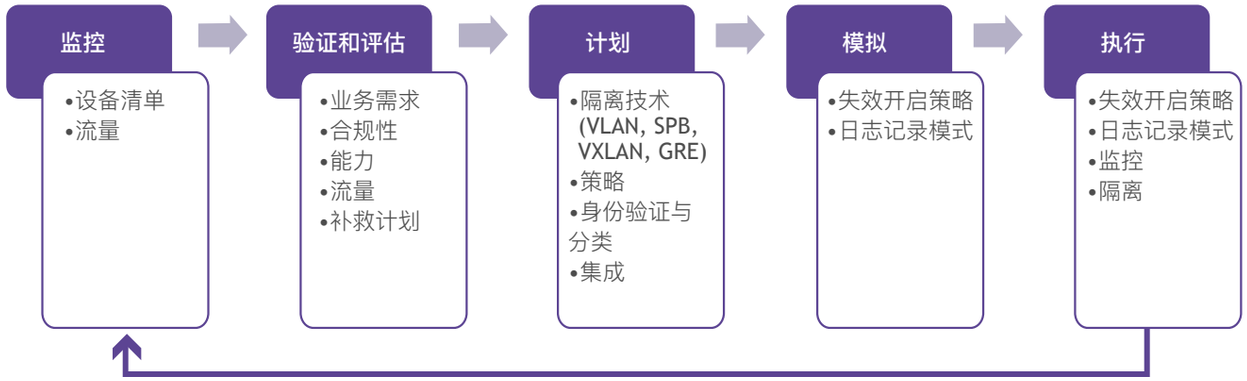


图1-方法

第一步：监控

首先，您需要开始监控和构建网络中内容的地图和设备清单库。

升级到零信任架构需要详细了解资产（物理资产和虚拟资产）、目标（包括用户权限）以及接触网络或在网络上运行的业务流程。信息不完整通常会导致由于信息不足而拒绝访问的故障。如果组织内部存在未知的“影子 IT ”或“影子物联网”，这个问题尤为明显。

开始监控设备和流量。创建包含网络上所有设备的明细清单报告，按设备类型、制造商、型号、操作系统等进行分类。报告还应显示上次看到设备的位置和交换机端口或 SSID 。这些信息可以从 MAC 地址、 DHCP 签名和 HTTP 用户代理等元素中收集。

大多数第三方工具只提供 IP 地址，而不提供设备类型。最理想的是有一个工具来创建物联网/设备清单库，以便为每种类型的设备快速便捷地创建 NAC 配置文件。

创建策略还需要流量信息。根据您拥有的设备，您可以从 sFlow、Netflow 或深度数据包检测（DPI）等流量监控工具获取此类信息。

这个过程将是反复的。第一次启用监控时，报告可能意义不大，但随着您进入其他步骤，报告将变得更加具体和有用。在这一步收集的信息将是进行后续步骤的关键。

第二步：验证和评估

第二步是验证这些发现。评估业务需求。任何不合理的影子物联网都应该删除，因为增加了不必要的攻击面。对于其余部分，您需要确定目标（用户和设备）、流量和工作流，因为这些需要体现在您的策略中。例如，谁将有权访问特定资产，以及允许他们对这些资产做些什么。应用最小权限原则。

微隔离并不意味着放松密码策略或固件更新等其他安全策略。需要对个别能力进行评估。这些设备能否支持基于证书的身份验证?是否有管理工具来允许颁发和应用这些证书?需要什么流量?您可能需要从制造商处获取这些信息，但也应该将其与自己的流量分析报告进行对比。如果发现不符合公司策略的资产，就需要制定补救计划来使其符合规定，或者需要实施其他的控制措施。

第三步：计划

在这个阶段，您已经了解了资产、目标（用户）、流量和工作流。现在，您需要将这些信息转化为身份验证和安全策略，以实施所需的微隔离架构。如前所述，为了达到最佳效果，您应该将宏隔离和微隔离结合使用。请记住，在大多数改造项目的场景中，您将受到现有架构的限制。

对于宏隔离，可以使用 VLAN、VRF、SPB VPN、VXLAN 或 GRE 隧道等多种选项，也可以使用私有 VLAN 等特殊功能。每种方法都有其各自的优缺点，适用于不同的情况。对于微隔离，您需要知道每个用户或设备类型的配置文件中要包含哪些策略。最后，您需要定义如何将用户和设备映射到其网段和策略。这可以归结为身份验证或分类，其中可以包括设备指纹识别。

理想情况下，您应该投资于允许您创建灵活身份验证策略的技术（软件定义的隔离），以便轻松更新网络配置文件。

我们建议您按以下顺序设计身份验证流程：

1. 使用 RADIUS 服务器通过 802.1x 证书进行身份验证。身份验证生成身份验证记录。这是可以与防火墙共享的信息。
2. 如果您无法通过 802.1x 证书对设备进行身份验证，就应该尝试 MAC 身份验证。MAC 身份验证远不如 802.1x 身份验证安全，但总比没有身份验证好。使用 MAC 身份验证，直到准备好升级到 802.1x 身份验证。
3. 如果没有返回配置文件，则可以尝试进行指纹识别，还可以使用指纹识别映射到配置文件段和规则。这不会生成身份验证或账号记录，但会在物联网明细数据库中记录。
4. 最后，如果没有返回配置文件，或者其他所有操作都失败了，则可以使用默认的“全面拦截（catch all）”。在出现此情况的初期阶段，您仍然需要将设备映射到某个配置文件，引导向与配置文件相符的相同网段和规则并将设备记录在设备明细数据库中。

这个流程应该以一种灵活的方式进行结构化，以便您可以根据进度进行调整。例如，您可能希望首先删除 MAC 身份验证，从明细清单报告中获取 MAC 地址列表后再添加。例如，在完善优化流程时，可以将与默认配置文件关联的网段和规则更改为只允许访问一个堡垒主机的超严格规则。

您可能还希望与防火墙共享设备角色，以便防火墙规则可以基于设备角色，而不仅仅是基于子网/IP 地址。这种集成有两方面的优点。首先，防火墙可以对这些物联网设备应用精细化策略。其次，防火墙策略现在是基于用户或角色的，因此不再与子网或 IP 地址绑定，这使得未来可以设计和隔离网络。

这个过程将是反复的，在使用身份验证和隔离方面更加成熟时，就需要进行调节、调整和完善优化。

第四步：模拟

无论您做了多少计划，都不可能一次就做好。如果身份验证方案设计出现任何错误或安全策略“允许列表”有任何遗漏，业务流程都将中断。您需要以“失效开启”模式应用身份验证和访问策略。也就是说，网络仍然允许未通过身份验证的设备和用户，并且仍然允许意外的流量。但所有这些都将被记录下来，并且可以使用这些日志来改进身份验证和策略方案。

第五步：执行

经过一些微调后，您将不再看到身份验证失败或合法流被拒绝的信息。然后，您可以将这些策略从“失效开启”移到“失效关闭”，这意味着恶意设备将被阻止，意外流将被丢弃。

不言而喻，您将需要继续监控意外的设备和流量——必要时重复整个过程。

其他注意事项

我们建议您也投资一个外部入侵检测系统（IDS），作为持续监控、日志记录和隔离的一部分。尽管交换机本身可以直接识别一系列分布式拒绝服务（DDoS）攻击，但外部入侵检测系统还可以检测到更广泛的攻击，如病毒或其他异常情况。您可能还记得几年前，多个视频监控摄像头被 Mirai 恶意软件感染，也就是这些设备对全球 DNS 服务器发起协同攻击的那一天，这些攻击影响了 Twitter 、Spotify 或 Paypal 等服务。您的交换机可能无法检测到这些攻击，但专用的入侵检测系统肯定会检测到。

一旦检测到攻击，入侵检测系统将通知您的网络管理系统（NMS）受影响设备的 IP 地址。理想情况下，您的网络管理系统将能够在其数据库中找到这些设备，并将其配置文件更改为“隔离对象（quarantine role）”。

“隔离对象”是限制性很强的角色，通常只允许与堡垒主机通信，因此可以通过设置强密码或更新其固件等方式修复设备。

为什么选择 ALE?

阿尔卡特朗讯企业通信数字化时代网络解决方案将稳健灵活的软件定义隔离与动态 DPI NAC 策略相结合，允许逐步向零信任架构发展演进。

数字化时代网络是阿尔卡特朗讯企业通信的发展蓝图，使企业和组织能够进入数字化时代并发展其数字化业务。这基于三大支柱：

- 一个自治型网络，能够轻松、自动和安全地连接人员、流程、应用程序和对象。ALE 自治网络基于精简的产品系列，并配有真正统一的管理平台，在 LAN 和 WLAN 中提供通用的安全策略。自治网络可灵活部署于室内、室外和工业环境。网络管理可以在本地、云端或混合部署的方式提供，具体取决于客户的偏好。
- 安全高效地接入物联网设备：隔离功能将设备保持在其专用的分段中，并将设备和网络受损的风险降至最低。物联网隔离可以帮助企业轻松、自动地了解设备运行是否正常，并有助于保持网络安全。
- 业务创新，通过工作流自动化实现：将用户、应用程序和物联网指标与地理位置数据实时集成到协作平台，简化了新的自动化数字业务流程和服务的创建和推出，包括在出现任何违规行为时通知安全和网络管理员。

您是否有创建物联网/设备清单库的工具？您是否有可以监控应用程序流的工具？您当前的交换机和无线接入点是否已准备好进行软件定义的隔离？如果您目前没有这些工具，请与我们联系，我们愿意助您一臂之力。

已知的事实

我们来总结一些关键要点：

- 要获得真正高效的零信任架构，必须将宏隔离和微隔离结合使用
- 零信任架构有五个步骤：监控、验证和评估、计划、模拟和执行
- 基于微隔离的零信任架构依赖于三大支柱：身份验证（802.1x EAP-TLS 是黄金标准）；与用户或设备角色相关的差异化策略（这些策略可以追溯到最小权限原则）；以及持续监控和隔离
- 在混合和移动环境中，微隔离必须是软件定义的，也就是说，它必须是动态且基于策略的，而不是静态定义的，否则就不切实际

通过微隔离升级到零信任架构是一个过程，任何规模的企业都无法在一个升级换代周期内完成。但在每次升级换代、重新设计或持续改进周期中，如果您实施了正确的基础架构和设计就可以更接近这个目标。

阿尔卡特朗讯企业通信致力于开发网络技术和解决方案，帮助企业通过数字化转型发挥其业务潜力。

Alcatel·Lucent Enterprise