paloalto TECHDOCS

解密最佳实践

Version 10.2

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

- For the most recent version of this guide or for access to 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

January 18, 2022

Table of Contents

解密最佳实践

您无法保护您的网络免受无法看到和检查的威胁。Gartner指出，到2020年，大约70%的新恶意软件活动使用了各种形式的加密。谷歌的 透明度报告 表明无论您如何分析Google网络流量，在大多数情况下，高达95%的流量都是加密的。解密 该流量可保护您的网络免受隐藏威胁。

本文档是部署前、部署和部署后最佳做法的简化清单，您可以按照这些最佳做法实现解密。每个部分都包含指向 PAN-OS 管理员指南中详细信息的链接，包括如何配置解密策略规则和配置文件。

- 规划 SSL 解密最佳实践部署
- 使用最佳实践部署 SSL 解密
- 遵循部署后 SSL 解密最佳实践

规划 SSL 解密最佳实践部署

准备部署解密 通过制定解密策略和推出计划。启用解密可能会改变用户与某些应用程序和网站交互的方式，因此规划、测试和用户教育对于成功部署至关重要。

STEP 1 | 设定目标。

- 计划解密与防火墙一样多的非私密或敏感流量 资源 许可证。这通过暴露和阻止加密威胁来减少攻击面。了解当地法律法规，了解您可以合法解密的流量和用户通知要求。
- 从基于端口迁移到基于应用程序 安全 创建和部署解密策略规则之前的策略规则。如果基于基于端口的安全策略创建解密规则，然后迁移到基于应用程序的安全策略，则此更改可能会导致解密规则阻止您打算允许的流量，因为安全策略规则可能会使用应用程序默认端口来防止流量使用非标准端口。在部署解密之前迁移到基于 App-ID 的规则可确保在测试解密部署时，发现安全策略配置错误并在将解密推广到一般用户群之前修复它们。

STEP 2 | 与利益相关者合作并对其进行教育 例如法律，财务，人力资源，高管，安全和IT/支持，以制定解密部署策略。

- 获取解密流量所需的批准，以保护企业。
- 确定要解密的流量并确定其优先级：
  - 确定要解密的应用程序（已批准、未批准）。不允许使用未经批准的加密应用程序。
  - 确定要解密的设备（企业、BYOD、移动设备等）。

    企业无法控制 *BYOD* 设备。如果允许网络上的 *BYOD* 设备，请解密其流量，并将其应用于其他网络流量的相同安全策略。为此，请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，并明确通知用户其流量将被解密。向 *BYOD* 用户介绍该过程，并将其包含在公司的隐私和计算机使用策略中。
  - 确定是否要对不同的组（如不同的员工组、承包商、合作伙伴和来宾）使用相同的解密策略。
- 识别您无法解密的流量：
  - 中断 解密的流量 技术原因 例如证书固定、不支持的密码或相互身份验证。
  - 您的流量 选择不解密 例如金融，健康，政府和其他敏感类别，包括用户和高管等组。
  - 完全了解除解密之外的流量。您无法查看加密流量，并且防火墙无法将威胁防护配置文件应用于加密流量。
- 准备更新的法律和 HR 计算机使用策略，以分发给所有员工、承包商、合作伙伴、来宾和任何其他网络用户，以便在推出解密时，用户可以了解其数据并扫描其数据以查找威胁。
- 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之间进行权衡。了解要如何处理证书验证有助于确定如何配置 SSL 转发代理解密配置文件。
- 确定要记录的流量。请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以及可以存储日志的位置。

将防火墙放置在可以看到所有网络流量的位置，以便没有加密的流量因绕过防火墙而无意中获得对网络的访问权限。

STEP 3 | 制定计划以推出您的 公钥基础结构 (PKI).

- 如果已有 PKI，请从企业根 CA 生成 SSL 转发信任 CA 证书作为从属证书。这使得部署更容易，因为网络设备已经信任企业根 CA，因此您不会遇到证书问题。如果您没有企业根 CA，请考虑获取一个。

  或者，在防火墙上生成自签名根 CA 证书，并在该防火墙上创建从属的正向信任 CA 证书以安装在网络设备上。自签名证书最适合没有企业根 CA 的小型公司和概念证明 （POC） 试验。

  

  与*BYOD*设备类似，企业不控制来宾设备。如果允许网络上的来宾设备，请解密其流量，并对其进行约束，使其遵守应用于其他网络流量的相同安全策略。为此，请通过身份验证门户重定向来宾用户，指导他们如何下载和安装 *CA* 证书，并明确通知用户其流量将被解密。将此过程包含在公司的隐私和计算机使用策略中。

- 生成 分开 前向信任和前向不信任的 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 对转发不受信任的证书进行签名#转发不受信任的证书警告用户，签名服务器的证书不是合法的，他们不应继续访问站点。如果受信任的根 CA 对不受信任的证书进行签名，则客户端信任应不受信任的证书，因为客户端信任根 CA。
- 为每个防火墙生成单独的从属正向信任 CA 证书。使用单独的从属 CA 使您能够 吊销证书 在不影响部署的其余部分的情况下停用设备（或设备对）时，如果需要吊销证书，则可以减少影响。单独的 CA 证书可帮助技术支持解决用户问题，因为证书错误消息包含有关流量所经过的防火墙的信息。尽管在所有防火墙上使用一个“转发信任”从属 CA 更易于部署，但在每个防火墙上使用单独的证书可提供最佳安全性。
- 如果您需要为私钥提供额外的安全性，请考虑 将它们存储在 HSM 中.

STEP 4 | 对防火墙性能进行基线测量，以了解资源消耗和可用防火墙资源，以便在部署解密后比较性能并估计 防火墙部署的大小 需要支持要解密的流量。

- 使用您的 Palo Alto Networks SE/CE 来调整防火墙部署的大小，并避免大小调整错误。
- 记下当前可用的防火墙资源。通常，安全性越严格，解密消耗的资源就越多。影响您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。完美前向保密 （PFS） 临时算法（如 DHE 和 ECDHE）比 RSA 消耗更多的资源，但提供更高的安全性，因为防火墙会为每个会话生成一个新的密码密钥。如果攻

击者破坏了会话密钥，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。

- 证书身份验证。RSA 证书身份验证（这与 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 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。
- 这 防火墙模型和资源.较新的防火墙型号比较旧的型号拥有更多的资源。

- 事务大小会影响性能。测量所有流量的平均事务大小，然后测量端口 443（HTTPS 加密流量的默认端口）上流量的平均事务大小，以了解防火墙上加密流量与总流量和平均事务大小的比例。

这些因素的组合决定了解密如何消耗防火墙处理资源。如果防火墙资源有问题，请对优先级较高和风险较高的流量使用更强的解密，并使用处理器密集程度较低的解密来解密和检查优先级较低的流量，直到可以增加可用资源。

调整防火墙大小以包括要解密的流量增长的余量，因为每天加密的流量越多。

STEP 5 | 规划分阶段、按优先级排列的部署.

- 确定早期采用者以支持解密，并让部门经理参与该计划。
- 设置 POC 以在将部署策略推广到一般用户群之前对其进行测试。测量解密 POC 部署影响防火墙 CPU 和内存利用率的方式，以帮助了解防火墙大小调整是否正确。POC还可以揭示在技术上破坏解密的应用程序。
  - 向 POC 参与者介绍更改以及如何联系技术支持。
  - 为解密 POC 设置技术支持 POC，以便支持人员有机会开发支持推出的最佳方式。
  - 分阶段解密。计划先解密风险最高的流量（最有可能隐藏恶意流量的 URL 类别，例如游戏或高风险流量），然后在获得经验时解密更多流量。或者，先解密不影响您业务的网址类别（如果出现问题，也不会影响业务），例如，新闻 Feed。在这两种情况下，解密一些URL类别，听取用户反馈，运行报告并检查 解密日志 以确保解密按预期工作，然后逐步解密更多的URL类别等。计划制作 解密排除项 以从解密中排除网站，如果您由于技术原因或选择不解密网站而无法解密它们。
  - 衡量 POC 是否成功并微调部署实践。
- 在常规推出之前对用户群体进行教育。POC 有助于确定最重要的沟通点。
- 向所有员工、承包商、合作伙伴、来宾和任何其他网络用户分发更新的法律和 HR 计算机使用策略。确保每个人都了解在向每个部门或组推出解密时可以解密和扫描其数据以查找威胁。
- 创建切合实际的计划，以便有时间评估部署的每个阶段。

使用最佳实践部署SSL解密

STEP 1 | 生成和分发 解密策略的密钥和证书.

- 如果您有企业PKI，请为来自企业根CA的转发代理通信生成转发信任CA证书。否则，请在防火墙上生成自签名根CA证书，在该防火墙上创建从属CA，然后将自签名证书分发到所有客户端系统。自签名证书适用于实验室测试、小型部署和POC。
- 为每个防火墙生成一个唯一的从属转发信任CA（或为所有防火墙生成一个转发信任CA，具体取决于 规划-一个证书更容易部署，但单独的证书提供了最佳的安全性和其他好处）。不同的PKI平台具有不同的扩展证书管理的功能。
- 如果不使用企业CA，请将“转发信任CA”证书导入客户端系统的信任CA存储。
- 不导入转发 取消信任 CA证书放入客户端系统上的CA信任存储区中，否则不受信任的证书将不会作为不受信任站点的触发器。（但是，如果防火墙自签名根CA未作为受信任的颁发者安装在客户端系统上，则可以使用自签名转发不受信任证书。）
- 使用 自动化方法 将转发信任证书分发到连接的设备，例如Palo Alto Networks GlobalProtect门户、Microsoft AD证书服务（使用组策略对象）、商业工具或开源工具。
- 如果从企业根CA生成证书，请在防火墙上导入证书。
- 在安全存储库中备份防火墙的转发信任CA证书的私钥（而不是防火墙的主密钥），以便在出现问题时仍可以访问转发信任CA证书。
- 如果从企业根CA生成证书和私钥，阻止导出私钥.(You可以从您的企业CA将它们安装在新的防火墙和Panorama上，因此您不需要从PAN-OS导出它们。）
- 如果您的计划要求使用HSM，将私钥存储在HSM上.

STEP 2 | 配置解密配置文件 以控制协议、证书验证和故障处理。

- SSL正向代理服务器解密配置文件 控制服务器证书验证、会话模式和出站流量的故障检查。阻止具有过期证书、不受信任的颁发者、不受支持的版本和不受支持的密码套件的会话。除非有重要的应用程序需要客户端验证，否则请封锁具有客户端验证的阶段作业，在这种情况下，您应该建立允许客户端验证的个别“解密”设定档，并仅将其套用至需要客户端验证的流量。
- SSL入站检查解密配置文件 控制会话模式和入站流量的故障检查。阻止具有不支持的版本和密码套件的会话。
- SSL协议设置 受控密码套件元素：SSL转发代理和SSL入站检查通信的协议版本、密钥交换算法、加密算法和身份验证算法。尽可能使用最强的密码。对于正向代理，请设置协议 最小版

本 至 **TLSv1.2** 和 最大版本 至 最大值 以阻止弱协议。对于SSL入站检查，使用与要检查其入站通信的服务器的功能相匹配的协议设置创建单独的配置文件。

请使用最强的密码套件。创建单独的解密策略和配置文件以最大限度地提高安全性。如果您出于业务目的所需的旧站点仅支持较弱的密码，请创建单独的解密配置文件以允许该通信，并在解密策略中仅将其应用于必要的站点。使用相同的技术来微调不同*URL*类别的安全性与性能。

许多移动应用程序使用固定证书。由于*TLSv1.3*会加密证书信息，因此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。对于这些应用程序，请确保解密配置文件 最大版本 设置为*TLSv1.2*，或对通信应用“不解密”策略。

- 无解密配置文件 控制您选择不解密通信的服务器证书验证。阻止具有过期证书和不受信任颁发者的会话。

  请勿将“无解密”配置文件应用于*TLSv1.3*流量。证书信息已加密，因此防火墙无法阻止基于证书信息的会话。

- 对于SSL正向代理和无解密流量，配置证书吊销列表（CRL）和联机证书状态吊销（OCSP）证书撤销 检查以确认站点证书未被吊销。
- SSH代理配置文件 控制SSH隧道通信的会话模式和故障检查。阻止具有不支持的版本和算法的会话。

的最佳做法解密配置文件设置 数据中心 并且对于周界（因特网网关）用例与一般最佳实践设置略有不同。

STEP 3 | 设定 解密策略规则 定义要解密的流量，并使 基于策略的例外 为了交通你 *choose* 而不是解密。

- 创建策略规则，以排除您选择不解密的特定目标IP地址（例如财务服务器）、源用户和组（例如主管或HR人员）、源设备和应用程序端口。将这些规则放在解密规则库的顶部，位于解密通信的规则之前。对于除TLSv1.3流量之外的所有流量，请将“No Decryption”配置文件附加到这些流量以应用SSL 服务器证书验证控件 加密的流量。这可防止无意中解密您不想解密的通信。
- 使用“URL类别”、“自定URL类别”和“外部动态列表”（EDL）指定不解密的URL，例如金融服务、医疗和医药、政府以及任何其他由于业务、法律或法规原因而不想解密的类别。在IP地址动态变化（例如Office 365）或成员资格频繁更改的环境中使用EDL，以便无需提交即可进行更新。

  创建EDL或自定义URL类别，使其包含您选择不解密的所有类别，以便您只需要一个解密策略规则。

  将这些规则放在解密规则库中解密通信的规则之上。
- 设定 解密日志记录和日志转发.
- 如果您使用 解密镜像 要将解密的网络通信复制并发送到网络通信收集工具，请注意可能禁止镜像或控制可以镜像的网络通信的当地隐私法规。

- 创建策略以解密其余流量，方法是配置 SSL转发代理,SSL入站检查的 SSH代理服务器 规则。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、内容交付网络和高风险URL类别。将SSH代理限制为管理网络设备、记录所有SSH流量和配置 多重身份验证 以防止未经授权的SSH访问。

STEP 4 | 将站点添加到 SSL解密排除列表 (器械 > 证书管理 > **SSL**解密排除），如果它们在POC测试期间从技术上破坏了解密，并且不在排除列表中。（对阻止解密的站点进行解密在技术上会导致阻止该通信。）

STEP 5 | 在安全策略中，阻止快速UDP Internet连接（QUIC）协议.

Chrome和一些其他浏览器使用QUIC而不是TLS建立会话，但QUIC使用防火墙无法解密的专有加密，因此潜在的危险通信可能会以加密通信的形式进入网络。创建两个规则，一个用于阻止标准端口上的QUIC应用程序，另一个用于阻止UDP端口80和443。阻止QUIC会强制浏览器使用TLS。

STEP 6 | 将解密的流量转发到WildFire 检查是否有恶意软件。

STEP 7 | 缓慢执行解密.

解密一些URL类别，查看用户反馈，并运行报告以确保解密按预期工作。逐步解密更多的URL类别，直到您达到您的目标。从优先级最高的流量（最有可能包含恶意流量的URL类别，如游戏）开始，随着经验的积累和过程的改进，解密更多的流量。一个更保守的替代方案是首先解密不影响业务的URL类别，例如新闻提要。

遵循部署后SSL解密最佳实践

部署解密后，请确保一切都按预期工作，并采取措施确保它继续按预期工作。

STEP 1 | 验证 解密按预期工作。

STEP 2 | 测量防火墙性能以确保其在可接受的标准范围内，以便了解解密对性能的影响。

如果要解密的流量超过防火墙资源支持的流量，请向上扩展，以便有足够的资源来解密所有要解密的流量，从而保护网络。

STEP 3 | 在雇用新员工时对他们进行教育，使他们了解您的解密策略，如果他们因为使用弱密码套件而无法访问特定站点，他们也不会感到惊讶。

STEP 4 | 定期检查和更新解密策略和配置文件。

STEP 5 | 用途 解密故障排除工具 例如应用程序命令中心的 **SSL**活动 小组件和解密日志（监控器 > 记录档 > 解密）以监视解密业务并解决解密问题。

解密疑难解答工作流示例 向您展示如何使用这些工具调查问题。

STEP 6 | 当您需要更改防火墙为其执行 SSL入站检查,添加新证书 在服务器上进行更改之前，请将该服务器的解密策略规则添加到该服务器的解密策略规则。解密策略规则支持多个服务器证书，因此您可以保留旧证书，也可以将新证书添加到规则中。这样可以避免在防火墙只有旧证书时，由于更改服务器上的证书而导致的解密中断。将新的服务器证书添加到解密策略规则可确保在更改服务器上的证书时，防火墙具有正确的证书以继续无缝解密通信。

在更改服务器证书后，请确保从解密策略规则和防火墙中删除无效证书。

STEP 7 | 使用Palo Alto Networks文档和其他资源了解有关解密的更多信息并查找以下信息：

- 的 PAN-OS管理员指南 提供了有关Palo Alto Networks下一代防火墙的详细信息。
- Palo Alto Networks Live社区有一个 解密资源列表 关于解密配置、设置和管理的文章。
- 要查找缺少的中间证书，请访问 SSL实验室（资格认证）.
- 要了解服务器支持哪些密码套件，请访问Qualys SSL Labs 服务器SSL测试页.
- 要查看世界上150，000个最受欢迎的站点上使用的不同密码和协议的百分比的最新统计数据，以便了解趋势并了解全球对更安全密码和协议的支持有多广泛，请访问Qualys SSL Labs SSL脉冲页面.