解密最佳实践

Version 10.0 (EoL)

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

October 28, 2020

Table of Contents

解密最佳实践

对于无法发现或检测到威胁，您就无法为您的网络提供防御。据 Gartner 预测，2020 年有 70% 以上的新恶意软件活动会使用各种形式的加密技术。Google 的报告表明，无论如何分析 Google 的网络流量，在大多数情况下，超过 90% 的流量都是加密的。解密流量保护网络免受隐藏的威胁。

本文件是您部署前、部署中和部署后最佳实践的简化检查列表，您可以遵循这些最佳实践来解密。各部分都包含到了 PAN-OS 管理指南里详细信息的链接，包括，如何配置解密策略规则和配置文件。

- 计划您的 SSL 解密最佳实践部署
- 使用最佳实践进行部署 SSL 解密
- 跟踪部署后的 SSL 解密最佳实践

计划您的 SSL 解密最佳实践部署

通过开发一个解密策略和推出计划以准备部署解密。打开解密可能会改变用户与某些应用程序和网站交互的方式，因此，计划、测试和用户教育对于成功部署至关重要。

STEP 1 | 设定目标。

- 根据防火墙资源数量，计划解密尽可能多非私密或敏感流量。这样，通过暴露和防止加密的威胁，可以减少攻击面。了解当地有关流量的法律法规，您可以合法地解密流量和用户通知要求。
- 创建和部署解密策略规则前，把基于端口的安全策略规则迁移到基于应用程序的安全策略规则。如果您创建基于端口安全策略的解密规则，然后迁移到基于应用程序的安全策略，这种改变可能导致解密规则阻止原计划允许的流量，因为安全策略规则可能会使用应用程序默认端口来防止应用程序流量使用非标准端口。在部署解密前迁移到基于 App-ID 的规则可以确保在测试解密部署时，您将发现安全策略错误配置，并在向一般用户发布解密之前将其修复。

STEP 2 | 与涉及（如法律、财务、HR、高管、安全和 IT/ 支持）的利益相关者合作并培训他们制定解密部署的策略。

- 获得解密流量以确保企业安全的批准。
- 识别和区分要解密流量：
  - 决定解密哪些应用程序（已批准、未批准）。不允许加密未经批准的应用程序。
  - 决定解密哪些设备（公司、BYOD、移动等）。

    企业不控制 *BYOD* 设备。如果您在网络上允许 *BYOD* 设备，则对其流量进行解密，并使其服从与应用于其他网络通信量相同的安全策略。为此，可以通过身份验证门户重定向 *BYOD* 用户，指导他们如何下载和安装 *CA* 证书，并清楚地通知用户他们的流量将被解密。培训 *BYOD* 用户有关这个过程，并将其纳入公司的隐私和计算机使用策略。
  - 决定是否要对不同的组（例如不同的雇员组、承包商、合作伙伴和客户）使用相同的解密策略。
- 识别无法解密的流量：
  - 由于技术原因（如证书锁定、不支持的密码或交互认证）导致解密中断的流量。
  - 您选择不解密的流量，如金融、卫生、政府和其他敏感类别，包括用户和管理人员之类的用户组。
  - 完全理解除解密之外的流量。无法看到加密的流量，且防火墙不能对加密流量应用威胁预防配置文件。
- 准备更新的法律和 HR 计算机使用策略，分发给所有员工、承包商、合作伙伴、客人和任何其他网络用户，以便在您解密时，用户能够理解他们的数据可以解密和扫描以便发现威胁。
- 决定如何处理证书验证。您的业务模型可能需要在安全性和用户体验间权衡。了解如何处理证书验证将有助于确定如何配置 SSL 转发代理解密配置文件。
- 识别需要登录的流量。注意当地的法律和法规差异，以及它们如何影响您可以记录的流量和存储日志的位置。

  将防火墙放置在它们可以看到所有网络流量的地方，这样就不会有加密的流量因为绕过防火墙而无意中获得对您的网络的访问。

STEP 3 | 制定一个推广公钥基础设施 (PKI) 的计划。

- 如果您已有 PKI，则可以从企业 根 CA 生成 SSL 转发信任 CA 证书，并将其作为从属证书。这样更容易部署，因为网络设备已信任企业根 CA，所以不会遇到证书问题。如果您没有企业根 CA，可以考虑获取一个。

  或者，在防火墙上生成自签名的根 CA 证书，并在该防火墙上创建从属转发信任 CA 证书，以便安装在网络设备上。自签名证书最适合没有企业根 CA 的小企业以及概念验证 (POC) 试验。

类似于 *BYOD* 设备，企业不控制客户设备。如果您在网络上允许客户设备，则对其流量进行解密，并使其服从与应用于其他网络通信量相同的安全策略。为此，可以通过捕获门户重定向用户，指导他们如何下载和安装 *CA* 证书，并清楚地通知用户他们的流量将被解密。将此过程包括在公司的隐私和计算机使用策略中。

- 为转发信任和转发不信任生成单独的 CA 证书。不要对两个证书使用相同的 PKI 从属 CA，也不要使用受信任的根 CA 签署转发不信任证书！转发不可信证书警告用户签署服务器的证书不合法，并且不应继续访问该站点。如果受信任的根 CA 签署不信任证书，则客户端会信任不应受信任的证书，因为客户端信任根 CA。
- 为每个防火墙生成一个独立的从属转发信任 CA 证书。使用独立的从属 CA，使您可以在解除设备（或设备对）时撤消证书，而不会影响到部署的其余部分，并在需要撤销证书时减少影响。单独的 CA 证书可以帮助技术支持解决用户问题，因为证书错误消息包含了关于所穿越的防火墙的信息。尽管在所有的防火墙上使用一个转发信任从属 CA 更容易部署，但是，在每个防火墙上使用单独的证书安全性最好。
- 如果您的私钥需要更高的安全性，请考虑将其存储在 HSM 中。

STEP 4 | 对防火墙性能进行极限测量，了解资源消耗情况以及可用的防火墙资源，从而在部署解密后对比性能，同时估计所需的部署部署规模，以支持要解密的流量数量。

- 与您的 Palo Alto Networks SE/CE 合作，评估调整防火墙部署大小并避免制定标准的错误。
- 注意当前可用的防火墙资源。通常，安全性越高，解密消耗的资源越多。影响可以解密的流量的因素包括：
  - 要解密的 SSL 流量。
  - TLS 协议版本。
  - 密钥大小。
  - 密钥交换算法。完全向前保密 (PFS) 临时算法（如 DHE 和 ECDHE）比 RSA 消耗的资源多，但可以提供更高的安全性，因为防火墙为每个会话生成新加密密钥。如果攻击者危及会话密钥，PFS 会阻止攻击者使用它来解密同一客户端和服务器之间的其他会话，而 RSA 则不会。
  - 证书认证。RSA 证书身份验证（与 RSA 密钥交换算法不同）比 ECDSA 证书身份验证消耗更少的 CPU 周期，但是 ECDSA 提供了最高级别的安全性。
  - 加密算法。密钥交换算法确定加密算法是 PFS 还是 RSA。
  - 防火墙模型和资源。较新的防火墙模型比旧的模型具有更多的资源。
- 交易的大小影响性能。测量所有流量的平均事务大小，然后测量端口 443 的流量的平均交易大小（HTTPS 加密流量的默认端口），了解防火墙上加密流量相对于总流量和平均交易大小的比例。

这些因素的组合决定了解密如何消耗防火墙处理的资源。如果防火墙资源有问题，对优先级较高和高风险的流量使用更强的解密，并使用更少的处理器密集型解密来解密和检查低优先级的流量，直到您可以增加可用的资源。

调整防火墙规模以包括需要解密的流量的增长空间，因为每天都有更多的流量被加密。

STEP 5 | 计划阶段性的优先部署。

- 识别早期采用者以支持解密，并让部门经理参与计划。
- 设置 POC 来测试部署策略，然后将其发布给一般用户群体。测量解密 POC 部署影响防火墙 CPU 和内存利用率的方式，帮助了解防火墙大小是否正确。POC 还可以显示在技术上破坏解密的应用程序。
  - 教育 POC 参与者关于变更和如何联系技术支持。
  - 为解密 POC 建立一个技术支持POC，以便支持有机会开发支持推出的最佳方法。
  - 解密阶段。计划先对最危险的流量进行解密（URL 类别最有可能包含恶意流量，如赌博或高风险），然后在获得经验时进行解密。或者，先解密不影响业务的 URL 类别（如果出现错误，也不会影响业务），例如，新闻推送。在这两种情况下，解密一些 URL 类别，考虑用户反馈，运行报告并检查解密日志，确保解密符合预期，然后，逐步解密更多的 URL 类别等等。如果由于技术原因或因为选择不解密而不能对站点进行解密，则计划排除解密，将站点排除在解密之外。

- 评估 POC 的成功并微调部署实践。

- 全面推出前教育用户群体。POC 有助于确定重要的通信点。
- 向所有员工、承包商、合作伙伴、来宾及任何其他网络用户分发最新的法律和人力资源计算机使用政策。对每个部门或组施行解密时，确保所有人了解，为了防范威胁，您可以解密和扫描他们的数据。
- 创建现实的时间表，以便有时间来评估每个阶段的推出。

使用最佳实践进行部署 SSL 解密

STEP 1 | 生成和分发解密策略的密钥和证书。

- 如果您有 Enterprise PKI，可以从您的企业根 CA 生成 Forward Trust CA 证书，用于转发代理流量。否则，在防火墙生成自签名的根 CA 证书，在该防火墙创建从属 CA，然后，将自签名证书分发给所有客户端系统。自签名证书可以用于实验室测试、小规模部署和 POC。
- 为每个防火墙生成唯一从属 Forward Trust CA（或者为所有防火墙生成一个 Forward Trust CA，具体取决于您的规划。一个证书更易于部署，但不同的证书可以提供最佳安全性和其他优势）。不同的 PKI 平台具有不同的扩展证书管理功能。
- 如果不使用 Enterprise CA，则将 Forward Trust CA 证书导入到客户端系统的信任 CA 存储区。
- 请勿将 Forward *Untrust* CA 证书导入到客户机系统上的 CA 信任存储区，否则，不可信证书将不作为不可信站点的触发器。（但是，如果在客户端系统上没有将防火墙自签名根 CA 安装为可信发行者安装，则可以使用自签名的 Forward Untrust 证书。）
- 使用自动配置方法将转发信任证书分发到连接的设备，例如 Palo Alto 网络全球保护门户、Microsoft 广告证书服务证书服务（使用组策略对象）、商业工具或开源工具。
- 如果您从企业根 CA 生成证书，则可以在防火墙上导入证书。
- 在安全存储库中备份防火墙的 Forward Trust CA 证书的私钥（不是防火墙的主密钥），以便如果出现问题，您仍然可以访问 Forward Trust CA 证书。
- 如果从企业根 CA 生成证书和私钥，则会阻止导出私钥。（您可以在新防火墙和 Panoramas 上从企业 CA 安装这些私钥，因此无需从 PAN-OS 将其导出。）
- 如果您的计划要求使用 HSM，则将私钥存储在 HSM 上。

STEP 2 | 采用配置解密配置文件的方式来控制协议、证书验证和故障处理。

- 采用SSL 转发代理解密配置文件来控制服务器证书验证、会话模式和出站流量故障检查。使用过期的证书、不可信发行者、不支持的版本和不支持的密码套件会话。除非一个重要的应用程序需要客户端身份验证，否则将阻塞使用客户端身份验证的会话，在这种情况下，您应该创建一个允许客户端身份验证的单独的解密配置文件，并且仅将其应用于需要客户端身份验证的通信。
- 采用SSL 入站检查解密配置文件控制入站流量的会话模式和故障检查。使用不支持的版本和不支持的密码套件进行会话。
- SSL 协议设置为 SSL 转发代理和 SSL 入站检查流量控制密码组元素：协议版本、密钥交换算法、加密算法和认证算法。尽可能利用最强的密码。对于转发代理，将协议**Min Version**（最低版本）设置为 **TLSv1.2**，并将 **Max Version**（最高版本）设置为 **Max**（最高）以阻止弱协议。为 SSL 入站检查，创建具有与您正在检查入站流量的服务器的功能匹配的协议设置的单独配置文件。

  尽可能使用最强大的密码组。创建单独的解密策略和配置文件，最大限度提高安全性。如果因业务目的而需要保留的旧站点仅支持弱密码，则创建一个单独的解密配置文件来允许流量，并且仅对必要的网站将其应用到解密策略中。对于不同的 *URL* 类别，利用同样的技术微调安全与性能。

  许多移动应用程序使用锁定证书。因为 *TLSv1.3* 会加密证书信息，防火墙无法自动将这些移动应用程序添加到 *SSL* 解密排除列表中。对于这些应用程序，请确保将解密配置文件的 *Max Version*（最高版本）设置为 *TLSv1.2*，或者将无解密策略应用到流量。
- 没有解密配置文件控制服务器证书来验证您选择的不解密流量。阻止过期证书和不可信发行者的会话。

  不要将无解密配置文件应用到 *TLSv1.3* 流量。证书信息经过加密，因此防火墙无法基于证书信息阻止会话。
- SSL 转发代理和无解密流量，配置证书撤销列表 (CRL) 和在线证书状态撤销 (OCSP) 证书撤销来检查，验证没有被撤销的站点证书。

- SSH 代理配置文件控制 SSH 通道业务的会话模式和失败检查。使用不支持的版本和不支持的算法进行块会话。

数据中心和周边（Internet 网关）用例的最佳实践解密配置与一般最佳实践设置稍有不同文件设置。

STEP 3 | 配置解密策略规则，以定义要解密的流量，并为您选择不解密的流量创建基于策略的异常。

- 创建策略规则以排除特定目标 IP 地址（例如，财务服务器）、源用户和组（例如，管理人员或 HR 人员）以及您选择不解密的应用程序端口。解密流量规则前，将这些规则置于解密规则库的前面。对于除 TLSv1.3 流量外的所有流量，将一个不解密配置文件附加到流量，从而将 SSL 服务器证书验证控制应用到加密流量。这样可以防止无意中解密您不希望解密的流量。
- 使用 URL 类别、自定义 URL 类别和外部动态列表 (EDL) 指定不解密的 URL，例如金融服务、健康和医疗、政府以及出于业务、法律或监管原因而不希望解密的任何其他类别。在动态更改 IP 地址（例如 Office 365）或频繁更改成员的环境中，使用 EDL 进行更新，但不必提交。

  创建一个 EDL 或自定义 URL 类别，其中包含您选择不对其解密的所有类别，从而只需要一个解密策略规则。

  将这些规则置于解密规则库中解密流量的规则之上。
- 配置解密日志和日志转发。
- 请注意本地隐私规则，如果您使用解密镜像将解密的流量复制并发送到流量收集工具，这些规则可能禁止镜像或控制您可以镜像的流量。
- 通过配置 SSL 转发代理、SSL 入站检查和 SSH 代理，创建策略来解密其余的流量。始终解密在线存储和备份、基于 Web 的电子邮件、Web 托管、个人站点和博客、内容传递网络和高风险 URL 类别。将 SSH 代理限制为管理网络设备、记录所有 SSH 流量的管理员，并且配置多因素身份验证来防止未经授权的 SSH 访问。

STEP 4 | 在 POC 测试期间，如果站点从技术上破坏了解密，并且不在排除列表中，请将站点添加到 SSL 解密排除列表（**Device**（设备）> **Certificate Management**（证书管理）> **SSL Decryption Exclusion**（**SSL** 解密排除））中。（解密在技术上阻止解密的网站会导致该网站的流量被阻止。）

STEP 5 | 在安全策略中，阻止快速 UDP 网络连接 (QUIC) 协议。

Chrome 和其他一些浏览器使用 QUIC 而非 TLS 建立会话，但 QUIC 使用的是防火墙无法解密的专有加密，因此潜在危险流量可能以加密流量的形式进入网络。创建两条规则，一条用于阻止标准端口上的 QUIC 应用程序，另一条用于阻止端口 80 和 443 上的 UDP。阻止 QUIC 强制浏览器使用 TLS。

STEP 6 | 将解密的流量转发给 WildFire，以检查是否有恶意软件。

STEP 7 | 慢慢地解密。

解密几个 URL 类别，查看用户反馈，并运行报告，确保解密工作如预期进行。逐步解密更多的 URL 类别，直到达到您的目标。从优先级最高的流量（URL 类别最可能包含恶意流量，如游戏）开始，然后根据经验进行解密并细化过程。更保守的替代方案是解密不影响业务的 URL 类别，例如，新闻推送。

跟踪部署后的 SSL 解密最佳实践

在您部署解密后，确保一切都按照预期工作，并采取步骤确保其继续按照预期工作。

STEP 1 | 验证解密是否如预期工作。

STEP 2 | 测量防火墙性能，确保防火墙性能在可接受的规范内，以便于您了解解密对性能的影响。

如果您需要解密的流量超过防火墙资源的支持能力，则可以扩展资源，以便有足够的资源来解密想要解密的所有流量并保护网络。

STEP 3 | 在雇佣新员工时提供培训，让他们了解您的解密策略，这样，当他们在使用弱密码组时，如果无法访问某个特定的网站，他们也不会感到惊讶。

STEP 4 | 定期检查并更新解密策略和配置文件。

STEP 5 | 使用解密故障排除工具（如应用程序命令中心的 **SSL Activity**（**SSL** 活动）小部件）和解密日志（**Monitor**（监视）> **Logs**（日志）> **Decryption**（解密））监视解密流量并解决解密问题。

解密故障排除工作流程实例将诶少如何使用工具来调查问题。

STEP 6 | 使用 Palo Alto 网络文档和其他资源了解更多关于解密的信息，便于查找信息：

- PAN-OS 管理员指南提供了关于Palo Alto Networks 下一代防火墙的详细信息。
- Palo Alto 网络 Live 社区有一篇关于解密配置、设置和管理的文章的解密资源列表。
- 要想查找缺少的中间证书，请访问 SSL 实验室 (Qualys)。
- 要了解服务器慧支持哪些密码套件，请访问 Qualys SSL 实验室服务器 SSL 测试页面。
- 要想查看全球 15 万个最流行的站点中不同密码和协议使用的百分比的最新统计数据，解趋势并了解全球范围内对安全密码和协议的广泛支持，请访问 Qualys SSL 实验室 SSL Pulse 页面。