AKAMAI 解决方案简介

通过分段实现用户身份访问管理

现代混合数据中心的额外关键控制层

要减少当今 IT 环境的攻击面，企业需要做的不仅是为特定应用程序创建严格的控制措施、对其实施隔离，使其免受危害。这些做法作为一些初始的举措确实很重要，在某些应用场景中也非常有用，比如入侵控制或合规保证。但是，如果没有支持用户身份访问管理的分段解决方案，企业就会存在安全盲点，难以监测使用或进入企业网络的每一个人。

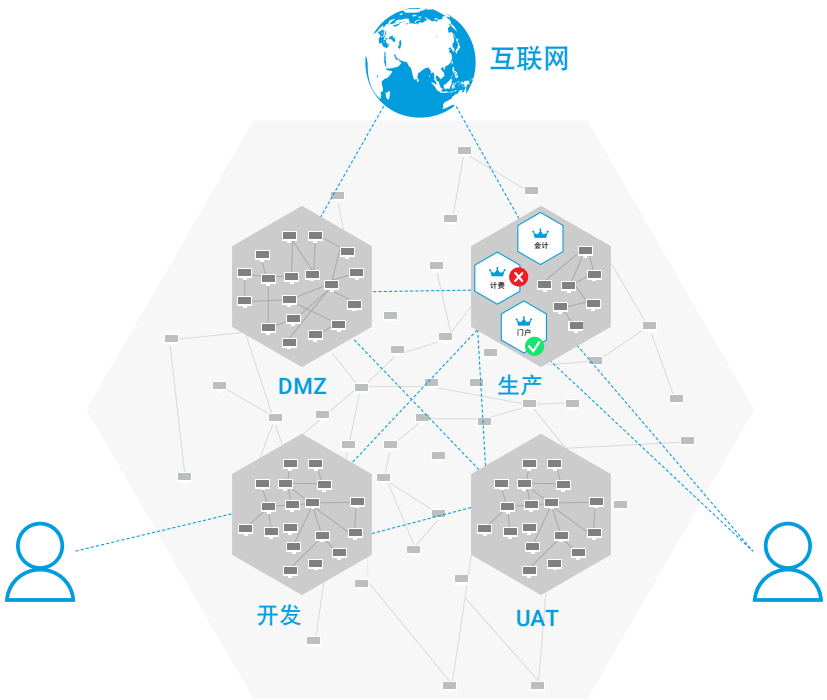
在实施应用程序分段之后，下一个重要步骤就是利用分段解决方案，创建策略来规定谁能访问这些应用程序，确保这些应用程序在整个网络的所有架构（不论属于何种类型）都同样安全无虞。

应用场景：用于管控用户身份访问的分段

管理用户访问权限

利用 Active Directory 用户组，Akamai Guardicore Segmentation 可管理用户从任何环境对任意应用程序或工作负载的访问。特定用户组可以通过特定端口或进程访问特定服务器，而其他用户组则不具备这种权限。用户组拥有自己的权限，管理员可以阻止此外的全部访问权限。由于不需要中央防火墙，您可以在特定网络分段的工作负载之间使用精细的访问控制。

用户访问控制



为什么要针对用户访问控制实施分段？

随时随地控制用户访问
相应策略将应用于笔记本电脑、台式机、VDI、虚拟或裸机服务器以及云基础架构

软件定义的分段
不需要更改网络或架构、不需要布线、不需要服务器停机，也不需要重启系统

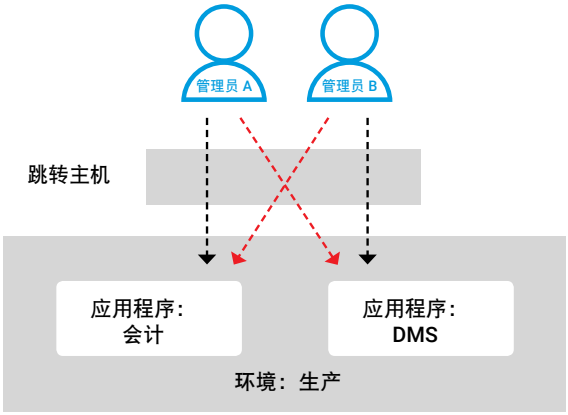
快速且强大
策略创建简单直观，无论对新会话还是活动会话，均会立即生效

成本效益出色
与使用传统跳转主机基础架构的类似应用场景相比，成本最多可降低 60%

Akamai

妥善处理同步用户访问

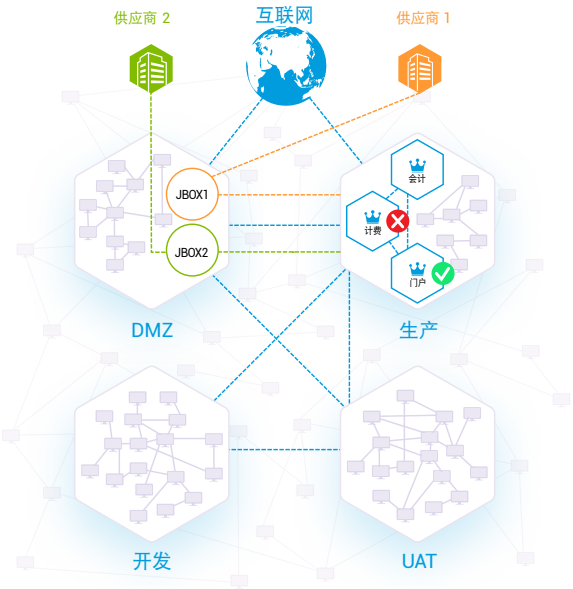
管理员可以通过同一跳转主机或终端服务器访问不同的应用程序，即使多位管理员同时登录时也不例外。与此同时，不同的策略将无缝工作，允许一个用户访问其有权访问的内容，同时阻止另一个用户，保证任何用户自己的服务或访问都不会发生中断。



控制第三方访问

基于用户身份，Akamai Guardicore Segmentation 可控制第三方访问管理，例如外部供应商或 SaaS 提供商的访问管理服务。借助用户组，每个第三方连接都可以针对数据中心和特定应用程序定义自己的访问策略，允许用户按自身角色的需求获得访问权限，而且不会获得多余的权限。

第三方访问控制



应用程序分段和用户身份访问管理强强联手，为保护现代企业数据中心打出了一记有力的“组合拳”。

想了解这些方法如何协同运作？请联系我们的专家。

扫码关注，获取最新CDN前沿资讯