利用 *Palo Alto Networks* 实施零信任的最佳实践

9.1

techDOCS paloalto NETWORKS

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- To ensure you are viewing the most current version of this document, or to access related documentation, visit the Technical Documentation portal: docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page: docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

December 18, 2019

Table of Contents

零信任最佳实践

本文档介绍什么是零信任策略，以及如何在您的网络中使用五步部署法来实施该策略。该方法可以指导您确定关键保护面，映射关键事务流，构建零信任网络，创建零信任策略和维护部署的最佳实践。具体部分包括 Palo Alto Networks 提供的详细信息链接，其中包括如何配置新一代防火墙（物理和虚拟）以及 Palo Alto Networks 防止数据泄露的安全能力。

- 什么是零信任，为何需要零信任？
- 零信任观点
- 五步实施法
- 零信任资源

什么是零信任，为何需要零信任？

零信任是一种业务驱动的战略方法，根据对特定业务来说重要的内容，可以在保护面中保护最关键的数据、应用程序、资产和服务 (DAAS) 以及用户。零信任策略与基础设施无关的，因此，您可以将其应用于所有物理和虚拟位置 — 网络、公共云、私有云和端点。零信任背后的概念很简单：信任就是一种漏洞。在数字环境中，一切（数据包、身份、设备或服务）不可信，一切需要验证。数字世界不存在绝对信任。

该策略的实施不可能一蹴而就，因为每个环境和保护面都可能不同；而且，随着业务的变化，目标和 DAAS 元素也会发生变化。策略是特定于业务的，而安全策略特定于保护对您的特定业务重要的资产。

零信任策略的目标是从网络中消除信任。消除信任有助于防止数据泄露，通过自动化和减少规则库可简化操作，还可以简化法规遵从性和审核，因为零信任环境是为遵从性和易于审核而设计的。

零信任观点

理解零信任后，您就会看到信任的本质 — 一种容易被攻击者利用的漏洞。攻击者可以窃取凭证，欺骗数据包头中的信息甚至“受信任”的员工或合作伙伴。Edward Snowden 是一位值得信赖的用户，他的防病毒软件和工作站上的补丁级别都符合要求。他还使用了多重身份验证。但是，没有人关心他在网络上的位置或者他生成的数据包，因为他是一位值得信任的用户，所以他可以探索网络，找到并泄露敏感数据。我们得到的教训是，数字信任的结果是数字背叛；不要信任任何身份、应用程序或数据。如果采用零信任观点，则：

- 将安全性与业务功能保持一致，因为业务功能决定需要保护的资产。
- 当他们访问资源时，检查并记录第 7 层的所有数据包。
- 以安全的方式访问所有资源，不论其位置如何。
- 在所有位置应用一致的安全策略。
- 集中管理安全和分段策略。
- 适应业务变化时发生的变化。

信任是通过实现零信任策略来避免的一个失败点。

零信任高级最佳实践

下面的最佳实践可以帮助您将网络转换为零信任架构：

- 在构建零信任环境之前，先定义您想要的业务结果。零信任模型支持并帮助您实现安全业务功能。
- 从内到外（而不是从外到内）设计，先保护对您的企业最有价值的资产。您最有价值的资产更可能位于您的数据中心内，而不是在您的边界。
- 使用集中管理的集成平台来降低总拥有成本，而不是使用不能在一起良好协作的单点产品集合。Palo Alto Networks 在平台元素之间共享信息，并通过使用 Panorama、GlobalProtect 和 Prisma Access 实现集中管理和简化操作，从而在所有位置提供一致的策略、预防和保护。
- 使用 Palo Alto Networks 新一代防火墙作为分段网关，在一个平台上整合安全技术，并使用 App-ID、User-ID 和 Content-ID 在第 7 层的所有位置应用一致的安全策略。分段网关根据应用程序、用户和数据对网络进行分段和控制，并且应提供精细的访问控制，保护所有的流量，因为它会穿过微边界并获得访问保护面的权限。

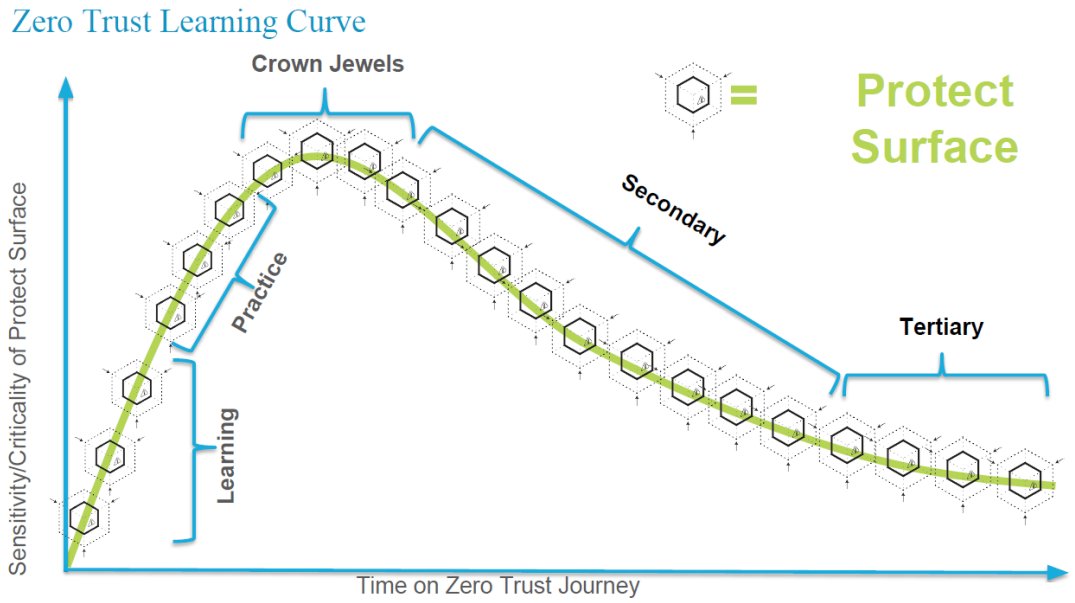
  您不需要更改基础架构来创建微边界，因为在第 7 层策略中创建微边界的方法是只允许经过授权的用户访问他们出于业务目而需要访问的保护面。
- 根据对您的业务有价值的资产分段网络，防止未经授权的横向移动。
- 应用最低权限访问保护面原则。确定谁需要访问什么资源，如何访问以及何时访问。仅允许每个用户和设备所需的准确访问级别，声明标识（包括适当的授权），然后将第 7 层策略映射到标识。
- 解密、检查和记录通过第 7 层的每个数据包，即法规、遵从性和您的业务实践允许您检查的数据包。您必须检查和记录第 7 层的流量。请记住，每一位攻击者都知道如何绕过第 3 层和第 4 层的安全控制。
- 为标记工作负载创建分组对象的策略并动态注册标记，从而帮助您自动实施安全策略。
- 在制定策略和设计网络时，开发运营、维护和不断更新预防控制的流程。记录流程，教育并培训人员，设置基线，并根据基线衡量进展。
- 逐步过渡到零信任环境，一次只过渡一个部分，从一个或多个非关键部分开始，并从中学习和积累经验。零信任分段与旧分段共存，因此，您可以使用安全的迭代方法，而不是危险的“推到重来”方法。

当应用程序的重要性降低时，您可以减少保护措施。例如，您不需要对聊天应用实施同样的保护，但需要对商业关键应用实施。与业务负责人协作有助于确定最需要保护的应用程序。

如何开始实施零信任？

通过教育和合作开启零信任安全之旅。您以及其他要确定什么对您的业务有价值以及如何保护它的利益相关者需要理解零信任的概念、原则和目标。

1. 建立零信任卓越中心这是一个由业务领导（业务和技术决策者）、IT、信息安全、基础设施、应用程序开发人员以及其他利益相关者共同组成的跨职能团队。该团队定义和识别每个保护面以及组成每个保护面的数据、应用程序、资产和服务（DAAS 元素）。他们为您的业务优先考虑最有价值的保护面，计划并实施零信任策略。当业务发生变化时，该团队继续参与部署的维护。业务负责人可以说明期望的业务结果，法规遵从性要求和业务资产的价值。
2. 参加零信任研讨会，让每个人做好准备，让所有站在同一立场上。如需详细信息和安排研讨会，请联系 Palo Alto Networks 销售代表。
3. 按照五步实施法映射要构建的分段网络。
4. 从一个或多个易于理解的低风险（对业务运营来说非关键的部分）小分段开始过渡，从经验中学习。不要从关键资产开始。接下来，通过一个或多个练习分段测试学习情况。如果您觉得已经准备就绪，请将最重要的业务保护面（构成保护面的 DAAS 元素）置于零信任微边界，即每个保护面一个微边界。然后，将下一组最有价值的保护面过渡至零信任，以此类推。



五步实施法

实施零信任策略的五步部署法会提供清晰的逻辑路径来帮助您保护环境、应用程序、资产、服务和用户。应用此方法的方式取决于要保护的资产以及业务需求（对您的业务至关重要的资产），但是您努力的结果是相同的：

- 有效分段网络，有效防止横向移动。
- 保护业务关键数据和系统免受未经授权的应用程序和用户的访问。
- 保护业务关键型应用程序免受未经授权的访问和使用。
- 无缝跨网络、云和端点执行策略，以简化管理并在任何位置应用一致的策略。

无论您是在云中、私有网络上还是在端点上实施零信任策略，该五步法都有效，而与基础设施无关。

第 1 步：定义保护面

保护面是对您的业务有价值的资产边界：为了确保业务正常运营而需要提供保护的数据、应用程序、资产和服务 (DAAS)。通过定义保护面，您可以专注于防御对业务真正重要的资产，而不需要努力识别和保护整个攻击面或只关注边界。保护面也比攻击面或边界小得多，所以更容易保护。

根据对业务最重要的 DAAS 元素，定义您的保护面：

- 数据 **(D)**。需要保护什么数据？想一想您的哪些数据有知识产权，例如专有代码或流程、个人识别信息 (PII)、支付卡信息 (PCI) 和个人健康信息 (PHI)，如《健康保险可携性和问责法案》(HIPAA)。
- 应用程序 **(A)**。哪些应用程序使用敏感信息？哪些应用程序对您的业务职能至关重要？
- 资产 **(A)**。哪些资产最敏感？可能包括 SCADA 控件、POS 终端、医疗设备、制造设备和关键服务器组，具体取决于您的业务。
- 服务 **(S)**。攻击者可以利用哪些服务来破坏 IT 运营并对业务造成负面影响，例如 DNS、DHCP 和 Active Directory？

每个关键 DAAS 元素都是保护面的一部分（或者在某些情况下就是保护面）。例如，如果您的业务提供医疗保健服务，则个人健康信息 (PHI) 对您的业务至关重要。数据是患者信息。应用程序是用于访问 PHI 数据的应用程序 — 例如，EPIC。资产是存储数据的服务器和生成 PHI 的设备，如医学扫描仪或医生工作站。服务是用于访问数据的服务，如单点登录服务和 Active Directory。

按照五步部署法操作时，您要将每个保护面放在其微边界中（按 Palo Alto Networks 充当分段网关的物理或虚拟新一代防火墙分段），以便精确控制可以访问该元素的用户、访问方式和访问时间。以适合保护面的方式保护每个保护面。与包含具有不同访问需求的用户需要访问的 DAAS 元素的广泛边界相比，微边界更易于管理和防御。同时，它可以将保护措施移至更靠近关键数据的位置。

根据企业运营的关键因素，确定需要保护的资产的优先级。最有价值的资产往往在数据中心或云中。在一个或多个非关键保护面上实现零信任以积累经验后，您可以开始保护最关键的保护面。开始时，您可能不了解数据中心内的所有应用程序，但您了解最关键的应用程序。然后，继续为保护优先级列表上的下一组保护面实施，以此类推，继续浏览列表，直到达到安全目标。

使用以下工具可获得对网络流量的可见性，帮助您识别构成最关键保护面的 DAAS 元素：

- 团队的业务知识。例如，业务领导可以谈论应用程序的战略价值。
- 以 Virtual Wire (vwire) 模式透明地将一个或多个新一代防火墙插入您的网络中，这是一种透传模式，不需要更改拓扑结构（因为 vwire 接口没有 IP 或 MAC 地址）即可获得可见性。检查流量日志以查看和分析网络流量。如果您的网络中有受管防火墙，请使用 Panorama 日志。

- 在 Cortex Data Lake 中查看日志，并使用第三方资产发现工具。该工具与 Palo Alto Networks 的集成合作伙伴之一提供的 Cortex 配合使用。
- 使用 Prisma SaaS 发现用户、资产和 SaaS 应用程序的资产，并获得对这些应用程序的可见性。
- 如果在新一代防火墙或管理防火墙的 Panorama 上运行 PAN-OS 9.0，请使用策略优化器来帮助确定现有安全策略规则中的关键应用程序。（策略优化器甚至会显示基于端口的规则中的所有应用程序。）如果无法使用策略优化器，请使用 Expedition 获取对应用程序的可见性。
- 用于自动发现应用程序依赖性的应用程序依赖性映射工具（应用程序使用的资源，如数据库、负载均衡器、服务器等）。

第 2 步：映射保护面事务流

在关键 DAAS 元素和用户之间映射事务流（交互），了解它们的相互依赖关系 — 谁有业务原因访问各元素，以什么方式以及在什么时间访问。映射事务流以了解和构建网络。映射可帮助您了解如何创建只允许授权用户使用指定应用程序访问特定数据和资产的安全策略（最低权限访问原则）。

映射事务流的方法许多，一些定义保护面的技术也适用于映射其事务流：

- 如果您有现有的流程图，则可以直接利用（遵从性和审核有时要求企业创建流程图）。
- 与应用程序、网络和企业架构师以及业务代表合作，了解应用程序的目的，以及架构师和业务代表设想的事务流。
- 在网络中以 virtual wire (vwire) 模式透明地插入一个或多个新一代防火墙，以获得对流量的可见性。检查流量日志以查看和分析流量。
- 使用 Palo Alto Networks 集成合作伙伴的第三方工具。
- 使用 Cortex Data Lake 的登录信息获取对映射事务流的可见性。Cortex Data Lake 会汇总来自新一代防火墙、VM-Series 防火墙、Prisma Access 和 Traps 的日志。
- 对于应用程序，映射工作流，包括跨网络的应用程序数据流，每个应用程序所需的计算对象以及使用每个应用程序的人员。
- 对于数据，找出谁使用数据，在何处收集、存储、使用和传输数据，以及数据在使用后如何存储、加密、存档或销毁。
- 对于资产，找出资产的位置，谁使用资产，何时使用资产，以及资产适合在何处融入工作流。
- 对于服务，映射整个环境中的服务工作流。

除了揭示谁在何时何地使用了哪些应用程序之外，映射事务流还提供精细的可见性，以帮助进行灾难恢复规划和实现遵从性。它还让您可以优化工作流，以及检查谁有合法的业务理由访问各保护面中的 DAAS 元素。

了解通过网络的事务流后，您就知道如何对网络分段以及在何处插入控件，因为您将了解谁使用各保护面，如何使用，位于何处，以及通过与哪些元素交互来启用关键应用程序。

第 3 步：构建零信任网络

凭借对保护面和事务流的理解，开始基于对您的业务有价值的资产来构建零信任网络。从内向外构建在第 1 步：定义保护面中识别的业务关键型保护面。在开发架构时，要注意操作和维护的方便性，以及适应保护面和业务变更的灵活性。运行最佳实践评估工具以设置最佳实践配置基线，并衡量零信任目标的实现进度。

该架构的基石是分段网关 — 连接您的网络分段并执行第 7 层策略的 Palo Alto Networks 物理或虚拟网络新一代防火墙。通过一个分段网关运行所有的流量，将分段网关放置在离其保护的资源尽可能近的位置，并将其与其他 Palo Alto Networks 网络功能结合使用，从而尽可能实现自动化。新一代防火墙：

- 在第 7 层策略中，为每个保护面创建一个微边界。这样可以阻止横向移动，因为微边界为谁 (User-ID) 以什么方式 (Content-ID) 以及在何时通过分段网关访问什么应用程序 (App-ID) 和资源提供了精细的策略控制。根据事务如何在网络中流动以及用户和应用程序如何访问数据和服务进行分段。
- 将进入和退出保护面的所有流量的安全功能聚合到一个控制点。分段网关应该执行策略，解密加密流量，并应用保护措施，例如：
    - DNS 安全（使用 DNS 安全服务，从而提供多种实时威胁情报来源，无限扩展的 DNS 请求实时分析以及先进的 DNS 签名）。

    - 入侵防护（漏洞防护、防间谍软件和防病毒软件配置文件）。
    - 阻止潜在危险文件类型。
    - 阻止未知和 1 日威胁 (WildFire)。
    - URL 过滤。
    - 数据丢失防护 (DLP)。
- 实时解密和检查第 7 层的流量。
- 记录从第 2 层到第 7 层的每个数据包。从受管防火墙的 Panorama、个人防火墙（非 Panorama 管理的防火墙）、Prisma Access（以前称为 GlobalProtect™ 云服务）以及 Traps 将日志发送到 Cortex Data Lake，从而为物理和 VM-Series 防火墙集中和聚合本地部署以及虚拟（私有和公共云）日志存储。
- 使用 API 实现与合作伙伴的第三方防御工具紧密集成。
- 检测事件并自动响应的自动化反馈循环。
    - 标记工作负载并使用标记作为过滤条件来确定安全策略中动态地址组的成员。这样可以根据 HTTP(S) 服务器日志转发事件自动执行操作。日志转发事件通过动态添加或删除安全策略中实时使用的动态地址组的成员来触发该操作。安全策略决定是允许还是拒绝动态地址组的成员访问，并通过防火墙执行操作。例如，在防间谍软件安全配置文件中执行 DNS Sinkhole，从而自动隔离尝试访问该 Sinkhole 的可能被入侵的系统。使用标记和日志转发从动态地址组动态添加和删除这些系统。该动态地址组附加到一个策略规则，而该策略规则会阻止和记录所有传送到 Sinkhole 的流量。随后，当收到日志警报通知时，您可以调查可能受到入侵的系统。
    - 使用 Cortex XDR 自动分析您的网络，发现表明可能存在入侵的异常行为，并针对该行为发出警报，以便调查和纠正问题。Cortex XDR 提供对网络流量的可见性，通过关联日志简化威胁调查，并让您能够识别警报的根本原因和立即做出响应。使用 Cortext XDR API 来与 Demisto 集成，使用为您的业务流程定制的 Desmisto 响应剧本实现自动响应，从而将响应时间从几天缩短到几分钟。
    - 使用 WildFire 自动发现新恶意软件。当 WildFire 在全球任何位置发现恶意软件时，最多只需五分钟，WildFire 便可以更新您的安全配置文件，从而为您提供保护，防范新恶意软件。
- 使用 Panorama 中的模板和模板堆栈实现自动策略部署。
- 使用 Ansible、Terraform 和 Python 之类的工具自动处理、编排和加速保护 Prisma Cloud 部署。

Palo Alto Networks 使您能够构建零信任环境，并在所有位置应用一致的安全保护：

- 与单独管理防火墙相比，Panroma 为多个新一代防火墙集中管理策略控制，提高了操作效率。
- 公司网络和数据中心：使用新一代防火墙将网络划分为保护面的微边界。
- 公共云：在云环境中使用 Prisma Access（利用本地部署或 VM-Series 新一代防火墙）和 Prisma Cloud（基于 API 的云基础架构安全解决方案）实施零信任策略。虚拟私有云 (VPC) 定义保护边界，从而分段工作负载。
- 私有云：使用 VM-Series 防火墙实施零信任策略。
- 分支机构和移动用户：使用 Prisma Access 提供基于云的安全保护，避免来回访问公司网络资源。配置适用于用户的 Prisma Access和适用于网络的 Prisma Access 以保护分支机构。

  或者，将本地部署新一代防火墙与 GlobalProtect 订阅服务结合使用，从而将安全策略和实施扩展到远程用户以及分支机构。
- 端点：为分段使用新一代防火墙，以及第一层保护，并为第二层保护使用 Traps。使用 GlobalProtect（本地部署安装）或 Prisma Access（使用 Panorama 安装，并在云中进行管理）VPN 执行一致的策略，从而将策略扩展到远程端点，并让策略与用户一起移动。在移动用户端点上，Prisma Access 需要 GlobalProtect 应用。在所有情况下，请在受管端点上安装 GlobalProtect 应用，并在非受管端点上使用 GlobalProtect Clientless VPN。所谓非受管端点，就是您无法或不希望安装客户端（如合作伙伴系统或个人设备）的端点。如果适合保护高价值资产，则应用多重身份验证。
- SaaS 应用程序：使用 Prisma SaaS 扫描、分析、分类和帮助保护 SaaS 应用程序。通过新一代防护墙为非受管设备转发 SaaS 应用程序流量（受管设备的流量直接通过 Prisma Access、GlobalProtect 或新一代防火墙）。

第 4 步：创建零信任策略

零信任策略由白名单规则组成 — 这些规则只允许授权用户在正确的时间和位置使用指定的应用程序访问特定的资源。如果流量不符合规则，防火墙会自动阻止流量。这一点很重要，因为：

- 了解希望允许哪些应用程序来支持您的业务，比识别和阻止不希望允许的所有应用程序的无休止任务容易得多。
- 所有入侵和恶意活动都发生在允许规则上。将安全重点放在允许的流量上，并且只允许业务所需的流量。

零信任策略基于 Kipling 方法。回答 Rudyard Kipling 的六个问题“谁、什么、何时、何地、为何以及如何”，对于是允许还是阻止流量，以及如何创建安全策略来保护每个表面，您就会知道如何决定。Palo Alto Networks 提供了在安全策略中实施 Kipling 方法的功能：

- 谁应访问资源？
  - 在策略中，通过 User-ID 可以识别用户，并让您控制谁可以访问资源。利用最小权限访问策略（谁需要知道？），只允许有合法业务理由进行访问的个人、组和设备访问资源。
  - 当用户尝试访问资源时，创建身份验证策略来验证用户的身份。身份验证策略还确定是否需要多重身份验证 (MFA)。
  - 在防火墙允许访问敏感服务、应用程序和资源之前，除了要在强制网络门户中输入密码，至少要要求另外使用一个身份验证因素（例如，发送到手机或电子邮箱的一次性使用代码）进行身份验证（即 MFA），从而保护敏感服务和应用程序。对于远程用户，配置 GlobalProtect 来提供 MFA 通知（还必须在防火墙上配置 MFA）。
  - 对于使用 GlobalProtect 的设备，通过配置主机信息配置文件 (HIP) 来定义主机的访问策略，在这些主机上执行策略，并阻止不符合安全和维护标准的设备访问资源。例如，您可以使用 HIP 来确保已启用加密的端点，主机的防病毒签名是否最新，等等。如果主机不符合 HIP 要求，安全策略会阻止访问。
- 使用什么应用程序访问资源？
  - 使用 App-ID 创建基于应用程序的第 7 层策略。该 App-ID 用于识别应用程序（与端口、协议或规避策略无关），从而在您的网络上仅允许正确的应用程序。基于第 3 层和第 4 层的策略要依赖 IP 地址，而攻击者可以通过 IP 地址来欺骗该策略，让端口对规避应用程序开放。
  - 应用程序默认的服务，从而在默认端口上安全启用应用程序，并阻止规避应用程序通过非标准端口访问您的网络。
  - 如果是运行 PAN-OS 9.0 或更高版本的防火墙，或者如果管理防火墙的是运行 PAN-OS 9.0 或更高版本的 Panorama 设备，请使用策略优化器检查现有策略（包括基于应用程序的规则和基于传统端口的规则），识别未使用的规则并识别具有未使用的应用程序的规则。对于运行旧版本 PAN-OS 的防火墙，请使用 Expedition 检查策略规则。如果需要将旧版配置迁移到 PAN-OS 设备，请按照迁移到基于应用程序的策略的最佳实践操作。
- 用户何时访问资源？

  对于用户仅在特定时间段内访问的应用程序，请将计划（在 Panorama 设备和防火墙上，访问**Objects**（对象）> **Schedules**（计划））应用到策略规则，从而阻止工作时间外的可疑访问。为了减少被发现的机会，对手经常在正常工作时间之外攻击并试图窃取数据。
- 资源位于何处？

  将目标资源的位置添加到策略中。在适当时，还要限制流量的来源（区域和 IP 地址）。
- 为何访问数据 — 如果丢失，数据有何价值（负面影响）？

  对数据进行分类以了解其负面影响 — 为何数据值得保护？如果攻击者泄露了数据，您必须披露损失吗？设置数据过滤以防止敏感信息离开网络，并使用数据分类工具提供关于数据的元数据。了解数据的负面影响可以帮助您确定如何保护数据，在使用后要对数据采取哪些措施，以及如何在策略中标记数据。
- 如何允许访问资源？

  应用 Content-ID 和最佳实践来防范应用程序流量中的威胁：

- 对安全策略采用最小特权访问原则。只允许具有合法业务理由的用户在适当的时间以适当的方式访问他们因业务目而需要访问的应用程序。
- 记录通过第 7 层的所有内部和外部流量。防火墙策略规则默认已启用。将日志转发到 Cortex Data Lake（或 Panorama 或日志收集器）以合并日志，从而更轻松地进行彻底分析。
- 对所有本地和远程用户，跨所有位置（网络、云、端点）一致地应用策略和威胁预防，这样，对于所有应用程序和所有资源，无论用户在何处，策略都可以跟随用户。不一致的策略会增加漏洞，且难以理解和维护，还可能对遵从性需求和审核产生负面影响。使用物理新一代防火墙和虚拟 VM-Series 防火墙作为分段网关，在网络和云中应用一致的零信任、第 7 层和 Kipling 方法策略。使用 Prisma Access（云）和 GlobalProtect（本地部署安装和使用 Prisma Access）将一致的零信任策略扩展到端点。对于非受管端点（您不想或不能在其上安装客户端的端点），请使用 GlobalProtect 无客户端 VPN 来应用一致的策略。创建并重新使用 Panorama 模板和堆栈在所有相似位置应用一致的策略，如数据中心或边界。
- 配置安全配置文件（IPS 的漏洞防护配置文件、防范包括 1 日恶意软件的防病毒和 WildFire 配置文件，阻止命令和控制威胁的防间谍软件配置文件，阻止或警报风险文件类型的文件阻止配置文件，以及控制网站访问，帮助阻止网络钓鱼攻击，以及为搜索引擎执行安全搜索的 URL 过滤），并将其应用到所有允许的流量。对于数据中心防火墙和边界防护墙安全配置文件，请遵循最佳实践。
- 使用 WildFire 最佳实践检测和防范零日恶意软件。
- 根据法规和业务要求，使用解密最佳实践解密解密尽可能多的流量，从而检查尽可能多的流量。您无法保护您的网络免受您看不到的威胁。
- 使用 DNS 安全服务为 DNS 签名提供无限可扩展的实时访问，实时分析 DNS 请求以及使用机器学习和预测分析生成的高级 DNS 签名。
- “如何”还包括确定在使用后如何处理敏感数据 — 使用加密、令牌化或屏蔽对其进行抽象，或通过归档进行处置，或将其删除。归档旧数据（在大多数系统上，大约 80% 的数据有两年或两年以上没有被访问过）。
- 使用 Cortex XDR 完善和改进策略。

通过 Kipling 方法，您可以创建适当保护每个保护面的安全策略，因为该方法会引导您了解谁应该访问数据，应该如何访问，何时访问，以及要应用的保护。您可以根据 Kipling 方法制定业务声明，从而开发策略规则。例如：

	谁	什么	何时	何处	为何	如何
方法	User-ID	App-ID	时间限制	系统对象	分类	内容 ID
本地部署	Epic_Users	Epic	任何	Epic_Srvr	负面影响（数据价值高）	解密、检查（安全配置文件），日志流量
云	销售	Salesforce	工作事件	美国	负面影响（数据价值高）	解密、检查（安全配置文件），日志流量

在两种情况下，防火墙都只允许满足 Kipling 方法中的所有条件且通过检查的流量。防火墙会自动拒绝所有不符合允许规则的流量。

除了安全、身份验证和解密策略外，还要使用 DoS 和区域保护最佳实践来保护重要服务器免受 DoS 攻击。

对于未配置的防火墙，使用 IronSkillet 1 日配置模板来实施 *1* 日最佳实践策略，然后调整该策略以最适合您的保护面。

第 5 步：监视和维护网络

安全性是一个迭代过程，因为日志记录和监视可以揭示需要改进的方面，而且您的业务和网络会随着时间的推移而变化。按照您在构建网络时开发的操作流程来维护和不断更新防御控制。

- 解密、检查并记录通过第 7 层的所有流量（内部和外部）
- 从受管防火墙的 Panorama、个人防火墙（非 Panorama 管理的防火墙）、Prisma Access 以及 Traps 将日志转发到 Cortex Data Lake，从而集中和聚合本地部署和虚拟（私有和公共云）日志存储。这为网络流量和保护面提供了可见性。
- 基于来自 Cortex XDR 的情报，更新策略并可能添加新的保护面。Cortex XDR 使用 Cortex Data Lake 数据和机器学习，根据网络的正常行为自动分析网络并识别可能表明存在入侵或其他威胁的异常行为。以不属于保护面的 DAAS 元素为目标的威胁活动可能注重在最初定义保护面时没有考虑到的保表面。
- 使用 Cortex XDR 获得对网络流量的可见性，通过关联日志简化威胁调查，并使您能够识别警报的根本原因和立即作出响应。
- 使用 Cortext XDR API 来与 Demisto 集成，使用为您的业务流程定制的 Desmisto 响应剧本实现自动响应，从而将响应时间从几天缩短到几分钟。
- 使用 Prisma Cloud 聚合并提供配置数据、用户活动信息以及网络流量信息的可见性。Prisma Cloud 分析数据，提供简单和可行的见解。
- 按照应用程序和威胁内容更新的最佳实践，以获得新的和修改过的 App-ID，并保持威胁签名处于最新状态。
- 使用最佳实践评估工具衡量最佳实践配置的进度，并帮助您过渡到最佳实践安全状态。
- 监视网络活动，使用预定义报告和生成自定义报告，从而获得对您的环境的可见性。
- 在网络和业务发展的过程中，让跨职能团队相互协作，帮助维护零信任部署，创建教育和培训计划，确保团队的新成员理解策略和实施方法。
- 随着自动化能力的提高，继续实现自动化操作以及响应。

零信任资源

以下技术文档、白皮书、网络广播、视频和其他资源为您的零信任策略提供了更多信息和上下文。除了本文档中提供的信息和列出的资源外，您还可以让 Palo Alto Networks 专业服务咨询团队的专家来帮助您设计和实施零信任策略。

- 如何构建零信任网络（点播网络广播）
- 零信任实施解密（点播网络广播）
- 零信任概述
- 零信任（Palo Alto Networks 零信任网页）
- 零信任执行最佳实践（过渡路线图）
- 简化零信任实施的五步部署法（白皮书）
- 保护云安全：零信任云安全
- 零信任云安全（视频）
- 零信任的真相（信息图）

Palo Alto Networks 技术文档

过渡到最佳实践：

- BPA 入门
- 如何运行 BPA（视频）
- 理解 BPA 结果（视频）
- Live 社区最佳实践评估页面

最佳实践文档门户：

- 最佳实践入门
- 互联网网关最佳实践安全策略
- 数据中心最佳实践安全策略
- 迁移到基于应用程序的策略的最佳实践
- 确保管理员访问安全的最佳实践
- 应用程序和威胁内容更新的最佳实践
- 解密最佳实践
- DoS 和区域保护最佳实践
- WildFire 部署最佳实践

Expedition

IronSkillet（1 日配置模板）

客户支持

预防状态评估（对您的预防能力的补充性咨询评估）

Palo Alto Networks NextWave 技术合作伙伴