paloalto TECHDOCS

数据中心最佳实践安全策略

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

December 8, 2023

Table of Contents

数据中心安全策略最佳实践清单

数据中心保存有公司最具价值的资产，包括专有源代码、知识产权、敏感的公司数据和客户数据。客户和员工相信您可以维护其数据的机密性和完整性，并期望数据始终可用，因此，必须执行数据中心最佳实践安全策略，从而保护您的数据，防止成功攻击。因为攻击者可能来自网络内部，也有可能来自其凭据已受到攻击的合作伙伴和承包商，因此，强化网络外围是不够的，而且如果攻击者在您的网络中获得立足点，攻击者就可以在设备与设备之间进行横向移动，从网络内部进行攻击。

如果您已熟悉 Palo Alto Networks 平台，则可以使用该简化清单逐步完成部署前的规划、部署活动和部署后的维护，以实施和维持数据中心安全策略最佳实践，从而节省时间。每个部分均包含整个数据中心最佳实践安全策略文档或 PAN-OS 管理员指南中详细信息的链接，包括如何配置策略规则、安全配置文件、DoS 攻击预防和用户身份验证，如何对网络进行分段等。

- 规划数据中心最佳实践部署
- 部署数据中心最佳实践
- 遵循数据中心后期部署最佳实践

规划数据中心最佳实践部署

通过制定策略和推出计划，可在数据中心内做好实施最佳实践的准备。利用主动实施安全策略（创建允许您想要允许的用户和应用程序流量，并拒绝所有其他流量的规则），以实现零信任基础架构。

STEP 1 | 设定目标。

- 定义数据中心网络的未来理想状态，这样，您便有需要努力的明确目标，并知道何时实现这些目标。
- 保护在其内会启动连接的每个区域的通信流：
  1. 流入数据中心的本地用户流量。
  2. 从 Internet 流向数据中心的流量。
  3. 从数据中心流向 Internet 的流量。
  4. 在数据中心内服务器或 VM 之间流动的流量（数据中心内部的东西流量）。
- 数据中心不允许存在未知用户、应用程序或流量。
- 创建标准化的、可扩展的设计，以在整个数据中心进行统一复制和应用。

STEP 2 | 与 IT/支持、安全和需要访问数据中心的组（工程、法律、财务和 HR）等利益相关团队合作，制定访问策略。

- 标识需要访问的用户以及需要访问的资产。通过了解这些，您可以根据访问等级要求创建用户组，这样，就能按用户组设计有效的安全策略规则。
- 标识想要在数据中心允许（批准）的应用程序。要减少攻击面，应在合法的业务需要时使用经批准的应用程序。

STEP 3 | 访问您的数据中心，了解其当前的状态，以创建一个将数据中心安全转换到未来所需状态的计划。

- 列出实体和虚拟环境以及资产，包括：
  - 服务器、路由器、交换机、安全设备、负载均衡器和其他网络基础设施。
  - 标准和专有自定义应用程序，以及用于通信的服务帐户。将应用程序清单列表与要批准的应用程序列表进行比较。

    专注于想要允许的应用程序，因为允许列表安全策略规则会允许这些应用程序，默认拒绝所有其他应用程序，从而减少攻击面。将应用程序映射到业务需求。如果应用程序未能映射到业务需求，则对您是否真的需要允许该应用程序进行评估。
  - 对每个资产进行评估，有助于确定要首先保护的内容的优先级。问自己一些问题，例如“是什么定义了我们公司并将我们公司与其他公司区分开来？”、“日常运营必须使用哪些系统？”以及“如果此资产丢失，会有什么后果？”
- 与应用程序、网络和企业架构师，以及业务代表一起协作，确定数据中心流量的特征，了解典型的基线流量负载和模式，从而了解正常的网络行为。使用应用程序命令中心小组件和流量分析工具确定基线流量。

STEP 4 | 创建数据中心分段策略，防止已获得数据中心立足点的恶意软件横向移动，从而攻击其他系统。

- 将防火墙用作分段网关，提供对数据中心流量和系统的可见性，从而精确控制哪些用户可以使用哪些应用程序访问哪些服务。使用物理防火墙对非虚拟服务器进行分段和保护，使用 VM 系列防火墙对虚拟网络进行分段和保护。
- 使用防火墙灵活的分段工具（例如，区域、动态地址组、App-ID和 User-ID）设置粒度分段策略，从而保护敏感服务器和数据。
- 对执行类似功能，确需要同一分段内相同安全等级的资产进行分组。
- 对数据中心应用程序进行分段，方法如下：对构成应用程序层的服务器层进行分段（通常是一个由 Web 服务器层、应用程序服务器层和数据库服务器层组成的服务链），然后使用防火墙控制和检测层之间的流量。
- 考虑在数据中心内部使用 SDN 解决方案，以实现灵活的虚拟化基础架构，从而最大化地利用资源，并简化自动化和扩展。

STEP 5 | 计划使用方法的最佳实践检测数据中心所有流量并获得完全的可见性、减少攻击面，以及阻止已知和未知威胁。

- 将物理或虚拟防火墙置于可以看见数据中心所有网络流量的位置。
- 利用防火墙强大的工具集，创建与特定用户组相关联且受到安全配置文件保护的基于应用程序的安全策略规则。转发未知文件到WildFire，并部署解密，以阻止威胁以加密流量的形式进入数据中心
- 在内部模式下，将 GlobalProtect 用作控制数据中心访问的网关。
- 对用户进行身份验证，阻止未经授权的访问，并为访问敏感应用程序、服务和服务器的用户配置多重因素身份验证，尤其是需要访问数据中心的承包商、合作伙伴和其他第三方。
- 使用 Panorama 集中管理防火墙，以实现物理和虚拟环境内策略的一致实施，并实现集中可见性。
- 如果拥有多个数据中心，则重复使用模板和模板堆栈，以便在不同的位置统一应用安全策略。

STEP 6 | 随时间的推移逐步部署最佳实践；首先，应关注业务和网络上最有可能遭受的威胁，然后优先保护最具价值的资产。

考虑数据中心的所有用户、应用程序、设备和流量，然后创建与其相关的最佳实践安全策略，如果您尝试一次性完成所有操作，可能会非常困难。但是，通过优先保护您最具价值的资产，并规划分阶段的逐步实施，就可以顺利地从最佳期望安全策略转换到最佳实践安全策略，从而保护应用程序、用户和内容的安全。

部署数据中心最佳实践

在创建安全配置文件、解密配置文件、安全策略规则、身份验证策略规则和解密策略规则时执行数据中心最佳实践。

对于安全、身份验证和 *DoS* 策略规则，配置日志转发为 *Panorama* 或外部服务，以将日志集中，便于通过查看和分析，并将发送通知。

- 全局数据中心对象、策略和操作 — 创建定制应用程序，以识别和控制数据中心内具有安全策略的专有应用程序，配置严格的安全配置文件（防病毒、防间谍软件、漏洞防护、文件阻止和 WildFire 分析），配置严格的解密配置文件和策略，阻止已知恶意或不必要的流量，并在端点上安装 Cortex XDR Agent 来保护它们。
- 用户数据中心流量策略 — 配置严格的安全策略规则以仅允许适当的访问，确保用户经过身份验证并解密流量。
- Internet 到数据中心流量策略 — 防范各种风险，例如从受感染的外部服务器下载恶意软件、在数据中心端点放置命令和控制恶意软件、允许无意访问以及旨在破坏数据中心可用性的 DoS 攻击等。
- 数据中心到 Internet 流量策略 — 防范各种风险，例如数据渗漏、试图接入互联网并“调用主页”的命令和控制恶意软件以及试图下载更多恶意软件的受感染服务器上的其他恶意软件等。
- 数据中心内流量策略 — 防止恶意软件的横向移动，仅允许使用出于业务目的而需要使用的经批准的应用程序，并解密和记录流量。
- 数据中心安全策略规则库顺序 — 安全策略规则库中规则的顺序至关重要，因为当流量与规则匹配后，防火墙会对流量执行规则的操作，并且由于规则遮蔽，不会对该流量执行任何其他操作；遵循安全策略规则库最佳实践以避免出现遮蔽，并了解如何对规则库进行排序。

全局数据中心对象、策略和操作

如果使用自定义应用程序，请确保可以保护它们。配置安全配置文件和解密配置文件，并在所有数据中心端点上安装 Cortex XDR 代理。

- 自定义应用程序
- 安全配置文件
- 解密配置文件
- 流量阻止规则
- 在端点上安装 Cortex XDR 客户端

STEP 1 | 如果数据中心应用程序清单包含专有自定义应用程序，则为其创建自定义应用程序，从而在安全策略中进行指定。

STEP 2 | 配置严格的数据中心最佳实践安全配置文件，防止威胁破坏数据中心网络。

- 通过复制预定义配置文件，并在操作和 WildFire 操作列中更改 imap、pop3 和 smtp 解码器值为 **reset-both**（重置两者）以配置最佳实践防病毒配置文件。
- 通过复制严格的预定义配置文件来配置最佳实践防间谍配置文件。在 **Rules**（规则）选项卡上，针对所记录流量的低、中、高和关键严重性威胁启用单个数据包捕获。（对于未记录的流量，则应用单独的配置文件，无需启用数据包捕获。）

  在 DNS 签名选项卡上，如果防火墙无法查看到 DNS 查询的发起者（通常是当防火墙位于本地 DNS 服务器的北方），则将对 DNS 查询的 **Action**（操作）更改为 **sinkhole**（沉洞），这样就可以标识受感染的主机。DNS 沉洞将标识并跟踪尝试访问可疑域的潜在受损主机，并阻止其访问这些域。在沉洞流量上启用扩展的数据包捕获。

  仅允许流量流向批准的 *DNS* 服务器。使用 DNS 安全服务阻止恶意 *DNS* 服务器连接。
- 通过复制预定义的严格配置文件，并将除 simple-client-informational（单个客户端参考）和 **simple-server-informational**（单个服务器参考）之外每条规则的数据包捕获设置更改为 **single-packet**（单个数据包），从而配置最佳实践漏洞保护配置文件。如果防火墙标识出大量可影响性能的漏洞威胁，则为低严重性事件禁用数据包捕获。
- 严格的预定义文件阻止配置文件是最佳实践配置文件。如果受支持的关键应用程序阻止您封锁严格配置文件阻止的所有文件类型（在 **Monitor**（监控）> **Logs**（日志）> **Data Filtering**（数据筛选）中，您可以从数据筛选日志标识数据中心使用的文件类型），则复制严格配置文件，并在需要时进行修改。如果文件无需双向流动，则使用 **Direction**（方向）设置将文件类型限制为仅朝需要的方向流动。
- 预定义的 WildFire 分析配置文件是最佳实践配置文件。WildFire 可以更好地防御未知威胁和高级持续性威胁 (ATP)。

STEP 3 | 配置严格的数据中心最佳实践解密配置文件，防止未知流量进入数据中心。

- 执行 CRL/OCSP 检查，确保 SSL 解密期间显示的证书为有效证书。
- SSL 协议设置 :设置 **Min Version**（最小版本）为 **TLSv1.2**、**Max Version**（最大版本）为 **Max**（最大值），取消选择 **SHA1** 身份验证算法。（选择 TLSv1.2 时，将自动取消选择 3DES 和 RC4 弱加密算法。）对支持 TLSv1.3 的流量使用 TLSv1.3（许多移动应用程序使用证书锁定，这在使用 TLSv1.3 时可以防止解密，因此对于这些应用程序，请使用 TLSv1.2）。
- SSL 转发代理 :对于 **Server Certificate Verification**（服务器证书验证），将阻止具有过期证书、不可信颁发者和未知证书状态的会话，并限制证书延期。对于 **Unsupported Mode Checks**（不受支持的模式检查），则阻止具有不受支持版本、不受支持密码套件和客户端身份验证的会话。对于 **Failure Checks**（失败检查），在资源不可用时阻止会话则需要在用户体验（阻止可能会对用户体验产生负面影响）与可能允许威胁连接之间做出权衡。如果必须考虑此权衡，则还请考虑在部署中增加可用的解密资源。

- SSL 入站检查 :对于 **Unsupported Mode Checks**（不受支持的模式检查），则阻止具有不受支持版本和不受支持密码的会话。对于 **Failure Checks**（失败检查），则权衡类似于 SSL 转发代理。
- SSH 代理 :对于 **Unsupported Mode Checks**（不受支持的模式检查），则阻止具有不受支持版本和不受支持算法的会话。对于 **Failure Checks**（失败检查），则权衡类似于 SSL 转发代理。
- 将 No Decryption（无解密）配置文件应用到您因法规、合规性规则或业务原因而选择不解密的流量，TLSv1.3 流量除外（TLSv1.3 协议对证书信息进行加密，防火墙无法根据证书信息阻止流量）。阻止过期证书和不可信发行者的会话。

STEP 4 | 配置流量阻止规则，以拒绝已知为恶意，或业务原因不再需要的流量。

日志记录并监控阻止规则可能会泄露网络上您不知道，且可能是合法，也可能是一个攻击的用户和应用程序。安全策略规则中规则的排序对防止屏蔽至关重要（在流量可以匹配您打算其与之匹配的规则之前，与允许或阻止规则匹配的流量）。有些规则几乎相同，但对于标准和非标准端口，或是应用程序和源自其他源的应用程序，则会启用单独的报告。对于每个规则，请在 **Actions**（操作）选项卡上配置 **Log at Session End**（会话结束时记录），并设置日志转发，以跟踪和分析规则违规。

- 阻止源自 **application-default**（默认应用程序）端口上用户区域的所有应用程序。将此规则置于允许源自用户区域的合法应用程序流量的规则下游，以标识标准端口上的未知或期望以外的用户用户应用程序。

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected-App-from-User-Zone	User to DC BP	universal	Contractors Engineering-Users Finance-Users IT-Users	any	any	any	Web-Server-Tier-DC	any	any	any	application-default	Drop	none	

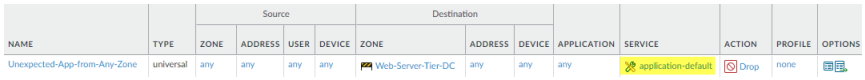
- 阻止源自 **any**（任何）端口上用户区域的所有应用程序，以捕获尝试使用非标准端口的用户流量。将此规则置于之前的 **application-default**（默认应用程序）阻止规则的下游，以标识非标准端口上的未知或期望以外的用户应用程序，这可能是自定义应用程序，也可能是规避应用程序。

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected-User-App-Any-Port	User to DC BP	universal	Contractors Engineering-Users Finance-Users IT-Users	any	any	any	Web-Server-Tier-DC	any	any	any	any	Drop	none	

- 阻止不希望存在于数据中心的应用程序，例如，规避和经常被利用的应用程序和业务所不需的应用程序。将此规则置于应用程序允许规则下游，例如，您可以在 **Filesharing**（文件共享）应用程序筛选器阻止所有其他文件共享应用程序之前允许批准的文件共享应用程序。

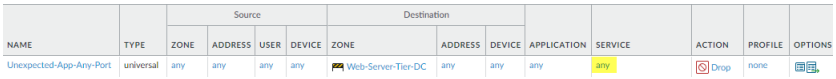
			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Block-Bad-Apps	User to DC BP	universal	any	any	any	any	App-Server-Tier-DC DB-Server-Tier-DC Engineering-DC-Infra Finance-DC-Infra IT Infrastructure SAP-Infra Web-Server-Tier-DC	any	any	Encrypted-Tunnels File-Sharing Remote-Access	any	Drop	none	

- 阻止 **application-default**（默认应用程序）端口上来自 **any**（任何）区域的所有应用程序，以标识预期以外的应用程序。规则匹配则可能表示需要修改允许规则的潜在威胁或应用程序更改。将此规则置于应用程序允许规则和先前的阻止规则下游。



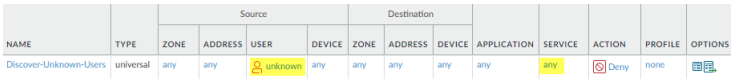
	NAME	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
	Unexpected-App-from-Any-Zone	universal	any	any	any	any	Web-Server-Tier-DC	any	any	any	application-default	Drop	none	

- 阻止源自 **any**（任何）端口上任何区域的所有应用程序，以标识非标准端口上预期以外的应用程序。请勿允许未知 tcp、未知 udp、或未同步 tcp 流量。将此规则置于应用程序允许规则和先前的阻止规则下游。



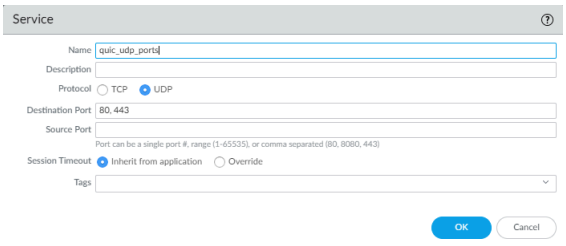
NAME	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected-App-Any-Port	universal	any	any	any	any	Web-Server-Tier-DC	any	any	any	any	Drop	none	

- 阻止任何端口上尝试运行应用程序的未知用户，以发现未知用户（User-ID 覆盖范围或攻击者中的缺口），标识受攻击的设备（包括打印机、读卡器和摄像机等嵌入式设备）。将此规则置于应用程序允许规则和先前的阻止规则下游。

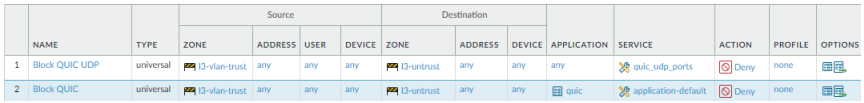


NAME	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Discover-Unknown-Users	universal	any	any	unknown	any	any	any	any	any	any	Deny	none	

- 除了阻止不必要的潜在恶意流量外，请阻止 快速 UDP Internet 连接 (QUIC) 协议，除非出于业务原因，否则您会希望允许加密的浏览器流量。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。阻止 QUIC 应用程序和 UDP 端口 80 和 443，以强制浏览器使用 TLS。首先创建包含 UDP 端口 80 和 443 的服务（**Objects**（对象） > **Services**（服务））：



使用此服务指定用于阻止 QUIC 的 UDP 端口。在第二条规则中，阻止 QUIC 应用程序，以便让规则库中的前两条规则阻止 QUIC：



	NAME	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
1	Block QUIC UDP	universal	l3-vlan-trust	any	any	any	l3-untrust	any	any	any	quic_udp_ports	Deny	none	
2	Block QUIC	universal	l3-vlan-trust	any	any	any	l3-untrust	any	any	quic	application-default	Deny	none	

STEP 5 | 在所有数据中心端点上安装 Cortex XDR 客户端，以阻止端点上的恶意软件和漏洞利用工具。

Cortex XDR 客户端以相同的方式保护所有端点，因此，对于其他网络区域，数据中心的部署流程和恶意软件保护策略最佳实践相同。

用户数据中心流量策略

为需要访问数据中心的用户配置安全策略、身份验证策略和解密策略。

- 用户安全策略规则
- 用户身份验证策略规则
- 用户解密策略规则

STEP 1 | 为用户流量创建应用程序允许列表安全策略规则，以允许适当的访问。

将用户访问的允许规则置于规则库顶部，即阻止规则的上游，以防止意外阻止合法流量。对于每个规则，请在 **Actions**（操作）选项卡上配置 **Log at Session End**（会话结束时记录），并设置日志转发，以跟踪和分析规则违规。

- 启用员工用户对企业内部 DNS 服务器的访问。该规则允许任何用户，因为用户在登录之前访问 DNS 服务。该规则对源区域、目的服务器和应用程序实施严格控制，并对流量应用安全配置文件。

  阻止访问 *Internet* 网关上的外部 *DNS* 服务器，从而防止 *DNS* 流量从 *Internet* 流入到公共服务器。仅允许访问经批准的 *DNS* 服务器，并使用 DNS 安全服务阻止恶意 *DNS* 服务器连接。

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
DNS Services	User to DC BP	universal	any	any	any	any	IT Infrastructure	DNS-Servers	any	dns	application-default	Allow		

- 允许必要的 IT 人员对数据中心管理接口进行安全的特权访问。限制此规则到管理接口（在本示例中，使用地址组标识设备，使用自定义服务标识管理接口）和必要的应用程序。使用专用 VLAN 将管理流量与其他流量分开，并在相同的子网上部署管理接口。

  如果同一 *IT* 用户组也管理数据中心的交换机、路由器和其他设备，则将其添加到目标，并将其端口添加到自定义服务，这样，此规则可确保连接到其管理接口的流量的安全。如果不同的 *IT* 用户组管理不同的数据中心资源，则为每个组创建单独的安全策略规则和相应的解密和身份验证策略规则。

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
IT DC Server Management	User to DC BP	universal	IT-Users	any	it-superusers	any	IT-Server-Access-DC	IT-Server-Management	any	ms-rdp ssh ssl	Custom-IT-Ports	Allow		

- 允许员工用户组的所需访问。这些规则可限制每个用户组（或用户）仅访问必要的应用程序和服务器。在本示例中，工程用户组仅访问开发服务器和应用程序。

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Engineering Resources	User to DC BP	universal	Engineering-Users	any	api-users engg-users	any	Engineering-DC-Infra	Dev-Servers	any	oracle-bi perforce profinet qlikview	application-default	Allow		

- 允许对承包商、合作伙伴、客户和其他第三方的有针对性的限制访问。在本示例中，限制对 SAP 承包商组的访问，这样，该组仅可以使用适当的应用程序仅限于对适当的 SAP 数据库服务器的访问。

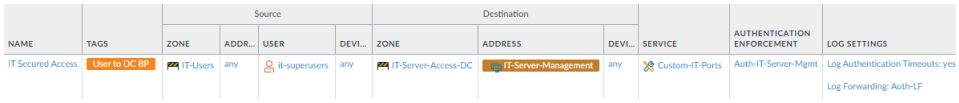
			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
SAP-Contractors	User to DC BP	universal	Contractors	any	sap-contractors	any	SAP-Infra	SAP DB Servers	any	ms-sql-analysis-service mssql-db mssql-mon sap	application-default	Allow		

STEP 2 | 为用户流量创建身份验证策略规则，以对数据中心访问进行身份验证。

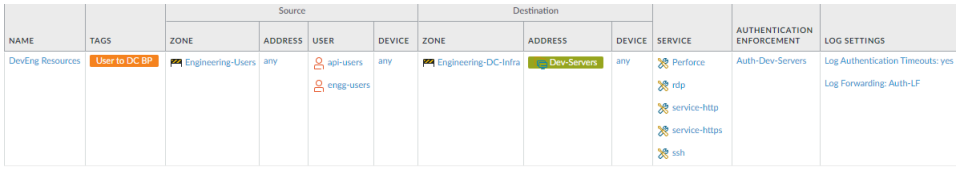
对于为其创建应用程序允许规则的每个用户组或用户，请创建模拟身份验证规则（因为 DNS 发生在用户进行登录身份验证之前，因此 DNS 允许规则应除外）。对于每个规则，请在 **Actions**（操作）选项卡上配置 **Log at Session End**（会话结束时记录），并设置日志转发，以跟踪和分析规则违规。

- 对需要专门访问权限的用户进行身份验证。在本示例中，对需要安全特权访问的 IT 人员进行身份验证，以从之前的允许规则管理数据中心服务器。因为特权用户的凭据遭到盗用，使攻击者掌握进入数据中心王国的钥匙，因此，需要多重因素身份验证 (MFA) 来防止凭据被盗。

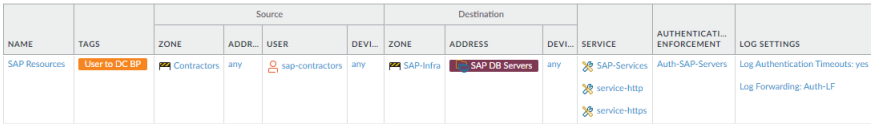
  如果同一 *IT* 用户组也管理数据中心的交换机、路由器和其他设备，则将其添加到目标，并将其端口添加到自定义服务，这样，此规则可确保连接到其管理接口的流量的安全。如果不同的 *IT* 用户组管理不同的数据中心资源，则为每个组创建单独的安全策略规则和相应的解密和身份验证策略规则。



- 对出于合法业务目的而访问数据中心的员工进行身份验证。在本示例中，从之前的允许规则对工程开发用户组进行身份验证。



- 对承包商、合作伙伴、客户和其他非员工组进行身份验证。需要对非员工组实施 MFA，以防止在第三方公司发生凭据被盗。在本示例中，从之前的允许规则对 SAP 开发人员进行身份验证。



STEP 3 | 为用户流量创建解密策略规则，解密允许的流量，这样，防火墙可以查看流量，检测流量，并对其应用安全策略。

对于每个解密策略规则，应用适当的最佳实践解密配置文件（(SSL 入站检查、SSL 转发代理、SSH 代理或不解密，包括用于 SSL 入站检查和 SSL 转发代理规则的最佳实践 SSL 协议设

置），以阻止弱协议和算法，验证服务器证书。对于每个 SSL 入站检查规则，导入通过解密进行保护的数据中心服务器证书。

仅出于以下两个原因从解密中排除流量：

- 由于固定证书或相互身份验证等技术原因，流量会破解解密。添加技术排除到 ***Device***（设备）> ***Certificate Management***（证书管理）> ***SSL Decryption Exclusion***（***SSL*** 解密排除）列表。
- 出于业务、法规、合规性，或财务、健康、军事或政府流量等其他原因而选择不解密的流量。为选择不解密的流量创建基于策略的解密排除。

- 解密先前创建的、允许 IT 特权访问管理服务器的安全策略规则中的流量。解密策略规则及其相关的解密配置文件的不同之处取决于 IT 组是否使用 SSL（SSL 转发代理解密配置文件）或 SSH（SSH 代理解密配置文件）访问管理端口。

  如果同一 *IT* 用户组也管理数据中心的交换机、路由器和其他设备，则将其添加到目标，并添加服务器证书，这样，此规则可解密连接到其管理接口的流量。如果不同的 *IT* 用户组管理不同的数据中心资源组，则为每个组创建单独的、严格的安全策略规则和相应的解密和身份验证策略规则。

  对于 SSL 特权访问：

		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
IT DC Management	User to DC BP	IT-Users	it-superusers	IT-Server-Access-DC	IT-Server-Management	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

  对于 SSH 特权访问：

		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
IT DC Mgmt-SSH	User to DC BP	IT-Users	it-superusers	IT-Server-Access-DC	IT-Server-Management	decrypt	ssh-proxy	DC BP Decryption	none	false	true

- 配置 SSL 入站检查，以解密源自员工用户组的允许流量。在本示例中，解密模拟工程开发用户组允许规则中的流量。

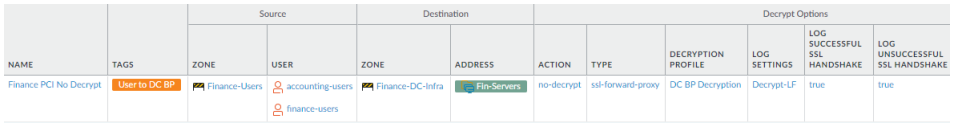
		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Engg to Dev Servers	User to DC BP	Engineering-Users	api-users engg-users	Engineering-DC-Infra	Dev-Servers	decrypt	ssl-inbound-inspection	DC BP Decryption	Decrypt-LF	true	true

- 配置 SSL 入站检查，以解密源自承包商、合作伙伴、客户和其他第三方的允许流量。在本示例中，解密模拟 SAP 承包商用户组允许规则中的流量。

		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
SAP Contractors to SAP Servers	User to DC BP	Contractors	sap-contractors	SAP-Infra	SAP DB Servers	decrypt	ssl-inbound-inspection	DC BP Decryption	Decrypt-LF	true	true

- 应用不解密配置文件，为出于业务、法规、合规性，或财务、健康、军事或政府流量等其他原因选择不解密的流量配置服务器验证。本示例展示如何在两组财务部用户访问 **Fin Servers**（财务服务器）地址组内的服务器时，从解密中将其排除。

不要将“无解密”配置文件应用到 *TLSv1.3* 流量，因为证书信息经过加密，所以防火墙无法基于证书信息阻止会话。



NAME	TAGS	Source ZONE	Source USER	Destination ZONE	Destination ADDRESS	Decrypt Options ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Finance PCI No Decrypt	User to DC BP	Finance-Users	accounting-users finance-users	Finance-DC-Infra	Fin-Servers	no-decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

Internet 到数据中心流量策略

配置 Internet 到数据中心的流量安全策略、解密策略和 DoS（拒绝服务）保护策略。

- Internet 到数据中心安全策略
- Internet 到数据中心解密策略
- Internet 到数据中心 DoS 保护策略

STEP 1 | 为 Internet 到数据中心流量创建应用程序允许列表安全策略规则，以控制并确保合作伙伴、承包商和客户访问的安全。

防止从受感染的外部客户端下载恶意软件，或是将恶意软件置于源自受感染的数据中心服务器上的外部服务器。为业务目的需要的应用程序创建允许规则，并创建外部动态列表 (EDL) 以阻止不良 IP 地址。对于每个规则，请在 **Actions**（操作）选项卡上配置 **Log at Session End**（会话结束时记录），并设置日志转发，以跟踪和分析规则违规。

在本示例中，将限制用于 Internet 到数据中心流量的应用程序和目标，并使用 **Negate**（否）选项阻止与 **Bad IPs List**（不良 **IP** 列表）EDL 的通信。

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Web Server Inbound	Internet to DC	universal	L3-External	~~Bad-IPs-List~~	any	any	Web-Server-Tier-DC	Web Servers	any	Acme	application-default	Allow		

为从 Internet 到其他服务器组（如果允许）和其他应用程序的流量创建类似规则。使每个规则特定于限制访问到仅需要的应用程序和服务器。

STEP 2 | 为 Internet 到数据中心流量创建解密策略规则，以解密允许流量。

配置 SSL 入站检查（并将目标服务器证书导入到防火墙）以解密安全策略规则允许用于 Internet 到数据中心流量的合作伙伴、承包商和客户流量。本示例展示的是前一步安全策略规则中的解密策略。

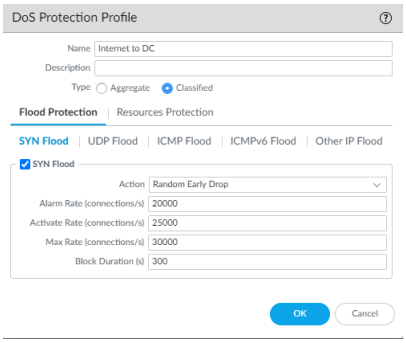
NAME	TAGS	Source ZONE	Source USER	Destination ZONE	Destination ADDRESS	Decrypt Options ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Internet to DC	Internet to DC BP	L3-External	any	Web-Server-Tier-DC	Web Servers	decrypt	ssl-inbound-inspection	DC BP Decryption	Decrypt-LF	true	true

创建解密规则，以便与 Internet 到数据中安全策略规则允许的流量相匹配。

STEP 3 | 创建 Internet 到数据中心 DoS 保护策略规则，以保护敏感服务器免遭拒绝服务 (DoS) 攻击，方法是：限制防火墙允许到服务器的每秒连接数 (CPS)，从而防止 SYN 泛滥攻击。

攻击者瞄准 Web 服务器层，因为如果他们将其攻下，就可以阻止对数据中心的大部分合法访问。应用具有 DoS 保护配置文件（限制传入的 CPS）的已分类DoS 保护策略规则，以防止可能影响服务器性能和可用性的流量峰值。

- 创建分类的 DoS 保护配置文件，以保护 Web 服务器层，防止 SYN 泛滥攻击。设置的 CPS 阈值取决于基线峰值 CPS 速率。



- 创建 DoS 保护策略规则，以指定正在保护的 Web 服务器，并对其应用分类的 DoS 保护配置文件。

NAME	TAGS	Source			Destination		SERVICE	ACTION	Protection		LOG FORWARDING
		ZONE/INTERFACE	ADDRESS	USER	ZONE/INTERFACE	ADDRESS			AGGREGATE	CLASSIFIED	
DC Web Server Protection	Internet to DC BP	L3-External	Bad IPs List	any	Web-Server-Tier-DC	Web Servers	service-http service-https	protect	none	profile: Internet to DC destination-ip-only	DoS-LF

要防止源自内部源的 SYN 泛滥攻击，则创建单独的 DoS 保护策略规则，从而将内部区域指定为源区域，而非 **L3-External**（**L3** 外部）。为外部和内部攻击创建单独的规则，以提供单独的报告，从而使对攻击尝试的调查变得更容易。

- 此外，为数据中心每个区域配置数据包缓冲区保护，以保护防火墙免遭可能会导致丢弃合法流量的单会话 DoS 攻击。

数据中心到 Internet 流量策略

配置数据中心到 Internet 的流量安全策略和解密策略。

- 数据中心到 Internet 安全策略
- 数据中心到 Internet 解密策略

STEP 1 | 创建数据中心到 Internet 允许规则，以保护到外部服务器的连接。

数据中心服务器可以从 Internet 上的服务器获得软件更新或证书状态。最大的风险是连接到错误的服务器。为更新创建严格的允许规则，以限制可访问的外部服务器和允许的应用程序（仅限默认端口）。这样，可防止受感染的数据中心服务器进行背景连线通讯，并通过非标准端

口上的 FTP、HTTP 或 DNS 等合法应用程序阻止数据泄露。此外，使用文件阻止配置文件的 **Direction**（方向）控制阻止出站更新文件，这样，就能仅允许下载软件更新文件。

对于每个规则，应用最佳实践安全配置文件，并在 **Actions**（操作）选项卡上配置 **Log at Session End**（会话结束时记录）。

与工程或其他组合作，更新软件，以记录并分析 *Web* 浏览会话，从而定义开发人员连接用于更新的 *URL*。

- 在这些示例中，允许工程服务器（**CentOS-Update-Servers**（**CentOS** 更新服务器）自定义 URL 类别）通过使用 **yum** 应用程序与 CentOS 更新服务器进行通信，并通过使用 **ms-update** 与 Microsoft 更新服务器（**Win-Update-Servers**（**Win** 更新服务器）自定义 URL 类别）进行通信（必须允许 **ssl**，因为 **ms-update**（**ms** 更新）与 SSL 相关）。

			Source			Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	ZONE	ADDRESS	APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
CentOS Update	DC to Internet BP	universal	Engineering-DC-Infra	Dev-Servers	any	L3-External	any	yum	application-default	CentOS-Update-Servers	Allow		

			Source			Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	ZONE	ADDRESS	APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
Windows Update	DC to Internet BP	universal	Engineering-DC-Infra	Dev-Servers	any	L3-External	any	ms-update ssl	application-default	Win-Update-Servers	Allow		

- 允许访问 DNS 和 NTP 更新（**NTP DNS Update Servers**（**NTP DNS** 更新服务器）自定义 URL 类别）。

阻止访问 *Internet* 网关上的外部 *DNS* 服务器，从而防止 *DNS* 流量从 *Internet* 流入到公共服务器。仅允许访问经批准的 *DNS* 服务器，并使用 DNS 安全服务阻止恶意 *DNS* 服务器连接。

			Source			Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	ZONE	ADDRESS	APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
NTP DNS Update	DC to Internet BP	universal	IT Infrastructure	DNS-NTP-Servers	any	L3-External	any	dns ntp	application-default	NTP-DNS-Update-Servers	Allow		

- 允许连接到 Internet 在线证书状态协议(OCSP)响应器，以检查身份验证证书的吊销状态，确保其有效。在防火墙上配置证书配置文件时，如果 OCSP 响应器无法访问，则可以设置 CRL 证书验证为 OSCP 的回退方法。

			Source			Destination						
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	ZONE	ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Cert Update	DC to Internet BP	universal	IT Infrastructure	IT-Server-Management	any	L3-External	any	ocsp	application-default	Allow		

STEP 2 | 创建数据中心到 Internet 解密策略规则，以解密前一步安全策略规则中允许的流量。

受到攻击的更新服务器会下载恶意软件，并在软件更新过程中进行传播，因此，关键是解密流量，以获得可见性。因为只有服务器账户可以启动更新流量且更新流量不包含个人信息或敏感信息，因此，不会存在隐私问题。

请勿解密 *OCSP* 证书吊销服务器的流量，因为，此流量通常使用 *HTTP*，因此，此流量是未加密的流量。此外，*SSL* 转发代理解密可能会破解更新过程，因为防火墙充当的是代理，并采用 *OSCP* 响应器可能视为无效的代理证书替换客户端证书。

- 解密数据中心和更新服务器之间的流量。在这两个示例中，对前一步中模拟安全策略规则允许的 CentOS 和 Windows 更新流量进行解密。

		Source		Destination			Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	ZONE	ADDRESS	URL CATEGORY	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
CentOS Update Decrypt	DC to Internet BP	Engineering-DC-Infra	Dev-Servers	L3-External	any	CentOS-Update-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

		Source		Destination			Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	ZONE	ADDRESS	URL CATEGORY	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Win Update Decrypt	DC to Internet BP	Engineering-DC-Infra	Dev-Servers	L3-External	any	Win-Update-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

- 解密数据中心服务器和 NTP 和 DNS 更新服务器之间的流量。在本示例中，对前一步中模拟安全策略规则允许的更新流量进行解密。

		Source		Destination			Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	ZONE	ADDRESS	URL CATEGORY	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
DNS-NTP Update Decrypt	DC to Internet BP	IT Infrastructure	DNS-NTP-Servers	L3-External	any	NTP-DNS-Update-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

数据中心内流量策略

配置数据中心服务器与应用程序层之间的流量安全策略和解密策略。

- 数据中心内安全策略
- 数据中心内解密策略

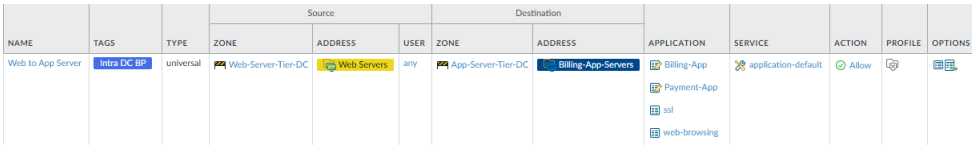
STEP 1 | 创建数据中心内应用程序允许规则，从而保护数据中心服务器免遭可能会受到攻击的其他数据中心服务器的影响。

常见的应用程序架构由三个服务器层构成：Web 服务器、应用程序服务器和数据库服务器。应用最佳实践安全配置文件到服务器层之间的大多数流量，以阻止威胁。请勿将安全配置文件应用至邮箱复制和备份流量等低价值、高容量的流量 — 防火墙已对原始流量进行检测，因此，在这些流量上花费 CPU 周期不会产生额外的价值。为这些应用程序创建允许规则，以防止误用。

对于每个规则，请在 **Actions**（操作）选项卡上配置 **Log at Session End**（会话结束时记录），并设置日志转发，以跟踪和分析规则违规。

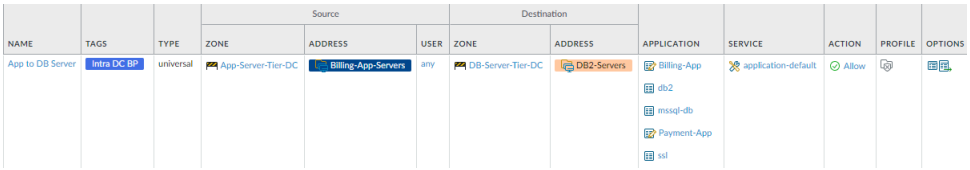
在本示例中，为用于创建自定义应用程序的两个内部财务专用应用程（**Billing-App**（计费应用程序）和 **Payment-App**（支付应用程序））序配置允许流量在应用程序服务器层之间流动的规则。

- 允许 Web 服务器层和应用程序服务器层之间的财务应用程序流量。



			Source			Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	ZONE	ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Web to App Server	Intra DC BP	universal	Web-Server-Tier-DC	Web Servers	any	App-Server-Tier-DC	Billing-App-Servers	Billing-App Payment-App ssl web-browsing	application-default	Allow		

- 允许应用程序服务器层和数据库服务器层之间的财务应用程序流量。



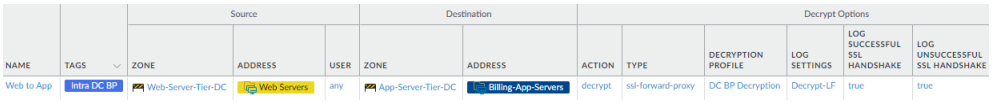
			Source			Destination						
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	ZONE	ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
App to DB Server	Intra DC BP	universal	App-Server-Tier-DC	Billing-App-Servers	any	DB-Server-Tier-DC	DB2-Servers	Billing-App db2 mssql-db Payment-App ssl	application-default	Allow		

STEP 2 | 创建数据中心内解密策略规则，以解密之前的安全策略规则中允许的流量。

很多人认为数据中心很安全，无需监视入侵者，因此，数据中心反而成为了攻击者的完美藏身之地。但是，网络其余部分存在的相同的基本原则在数据中心也是成立的：您无法保护自己免受看不见的东西的损害。对加密的数据中心流量进行解密，从而方便防火墙检查流量、控制访问、提供威胁可见性，从而保护您的宝贵资产。

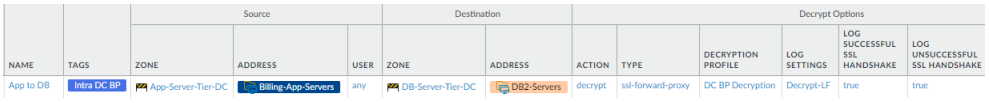
并非所有的数据中心流量都是加密的。不要花费资源来解密未加密的（明文）流量。

- 该规则为财务部门的计费服务器解密 Web 服务器层与应用程序服务器层之间的流量。



		Source			Destination		Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Web to App	Intra DC BP	Web-Server-Tier-DC	Web Servers	any	App-Server-Tier-DC	Billing-App-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

- 该规则为财务部门的计费服务器解密应用程序服务器层与数据库服务器层之间的流量。



		Source			Destination		Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
App to DB	Intra DC BP	App-Server-Tier-DC	Billing-App-Servers	any	DB-Server-Tier-DC	DB2-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

数据中心安全策略规则库顺序

在安全策略规则库中正确排序规则，以确保只允许您想要允许的应用程序和流量，避免规则产生意外影响。

数据中心安全策略规则库排序以正确的顺序展示前面示例中的完整规则库（允许规则和阻止规则），并解释每个规则的部署。安全策略规则库是安全策略规则的有序列表。

规则库中规则的顺序决定防火墙如何处理流量。当流量与规则库中的某个规则匹配时，防火墙会对流量执行规则的操作，并且不会将该流量与任何其他安全策略规则进行比较。这就是为什么安全策略规则库中规则的顺序至关重要的原因。如果规则的顺序错误，则流量可能会匹配您不希望其匹配的规则（这称为“遮蔽”）。

安全策略最佳实践手册包括安全策略规则库最佳实践，其中介绍了在构建安全策略规则库时应遵循的最佳实践。安全策略规则库最佳实践包括：

- 使规则库尽可能小，以便于管理。在某些情况下，您可以组合规则。一项良好的指导原则是，如果这些规则中的以下六个对象中有五个相同，则可以组合规则：源区域、目标区域、源 IP 地址、目标 IP 地址、服务端口和应用程序。
- 使用策略优化器来简化规则库。
- 使用应用程序组和地址组等组对象来简化规则库。
- 通常，将更具体的规则置于更通用的规则之前，以防止出现遮蔽。

遵循数据中心后期部署最佳实践

开始部署数据中心的最佳实践后，对网络进行监控，确保安全和访问按预期运行，然后在环境发生变化时维护数据库。

STEP 1 | 检查预定义应用程序报告（**Monitor**（监控） > **Reports**（报告） > **Application Reports**（应用程序报告） > **Applications**（应用程序）），以验证仅纳入安全策略规则允许的应用程序正在运行。

如果发现预期以外的应用程序，则查看安全策略规则，并对其进行优化，以消除预期以外的应用程序，或是纳入合法应用程序。

STEP 2 | 记录数据中心所有流量。

使用 Palo Alto Networks 的大量监控工具、日志记录工具、预定义报告和自定义报告以捕获并监控预期之外应用程序、用户、流量和行为的活动。

STEP 3 | 创建自定义报告，以监控阻止规则，从而阻止潜在攻击，并标识策略缺口和预期以外的行为，以便调整数据库。

STEP 4 | 创建自定义报告，以记录与规则库底部的预定义区域间默认允许规则匹配的数据中心内部流量，从而在默认情况下允许相同区域内的所有流量。

STEP 5 | 启用登录，并为与规则库底部的预定义区域间默认允许规则匹配的数据中心流量创建自定义报告，从而在默认情况下拒绝区域间的所有流量。

STEP 6 | 倾听并响应用户反馈。

用户抱怨无法访问应用程序，这说明在应用程序允许列表阻止其使用之前，网络上投入使用的规则库有缺口，或是应用程序有风险。

STEP 7 | 定期将您在规划期间采用的基线测量与当前测量进行比较，以评估进度、标识更改，并发现改进区域。

同时，重新审视未来理想的网络状态，以评估进度。如果采用 Panorama 管理防火墙，则监控防火墙健康状况，以便将设备与其基线性能以及相互之间进行比较，从而标识与正常行为的偏差

STEP 8 | 因为应用程序会进化，用户要求会发生变化，且内容更新会修改现有 App-ID 并引入新的 App-ID，因此，应随时间的推移对允许规则进行改进。

在安装新的内容发布之前，维护数据中心最佳实践规则库，并查看新的和修改过的 App-ID，这样，可以在更改影响策略时修改规则库。

STEP 9 | 使用 Palo Alto Networks 评估和检查工具对当前防御状态和最佳实践的使用情况进行评估。

STEP 10 | 有关每个规划、部署和后期部署的步骤，以及如何是您受益等详细信息，请参阅完整的数据中心最佳实践安全策略。

数据中心最佳实践安全策略

数据中心保存有公司最具价值的资产，包括专有源代码、知识产权、敏感的公司数据和客户数据。客户和员工相信您可以维护其敏感数据的机密性，并期望数据始终可用，因为，他们希望数据始终可用。要想保持业务的完整性和成功性，必须实施数据中心最佳实践安全策略，从而保护您的数据，防止攻击成功。

下列方法和建议以分阶段的优先级方式为您提供一个用于规划、设计和实施数据中心最佳实践安全策略的蓝图。如果尝试在网络所有区域上一次性实施所有保护，则创建数据中心最佳实践安全策略可能是一项艰巨的任务。但是，如果首先通过保护最具价值的资产来对最重要的保护内容进行评估，并开始实施数据中心最佳实践安全策略，则可以逐步过渡到允许您安全启用应用程序、用户和内容的安全策略，且不会带来任何不必要的风险。

数据中心安全策略最佳实践清单对预部署、部署和后期部署最佳实践进行概述，并在不需要详细说明的情况下提供更快实施最佳实践的办法。

什么是数据中心最佳实践安全策略？

数据中心最佳实践安全策略可保护公司的宝贵数据，保护您的客户、合作伙伴和供应商的机密信息，保护整个网络和业务运行的完整性，且有助于确保网络的持续可用性。此外，还可以阻止源自网络内外部以及随所有攻击媒介一同进入的攻击。

数据中心最佳实践安全策略可保护四种流量（发起连接的区域）：

1. 流入数据中心的本地用户流量。
2. 从 Internet 流向数据中心的流量。
3. 从数据中心流向 Internet 的流量。
4. 在服务器或 VM 之间流动的数据中心内部流量，也称为东西流量。

数据中心最佳实践安全策略可防止攻击者在数据中心获得立足点，阻止任何试图破坏数据中心的攻击者泄露数据，或是在网络内横向移动以攻击关键服务器。此外，还可以通过实施安全策略规则以实现与业务要求一致的最佳实践目标，从而阻止已知和未知威胁。它可以：

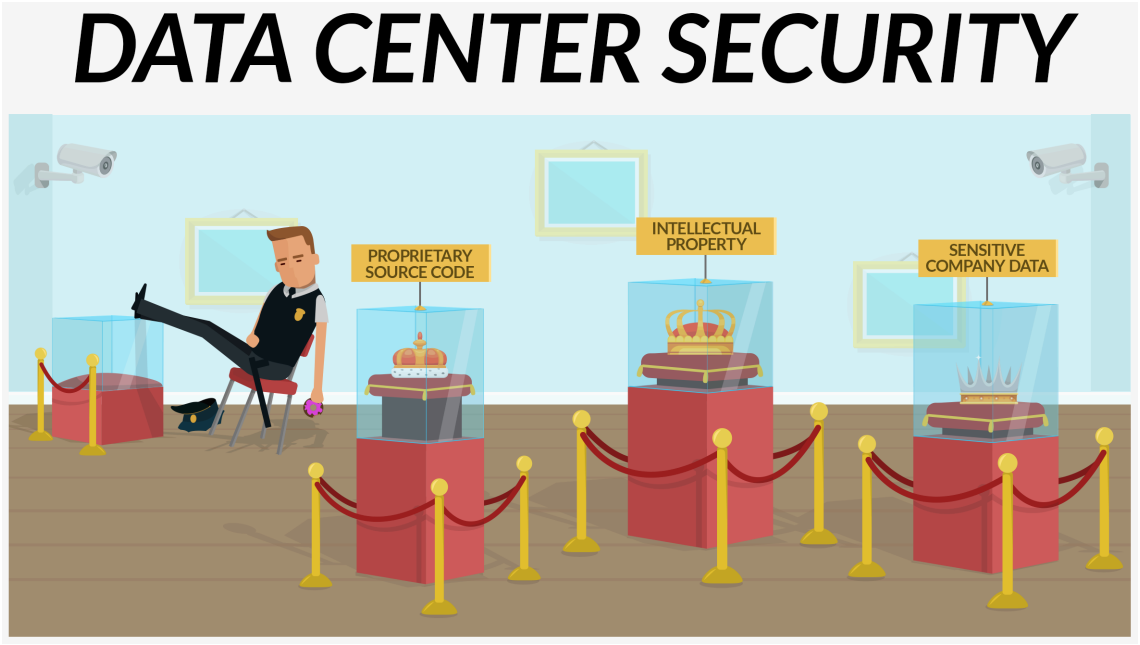
- 识别应用程序，无论端口、协议或规避技术如何，包括解密已加密流量。
- 识别并控制任何 IP 地址、位置或设备上的用户
- 防御通过应用程序传播的已知和未知威胁以及漏洞。
- 检测可能指示正在遭受攻击的异常行为。

此外，数据中心最佳实践安全策略还可在违反策略规则时捕获入侵者。违反规则可导致攻击停止，因为违规会导致下一代防火墙拒绝访问，并记录违规，这样就可以调查问题，并采取适当的行动。

为什么需要数据中心最佳实践安全策略？

保护网络的可用性、机密性和完整性，这样就可以安全地持续开展业务，并满足敏感数据保护规范要求，这一点至关重要。强化网络外部并允许网络内部保持柔性（因为网络内部是可信的）这种想法已过时，会让网络出现缺口，导致可从内部进行攻击，且并不适用于攻击者意志坚决、有足够资源且坚持在外围内找到立足点的场景。这就是为什么您需要向保护企业网络外围一样强有力地保护数据中心外围和内部。

内部攻击可能源自当前员工或现场承包商等。内部攻击的共同点是这种攻击均来自合法的用户或应用程序源。外部攻击可能源自网络犯罪分子、黑客活动分子和国家支持的攻击者，以及不太明显的攻击途径，例如受到攻击的合作伙伴或供应商系统，或是了解此网络的前雇员。外部攻击者的第一步是在网络内部获得立足点，将攻击转换为内部攻击。本质上而言，即使都源自外部，所有攻击均应属于内部攻击，因为一旦攻击者获得网络的访问权，就可以在整个网络中畅游。



如果攻击者窃取了合作伙伴的合法访问凭据，就可以伪装为合法用户访问您的数据中心。然后，在“柔软耐嚼的网络内部”，攻击者可以使用您的内部服务器和端点在整个网络中横向移动，并攻击关键系统。一旦外部攻击者攻击网络，则您将依靠网络、用户分段和网络内部的分层防御来保护您的数据，就像处理源自内部的攻击一样。

制定最佳实践安全策略有助于通过分段方式按照优先顺序保护数据中心免遭任何来源的攻击，首先保护最具价值的资产，然后逐步实施其他保护。从最佳期望安全策略逐步转换到最佳实践安全策略，这有助于通过切合实际的方式确保数据的机密性、组织的完整性以及数据中心的可用性。以下有关数据中心最佳实践安全策略设计和实施方面的建议展示了如何在最大限度减少对最终用户干扰的情况下通过同时分类所有流量来安全地启用应用程序、用户和内容。

数据中心最佳实践原则

以下最佳实践原则是实现攻击过程中所有阶段的检测和防护。

最佳实践原则	为什么重要？
检测所有流量，获得完整的可见性	通过查看网络流量，可以标识是否存在攻击者。检测流量，以查看流入、流经、以及流出数据中心的用户、应用程序和内容： ❑ 将下一代防火墙部署在能够检测所有网络流量的位置。若未部署有用于检测流入数据中心或在网络分段之间流动的流量的防火墙，则请勿允许此类流量。 ❑ 除非法规或合规性规则要求您使用健康、财务、政府或军事之类的流量，否则不得在进入或退出数据中心的所有流量上 ❑ 启用 SSL 解密。必须查看威胁，以保护您的网络免受威胁的影响。因为 50% 以上的网络典型流量都已加密，且此百分比仍在上升，因此，如果不解密流量，则无法完全保护您的网络。 ❑ 使用 App-ID 标识应用程序，并为专有应用程序创建自定义应用程序，这样，防火墙可以标识这些应用程序，并对其进行适当分类，然后采用正确的安全策略规则。这对于旧的遗留应用程序尤其重要，否则，这些应用程序将不会被正确分类，而被归类到“Web 浏览”或“未知 tcp”。 如果您有现用的应用程序替代策略，是专门为定义端口集合的自定义会话超时而单独创建的，则将现有的应用程序替代策略转换为基于应用程序的测量，方法为：将基于服务的会话超时配置为维护每个应用的自定义超时，然后迁移基于应用程序的规则管辖的规则。应用程序替代策略基于端口。使用应用程序替代策略维护端口集合的自定义会话超时时，您就无法通过应用程序了解这些流量的情况，所以就无从得知或控制哪些应用程序使用这些端口。基于服务的会话超时达到自定义超时时，同时维护应用程序可见性。 ❑ 对进入或退出数据中心的所有流量启用 User-ID，以便将应用程序流量及其内容相关的威胁映射到用户和服务。可以在网络区段（区域）上启用 User-ID，这样，必须对网络进行分段，以启用 User-ID。对网络进行分段是获得可见性和降低攻击面的最佳做法。 ❑ 在内部模式下将 GlobalProtect 部署为网关，以控制对数据中心的访问。GlobalProtect 通过检查用户信息来验证用户，并通过将主机信息定义的 HIP 对象和配置文件进行对比，以验证主机安全策略是否为最新。这可确保与网络相连的主机仍能保持您的安全标准级别。

最佳实践原则	为什么重要？
	❑ 对所有安全策略规则启用 **Log At Session End**（会话结束时进行记录）。 ***Log At Session Start***（在会话开始时记录）将消耗比仅在会话结束时记录更多的资源。在大多数情况下，您只能 ***Log At Session End***（在会话结束时记录）。仅在下列情况中才需同时启用 ***Log At Session Start***（在会话开始时记录）和 ***Log At Session End***（在会话结束时记录）：进行故障排除时、长期隧道会话（例如 *GRE* 隧道，除非您在会话开始时记录，否则您无法在 *ACC* 中看到这些会话），以及要获得对运营技术/工业控制系统 *(OT/ICS)* 会话（这些会话也是长期会话）的可见性时。 防火墙可通过查看流量使用其本机 App-ID、Content-ID、User-ID 和 Device-ID 技术将应用程序、威胁和内容与用户关联起来，而不管用户的位置或设备类型、端口、加密或规避技术如何。
缩小攻击范围	攻击面是软硬件网络交互的重中之重，包括应用程序、内容、用户、服务器、路由器以及其他物理和虚拟设备。减少攻击面可以减少攻击者用于攻击的漏洞。攻击面减少得越多，则越难攻击网络。 ❑ 评估数据中心，以便了解网络上的应用程序、内容和用户。 ❑ 通过创建基于应用程序的安全策略规则（仅在网络上允许具有合法业务用途的应用程序）以及用于封锁所有高风险应用程序（没有合法用途）的规则，主动地执行安全策略。 ❑ 使用在环境评估时获得的信息创建策略，以便根据业务要求、通用功能和全局策略要求将网络分段为区域，这样，每个区域内的资源均需要相同的安全等级。在数据中心内部，将诸如数据库、Web 服务器、应用程序服务器、开发服务器和生产服务器等应用程序层分段为区域。因为流量在区域间流动时必须穿过防火墙，因此，可以通过分段查看不同的应用程序层之间的流量。 通过粒度分段，您可以构建专注于每个区域业务要求并为每个分段提供适当保护的安全策略规则。此外，因为您可以通过 App-ID、Content-ID（威胁防护）和 User-ID 的组合标识应允许访问的流量，并拒绝其他访问的流量，因此，分段还有助于阻止数据中心内的恶意软件进行横向移动。 ❑ 在内部模式下将 GlobalProtect 部署为网关，以控制对数据中心的访问。 ❑ 要进一步减少攻击面，在允许应用程序流量的安全策略规则上，应用文件阻止配置文件以阻止恶意的和有风险的文件类型。通过使用防火墙的身份验证策略启用多重因素身份验证，从而防止凭据盗窃攻击，这样，即使攻击者已成功盗取凭据，但仍无法访问数据中心网络。
预防已知威胁	附加到安全策略的安全配置文件允许规则对流量进行扫描，以发现病毒、间谍软件、应用程序层漏洞利用、恶意文件等已知威胁。防火墙将根据安全配置文件的配置对这些威胁应用允许、警报、丢弃、阻止 IP 或连接重置等操作。

最佳实践原则	为什么重要？
	遵循内容更新的最佳实践，并在内容更新后尽快将其进行安装，以更新安全配置文件，然后应用最新保护到数据中心。安全配置文件是基本保护，易于应用至安全策略规则。 外部动态列表 (EDL) 可防止已知威胁。EDL 将恶意和有风险的 IP 地址、URL 或域导入防火墙，以防止已知威胁。EDL 来自可信的第三方、防火墙上预定义的 EDL、以及创建的自定义 EDL。EDL 可在防火墙上动态更新，无需执行提交操作。 预防已知威胁是启用解密很重要的另一个原因。如果不能查看威胁，则无论您是否了解该威胁，您都将是受害者，原因是您无法查看它。
预防未知威胁	如何检测之前从未见过的威胁？答案是转发所有未知文件到 WildFire进行分析。 WildFire 标识未知或目标恶意软件。当防火墙首次检测到未知文件时，防火墙会将文件转发至其内部目标，也会转发到 WildFire 云进行分析。WildFire 对文件（或电子邮件中的链接）进行分析，并在短短五分钟的时间内将判定返回给防火墙。WildFire 还包括用于标识文件的签名，以将未知文件转换为已知文件。如果文件包含威胁，则现在威胁成为已知威胁。如果文件是恶意文件，则下次当文件到达防火墙时，防火墙对其进行封锁。 您可以在 WildFire 提交日志中查看判定（**Monitor**（监控） > **Logs**（日志） > **WildFire Submissions**（**WildFire** 提交））。设置 WildFire 设备内容更新以每分钟自动下载和安装，让您始终拥有最新的支持。例如，支持将 Linux 和 SMB 文件首先交付至 WildFire 设备内容更新。

此外：

- 使用 Panorama 集中管理防火墙，以实现物理和虚拟环境内策略的一致实施，并实现集中可见性。
- 使用积极的安全实施，允许想要在数据中心网络上出现的流量，并拒绝其他流量。
- 创建标准化的、可扩展的设计，以在整个数据中心进行统一复制和应用。
- 获得管理人员、IT 和数据中心管理员、用户以及其他受影响方的支持。

通过关注特定业务和网络上最有可能发生的威胁对下一代安全进行分段，然后确定要进行保护的最重要的资产，并对其首先进行保护。请提出以下问题，以帮助对首先进行保护的资产进行优化：

1. 我们公司的优势在何处？什么属性可定义并将您的公司区分开来？什么资产映射到这些属性？与公司专有竞争力优势相关的资产应成为保护优先级阶梯的首级阶梯。例如，软件开发公司将优先考虑其源代码，而制药公司则会优先考虑其药物配方。
2. 是什么让企业的业务不会中断？公司日常运营需要哪些系统和应用程序的支持？例如，活动目录 (AD) 服务可让员工访问应用程序和工作站。若 AD 遭到破坏，则攻击者可以访问企业内所有

账户，从而全面访问您的网络。其他示例包括管理工具和身份验证服务器、以及包含用于业务操作所需的最关键数据的服务器等关键 IT 架构。

3. 如果资产丢失，该怎么办？资产丢失的后果越严重，保护此资产的优先级就越高。例如，用户体验可能成为区分服务公司的一个重要指标，因此，保护体验就具有最高优先级。专有流程和设备可能是区分制造公司的一个重要指标，因此，保护知识产权和专有设计就具有最高优先级。创建优先级列表，定义需要首先保护的资产。

定义数据中心网络的未来理想状态，并分阶段予以实现。定期重新审查您的定义，以纳入业务变化、新的法规和法律要求、以及新的安全要求。

如何部署数据中心最佳实践安全策略？

数据中心最佳实践安全策略的实施流程如下：了解数据中心网络及其资源，和防火墙的威胁防御能力，并基于此信息创建初始安全策略规则，从而首先保护您最具价值的资产。

- 如何评估您的数据中心 — 标识待保护的资产、这些资产面临的最大威胁、以及受访问约束的应用程序和用户，并确定这些的优先级。
- 如何解密数据中心流量 — 您无法保护您的网络免遭不能看到的威胁的影响。攻击者传递威胁的常用方法是加密流量。
- 创建数据中心分段策略 — 对数据中心进行分段，可防止已获得数据中心立足点的攻击者横向移动到其他区域。
- 如何创建数据中心最佳实践安全策略— 合法应用程序可以提供命令和控制恶意软件、常见漏洞和暴露 (CVE)、恶意软件内容的路过式下载、钓鱼攻击和 APT。最佳实践安全配置文件可保护允许流量免遭所有四个数据中心流量流动中包含的已知和未知威胁。
- 使用 Cortex XDR 客户端保护数据中心端点 — 防火墙阻止穿过网络的威胁。但是，在端点上执行的威胁并不通过网络，因此，不会穿过防火墙。在每个端点上安装 Cortex XDR 客户端，以防止端点本身的威胁。
- 创建数据中心流量阻止规则 — 阻止已知的恶意 IP 地址、攻击者经常利用的应用程序、旨在规避或绕过安全的应用程序、以及出于业务目的不需要存在于数据中心的应用程序。
- 定义初始用户到数据中心流量安全策略 — 未经授权的访问会对数据中心内的重要信息造成巨大风险。因为企业内部网络上的员工和其他用户经常是可信的，因此，安全预防措施可能比较松散。用户群和数据中心甚至可以存在于同一个额平面网络上。严格控制数据中心访问人员、不同用户组可以访安稳的资产、以及不同用户组对应用程序拥有的访问等级。
- 定义初始 Internet 到数据中心流量安全策略 — 保护数据中心服务器免遭 Internet 恶意流量的影响。因为受到攻击的数据中心会将服务器漏洞提供给第三方客户端，因此，利用服务器侧漏洞会打开数据中心，便于攻击者攻击，同时，让合作伙伴处于危险之中。
- 定义初始数据中心到 Internet 流量安全策略 — 隐藏在与 Internet 互联的受感染服务器上的命令和控制恶意软件可使用合法应用程序下载更多恶意软件。防止应用程序使用非标准端口，仅允许传输每个应用程序应合法使用的文件类型，并阻止恶意软件、钓鱼软件、代理匿名程序、对端到对端的 URL 类别，以及其他潜在恶意 URL 类别。
- 定义初始数据中心内部流量安全策略（东西流量） — 因为用户流量不会源自数据中心，且数据中心内部被视为可信，因此，数据中心的威胁经常被忽略。但是，如果攻击者攻击数据中心服务器，则服务器和 VM 之间的通信会传播恶意软件。最佳实践安全策略可防止攻击者在数据中心之间横向移动，并攻击更多系统，或是泄露数据。
- 记录并监控数据中心流量— 记录并监控允许和阻止流量可为转换并维护数据中心最佳实践安全策略的所有阶段提供信息。它可以在网络上显示应用程序、用户和流量模式，包括这些您可以不知道已经在此地存在的内容。此信息可为您调查潜在安全问题提供帮助。
- 维护数据中心最佳实践规则库 — 持续监控应用程序允许列表，这样，可以对规则进行调整，以适应新的受约束应用程序，并确定新的或修改过的 App-ID 如何影响您的策略。

数据中心安全策略规则库排序对安全策略规则库进行总结。

如何评估您的数据中心

要实现零信任安全模式，您必须了解数据中心的资产，并对其进行评估，这样，才可以确定首先需要进行保护最具价值的资产，并了解这些资产面临的主要风险。知道哪些人可以访问资产、允许的应用程序以及网络本身，可以对您需要的内容和您信任的内容进行评估，从而制定数据中心最佳实践安全策略，允许网络上出于合法业务目的的用户访问和应用程序。

1. 列出数据中心环境 — 列出数据中心的物理和虚拟环境，包括服务器、路由器、交换机、安全设备和其他网络架构，并列出数据中心的应用程序（包括内部开发的自定义应用程序）和服务账户。

   - 根据每个系统在网络中的角色以及对业务的重要性对其进行评估，从而确定需要首先保护的物理和虚拟架构的部分的优先级。例如，如果业务涉及信用卡交易，则处理信用卡交易的服务器以及用于承载信用卡信息的流量通信路径都是极具价值的资产，包含这些资产的应用程序就应优先处理。
   - 检查至少 90 天的流量日志，以列出数据中心网络上的应用程序。创建自定义报告，这有助于标识数据中心现有应用程序。使用数据中心应用程序清单指定想要在数据中心网络上批准或容忍的应用程序允许列表，包括内部开发的自定义应用程序。

     初始应用程序清单无需标识每个应用程序，因为，通过监控专为数据中心最佳实践安全规则库配置的阻止规则，就可以发现尚未标识的应用程序。重点放在列出您想要允许的应用程序和应用程序类型。当您完成应用程序允许列表后，就会阻止所有您未明确允许的应用程序。

     将应用程序映射到业务需求。如果应用程序未映射到业务需求，则对是否应允许其存在于网络上进行评估。明显不满足业务需求的应用程序会增加攻击面，并成为攻击者工具集的组成部分。即使不需要的应用程序是无辜的，但最佳做法是将其删除，这样，攻击者可以利用的攻击面就会更少。果多个应用程序执行相同的功能，例如，文件共享或即时消息，则考虑标准化一个或多个应用程序，以减少攻击面。

     如果任何内部自定义应用程序未使用应用程序默认端口，则记下需要用于支持自定义应用程序的端口和服务。考虑重写内部自定义应用程序，以使用应用程序默认端口。

     为需要在网络上进行类似处理的应用程序创建组，这样，您可以有效地将安全策略应用于应用程序组，而非单个应用程序。应用程序组可使安全策略的设计和实施更容易，原因是您可以将策略一次性应用于同一组内所有应用程序、更改整个组的策略、添加新的应用程序到组以应用该组的策略到新的应用程序、以及在多个安全策略规则中重新使用应用程序组。例如，设计用于数据中心存储应用程序的应用程序组可以包括 crashplan、ms-ds-smb 和 NFS 等应用程序。
   - 列出应用程序用于与数据中心服务器之间和数据中心服务器内部进行通信的服务账户。最佳做法是为每个功能使用一个服务账户，而非为多个功能使用同一个服务账户。这会限制对服务账户的访问，并使访问更加便捷，从而了解如何在系统受到攻击时使用服务账户。另一种最佳做法是标识已硬编码到应用程序的服务账户，这样，就可以基于此编写 IPS 签名，并监控账户的使用。

2. 表征数据中心流量 — 表征并映射数据中心流量，以了解数据如何流经您的网络，如何在用户和资源之间流动。聘用一个包含应用程序架构、网络架构、企业架构和业务代表的跨职能团队。表征通信流可为您提供有关网络流量的源和目标、典型流量模式和负载的信息，并帮助您了解网络上流量，对需要保护的最重要流量划分优先级。使用 应用程序命令中心小部件、Panorama 的 防火墙健康监控 功能、以及其他方法了解正常（基本的）流量模式，这有助于您了解可能表示有攻击的异常流量模式。
3. 评估数据中心分段— 对数据中心服务器层进行分段，这样，不同服务器层之间的通信必须通过下一代防火墙，以根据最佳实践安全策略进行解密、检查和保护，之后，源自用户群或 Internet 的通信将流经下一代防火墙。在数据中心外部，了解可以与每个数据中心区域进行通信的区域，然后，确定哪些区域应被允许与每个数据中心区域进行通信。
4. 评估用户群分段，并确定有权访问数据中心的人员 — 映射用户到组，以对用户群进行分段，这样，就可以实现对敏感系统访问实现更轻松地控制。例如，产品管理组的用户不应访问财务或人力资源系统。在活动目录（或您使用的任何系统）中，根据用户因合法业务目的所需的访问等级，创建粒度用户组，这样，您可以控制对系统和应用程序的访问。这包括按所需访问等级而分组的不同员工组以及不同承包商、合作伙伴、客户和供应商组。

   根据访问要求（而不仅仅是功能）创建用户组，从而减少攻击面，并为每个组仅授予适当级别的应用程序访问权限。通过营销或承包商等功能区域，可以创建多个已映射到应用程序访问要求的用户组。
5. 持续监控数据中心网络 — 记录并监控数据中心流量以揭示数据中心最佳实践安全策略中的缺口、暴露可能指示攻击的异常流量模式或预期以外的访问尝试，并诊断应用程序问题。

标识需要首先保护的最具价值的资产，然后标识可以在保护这些资产后进行迭代的资产。按顺序排除每个类别中需要保护的资产优先级。按顺序排定每个类别中需要保护的资产的优先级。对资产进行组织，先保护对特定业务更重要的资产。下表显示了一些可能性，但不全面。此外，在对首先要保护的资产确定优先顺序时，也请考虑法律合规性要求，以保护密码、个人信息和财务信息等数据。

表 **1:** 资产类别示例

最具价值的资产	其他有价值的资产	其余资产（迭代）
• 专利 • 源代码 • 产品设计、药物配方或用户数据等机密数据。 • 专有算法 • 代码签名证书和 PKI（这都是加密王国的密钥） • AD 域服务器（若丢失 AD，则攻击者可以创建凭据，实现对网络的无限制访问）	• 路由器和防火墙接口等关键 IT 基础架构 • 身份验证服务 • email • VPN，尤其适用于高度分散的企业 • 关键业务应用程序 • 文件共享服务器 • 数据库	• 网络实验室设备 • IT 管理系统 • 其他资产

最具价值的资产	其他有价值的资产	其余资产（迭代）
• 其他将您企业与其他企业区分开来的高价值资产		

对于每个企业而言，资产优先级都是独一无二的。对于服务公司来说，用户体验是区分公司与公司之间的一个重要指标，因此，最具价值的资产可能是确保最佳用户体验的资产。对于制造公司来说，最具价值的资产可能是专有工艺和设备设计。要确定首先保护哪些资产，其中一个方法是考虑丢失资产的后果。

如何解密数据中心流量

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。解密流量以暴露恶意软件非常关键，因为，典型网络的大部分流量都经过加密，而且数量在不断攀升。隐藏网络入侵、安装命令和控制恶意软件，以及使用加密的泄露数据的恶意软件活动的百分比越来越高。

要暴露加密应用程序和威胁，请安装物理的或虚拟新一代防火墙，这样，防火墙就可以查看数据中心的所有流量。解密所有可以解密的流量，尤其是高风险的流量类别和流向关键服务器的流量和业务关键型流量。解密流量可以识别这些流量，以便防火墙适当应用防病毒、漏洞保护、WildFire 和其他威胁防护。

要对流量进行解密，应创建解密配置文件，以指定如何处理 TSL 和 SSH 流量，以及选择不解密或不能解密的流量。解密配置文件为流量设置允许的协议、算法、模式和会话特征。可以将解密配置文件应用到解密策略规则，从而指定防火墙将解密配置文件应用至的流量。

防火墙支持两种类型的 SSL/TLS 解密和 SSH 解密：

- SSL 转发代理（出站流量）
- SSL 入站检查（入站流量）
- SSH 代理（通常用于管理网络设备的管理员的安全访问）

在数据中心内部，尽可能多地解密东西流量。如果因不正确的防火墙大小导致考虑性能，从而阻止您解密所有流量，则确定最关键服务器、最高风险的流量类别、以及不太可信的分段和 IP 子网的优先级，并在保留可接受性能的同时尽可能多地解密流量。需要提出的关键问题包括：“如果此服务器遭到攻击，该怎么办？”、“每种流量代表多大的风险？”、以及“对于我希望数据中心达到的性能等级，我愿意承受多少风险？”

对于从数据中心流向 Internet 的流量，解密除您必须做出例外的流量之外的所有流量。解密提供的可见性非常重要，因为您不想数据中心的服务器连接到恶意站点，传输恶意文件，或容易下载恶意软件。

在规划解密策略时，应考虑公司的安全合规性规则和位置。对于从用户流向数据中心的流量，尽管执行严格的解密策略可能最初会导致一些投诉，但这些投诉可让您关注已阻止的未受约束或不受欢迎的网站，因为，这些网络会使用弱算法，或是证书有问题。将投诉作为更好地了解网络上流量的工具。

此外，在解密策略中解密日志，如果资源允许，请记录成功和不成功的 SSL 握手。利用所有解密监控和故障排除工具来检查部署和优化策略以及配置文件。

解密流量会消耗防火墙资源。解密的通信量视每个数据中心而定。在确保防火墙部署的大小可以维持可接受的性能，且同时支持解密时，请考虑您希望解密的通信量（一些应用程序必须进行解密，而另一些应用程序则未加密，无需进行解密）、解密密码（更强、更复杂的密码要求更强的密码处理能力）、密钥大小（密钥越大，消耗的解密资源越多）、密钥交换类型（例如，*RSA* 密钥交换比 *PFS* 密钥消耗更多的处理资源）、以及防火墙的容量。与 *Palo Alto Networks* 销售团队和代表一起合作，根据特定网络适当调整防火墙部署的大小，这样，才可以解密流量，暴露威胁。

对于具有要求为其私钥提供极强安全的银行业务等业务的公司，可以使用第三方的硬件安全模块 (HSM) 来保护并管理公司的私钥，而非将其存储在防火墙上。

- 创建数据中心最佳实践解密配置文件
- 从数据中心解密中排除不合适的流量

创建数据中心最佳实践解密配置文件

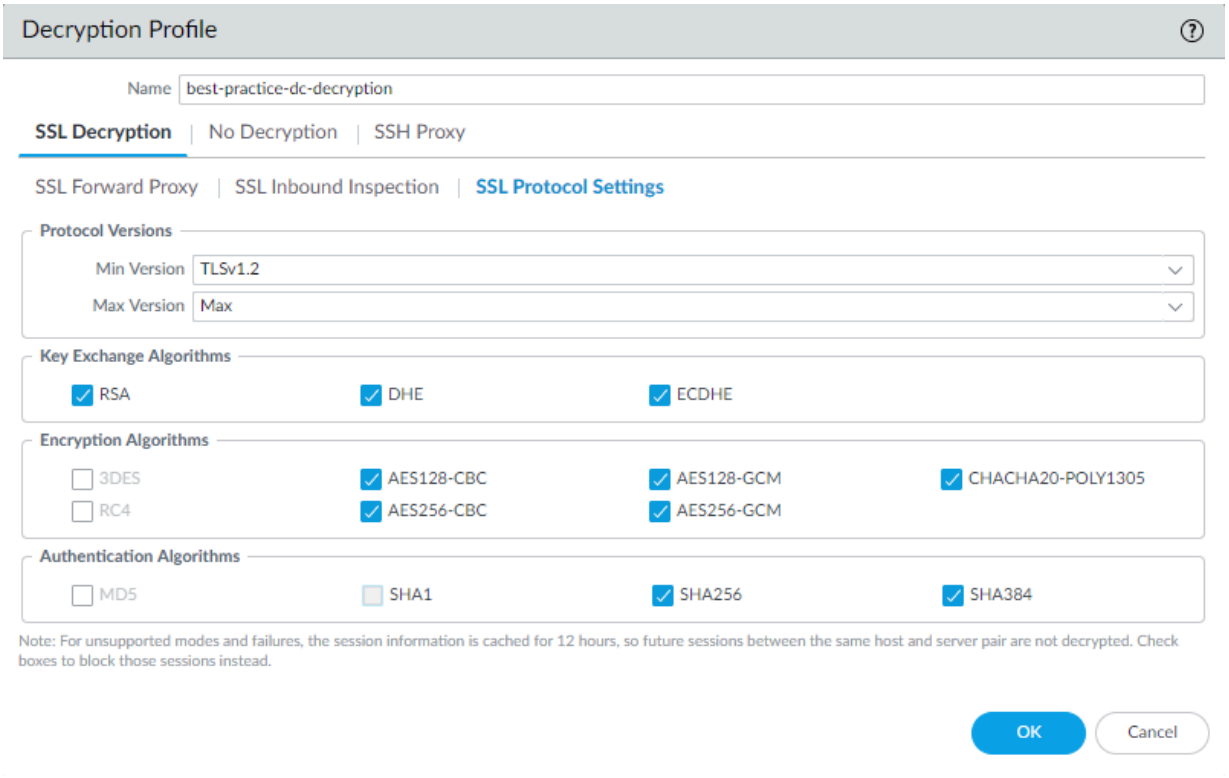
解密配置文件指定防火墙如何检查解密流量以及您不会解密或不选择解密的流量。防火墙检查协议、服务器证书、会话特征和密码（密钥交换算法、加密算法和身份验证算法）。您可以将解密配置文件（**Objects**（对象） > **Decryption Profile**（解密配置文件））应用于解密策略规则（**Policies**（策略） > **Decryption**（解密））。解密策略规则采用源、目标、服务类别和 URL 类别作为匹配标准，以定义待检查的流量，这样，您可以对应用解密配置文件的流量进行精细控制。您还可以在策略规则中配置解密日志和日志转发。

要解密出站流量，防火墙需充当内部客户端和外部服务器之间的转发代理。要检查入站流量，防火墙应对传入会话流量进行复制，并对复制进行解密和检查。

STEP 1 | 配置防火墙以执行 CRL/OCSP 检查，确保 解密期间显示的证书为有效证书。

STEP 2 | 配置 **SSL Decryption**（**SSL** 解密）> **SSL Protocol Settings**（**SSL** 协议设置）以阻止 TLSv1.0、TLSv1.1 和 SSLv3 等易受攻击的 SSL/TLS 版本，并避免 RC4 和 3DES 等弱加密算法和 MD5 和 SHA1 等弱身份验证算法拒绝会话。

SSL 协议设置应用于所有已解密流量。



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），从而阻止弱协议。尽可能使用最强的 TLS 协议。创建单独的解密策略和配置文件，最大限度提高安全性。例如，如果您是出于业务目的，您需要的遗留站点仅仅支持较弱的协议，则创建一个单独的解密配置文件以允许较弱的协议，并且仅将其应用于不支持最低 TLSv1.2 版本的站点。这也适用于不支持强算法的必要站点，并为不同的 URL 类别优化安全性与性能。

如果站点不包含合法的业务应用程序，则不得削弱您的安全状态来支持此站点 — 弱协议和密码包含攻击者可以利用的已知漏洞。如果站点输入您处于业务目的不需要使用的站点类型，则使

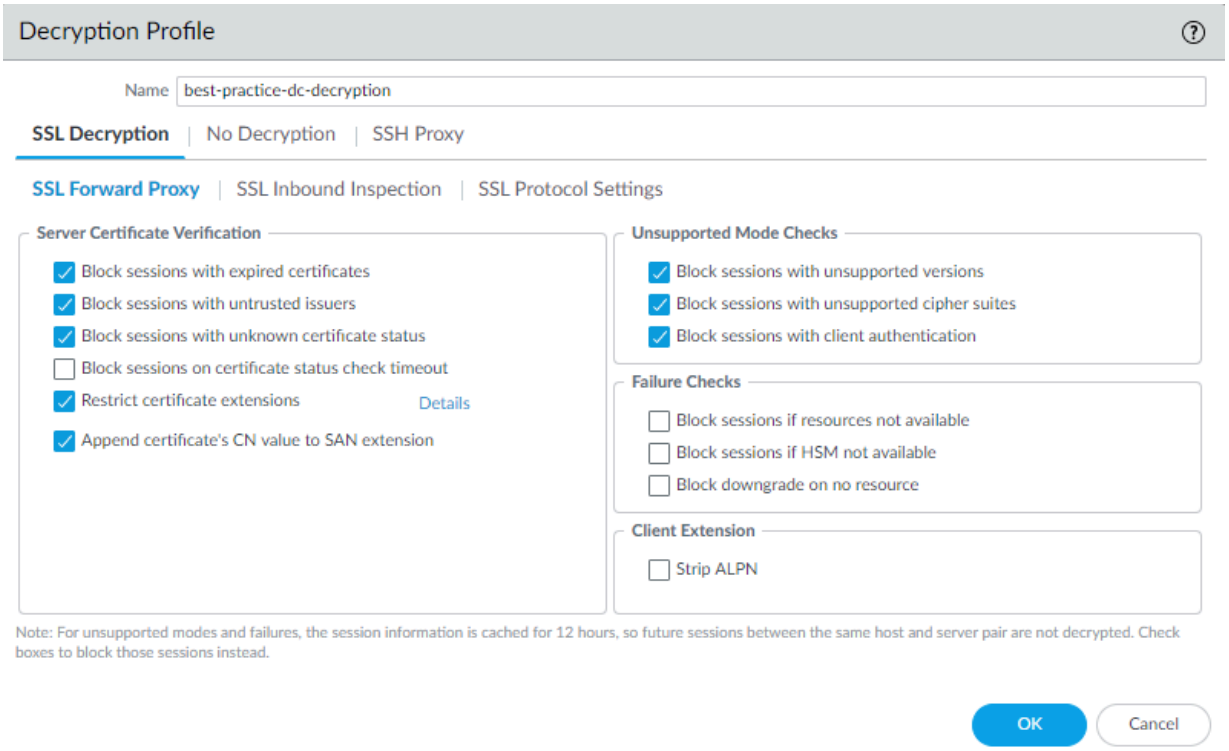
用 URL 筛选阻止对整个类别的访问。除非必须这样操作以支持重要的传统站点，否则不应支持弱协议或弱加密/身份验证算法。

设置 **Max Version**（最大版本）为 **Max**（最大），而不是特定版本，这样防火墙会随协议的改善自动支持最新和最佳协议。无论您是想将解密配置文件附加到管理入站（SSL 入站检查）或出站（SSL 转发代理）流量的解密策略规则，请避免允许弱算法。

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。

STEP 3 | 为出站流量配置 **SSL Decryption**（**SSL** 解密）> **SSL Forward Proxy**（**SSL** 转发代理）设置，阻止 TLS 协商过程中的异常，以及无法解密的会话。

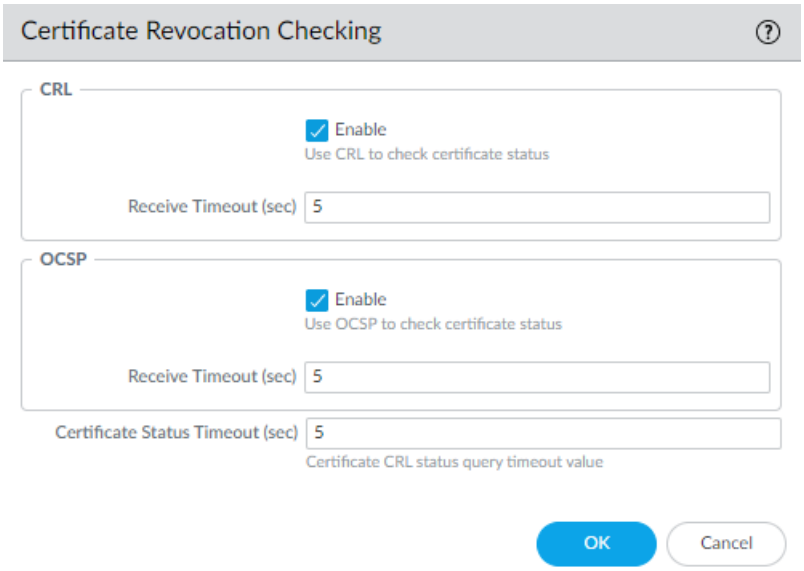
在某些情况下，设置的最佳做法取决于公司的安全合规性规则。将 SSL 转发代理解密配置文件应用于控制出站流量的安全策略规则。



阻止 TLS 协商过程的异常以及无法解密的会话。

- 服务器证书验证 — 是否需要检查 **Block sessions on certificate status check timeout**（阻止证书状态检查超时上的会话）框取决于您公司的安全合规性立场，因为这是更严格的安全和更好的用户体验之间的权衡。证书状态验证可以检查吊销服务器上的证书吊销列表 (CRL)，或使用在线证书状态协议 (OCSP) 查看颁发的 CA 是否已吊销，且证书不受信。但是，吊销服务器响应速度很慢，导致会话超时，即使是证书有效，防火墙也会阻止会话。如果您 **Block sessions on certificate status check timeout**（阻止证书状态检查超时上的会话），并且吊销服务器响应速度很慢，则可以使用 **Device**（设备）> **Setup**（设置）> **Session**（会话）

> **Decryption Settings**（解密设置），并单击 **Certificate Revocation Checking**（证书吊销检查），将默认超时值从五秒更改为其他值。



启用 CRL 和 OCSP 证书吊销检查，因为服务器证书可以包含 CRL 分发点 (CDP) 扩展中的 CRL URL 或颁发机构信息访问 (AIA) 证书扩展中的 OCSP URL。

虽然最佳做法是使用适当的证书，但某些证书可能会在主题备用名称 (SAN) 字段留空，可能会导致防火墙拒绝这些证书。如果 SAN 字段为空，则检查 **Append certificate’s CN value to SAN extension**（附加证书的 **CN** 值到 **SAN** 扩展）以自动将证书编号复制到 SAN 字段，这样，如果采用其证书的 SAN 字段未填充的站点开展业务，则可以接受其证书。否则，站点需要重新生成其证书，以符合正确的做法，并填充 SAN 字段。

阻止所有其他服务器证书验证异常。

- 不受支持的模式检查 — 如果不阻止带不支持版本和不支持密码套件的会话，则用户会受到一条警告消息，告知用户可以通过单击访问有风险的网站。配置严格的 SSL 协议设置的原因是为了阻止并保护使用这些弱（有风险的）协议版本和算法的服务器。此外，使用不支持模式检查阻止会话可保护您免受恶意后门和其他使用自定义和非标准解密以混淆其活动的威胁。

  使用客户端身份验证阻止会话可让您选择是否允许或阻止使用客户端身份验证的会话。虽然服务器身份验证可以是用于会话建立的唯一身份验证，但一些站点会使用相互身份验证（即服务器和客户端身份验证）以建立会话。使用 X.509 数字证书的客户端身份验证类似于服务器身份验证，因为两种方法均使用可信的证书颁发机构办法的数字证书来对会话进行身份验证。客户端证书充当客户端的数字标识符，驻留在客户端设备上，不能移植到其他设备。但是，因为防火墙需要客户端和服务器证书以执行双向解密，但防火墙仅知道服务器证书，因此，客户端身份验证可阻止防火墙解密会话。这会对用于客户端身份验证会话的解密进行破解。

  如果您不启用使用客户端身份验证阻止会话，当防火墙尝试解密使用客户端身份验证的会话时，防火墙会允许此会话，并在其包含服务器 URL/IP 地址、应用程序和解密配置文件的本地解密排除缓存中添加一个条目。条目会在缓存中保留 12 小时，然后年龄超时。如果同一

用户或不同的用户尝试在 12 小时内使用客户端身份验证访问服务器，则防火墙将会话与解密排除缓存条目进行匹配，不会尝试解密此流量，并允许加密会话。

如果排除缓存已满，则防火墙会在新条目到达时清除最旧的条目。如果更改解密策略或配置文件，则防火墙刷新排除缓存，因为更改策略或配置文件会更改会话的分类结果。

如果检查使用客户端身份验证阻止会话，则防火墙阻止使用客户端身份验证的会话，但不包括 SSL 解密排除列表上站点的会话（**Device**（设备）> **Certificate Management**（证书管理）> **SSL Decryption Exclusion**（**SSL** 解密排除））。

除了 SSL 解密排除列表上的预定义站点外，您可能需要运行来自使用客户端身份验证的其他站点上的网络流量。创建一个根据客户端身份验证允许会话的解密配置文件。将其添加到仅用于包含应用程序的服务器的解密策略。为了进一步提高安全性，您可能需要多重因素身份验证来完成用户登录过程。

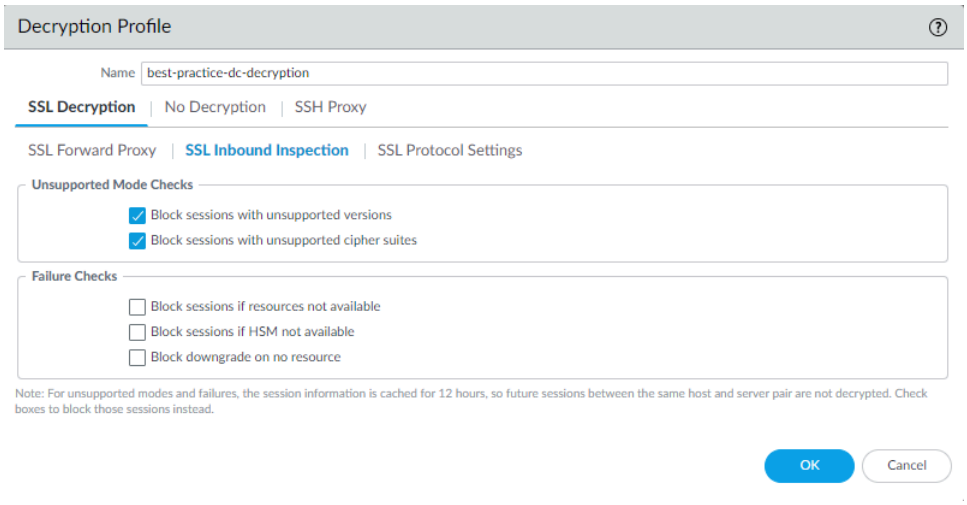
对于所有其他流量，则应用使用客户端身份验证阻止会话的解密配置文件。

- 失败检查 — 如果未在 **Block sessions if resources not available**（资源不可用时阻止会话），则风险是由于缺少处理资源，可能会允许有潜在危险的连接。如果在资源不可用时阻止会话，则可能会影响用户体验。是否执行失败检查取决于您公司的安全合规性立场以及您的业务对用户体验的依赖性，这与更严格的安全性相关。

  如果使用硬件安全模块 (HSM) 来存储私钥，则是否检查 **Block sessions if HSM not available**（**HSM** 不可用时阻止会话）就取决于与私钥必须来自何处以及如何想在 HSM 不可用时处理解密流量相关的合规性规则。例如，如果您的公司要求使用用于私钥签名的 HSM，则在 HSM 不可用时阻止会话。但是，如果您的公司对此不那么严格，则您可以考虑在 HSM 不可用时不阻止会话。（如果 HSM 关闭，则防火墙可以处理缓存有来自 HSM 响应的站点的解密，但不会处理其他站点的解密。）在这种情况下，最佳做法是根据您公司的政策行事。如果 HSM 对您的业务至关重要，则在高可用性 (HA) 对中运行 HSM（PAN-OS 8.0 支持 HSM HA 对中的两个成员）。
- **Block downgrade on no resource**（在无资源时阻止降级）— 如果防火墙没有适用于 TLSv1.3 的处理资源，则阻止将防火墙从 TLSv1.3 降级到 TLSv1.2。如果阻止降级，那么，一旦防火墙的 TLSv1.3 资源用完，就会丢弃使用 TLSv1.3 的流量，而不是降级到 TLSv1.2。如果不阻止降级，那么，一旦防火墙的 TLSv1.3 资源用完，就会降级到 TLSv1.2。但是，在资源不可用时阻止降级会让用户通常使用的站点暂时无法访问，从而可能会影响用户体验。是否执行失败检查取决于您公司的安全合规性立场以及用户体验的依赖性，这与更严格的安全性相关。您可能希望创建一个单独的解密策略和配置文件，以管理您不想降级 TLS 版本的敏感流量的解密。

STEP 4 | 配置 **SSL Decryption**（**SSL** 解密）> **SSL Inbound Inspection**（**SSL** 入站检查）设置，检查从外部客户端到内部服务器的流量，并阻止可疑会话。

将 SSL 入站检查解密配置文件应用于控制入站流量的安全策略规则。



- 不受支持的模式检查 — 防火墙不会解密其不支持的会话版本和密码。要防止攻击者使用不受支持的版本和密码嵌入网络，则阻止防火墙不支持的会话版本和密码。此外，使用不支持模式检查阻止会话可保护您免受恶意后门和其他使用自定义和非标准解密以掩盖其活动的威胁。

  在服务器上，仅启用防火墙支持的密码。确保此兼容性可在客户端和服务器之间实现更顺畅的协商。

- 失败检查 — 如果未在 **Block sessions if resources not available**（资源不可用时阻止会话），则风险是由于缺少处理资源，可能会允许有潜在危险的连接。如果在资源不可用时阻止会话，则可能会影响用户体验。是否执行失败检查取决于您公司的安全合规性立场以及您的业务对用户体验的依赖性，这与更严格的安全性相关。

  如果使用硬件安全模块 (HSM) 来存储私钥，则是否检查 **Block sessions if HSM not available**（**HSM** 不可用时阻止会话）就取决于与私钥必须来自何处以及如何想在 HSM 不可用时处理解密流量相关的合规性规则。例如，如果您的公司要求使用用于私钥签名的 HSM，则在 HSM 不可用时阻止会话。但是，如果您的公司对此不那么严格，则您可以考虑在 HSM 不可用时不阻止会话。（如果 HSM 关闭，则防火墙可以处理缓存有来自 HSM 响应的站点的解密，但不会处理其他站点的解密。）在这种情况下，最佳做法是根据您公司的政策行事。如果 HSM 对您的业务至关重要，则在高可用性 (HA) 对中运行 HSM（PAN-OS 8.0 支持 HSM HA 对中的两个成员）。

- **Block downgrade on no resource**（在无资源时阻止降级）— 如果防火墙没有适用于 TLSv1.3 的处理资源，则阻止将防火墙从 TLSv1.3 降级到 TLSv1.2。如果阻止降级，那么，一旦防火墙的 TLSv1.3 资源用完，就会丢弃使用 TLSv1.3 的流量，而不是降级到 TLSv1.2。如果不阻止降级，那么，一旦防火墙的 TLSv1.3 资源用完，就会降级到 TLSv1.2。但是，在资源不可用时阻止降级会让用户通常使用的站点暂时无法访问，从而可能会影响用户体验。是否执行失败检查取决于您公司的安全合规性立场以及用户体验的依赖性，这与更严格的安全性相

关。您可能希望创建一个单独的解密策略和配置文件，以管理您不想降级 TLS 版本的敏感流量的解密。

STEP 5 | 对于 SSH 流量，配置 SSH 代理解密配置文件设置。

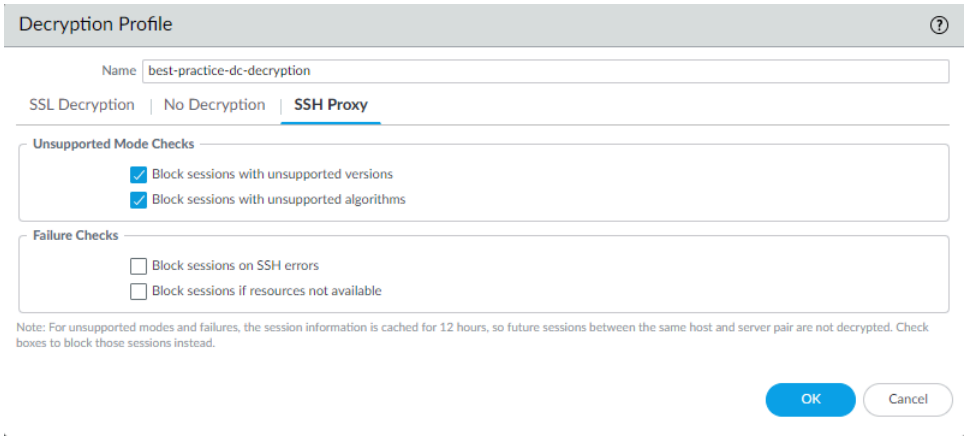
SSH 解密允许正常路由的 SSH 流量，拒绝 SSH 隧道（SSH 端口转发）流量，但不会在 SSH 流量上执行内容或威胁检查。SSH 隧道会话可以挖掘 X11 Windows 数据包和 TCP 数据包。一个 SSH 连接可能包含多个通道。将 SSH 解密配置文件应用于流量时，对于连接中的每个通道而言，防火墙会检查流量 App-ID，标识通道类型。通道类型可以是：

- 会话
- X11
- 转发的 tcpip
- 直接的 tcpip

当通道类型是会话时，防火墙将流量标识为允许的 SSH 流量，例如 SFTP 或 SCP。当通道类型是 X11、forwarded-tcpip 或 direct-tcpip 时，防火墙将流量标识为 SSH 隧道流量，并加以阻止。

对于大多数用户组，可能不会允许数据中心的 SSH 流量。SSH 通常用于访问服务器，这并不是您希望大多数用户拥有的功能，因为这会使您的数据中心服务器面临更大的风险，访问 Linux 服务器，并传输文件。您不能解密 SSH 流量，因此，使用 SSH访问数据中心资源的任何人必须是可信的 — 即便如此，所有威胁配置文件均应附加到允许 SSH 访问的任何规则，以扫描恶意软件、病毒、间谍软件等。

SSH 的示例用例是管理和维护数据中心服务器，并使用 SSH 进行远程访问的 IT 人员。

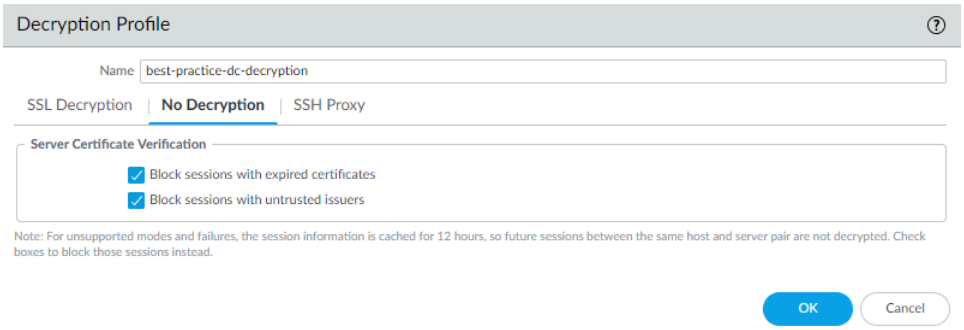


- 不受支持的模式检查 — 防火墙不会解密其不支持的会话版本和密码，且不受支持的版本和密码可能容易受到攻击。要防止攻击者使用不受支持的版本和密码嵌入网络，则阻止防火墙不支持的会话版本和密码。此外，使用不支持模式检查阻止会话可保护您免受恶意后门和其他使用自定义和非标准解密以掩盖其活动的威胁。
- 失败检查 — 如果未在 **Block sessions if resources not available**（资源不可用时阻止会话），则风险是由于缺少处理资源，可能会允许有潜在危险的连接。如果在资源不可用时阻止会话，则可能会影响用户体验。是否执行失败检查取决于您公司的安全合规性立场以及您的业务对用户体验的依赖性，这与更严格的安全性相关。

STEP 6 | 对于选择不解密的流量，配置 **No Decryption**（不解密）设置，阻止证书过期或发行者不被信任的加密会话访问站点。

将不解密配置文件仅用于出于法规或合规性规则等原因选择不解密的流量，不得将其用于由于锁定证书等技术原因不能解密的流量（将该通信添加到 SSL 解密排除列表中）。最佳做法是尽可能多地解密数据中心的流量。

请勿将不解密配置文件附加到用于您不解密的 *TLSv1.3* 流量的解密策略。与之前的版本不同，*TLSv1.3* 将加密证书信息，这样，防火墙就无法查看证书数据，也不会阻止过期证书会话或不可信颁发机构会话，因此，配置文件就会无效。（防火墙可对 *TLSv1.2* 以及更低版本执行证书检查，因为这些协议不会加密证书信息，您应对这些流量应用“不解密”配置文件。）但是，应为未解密的 *TLSv1.3* 流量创建解密策略，因为除非此解密策略可以控制该流量，否则，防火墙将不会记录未解密的流量。



从数据中心解密中排除不合适的流量

有两种类型的流量不适合解密：

- 因为使用证书验证、固定证书或不完整证书链等技术原因会破解解密的流量。
- 您选择不解密的流量。

防火墙会为因技术原因而破解解密的常用站点提供预定义的 SSL 解密排除列表（**Device > Certificate Management > SSL Decryption Exclusion**（设备 > 证书管理 > **SSL** 解密排除））。您可以通过单击站点主机名旁边的复选框，并单击禁用从列表中删除预定义站点，也可以将站点添加到此列表。仅将解密排除列表用于因技术原因会破解解密的站点，不得将其用于您选择不解密的站点。如果解密破解重要的应用程序，则将其添加到解密排除列表，以便为与应用程序相关的证书中的特定 IP 地址、域或公用名创建列外。如果进行解密，则有些内部自定义应用程序可能会中断。

如果解密配置文件允许 **Unsupported Modes**（不受支持的模式）（具有客户端身份验证、不受支持的版本、或不受支持的密码套件的会话），防火墙会自动将使用允许的不受支持模式的服务器和应用程序添加到本地解密排除缓存中（**Device**（设备） > **Certificate Management**（证书管理） > **SSL Decryption Exclusion**（**SSL** 解密排除） > **Show Local Exclusion Cache**（显示本地排除缓存））。阻止不受支持的模式时，您可以提高安全性，但也会阻止与使用这些模式的应用程序进行通信。

如果将站点排除在解密之外的技术原因是证书链不完整，则可以使用解密日志中的信息来修复不完整的证书链，以便您可以允许、解密和检查流量。

您可以因法规和法律合规性等原因选择不解密流量。例如，欧盟 (EU)《一般数据保护条例》(GDPR) 要求对所有个体的全部个人数据进行强有力的保护。GDPR 对所有公司都有影响，包括需要收集或处理 EU 居民个人资料的外国公司。不同的法规和合规性规则可能意味着您对不同国家或地区的相同数据采用不同的处理方法。企业通常可以在其公司数据中心解密个人信息，因为企业对这些信息具有拥有权。最佳做法是尽可能多地解密流量，这样，您才能查看并对其执行安全保护。

对于您选择不解密的流量，必须确保此流量是您不想要解密的流量，然后创建基于策略的排除，从而指定应用程序、用户组、源和目标、URL 类别和/或服务，以尽可能多地限制每个排除。解密排除越具体越好，这样，您就不会无意中从解密中排除超过必需的流量。

创建数据中心分段策略

一个未分段的平面网络很难进行防御，原因是如果攻击者获得对网络的访问，就可以在整个网络内横向移动，并破坏关键系统。在企业用于保存其最宝贵资产的数据中心内部，情况尤其如此。诸如 VLAN 和 ACL 之类的旧分段方法不能很好地扩展，难以自动化，且未考虑用户、内容或应用程序，因此，几乎无法控制流量或是监控流量。

创建分段策略，为数据中心资源提供更细粒度的控制，从而更好地查看流量。因为流量在流经分段时必须流经防火墙（分段网关），因此分段策略越精细，所获得的流量可见性就越高。借助分段策略，还可以更加轻松地实现合规性及合规性审计，因为您可以在非常精细的级别控制对敏感、个人和关键任务数据的访问，并且只允许对这些数据进行必要访问。这样可以保护数据并缩小审计范围。

数据中心分段策略取决于您的架构和业务目标，因此，无法实现“一刀切”。但是，您可以通过学习通用指南设计并实施分段策略，从而保护您数据中心的网络及其宝贵的信息。

- 如何对数据中心进行分段
- 如何对数据中心应用程序进行分段

如何对数据中心进行分段

如何对数据中心进行分段视您的业务需求和数据中心网络架构而定，包括可能会决定分段方法的 SDN 解决方案。例如，vwire 接口可控制 NSX 主机上的防火墙连接。因为 vwire 接口不能路由或切换 NSX 主机上的流量，因此，必须属于同一个区域，这样，特定租户（部门、客户或应用程序层）的所有资源均可以驻留到一个区域，且防火墙可以使用动态地址组对此区域内的应用程序流量进行分段。每个租户都拥有一个带自己 vwire 接口的单独区域。对于其他 SDN 解决方案，单独的虚拟防火墙实例可能会对流量进行分段。

Palo Alto Networks 下一代防火墙提供了灵活的流量分段工具：

- 区域 — 跨区域的流量需要通过防火墙进行检测。数据中心所有允许的通信均必须穿过防火墙，并进行全面的威胁检查（防病毒、防间谍软件、漏洞保护、文件阻止、WildFire 分析、以及专用于从企业流出的数据中心流量以及客户租户包含的应用程序的 URL 筛选）。默认情况下，防火墙拒绝区域之间的所有流量（区域间流量）。您必须编写特定的安全策略规则，以允许流量通过区域间，这样，仅您明确允许的流量可以从一个区域流向另一个区域。如何使用区域对数据中心进行分段取决于您需要将哪些资产与其他资产分开。例如，常见架构包括用于开发服务器和生产服务器的单独区域。您可以利用这些区域对包含支付卡信息 (PCI) 或个人身份信息 (PII) 等极敏感信息的服务器进行分段，对营销、工程和人力资源等公司不同的内部部门进行分段，以及对客户资源和客户托管的应用程序进行分段。

  考虑使用区域保护配置文件来保护区域免遭泛滥、侦察活动（端口扫描和主机扫描）、基于第三层数据包的攻击、以及基于非 IP 协议（第二层）数据包的攻击。
- 动态地址组 — 动态地址组是防火墙导入并在安全策略中使用的 IP 地址列表，用于动态（而非静态）定义组。添加或删除动态地址组中的 IP 地址可自动更新安全策略，无需在防火墙上执行

提交操作。在区域内，使用安全策略允许规则中的动态地址组支持特定应用程序和服务的服务器到服务器交互。例如，在 NSX 中，使用动态地址组对应用程序层中的服务器层进行分段。

- **User-ID** — 启用 User-ID 以根据用户组创建应用程序允许规则，对应用程序和服务器组中用户进行分段。

在制定数据中心分段计划时，请遵循以下一般准则：

- 如何评估您的数据中心，以便可以分阶段地对数据中心进行分段，并首先保护最具价值和最敏感的资产。
- 在数据中心内使用 SDN 解决方案（NSX、ACI、OpenStack 等）提供可扩展的、敏感的、且虚拟化的基础架构。SDN 是实现数据中心网络集中管理、最大化利用计算资源、扩展并自动化网络、控制和保护虚拟网络上流量安全的最佳方法。虽然您可以创建一个基本上可以复制 SDN 架构的非 SDN 架构，但这样做很困难、耗时，且容易出现导致中断的错误，不应视为最佳做法。SDN 解决方案可在不影响安全的前提下最大化地利用数据中心底层计算资源。
- 使用下一代物理防火墙对非虚拟化的旧式服务器进行分段，并保护其安全，然后使用 VM 系列防火墙对数据中心虚拟网络进行分段，并保护其安全。
- 对在同一数据中心分段内执行类似功能，且需要相同安全级别的资产进行分组。例如，将连接到 Internet 的服务器置于同一分段中。

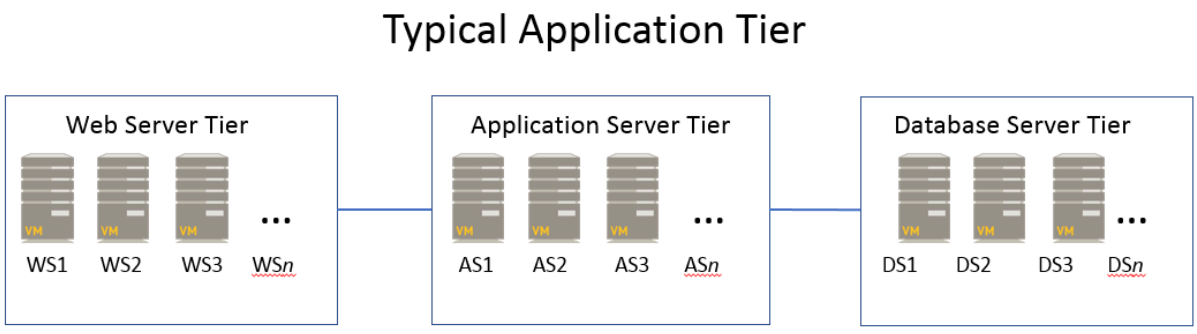
根据多项标准制定分段计划，以制定最能保护您业务的正确计划。

如何对数据中心应用程序进行分段

对数据中心应用程序分段，可防止恶意软件在应用程序之间移动，并为用户安全启动这些应用程序。应用程序层可为数据中心应用程序提供所需的资源和功能。应用程序层包括多个协同工作的服务器层，以完成与特定应用程序相关的请求和命令。通常，应用程序层包含三个服务器层：

- *Web* 服务器层 — 用户的应用程序接口。
- 应用程序服务器层 — 从 Web 服务器层获取请求，以处理和生成应用程序功能。
- 数据库服务器层 — 包含运行应用程序所需数据。

每个服务器层都包含功能相似且协同工作的服务器，这样，应用程序层可以向用户提供应用程序。



每个应用程序层内的服务器层都可创建一个 VM 服务链。服务链引导流量通过数据中心虚拟设备，以提供应用程序服务。在应用程序层中，Web 服务器可与包含应用程序代码的应用程序服务

器进行通信，且该应用程序服务器可与包含内容的数据库服务器进行通信。驻留在应用程序层中不同服务器层中的这三个服务器之间的通信就是服务链。

数据中心包含许多可专用于特定部门、客户、承包商或其他组的应用程序层。对数据中心应用程序基础架构进行分段，可防止应用程序资源之间未经授权且不必要的通信，并检测应用程序流量。

应用程序分段	如何对应用程序分段
应用程序层	通过为每个服务器层配置单独的防火墙区域，对每个应用程序层内的服务器层进行分段，这样，您可以控制对每组服务器的访问，并在每个服务器之间流动的流量通过防火墙时进行检测。例如，将 Web 服务器、应用程序服务器和数据库服务器放置在不同的区域，这样，服务器层之间的流量始终通过下一代防火墙进行全面检测。 根据业务需求，您可能需要为每个应用程序层创建多个区域，以分隔租户、均衡负载、将应用程序层用于不同的目的、提供不同级别的安全、或是连接到不同的服务器组。仅通过对同一区域内需要类似信任等级且需要与类似应用程序层的服务器进行分组，对数据中心进行分段，从而减少每个应用程序层的攻击面。
Web 服务器层	尽管会存在诸如 IT 部门配置直接安全访问数据中心服务器以方便管理的特殊情况，但流量通常会通过 Web 服务器进入数据中心。与其他服务器层一样，为每个 Web 服务器层创建单独的区域，以便对其应用粒度安全策略。 因为 Web 服务器层与数据中心外部的设备进行通信，因此，攻击者对其非常重视。将 Web 服务器层部署在单独网络上，例如，使用 VLAN。从 VLAN 流进和流出的所有流量，即进入或离开数据中心的所有流量，均必须通过下一代防火墙。要实现这一点，可以将下一代防火墙配置为默认网关，或是使用 NSX 等 SDN 解决方案来引导流量。 对 Web 服务器层中的服务器进行分段，可防止其相互之间进行通信。例如，通过使用 *NSX 分布式防火墙 (DFW)* 等传统规则可开放一个端口，或阻止层内的流量。
应用程序服务器的基础架构服务	对允许提供 DNS、DHCP 和 NTP 等关键基础架构服务，且仅使用适当的应用程序仅访问特定 IP 地址的服务器进行分段。 仅允许流量流向批准的 *DNS* 服务器。使用 DNS 安全服务阻止恶意 *DNS* 服务器连接。
应用程序	使用 App-ID 创建基于应用程序的允许列表安全策略规则，通过控制可以访问每个应用程序的人员，以及可以使用动态地址组访问哪些服务器组，从而对应用程序进行分段。您可以通过 App-ID 将粒度安全策略规则应用于可以驻留在同一计算资源但需要不同级别安全性和访问控制的应用程序。

应用程序分段	如何对应用程序分段
	创建自定义应用程序以唯一地标识专有应用程序，并对访问权限进行分段。如果您有现用的应用程序替代策略，是专门为定义端口集合的自定义会话超时而单独创建的，则将现有的应用程序替代策略转换为基于应用程序的测量，方法为：将基于服务的会话超时配置为维护每个应用的自定义超时，然后迁移基于应用程序的规则管辖的规则。应用程序替代策略基于端口。使用应用程序替代策略维护端口集合的自定义会话超时时，您就无法通过应用程序了解这些流量的情况，所以就无从得知或控制哪些应用程序使用这些端口。基于服务的会话超时达到自定义超时时，同时维护应用程序可见性。 要从基于端口、具有自定义应用程序超时功能的安全策略迁移到基于应用程序的策略，不能使用应用程序覆盖策略来维护自定义超时，原因在于您将失去应用程序的可见性。相反，应定义基于服务的会话超时，以维护每个应用程序的自定义超时，并迁移此规则到基于应用程序的规则。

请勿使用下一代防火墙对特定服务器层内的服务器进行分段。当您需要阻止服务器层内服务器之间的相互通信时，请使用 NSX DFW 等传统规则开放一个端口，或是阻止层内的流量。但是，服务器层内的服务器通常需要相互通信。例如，数据库服务器层可能是一个需要自由地相互通信的服务器群集。

如何创建数据中心最佳实践安全配置文件？

安全配置文件可通过扫描网络上允许流量以查找威胁的方式提供基础保护。安全配置文件提供一整套协作的威胁防护工具，可阻止对端到对端的命令和控制(C2)应用程序流程、危险的文件类型、尝试利用漏洞、以及防病毒签名，还可以标识新的和未知恶意软件。

因为 Palo Alto Networks 提供的预定义配置文件可简单添加到安全策略中，以允许规则，因此，应用安全配置文件花费的工作量较少。自定义安全配置文件也比较容易，原因是您可以复制预定义配置文件，并对其进行编辑即可。当然，您还可以在防火墙或 Panorama 上从头开始创建安全配置文件。

要检测网络流量中的已知和未知威胁，则添加安全配置文件到允许网络上所有流量的所有安全策略规则中，这样，防火墙就可以检测所有允许流量。防火墙对于安全策略允许规则匹配的流量应用安全配置文件，并根据安全配置文件设置对流量进行扫描，然后采取相应的操作保护网络。对最佳实践安全配置文件的建议是将其应用于所有四个数据中心通信流，其他说明的除外。

自动下载内容更新，并尽快进行安装，这样，可以在防火墙上拥有最新的威胁预防签名和内容（防病毒、防间谍软件、漏洞、恶意软件等），并阻止最新威胁。

- 创建数据中心最佳实践防病毒配置文件
- 创建数据中心最佳实践防间谍配置文件
- 创建数据中心最佳实践漏洞保护配置文件
- 创建数据中心最佳实践文件阻止配置文件
- 创建数据中心最佳实践 WildFire 分析配置文件

创建一个或多个安全配置文件组，以便一次性将所有配置文件应用到安全策略规则，而不是单独指定。

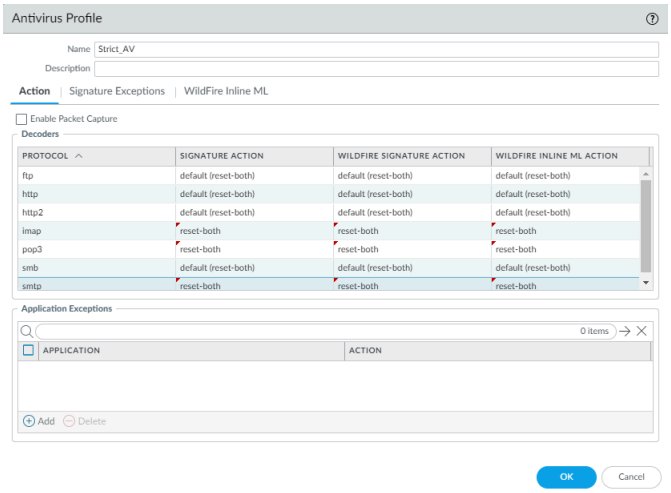
如果与 Internet 没有直接的出站连接，则数据中心防火墙无需使用 URL 筛选订阅。未直接连接到 Internet 的防火墙无需使用 PAN-DB URL 筛选解决方案，原因在于防火墙可以标识 Internet 的 URL，而非数据中心的专用 URL，因此，导入 PAN-DB 数据库并根据此库检查 URL 并不适用于数据中心流量。如果无法确定防火墙是否拥有 URL 流量，则获取试用的 URL 筛选订阅，并设置配置文件为对所有 URL 类别发出警报，从而标识任何 URL 流量。否则，URL 筛选将在网络外围防火墙（用户流量从这里进入和离开网络）中进行，而非数据中心外围。建自定义 URL 类别（**Objects**（对象） > **Custom Objects**（自定义对象） > **URL Category**（**URL** 类别）），以标识并控制对数据中心内部 Web 服务的访问。

创建数据中心最佳实践防病毒配置文件

克隆并编辑默认的防病毒配置文件。要确保业务关键型应用程序的可用性，请按照安全过渡步骤的建议从当前状态转移到最佳实践配置文件。要获得最佳实践配置文件，请按如下所示修改默认配置文件，并将其附加到允许流量的所有安全策略。防病毒配置文件包含协议解码器，该解码器会检测并预防病毒和恶意软件通过以下七种协议传输：FTP、HTTP、HTTP2、IMAP、POP3、SMB 和

SMTP。您可以为七种协议设置 WildFire 操作，因为防病毒配置文件也会根据 WildFire 签名和内联机器学习执行操作。

配置已复制的防病毒配置文件的最佳实践，以重置用于所有七个协议解码器和 WildFire 操作的客户端和服务器，然后将此配置文件附加到允许所有四个数据中心流量流动的规则中。



单元格左上角的红色三角形表示操作已修改（从默认值进行更改），且已修改的配置文件名为 **Strict_AV**。

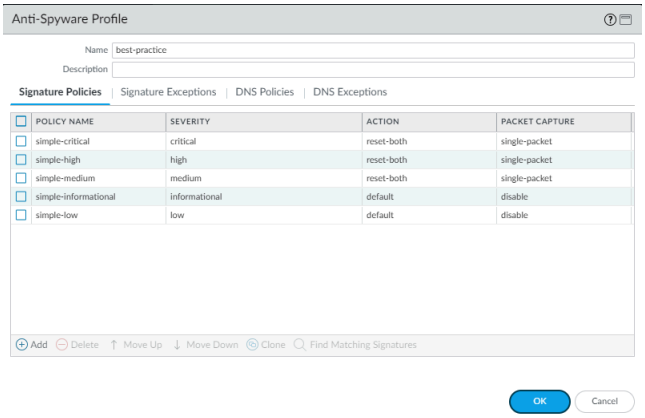
将防病毒配置文件的最佳实践附加到允许流量的所有安全策略规则，在恶意软件、勒索软件机器人和病毒等恶意文件尝试进入网络时加以阻止。例如：

- 数据中心内部流量 — 防病毒配置文件与漏洞保护配置文件一起，有助于防止攻击者利用漏洞，并在数据中心网络内部的服务器之间横向传播恶意软件和黑客工具。
- 从数据中心到 Internet 的流量 — 防病毒配置文件和防间谍配置文件一起，有助于标识并阻止命令和控制流量以及恶意软件和黑客工具的初始下载。

创建数据中心最佳实践防间谍配置文件

将防间谍配置文件附加到允许数据中心流量的所有安全策略规则防间谍配置文件检测从服务器或端点上安装的间谍软件发起的命令和控制(C2)流量，包括广告软件、后门、浏览器劫持、数据窃取和键盘记录等类别，并防止受损系统从您的网络建立出站连接。

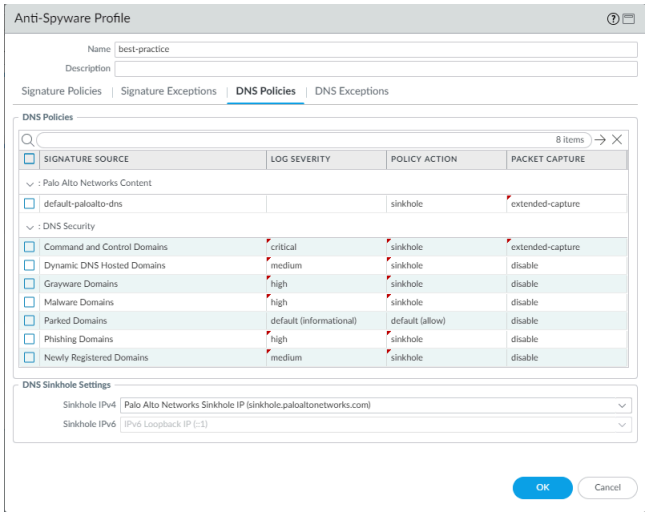
克隆并编辑预定义的严格防间谍软件配置文件。要确保业务关键型应用程序的可用性，请按照安全过渡步骤的建议从当前状态转移到最佳实践配置文件。如果已有一个设置为可以发送流量进行分析的沉洞，则启用带数据包捕获功能的 DNS 沉洞以帮助您跟踪尝试解决恶意域问题的端点。最佳实践防间谍配置文件保留默认**Action**（操作），以便在防火墙检测到中、高或关键级严重性威胁时重置连接，并启用这些威胁的单一数据包捕获 (PCAP)。



请勿为信息活动启用 PCAP，因为这将产生相对较大的流量，对于潜在威胁而言，它所起的作用有限。将扩展的 PCAP（与单一 PCAP 相对）应用到应用**alert**（警报）操作的高价值流量。使用与您用于确定记录哪个流量的相同逻辑应用 PCAP，获取您记录的流量的 PCAP。将单一 PCAP 应用到您阻止的流量。超出 PCAP 记录且发送到管理平面的默认数据包数量为 5 个，这也是推荐值。大部分情况下，捕获 5 个数据包可提供足够信息用于分析威胁。如果将太多 PCAP 流量发送至管理平面，捕获的数据包数量超过 5 个时，将导致 PCAP 被丢弃。

Action on DNS Queries（**DNS** 查询上的操作）的最佳实践是阻止或 沉洞已知恶意域的 DNS 查询。并在您无法查看 DNS 查询时，启用 PCAP。

仅允许流量流向批准的 *DNS* 服务器。使用 DNS 安全服务阻止恶意 *DNS* 服务器连接。



启用 DNS 阻断识别潜在的受影响的主机，这类主机通过追踪主机，并防止这些主机访问可疑的域名，尝试访问这些域名。防火墙无法看见 DNS 查询的发起人时（通常是在防火墙位于本地 DNS 服务器北部时），启用 DNS 阻断，以便识别受影响的主机。防火墙可看见 DNS 查询的发起人（通常是在防火墙位于本地 DNS 服务器南部时）或位于您阻止的流量上时，请勿启用 DNS 阻断。

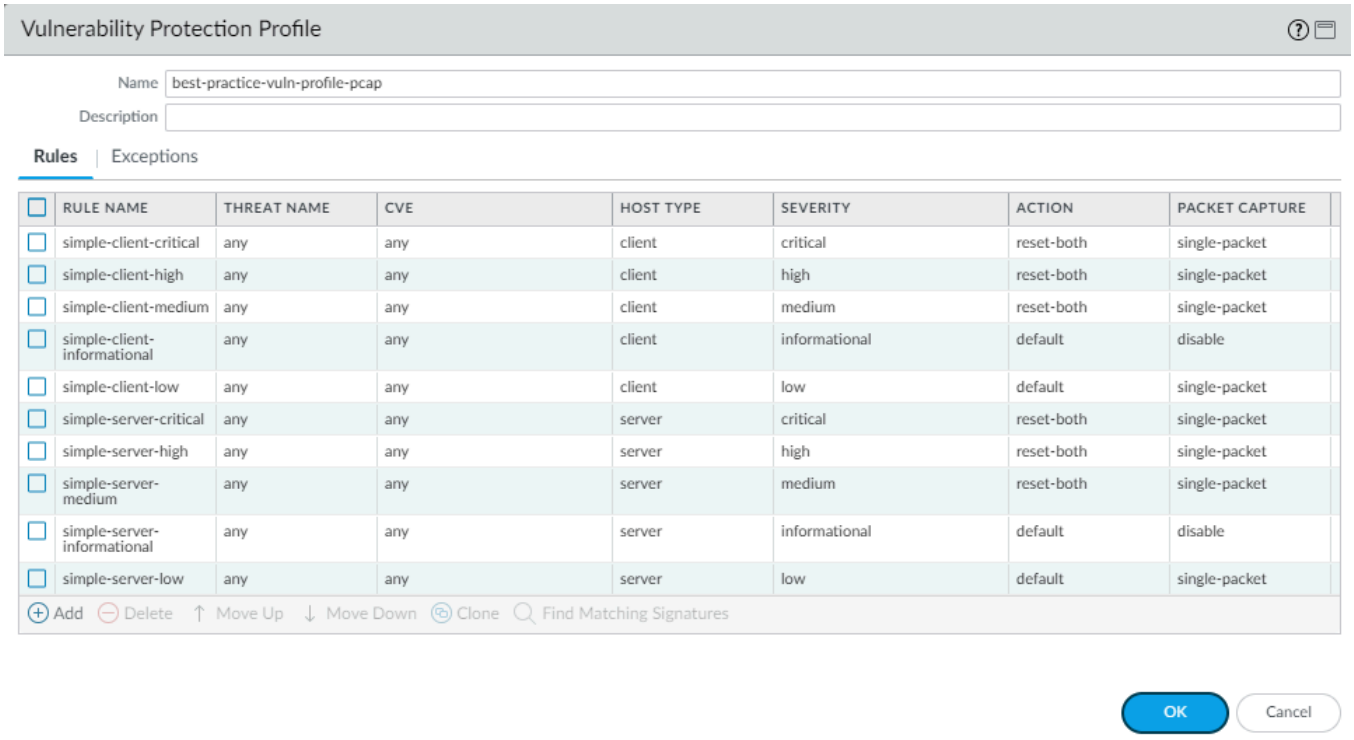
除了使用 DNS 沉洞保护主机外，将防间谍配置文件的最佳实践附加到所有安全策略规则中，以便流量在其离开网络时标识受感染的主机，并通过阻止受影响系统与恶意 C2 网络的通信阻止攻击者。如果系统无法与 C2 网络通信，则 C2 网络无法控制此系统。例如：

- 从用户到数据中心的流量、数据中心内部流量、以及从 Internet 到数据中心的流量 — 防间谍配置文件阻止对等式 C2 流量。
- 从数据中心到 Internet 的流量 — 防间谍配置文件和防病毒配置文件一起，有助于标识并阻止 C2 流量以及恶意软件和黑客工具的初始下载。

创建数据中心最佳实践漏洞保护配置文件

附加漏洞保护配置文件到允许流量的所有安全策略规则。漏洞保护配置文件可防止缓冲区溢出、非法代码执行、以及其他尝试利用客户端和服务器侧漏洞进行破坏，并在数据中心网络中横向移动。

克隆预定义的严格漏洞防护配置文件。要确保业务关键型应用程序的可用性，请按照安全过渡步骤的建议从当前状态转移到最佳实践配置文件。对于最佳实践配置文件，除 **simple-client-informational**（简单客户端信息） 和 **simple-server-informational**（简单服务器信息）外，双击每个规则的 **Rule Name**（规则名称）并将 **Packet Capture**（数据包捕获）从 **disable**（禁用）更改为 **single-packet**（单个数据包），以启用每条规则的 数据包捕获 (PCAP)，以便跟踪潜在攻击的来源。请勿更改其他设置。自动下载并尽快安装内容更新，以便保持签名集始终处于最新状态。



请勿为信息活动启用 PCAP，因为这将产生相对较大的流量，对于潜在威胁而言，它所起的作用有限。将扩展的 PCAP（与单一 PCAP 相对）应用到应用**alert**（警报）操作的高价值流量。使用与您用于确定记录哪个流量的相同逻辑应用 PCAP，获取您记录的流量的 PCAP。将单一 PCAP 应用到您阻止的流量。超出 PCAP 记录且发送到管理平面的默认数据包数量为 5 个，这也是推荐值。大

部分情况下，捕获 5 个数据包可提供足够信息用于分析威胁。如果将太多 PCAP 流量发送至管理平面，捕获的数据包数量超过 5 个时，将导致 PCAP 被丢弃。

添加最佳实践漏洞保护配置文件到允许流量的所有安全策略规则的原因是，如果没有严格的漏洞保护，攻击者可以利用客户端和服务器侧的漏洞要攻击数据中心。例如：

- 数据中心内部流量 — 严格的漏洞保护配置文件与防病毒配置文件一起，有助于防止攻击者利用漏洞，并在数据中心网络内部的服务器之间横向传播恶意软件和黑客工具。
- 从数据中心到 Internet 的流量 — 漏洞保护有助于防止受感染的数据中心服务器攻击 Internet 服务器。
- 从 Internet 到数据中心的流量 — 严格的漏洞保护配置文件可阻止尝试利用服务器侧漏洞攻击数据中心服务器。如果服务器遭到攻击，则漏洞保护有助于防止受感染的服务器向客户端提供漏洞、隔离感染，并阻止合作伙伴和客户免受水坑攻击。此外，漏洞保护还可以阻止使用阻止 IP 操作的暴力攻击。当暴力攻击签名触发操作时，防火墙会在配置的一段时间内阻止攻击者的 IP 地址。如果暴力攻击在此时间段过后恢复，则签名将再次触发阻止操作。如果暴力攻击在此时间段过后恢复，则签名将再次触发阻止操作。此暴力攻击可能会继续，但永远不会成功。

创建数据中心最佳实践文件阻止配置文件

使用严格的预定义文件阻止配置文件阻止恶意软件攻击活动中通常包含的文件，以及不属于上传/下载的真实用例的文件。阻止这些文件可缩小攻击范围。预定义的严格配置文件阻止批文件、DLL、Java 类文件、帮助文件、Windows 快捷方式 (.lnk)、BitTorrent 文件、压缩文件、tar 文件、解密的压缩文件、多级编码文件（加密或压缩多达四次的文件）、hta 文件和 Windows Portable Executable (PE) 文件（包括.exe、cpl、dll、ocx、sys、scr、drv、efi、fon 和.pif 文件。最后，预定义的严格配置文件警示所有其他类型的文件传输，让您了解其他文件传输会发生什么，以便您确定是否需要修改策略。

某些情况下，支持关键型应用程序的需求可能会阻碍您阻止所有类型的严格配置文件。按照安全过渡步骤的建议，帮助确定是否需要在网络的不同区域设置例外。查看数据筛选日志（***Monitor***（监控） > ***Logs***（日志） > ***Data Filtering***（数据筛选））以标识数据中心使用的文件类型，并与业务利益相关方谈论有关其应用程序所需的文件类型。基于此信息，如有必要，则克隆严格配置文件并视需要修改此文件，以允许仅一种您需要用于支持关键型应用程序的其他文件类型。还可使用方向 *(Direction)* 设置来限制文件类型双向流动，或阻止一个方向的文件。

NAME	LOCATION	RULE NAME	APPLICATIONS	FILE TYPES	DIRECTION	ACTION
basic file blocking	Predefined	Block high risk file types	any	7z, bat, chm, class, cpl, dll, exe, hlp, hta, jar, ocx, PE, pif, rar, scr, torrent, vbe, wsf	both	block
		Continue prompt encrypted files	any	encrypted-rar, encrypted-zip	both	continue
		Log all other file types	any	any	both	alert
strict file blocking	Predefined	Block all risky file types	any	7z, bat, cab, chm, class, cpl, dll, exe, flash, hlp, hta, jar, msi, Multi-Level-Encoding, ocx, PE, pif, rar, scr, tar, torrent, vbe, wsf	both	block
		Block encrypted files	any	encrypted-rar, encrypted-zip	both	block
		Log all other file types	any	any	both	alert

添加文件阻止配置文件的最佳实践到允许流量的所有安全策略的理由在于，其有助于防止攻击者通过文件共享应用程序和漏洞攻击包，或是通过感染访问数据中心或是 USB 棒上的用户将恶意软件传递到数据中心。

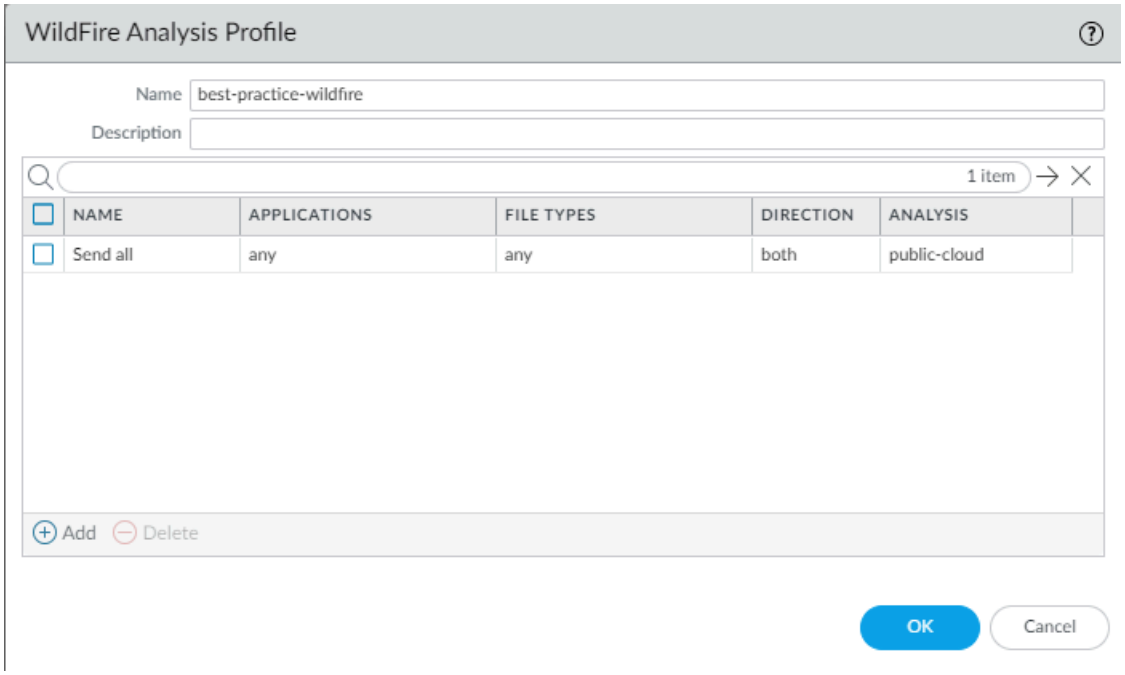
- 从用户到数据中心的流量 — 将严格的文件阻止配置文件附加到安全策略规则，以便不需要文件共享或协作的应用程序阻止可能会利用漏洞和恶意软件的危险文件类型。
- 数据中心内部流量 — 添加严格的文件阻止配置文件到安全策略规则，以阻止受感染的服务器与共享数据中心其他服务器共享恶意文件。这可以隔离感染，阻止通过数据中心传播恶意软件。
- 从数据中心到 Internet 的流量 — 将文件传输限制到正在使用的应用程序所需的文件类型。

如果不阻止所有 Windows PE 文件，则发送所有未知文件到 WildFire 进行分析。对于用户账户，设置 **Action**（操作）为 **continue**（继续），这有助于防止路过式下载，即，恶意 Web 站点、电子邮件或弹出窗口导致用户无意中下载恶意文件。告知用户，会出现一个他们非有意发起的文件传输的继续提示，这意味着可能受到恶意下载。

创建数据中心最佳实践 WildFire 分析配置文件

其他安全配置文件用于检测并阻止已知威胁。WildFire保护数据中心免受未知威胁的影响。配置防火墙，以通过预定义默认配置文件转发所有未知文件到 WidlFire 进行分析。未知威胁可以隐藏在许多不同的文件类型中，成功的攻击可能会在其造成损害后相当长一段时间内都不会被检测到。例如，WildFire 可以在攻击者发动破坏前标识加载到登台服务器上的恶意软件，并在攻击者实现其目标前找出漏洞扫描程序和横向移动辅助工具。能够阻止在过去几年中发生的多起大型企业数据泄露事件。可以控制已有、将有、或可能有文件传输活动流量的任何安全策略规则均应包含一个启用的 WildFire 分析配置文件。

设置 WildFire 设备内容更新以每分钟自动下载和安装，让您始终拥有最新的支持。例如，*WildFire* 设备内容更新中提供了对 *Linux* 文件和 *SMB* 文件的支持。



将默认 WildFire 分析配置文件附加到允许流量的所有安全策略规则中的原因是 WildFire 可提供针对未知威胁和高级持续性威胁 (APT) 的更好防御。例如：

- 从用户到数据中心的流量 — WildFire 标识数据中心中包含的未知恶意软件，例如 Confluence 或 SharePoint。
- 数据中心内部流量 — WildFire 标识数据中心服务器之间传播的未知恶意软件，以便在其产生损害之前发现恶意软件，从而防止数据泄露。
- 从数据中心到 Internet 的流量 — 因为此流量下载了用于软件和系统更新操作用的可执行文件，因此，必须在所有应用程序上运行 WildFire 以标识恶意行为。

通过电子邮件，SNMP 或系统日志服务器设置恶意软件警报，以便防火墙在遇到潜在问题时立即通知您。隔离受感染主机的速度越快，以前未知的恶意软件传播到其他数据中心设备的可能性就越小，同时修复问题也更容易。

必要时，可以根据流量方向限制发送用于分析的应用程序和文件类型。

如果流量生成的 *WildFire* 签名会导致重置或丢弃操作，那么防病毒软件配置文件内的 *WildFire* 操作设置可能会影响该流量。您可以排除诸如软件分发应用程序等内部流量，并由此部署定制程序以 安全 转换 至最佳实践，因为 *WildFire* 可能将定制程序识别为恶意软件并为其生成签名。检查 ***Monitor***（监控） > ***Logs***（日志） > ***WildFire Submissions***（***WildFire*** 提交）以查看是否有任何内部定制程序触发 *WildFire* 签名。

使用 Cortex XDR 客户端保护数据中心端点

Cortex XDR 客户端可保护服务器和 VM 等数据中心端点免遭端点上恶意软件和漏洞的攻击，而新一代防火墙则会阻止整个网络中到达端点的威胁（因此，必须穿过此防火墙）。当恶意软件或漏洞已存在于端点上，或是进入端点，如果端点执行此威胁（例如，通过 .exe 或 .dll 文件），则防火墙将发现不了该威胁，因为此操作发生在端点上，且没有流量通过防火墙，因此，防火墙没有可以查看的内容。但是，在每个端点上，Cortex XDR 客户端可以查看可执行文件中的威胁、文档中的宏、以及动态链接库文件等。当这些威胁试图运行时，陷阱就会在端点上开始行动，保护端点。

Cortex XDR 客户端和新一代防火墙可为数据中心端点提供双重保护，这样，防火墙保护端点免遭网络上威胁的攻击，而 Cortex XDR 客户端则监控驻留在端点内的威胁，从而保护端点。在端点安全管理器 (ESM) 上为端点配置的安全策略，以及在 Panorama 或防火墙上配置的安全策略并不会发生冲突，原因是他们管理不同位置的不同事件。Cortex XDR 客户端控制每个单独端点内的安全。防火墙控制穿过防火墙的流量安全。

在每个数据中心端点上安装 Cortex XDR 客户端。数据中心中 Cortex XDR 客户端的最佳实践与任何端点上的 Cortex XDR 客户端最佳实践一样，因为 Cortex XDR 客户端的上下文始终在端点本身，无论是“在数据中心”，还是”在用户组”，均无任何区别 — Cortex XDR 客户端以同样的方式保护所有端点。因此，数据中心的部署流程和恶意软件防护策略最佳实践等与网络的其他区域相同。

创建数据中心流量阻止规则

为数据中心四个通信流创建应用程序允许规则之前，创建阻止和日志记录规则，以阻止您不会在数据中心使用的应用程序，阻止已知的不良应用程序，并发现可能尚未在网络上发现的应用程序。被阻止流量的日志记录可提供潜在攻击相关的信息，有助于您进行调查。

当您发现未知应用程序时，请确认是否是允许的应用程序，或是这些应用程序代表有潜在威胁。如果这些规则发现这些应用程序均属于允许的应用程序，则相应地对应用程序允许规则进行调整。如果这些规则发现不合法的应用程序，则会重新显示潜在威胁警告，以便使用日志信息进行调查。如果这些规则发现这些应用程序均属非法应用程序，则其可能代表有潜在威胁，您可以使用记录信息对其进行调查。

如果发现未知应用程序是内部专有应用程序或其他类型的合法应用程序，则为每个未知应用程序创建自定义应用程序，这样，就可以对其进行标识，并对其使用安全策略。

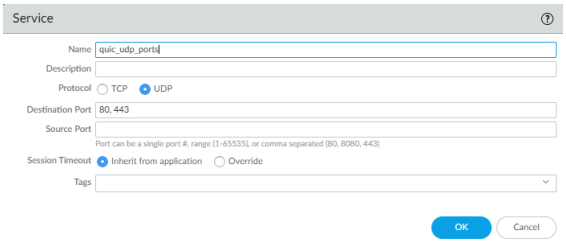
数据中心安全策略规则库排序向您展示如何通过创建用于数据中心四个通信流的所有其他规则对这些规则进行排序，这样，就不会出现一个规则屏蔽另一个规则的现象。

要在多个数据中心采用一致的安全策略，则可以重复使用模板和模板堆栈，这样，就可以将相同的策略应用于每个数据中心模板使用变量应用设备特定值，如 *IP* 地址、*FQDN* 等，同时维护全球安全策略并减少您需要管理的模板和模板栈数量。

STEP 1 | 阻止快速 UDP Internet 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。阻止 QUIC 会强制浏览器退回到 TLS，使防火墙解密流量。

创建安全策略规则以阻止其 UDP 服务端口（80 和 443）上的 QUIC，并创建单独的规则以阻止 QUIC 应用程序。对于用于阻止 UDP 端口 80 和 443 的规则，请创建一个包括 UDP 端口 80 和 443 的服务（**Objects**（对象） > **Services**（服务））：



使用此服务指定用于阻止 QUIC 的 UDP 端口。在第二条规则中，阻止 QUIC 应用程序，以便让规则库中的前两条规则阻止 QUIC：

	NAME	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
1	Block QUIC UDP	universal	l3-vlan-trust	any	any	any	l3-untrust	any	any	any	quic_udp_ports	Deny	none	
2	Block QUIC	universal	l3-vlan-trust	any	any	any	l3-untrust	any	any	quic	application-default	Deny	none	

STEP 2 | 阻止应用程序默认端口上来自用户区域的所有应用程序，识别预期以外的应用程序。

此规则可发现用户正在尝试使用，且您不知道正在您的数据中心运行的应用程序。监控与此规则匹配的流量，从而确定其是否是潜在威胁，或是您是否需要修改允许规则以启用对该应用程序的访问。必须将此规则部署在允许流量的规则的之后，否则，此规则将会阻止您想要允许的流量。

显示在此规则后的规则与此规则类似，不同之处在于其适用于任何源的流量，而非仅来自用户区域的流量。创建单独规则的原因在于，违反用户区域规则可能表示，您正在阻止某些用户执行商业活动时所需的合法应用程序，因此，您可能需要对允许规则进行修改，以允许特定用户组的用户使用此应用程序。非用户区域的违规可能表示应用程序发生了更改，或是出现潜在攻击。您可以通过为剩余流量创建单独规则来查看用户流量以及尝试进入数据中心的所有其他流量的单独日志，从而更便于调查潜在问题，并做出反应。

此规则适用于所有流量，必须置于下一个规则的上游，这样，您可以在首次记录用户区域违规后记录并监控尝试使用应用程序默认端口上的预期以外的应用程序，而无论其源是什么。

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected-App-from-User-Zone	User to DC BP	universal	Contractors Engineering-Users Finance-Users IT-Users	any	any	any	Web-Server-Tier-DC	any	any	any	application-default	Drop	none	

要创建此规则：

- 源区域包括所有用户区域和用户（您的部署可能比示例中显示的包含更多用户区域）。
- 目标区域是数据中心外围的数据中心 Web 服务器层（**Web-Server-Tier-DC**（**Web** 服务器层 **DC**））。
- 设置应用程序为 **any**（任何），设置服务为 **application-default**（默认应用程序），这样，规则适用于其标准端口上所有正在运行的应用程序。
- 设置操作为 **Drop**（丢弃），以默默地丢弃流量，不用发送信号到客户端或服务器。

STEP 3 | 阻止所有端口上来自用户区域的所有应用程序，以识别不应在此运行的应用程序。

此规则可用于标识用户尝试在非标准端口运行的已知合法应用程序，以及可能需要创建自定义应用程序的未知应用程序。调查与此规则匹配的任何流量源，确保不会允许未知 tcp、未知 udp

或未同步 tcp 流量。必须将此规则部署在允许流量的规则的之后，否则，此规则将会阻止您想要允许的流量。

我们还将在本节后面部分创建一个与此规则类似的阻止规则（***Unexpected-App-from-Any-Zone***（来自任何区域的预期以外的应用程序）），不同之处在于其适用于任何源的流量，而非仅来自用户区域的流量。创建单独规则的原因在于，违反用户区域规则可能表示，某些用户执行商业活动时所需的合法应用程序可能设计不正确，因此，您可能需要对应用程序进行修改。您可以通过为剩余流量创建单独规则来查看用户流量以及尝试进入数据中心的所有其他流量的单独日志，从而更便于调查潜在问题，并做出反应。

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected-User-App-Any-Port	User to DC BP	universal	Contractors Engineering-Users Finance-Users IT-Users	any	any	any	Web-Server-Tier-DC	any	any	any	any	Drop	none	

要创建此规则：

- 源区域包括所有用户区域和用户（您的部署可能比示例中显示的包含更多用户区域）。
- 目标区域是数据中心外围的数据中心 Web 服务器层（**Web-Server-Tier-DC**（**Web** 服务器层 **DC**））。
- 设置应用程序为 **any**（任何），设置服务为 **any**（任何），这样，规则适用于任何端口上所有正在运行的应用程序。
- 设置操作为 **Drop**（丢弃），以默默地丢弃流量，不用发送信号到客户端或服务器。

STEP 4 | 阻止可规避或绕过安全机制的应用程序。攻击者经常利用这些应用程序，或者数据中心不需要这些应用程序。

此规则可保护数据中心免受您已知在数据中心不需要的应用程序的影响。虽然安全策略的最佳实践的目的是使用应用程序允许规则进行积极实施，但明确阻止并记录具有潜在危险的应用程序的活动（未经批准的文件共享应用程序、远程访问应用程序或加密隧道等）可提供对潜在威

胁的可见性以及相关信息。即使在已开发一份可靠的应用程序允许列表之后，也请在规则库中保留此应用程序阻止规则，因为源自已尝试违规的日志有助于对潜在攻击的调查。

使用此规则仅阻止您从不希望出现在数据中心的应用程序。

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Block-Bad-Apps	User to DC BP	universal	any	any	any	any	App-Server-Tier-DC DB-Server-Tier-DC Engineering-DC-Infra Finance-DC-Infra IT Infrastructure SAP-Infra Web-Server-Tier-DC	any	any	Encrypted-Tunnels File-Sharing Remote-Access	any	Drop	none	

要创建此规则：

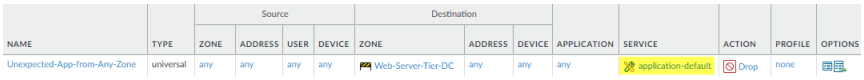
- 因为要阻止任何人均不能在数据中心使用的应用程序，因此，将源区域、地址、用户和设备设置为 **Any**（任何）。
- 指定目标区域中所有数据中心区域，以保护所有数据中心服务器免受不良应用程序的影响。
- 为想要阻止的任何类型（类别）的应用程序创建应用程序筛选器，并指定任何其他应用程序。本示例包含用于加密隧道、远程访问和文件共享的应用程序筛选器。通过消除不必要的应用程序来阻止您在数据中心中不使用的应用程序，从而减少攻击面，同时也降低风险。使用应用程序筛选器（而非应用程序组）或列出单独应用程序的优势在于筛选器可自动更新，因此，无需在出现新应用程序时进行维护。
- 设置服务为 **any**（任何）以捕获非标准端口和默认端口上不需要的应用程序。
- 设置操作为 **Drop**（丢弃），以默默地丢弃流量，不用发送信号到客户端或服务器。

示例规则中显示的应用程序筛选器不是一个全面的列表。对根据如何评估您的数据中心而创建的应用程序进行评估，并添加您不想此规则允许的应用程序。将阻止规则放置在允许列表的下游位置可允许对规则实施例外。例如，IT 需要使用远程访问应用程序管理数据中心设备，因此，在阻止所有其他用户的远程访问应用程序之前，必须允许此远程访问应用程序。另一个示例是您可以在处于此阻止规则之前的允许规则内批准一个或两个文件共享应用程序，然后，此规则内的应用程序筛选器将阻止所有剩余的此类应用程序。如果存在您从不希望出现在您网络上的应用程序组或单个应用程序，且没有例外，则可以创建特定的阻止规则来仅阻止这些应用程序，并将其置于规则库的顶部，即应用程序允许规则的上方。但是，如果这样操作，则必须确保阻止的应用程序没有合法的业务用途，因为用户将无法访问这些应用程序。

STEP 5 | 阻止应用程序默认端口上来自任何区域的所有应用程序，识别预期以外的应用程序。

此规则可发现您不知道已在数据中心运行的来自任何区域的应用程序。违反此规则意味着应用程序已发生更改，或是出现潜在威胁。对匹配此规则的流量进行监控，以确定其是否为潜在威胁，或是否需要修改您的应用程序允许规则。必须将此规则置于允许流量的允许规则的之后，

否则此规则将会阻止您想要允许的流量；以及步骤 1 中的规则之后，这样，就不会捕获来自用户区域的流量。



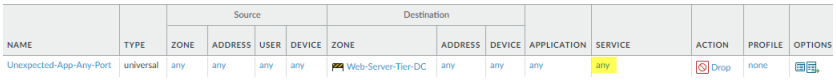
		Source				Destination							
NAME	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected-App-from-Any-Zone	universal	any	any	any	any	Web-Server-Tier-DC	any	any	any	application-default	Drop	none	

要创建此规则：

- 源设置为 **any**（任何），以覆盖所有尝试进入数据中心的剩余流量（步骤 1 中的规则可在流量到达此规则之前阻止并标识预期以外的用户应用程序）。
- 目标区域是数据中心外围的数据中心 Web 服务器层（**Web-Server-Tier-DC**（**Web** 服务器层 **DC**））。
- 设置应用程序为 **any**（任何），设置服务为 **application-default**（默认应用程序），这样，规则适用于其标准端口上所有正在运行的应用程序。
- 设置操作为 **Drop**（丢弃），以默默地丢弃流量，不用发送信号到客户端或服务器。

STEP 6 | 阻止所有端口上来自任何区域的所有应用程序，以识别不应在此运行的应用程序。

此规则可用于标识尝试在非标准端口运行的已知合法应用程序，以及可能需要创建自定义应用程序的未知应用程序。调查与此规则匹配的任何流量源，确保不会允许未知 tcp、未知 udp 或未同步 tcp 流量。必须将此规则放置在允许流量的允许规则的下游位置，否则，此规则将会阻止您想要允许的流量；以及上游规则的下游位置，这样，就不会捕获来自用户区域的流量。



		Source				Destination							
NAME	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected-App-Any-Port	universal	any	any	any	any	Web-Server-Tier-DC	any	any	any	any	Drop	none	

要创建此规则，可使用 **Unexpected-App-from-User-Zone**（来自用户区域的预期以外的应用程序）规则中相同的设置，除了不在源中指定用户区域外，请指定 **any**（任何）区域以覆盖所有尝试进入数据中心的剩余流量，并设置服务为 **any**（任何）以覆盖非标准端口。

STEP 7 | 发现尝试在任何端口上运行任何应用程序的未知用户。

此规则通过查找未知用户标识 User-ID 覆盖范围内的差距。此外，还可以标识用户社区中尝试访问数据中心的受影响或嵌入式设备。（嵌入式设备无用户界面、打印机、读卡器和摄像机等，但攻击者可以损害这些设备，并在攻击中予以使用。

		Source				Destination							
NAME	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Discover-Unknown-Users	universal	any	any	unknown	any	any	any	any	any	any	Deny	none	

此规则几乎与用于阻止区域间通信的区域间默认规则相同（除非另一条规则允许此流量），只不过它不会丢弃来自所有用户的流量，而是仅丢弃来自未知用户的流量。这样，您可以单独记录规则匹配情况，更便于调查尝试访问数据中心的未知用户。

定义初始用户到数据中心流量安全策略

要开始执行开发数据中心应用程序允许列表，则首先为流向数据中心的用户流量定义初始的最佳实践安全策略。最终目标是实施积极的安全措施，通过零信任架构保护您的数据中心。您可以通过明确控制谁可以访问数据中心、可以访问哪些数据中心应用程序以及可以访问数据中心内的哪些资源来实现这一目标。只允许具有合法业务理由的用户访问数据中心。最佳实践安全策略制定完毕后，任何未知用户均将无法访问数据中心，任何未知应用程序或资源均不会驻留在数据中心内。

用户访问给数据中心带来的风险包括：攻击者控制数据中心外部的网络设备并利用它横向移动到数据中心植入恶意软件、窃取数据、控制数据中心设备、将恶意软件意外下载到数据中心，以及未经授权访问数据中心应用程序和资产。

以下部分向您展示允许的应用程序流量类型以及如何控制流量，如何对用户进行身份验证以防止未经授权的用户访问数据中心，以及如何解密流量：

- 用户到数据中心流量安全方法
- 创建用户到数据中心应用程序允许规则
- 创建用户到数据中心验证策略规则
- 创建用户到数据中心解密策略规则

用户到数据中心流量安全方法

用于保护流入数据中心的用户流量的传统旧方法使宝贵的资产面临风险，而最佳实践方法则能保护您的宝贵资产。

传统方法	Risk	最佳实践方法
因为数据中心位于可信网络内部，因此，基于端口的规则可提供足够的安全性。	恶意应用程序通过端口号欺骗、端口隧道使用、或是使用避免检测的端口跳跃来访问网络。	应用程序允许规则将应用程序、用户和服务器联系在一起，这样就只有使用已批准应用程序的合法用户才能访问数据中心内相应的服务器组。

传统方法	Risk	最佳实践方法
		从基于端口的规则转换为基于应用程序的规则时，在数据库中，将基于应用程序的规则置于其将替换的基于端口的规则的上游。重置两个规则的策略规则触发计数器。如果流量到达基于端口的规则，则其策略规则的命中数会增加。调整基于应用程序的规则，直到一段时间内无流量到达基于端口的规则，然后删除基于端口的规则。
信任内部用户，并允许用户访问的应用程序，从而根据凭据以及可能的 IP 地址规则确定是否可以允许此访问。	攻击者访问数据中心端点，然后横向移动到数据中心其他端点，以利用被盗的凭据或服务器侧漏洞。未知用户可以访问数据中心端点。	启用 User-ID，阻止未知用户，以及允许已批准用户的访问。为员工、合作伙伴和承包商创建单独的身份域。对合作伙伴、承包商和敏感服务器访问使用多重因素身份验证 (MFA)。
因为数据中心位于可信网络的内部，因此，必须对未知文件进行分析。	用户可能会无意中从文件共享和其他云应用程序中下载恶意软件。	发送所有未知文件到 WildFire 进行分析，标识新的和未知恶意软件，从而进行保护。
源自多个供应商的威胁防御配置文件集合。	各种工具的集合会为攻击者留下安全漏洞，可能无法很好地协同工作。	Palo Alto Networks 通过安全工具的一系列协同合作来阻塞安全漏洞，防止遭受攻击。

创建用户到数据中心应用程序允许规则

评估数据中心时，可获得相关信息，有针对性地确定哪些人有权访问哪几组服务器上运行的哪些应用程序，从而制定一组应用程序允许规则。制定应用程序安全策略允许规则（**Policies**（策略） > **Security**（安全））， 从而确保只有您明确允许的用户才能在相应的几组服务器上使用与其工作相关的应用程序。不必要的访问、未知用户和未知应用程序都将不被允许。

使用预定义的已批准标签标记所有经批准的应用程序。全景图和防火墙认为不带批准标记的应用成为是未批准的应用程序。

数据中心安全策略规则库排序向您展示如何通过创建用于其他三个数据中心通信流的所有其他规则对这些规则和阻止规则进行排序，这样，就不会出现一个规则屏蔽另一个规则的现象。

要在多个数据中心采用一致的安全策略，则可以重复使用模板和模板堆栈，这样，就可以将相同的策略应用于每个数据中心模板使用变量应用设备特定值，如 *IP* 地址、*FQDN* 等，同时维护全球安全策略并减少您需要管理的模板和模板栈数量。

以下每一条允许规则：

- 已附加最佳实践安全配置文件组，其中包含最佳实践安全配置文件。使用安全配置文件组，您可以一次性将所有最佳实践配置文件应用到规则，而不是单独指定每个配置文件。利用安全配置文件组可以更快速轻松地配置恶意软件、漏洞、C2 流量以及已知和未知威胁防御。
- 在会话结束时记录流量，以便跟踪和分析违反规则的情况，并且包括日志转发。将日志转发到日志服务器，如果适用，还会将日志电子邮件转发给适当的管理员。

STEP 1 | 启动对内部企业 DNS 服务器的适当用户访问（请勿启用对外部 DNS 服务器的访问）。

此规则限制对企业 DNS 服务器的访问，从而减少攻击面，有助于保护内部主机和服务相关的 DNS 条目。为避免通过公共 DNS 发现，不得将内部企业资源的 DNS 条目存储在公共可用的 DNS 服务器中，这样，攻击者可以获取这些条目的唯一途径就是攻击企业 DNS 服务器，此时，您的 DNS 服务器将成为攻击目标。

在内部网关（网络外围）中，阻止到公共 *DNS* 服务器的所有 *DNS* 流量。请勿允许 *DNS* 流量流出到 *Internet*。

因为用户需要在登录前访问 DNS 服务，因此，此规则是不允许策略规则中“任何”用户的最佳实践的一个例外。此规则可保护对 DNS 服务的访问。要创建此规则：

- 限制访问数据中心 **IT infrastructure**（**IT** 基础架构）中适当的目标区域。
- 配置 **DNS Servers**（**DNS** 服务器）的地址组，并仅限制对该组的访问。
- 阻止通过除 **dns** 之外任何应用程序的访问。
- 将最佳实践安全配置文件组应用于 DNS 流量非常重要，因为如果攻击者劫持了您的 DNS 服务器，则攻击者可将流量重定向到看起来与用户尝试访问的合法网站相似的钓鱼网站。

STEP 2 | 允许必要的 IT 人员通过安全的方式特权访问数据中心服务器，以进行管理和维护。

此规则展示如何保护拥有特权账户的用户访问关键系统。特权账户需要高级别的信任，并允许管理访问包含公司最有价值数据的关键系统，因此，必须严格控制并监控特权账户。利用 App-

ID 仅指定 IT 用户管理数据中心服务所需的应用程序，这样，防火墙可拒绝任何其他应用程序的访问。在本示例中，一组 IT 用户需要以管理员的身份进行访问，从而管理数据中心服务器。

针对数据中心服务器进行管理的 *IT* 特权访问应仅限于管理接口，应位于专有 *VLAN* 中，这样，服务器管理流量可与其他流量分来。管理接口应位于同一子网。请勿允许数据接口上此类访问。如果 *IT* 组使用 *SSH* 或 *RDP* 进行管理访问，则请勿因为其他原因允许 *SSH* 或 *RDP* 访问。

IT 网络团队的组织可决定允许 *IT* 特权访问的人员。对于每种类型的特权访问，根据其访问要求对服务器和其他设备进行分组。仅允许必要的 *IT* 用户仅通过使用设备管理所需的应用程序访问每组服务器。

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
IT DC Server Management	User to DC BP	universal	IT-Users	any	it-superusers	any	IT-Server-Access-DC	IT-Server-Management	any	ms-rdp ssh ssl	Custom-IT-Ports	Allow		

要创建此规则：

- 因为只有一个子集的 IT 用户可以管理数据中心服务器，因此，请利用 Use-ID 专门为需要此级别访问特权的 IT 用户创建组（在本示例中为 **it-superusers**）。
- 创建包含您希望 **it-superusers** 进行管理的服务器管理接口地址的静态地址组 (**IT-Server-Management**)，并在 **IT-server-access-DC** 区域中将将目标限制为此地址组。
- 仅允许在默认端口上使用 IT 超级用户执行其业务职责所需的应用程序。在本示例中，此规则允许 **ssl**、**ssh** 和 **ms-rdp**应用程序。

  示例是允许的应用程序。允许 *IT* 部分用于管理数据中心服务器的应用程序。在某些情况下，通过 *SSL* 的应用程序可能需要添加特定应用程序，以便根据 *App-ID* 进行正确识别。

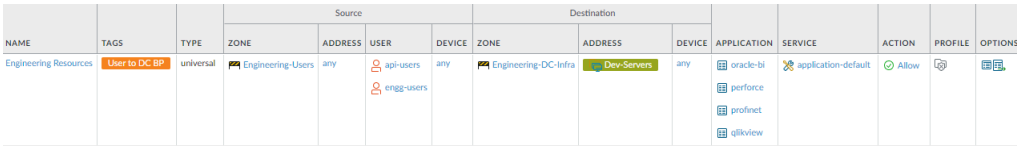
此外，IT 人员还可以管理数据中心的交换机、路由器和其他设备。如果同一组的 IT 用户使用相同的应用程序管理这些资源，则可以将其添加到目标区域和地址，以便此规则允许 IT 超级用户访问这些设备的管理接口。如果不同的 IT 用户组管理不同的数据中心资源组或是使用不同的应用程序，则为每个用户组和每组应用程序创建单独的、严格的安全策略规则。

因为拥有特权账户的用户组可以访问关键系统，因此，在创建用户到数据中心验证策略规则时，要求 MFA 阻止访问。如果攻击者损害其凭据，则为每个特权访问规则创建相应的身份验证策略和解密策略规则。

STEP 3 | 允许员工用户组出于合法的商务目的进行访问，以便与数据中心服务器进行通信。

此规则展示如何限制每个用户组（或在某些情况下，单个用户）仅访问必要的应用程序和服务器。例如，工程师需要访问数据中心的开发服务器。要创建安全策略规则，则创建包含该组所

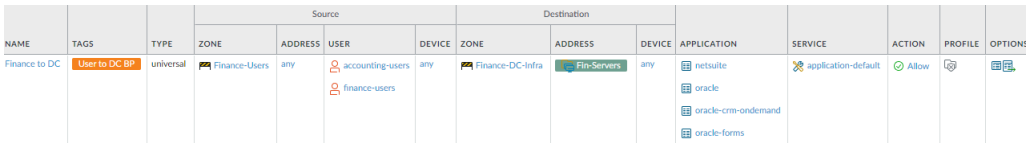
使用全部数据中心开发服务器 IP 地址的动态地址组，确定工程师需要在这些服务器上使用的应用程序，并基于这些组构建规则。



要创建此规则：

- 指定需要访问数据中心工程服务器的工程用户组，在本示例中，为 **api-users** 和 **engg-users**。
- 限制对数据中心开发服务器的访问，方式如下：为其创建一个动态地址组（**Dev-Servers**），然后将其设置为目标地址。
- 限制在默认端口上只能访问出于业务目的而需要访问的应用程序。

使用相同的方法为每个用户组创建粒度允许规则（如果需要，也可以为单个用户执行此操作），这样，每个组仅能使用默认端口上运行的合法应用程序访问出于业务目的而需要访问的服务器组。例如，仅允许需要访问包含 PCI 的服务器的财务部用户组通过实现业务目标所需的已批准财务应用程序访问这些服务器。



与工程用户用于访问数据中心服务器的允许规则类似，此规则仅允许**finance-users** 和 **accounting-users** 组中的用户使用特定应用程序访问 **Fin-Servers** 动态地址组内的服务器。此规则将最佳实践安全配置文件应用于允许的流量和日志活动。

STEP 4 | 允许承包商、合作伙伴、客户和其他第三方对于数据中心实施的有针对性的限制访问。

此规则展示如何严格控制第三方用户的访问，这样，此类用户仅使用其所需服务器上需要的应用程序。例如，公司雇佣一组 SAP 开发人员承包商。SAP 开发人员需要访问数据中心的 SAP

数据库，并进行 SQL 查询。但是，SQL 还要在 SAP 开发人员不应访问的生产数据库上运行。公司需要对三个访问向量进行控制：

- 用户组 — SAP 开发人员承包商。
- 应用程序 — MS-SQL 和 SAP。
- 服务器 — 仅限 SAP 数据库服务器。拒绝访问数据中心的所有其他服务器。

用于隔离 SAP 承包商用户组的 User-ID、用于限制该组仅使用必要应用程序的 App-ID、以及限制只能访问数据中心 SAP 数据库服务器的动态地址组这三者的组合可使公司提供 SAP 承包商需要执行其职责（但不包含其他）所需的访问权限。

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
SAP-Contractors	User to DC BP	universal	Contractors	any	sap-contractors	any	SAP-Infra	SAP DB Servers	any	ms-sql-analysis-service mssql-db mssql-mon sap	application-default	Allow		

要创建此规则：

- 指定源区域和用户，以限制对 **Contractors**（承包商） 区域中 **sap-contractors** 组内用户的访问。
- 将目标限制为 **SAP-Infra** 区域内的 SAP 数据库服务器（**SAP DB Server**（**SAP DB** 服务器）动态地址组）。
- 仅允许 SAP 承包商在默认端口使用履行其业务职责所需的应用程序。在本示例中，此规则允许 **ms-sql-analysis-service**（**ms sql** 分析服务）、**mssql-db**、**mssql-mon** 和 **sap** 应用程序。

细粒度安全策略允许规则可阻止非业务目的所需访问，并通过减少攻击面来降低风险。为每个需要访问数据中心的第三方组创建类似的允许规则。

如果攻击者窃取凭据或是以其他方式攻击第三方系统，则需要多重因素身份验证（MFA；创建用户到数据中心验证策略规则）阻止此访问，而非使用可信任的第三方用户和公司保护其凭据。MFA 身份验证可防止过去几年曾发生过的几起著名数据泄露事件再次发生。

通过查看预定义应用程序报告（**Monitor**（监控） > **Reports**（报告） > **Application Reports**（应用程序报告） > **Applications**（应用程序））确认仅在安全策略规则中明确列入允许列表的应用程序正在运行。如果在报告中看到预期以外的应用程序，则查看应用程序允许规则，并对其进行优化，这样，就不会再允许预期以外的应用程序。

创建用户到数据中心验证策略规则

在用户可以登陆数据中心服务、应用程序和其他资源之前，身份验证策略规则要求用户证明自己的身份。身份验证对于保护最有价值的资产尤其重要，因为如果攻击者窃取凭据，并通过防火墙进行身份验证，则攻击者可能可以访问并攻击数据中心的任何资产。

要访问敏感服务器以及第三方用户访问服务器（例如，SAP 开发承包商访问数据中心的 SAP 服务器），则执行多重因素身份验证 (MFA)，防止攻击者使用被盗凭据访问这些系统。使用 MFA 的身份验证策略可以防止过去几年来曾发生过的几起高调的泄露事件再次发生。

创建身份验证策略规则之前（**Policies**（策略）> **Authentication**（身份验证）），必须 配置身份验证策略相关性，以便将身份验证方法、身份验证类型、如何访问身份验证服务器、以及将身份验证门户用于指定谁可以使用何种服务在哪一个服务器上进行身份验证的身份验证策略规则等关联起来。

STEP 1 | 对出于合法业务目的使用数据中心服务器的员工用户组和单个人进行身份验证。

此规则展示如何对组用户进行身份验证，以便其可以在必要的服务器上访问其业务活动所需的服务。例如，工程师需要进行身份验证，然后才可以访问开发服务器和应用程序。

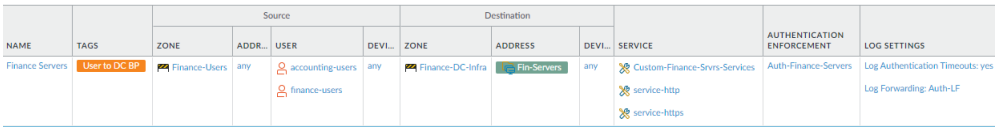
		Source				Destination					
NAME	TAGS	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	SERVICE	AUTHENTICATION ENFORCEMENT	LOG SETTINGS
DevEng Resources	User to DC BP	Engineering-Users	any	api-users engg-users	any	Engineering-DC-Infra	Dev-Servers	any	Perforce rdp service-http service-https ssh	Auth-Dev-Servers	Log Authentication Timeouts: yes Log Forwarding: Auth-LF

要创建此规则：

- 指定需要在访问数据中心工程服务器之前进行身份验证的工程用户组，在本示例中，为 **api-users** 和 **engg-users**。
- 将这些用户组的身份验证应用于数据中心开发服务器访问请求，方式如下：为其创建一个动态地址组（**Dev-Servers**），然后将其设置为目标地址。
- 将身份验证规则应用于工程组出于商务目的需要使用的服务，在本示例中，为 **Perforce**、**rdp**、**service-http**、**service-https** 和 **ssh**（开发人员可能需要使用 SSH 和 RDP 访问 Linux 服务器，应在被允许访问这些服务器之前进行身份验证）身份验证规则中的服务取决于这些组需要使用的服务。
- 配置身份验证执行对象（**Auth-Dev-Servers**），指定身份验证方法和身份验证配置文件，并将其添加到规则。
- 记录活动，这样就可以跟踪和分析规则违规（可能是尝试性攻击）。

另一个身份验证用例是当组需要访问一组特定服务器时。例如，财务部门用户需要使用特定服务访问敏感支付卡信息 (PCI)，并应在授权访问之前进行身份验证。要针对这些服务对用户进行

身份验证，则此规则使用自定义服务组（**Objects**（对象） > **Service Groups**（服务组）），该组仅包含防火墙应对财务部用户进行身份验证的服务。

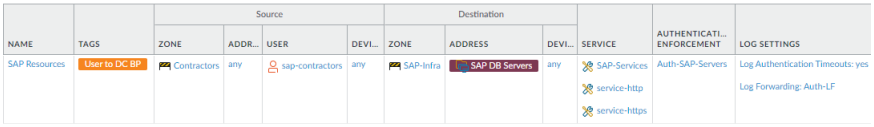


要创建此规则：

- 指定需要在访问数据中心财务服务器之前进行身份验证的用户组，在本示例中，为 **accounting-users** 和 **finance-users**。
- 将这些用户组的身份验证应用于数据中心财务服务器访问请求，方式如下：为其创建一个动态地址组 **(Fin-Servers)**，然后将其设置为目标地址。
- 将身份验证规则应用于财务部用户出于业务目的需要使用的服务，在本示例中，为 **service-http**、**service-https** 和自定义服务组 **Custom-Finance-Srvrs-Services**中定义的服务。因此，用户必须在访问这些服务之前进行身份验证。
- 配置身份验证执行对象（**Auth-Finance-Servers**），指定身份验证方法和身份验证配置文件，并将其添加到规则。
- 记录活动，这样就可以跟踪和分析规则违规（可能是尝试性攻击）。

STEP 2 | 对需要访问数据中心的承包商、合作伙伴、客户和其他非员工组进行身份验证。

因为您对公司和人员的业务和安全实践的控制程度低于对员工的控制，因此，此规则要求对承包商、合作伙伴和客户等第三方用户组进行 MFA。要求这些用户进行至少双重因素的身份验证可保护您的数据中心免遭第三方公司窃取凭据。



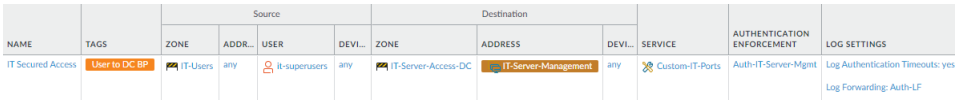
要创建此规则：

- 将身份验证规则应用于 SAP 承包商出于商务目的需要使用的服务。创建自定义服务组（**Sap-Services**（**Sap** 服务）），以定义 SAP 承包商可以在其上进行身份验证并添加其他必要服务的端口。在本示例中，为 **service-http** 和 **service-https**。
- 配置身份验证执行对象（**Auth-SAP-Servers**），指定身份验证方法和身份验证配置文件，并将其添加到规则。在这种情况下，身份验证类型必须为支持 MFA 的类型，且您必须 **Add**（添加）MFA 服务器配置文件到身份验证配置文件（**Factors**（因素）选项卡），并执行剩余的步骤，以配置 MFA。

  配置 MFA，对访问敏感系统的所有用户和用户组进行身份验证，以防止攻击者窃取凭据。
- 记录活动，这样就可以跟踪和分析规则违规（可能是尝试性攻击）。

STEP 3 | 对需要专门访问权限的用户进行身份验证，例如，需要安全访问数据中心以进行管理和维护的 IT 人员。

此规则展示如何为具有管理访问关键系统的特权账户的用户配置身份验证。因为攻击特权用户的凭据可让攻击者获取数据中心王国及其宝贵资产的密钥，因此，您至少需要实施双重因素身份验证，确保仅合法用户拥有访问权，从而保护凭据免遭盗用。此示例展示了如何对需要访问数据中心服务器管理接口的相应 IT 用户进行身份验证。



		Source				Destination					
NAME	TAGS	ZONE	ADDR...	USER	DEVI...	ZONE	ADDRESS	DEVI...	SERVICE	AUTHENTICATION ENFORCEMENT	LOG SETTINGS
IT Secured Access	User to DC BP	IT-Users	any	it-superusers	any	IT-Server-Access-DC	IT-Server-Management	any	Custom-IT-Ports	Auth-IT-Server-Mgmt	Log Authentication Timeouts: yes Log Forwarding: Auth-LF

要创建此规则：

- 指定需要在访问数据中心服务器管理接口之前进行身份验证的特权账户用户，在本示例中，为 **it-superusers** 组。
- 将这些用户组的身份验证应用于数据中心管理接口访问请求，方式如下：为其创建一个动态地址组（**IT-Server-Management**（**IT** 服务器管理）静态地址组），然后将其设置为目标地址。
- 将身份验证规则应用于 IT 特权人员出于业务目的需要使用的服务，在本示例中，自定义服务组 **Custom-IT-Ports** 可标识所有服务器管理端口（应放置在同一子网上）。
- 配置并应用身份验证执行对象（在本示例中，为 **Auth-IT-Server-Mgmt**（身份验证 **IT** 服务器管理）），以进行身份验证。**Add**（添加）MFA 服务器配置文件到身份验证配置文件（**Factors**（因素）选项卡）并执行剩余的步骤以配置 MFA。因为需要确定所有拥有特权账户、有权限管理设备的 IT 用户身份，所以使用 MFA 就非常关键。

  为了进一步降低攻击者使用被盗凭据攻击数据中心的机会，或是工作站无人值守但未锁定时的适当时机，配置 MFA 时，请配置用于身份验证因素的身份验证时间戳。由于数据中心的数据很有价值，因此最好是对服务和应用程序的安全进行优化。
- 记录活动，这样，可以跟踪和分析规则违规。

此外，IT 人员还可以管理数据中心的交换机、路由器和其他设备。如果同一组的 IT 用户管理这些资源，则可以将其添加到目标区域和地址，以便此规则在 IT 超级用户访问这些设备的管理接口之前对其进行身份验证。如果不同的 IT 用户组管理不同的数据中心资源组，则为每个用户组创建单独的、严格的安全策略规则和相应的身份验证策略和解密安全策略。

请勿以明文形式发送凭据。例如，如果使用 *RADIUS*，则使用支持的 EAP 方法在 TLS 内安全传输凭据。

创建用户到数据中心解密策略规则

为从用户群体进入数据中心的流量创建解密策略规则，以提供可见性，从而可以检测流量，并保护最有价值的资产。在创建允许用户组（或特定用户）访问数据中心一组服务器的安全策略规则时，需创建一个解密策略规则，以解密此流量。

因为数据中心包含最有价值的资产，因此，解密您可以解密的所有数据中心流量。首先，解密流向最关键服务器的流量，接下来解密高风险流量类别，然后解密源自最不可信的网络分段的流量（例如，优先解密源自合作伙伴、客户或承包商的流量，再解密源自可信任的内部区段的流量），最后，加强工作强度，直至将解密应用至流向数据中心所有资产的流量。尽可能多地解密流量，同时保持可接受的性能。

从数据中心解密中排除不合适的流量。个人信息相关的法规和合规性因国家/地区而异，即使是国家不同的地区内，也会不一样。不同的公司可能对跟人信息制定有不同的合规性规则。尽可能多地解密流量，但是，如果数据中心包含法规或公司规则要求不解密的信息，则请勿解密这些流量。

在创建用户到数据中心应用程序允许规则中，已创建安全策略规则，以允许 DNS 访问，允许工程用户访问工程开发服务器，允许 SAP 承包商开发人员仅访问 SAP 开发服务器，并允许一组特定的 IT 用户访问数据中心服务器进行管理。此时，我们会创建解密策略规则（**Policies**（策略） > **Decryption**（解密））以解密这些规则允许的流量。

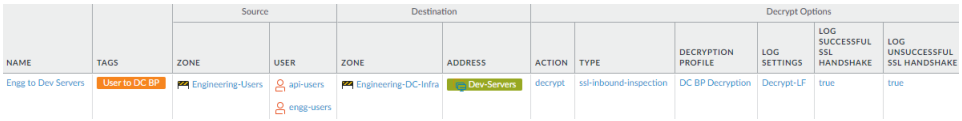
就这些通信流而言，解密策略规则共享一些共同元素：

- 创建解密策略规则时，目标是解密流量，因此，安全策略规则可以对其进行检查，并根据策略允许或阻止它。要实现这一点，解密策略规则必须使用与模拟安全策略规则相同的源区域和用户，以及相同的目标区域和地址（通过由动态地址组进行定义，这样，在添加或删除服务器时，可以更新防火墙，无需执行提交操作）。在安全策略和解密策略中定义的相同源和目标均是适用于相同流量的策略。
- 除了步骤 4 中所示的个人敏感信息外，所有这些规则的操作均属解密。
- 对于每条规则，配置解密日志和日志转发。在防火墙资源允许的范围内记录尽可能多的解密流量。
- 使用 SSL 入站检查对传入流量进行解密的解密规则要求使用适当的服务器证书。
- 所有这些解密规则均会使用数据中心最佳实践解密配置文件，如创建数据中心最佳实践解密配置文件所示。

STEP 1 | 解密从员工用户组流向数据中心服务器的允许流量。

此规则展示如何解密从用户组流向该组允许访问的数据中心服务器的流量，以提供该流量的可见性。例如，我们创建的应用程序允许规则中包括了允许工程用户访问数据中心开发服务器的

安全策略规则。要保护开发服务器，则解密传入流量，这样，防火墙可对其进行检测，并应用威胁防护配置文件。



		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Engg to Dev Servers	User to DC BP	Engineering-Users	api-users engg-users	Engineering-DC-Infra	Dev-Servers	decrypt	ssl-inbound-inspection	DC BP Decryption	Decrypt-LF	true	true

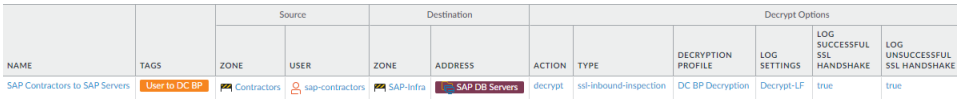
要创建此规则：

- 指定与模拟安全策略规则中相同的源和目标。在这种情况下，源用户是 **Engineering-Users** 区域内的 **api-users** 和 **engg-users** 用户组，目标是 **Engineering-DC-Infra** 区域中的 **Dev-Servers** 动态地址组内指定的服务器。
- 在“选项”选项卡上，设置操作为 **Decrypt**（解密），设置解密类型为 **SSL Inbound Inspection**（**SSL** 入站检查）。指定开发服务器的服务器证书，并应用数据中心最佳实践解密配置文件，以对流量上使用 SSL 入站检查和 SSL 协议设置。

根据源区域和用户组（或用户）以及目标区域和服务器组（由动态地址组成员定义），为每个用户组（或单个用户，如果适用）允许的数据中心流量创建类似的解密策略规则。

STEP 2 | 解密源自承包商、合作伙伴、客户和其他第三方的允许流量。

此规则展示如何解密从第三方组到允许其访问的数据中心服务器的流量。例如，允许规则包含安全策略规则，允许对数据中心 SAP 数据库服务器的 SAP 开发人员承包商进行有限访问。解密传入流量，这样，防火墙可对其进行检测，并对其应用威胁防护配置文件，从而保护 SAP 数据中心服务器。



		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
SAP Contractors to SAP Servers	User to DC BP	Contractors	sap-contractors	SAP-Infra	SAP DB Servers	decrypt	ssl-inbound-inspection	DC BP Decryption	Decrypt-LF	true	true

要创建此规则：

- 指定与模拟安全策略规则中相同的流量源和目标。在这种情况下，源用户是 **Contractors**（承包商）区域内的 **sap-contractors** 用户组，目标是 **SAP-Infra** 区域内的 **SAP DB Servers**（**SAP DB** 服务器）动态地址组内指定的服务器。
- 在“选项”选项卡上，设置操作为 **Decrypt**（解密），设置解密类型为 **SSL Inbound Inspection**（**SSL** 入站检查）。指定开发服务器的服务器证书，并应用数据中心最佳实践解密配置文件，以对流量上使用 SSL 入站检查和 SSL 协议设置。

根据源区域和用户组以及目标区域和服务器组（由动态地址组成员定义），为每个第三方组允许的数据中心流量创建类似的解密策略规则。

STEP 3 | 解密特权允许访问数据中心服务器的流量（如果法规或合规性规则禁止解密与个人信息相关的流量，则应将其除外）。

此规则展示如何解密特权访问流量，因为无论您有多信任此用户，您都应尽可能多地解密流量，以提供用户保护数据中心所需的可见性。如果未对允许流量进行解密，则无法应用威胁防

护配置文件，并且，如果流量隐藏有恶意软件或其他威胁，则将无法看见。此示例引用先前已创建的安全策略允许规则，以便为 IT 超级用户提供对数据中心服务器的管理接口访问。

如果负责管理和维护数据中心服务器的 *IT* 组使用 *SSH*，则无法解密 *SSH* 流量。您可以配置 SSH 代理来阻止 *SSH* 隧道，并防止 *SSH* 传播潜在恶意软件内容和应用程序。如果 *IT* 组使用 *SSL*，则使用 *SSL* 转发代理（而非 *SSL* 入站检查）创建解密策略规则。这样做的原因是 *SSL* 入站检查要求服务器证书以执行解密。因为 *IT* 管理许多数据中心服务器，因此，为每个服务器创建 *SSL* 入站检查规则会很麻烦，也很难管理。*SSL* 转发代理解密可在此用例中更好地扩展。

以下示例展示的是用于 SSL 转发代理的解密策略规则的用例。

		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
IT DC Management	User to DC BP	IT-Users	it-superusers	IT-Server-Access-DC	IT-Server-Management	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

要创建此规则：

- 指定与模拟安全策略规则中相同的流量源和目标。在这种情况下，源用户是 **IT-Users** 区域内的 **it-superusers** 用户组，目标是 **IT-server-access-DC** 区域内的 **IT-Server-Management** 动态地址组内指定的服务器。
- 在 Options（选项）选项卡上，将 Action（操作）设置为 **Decrypt**（解密），将解密类型设置为 **SSL Forward Proxy**（**SSL** 转发代理）。应用数据中心最佳实践解密配置文件，以对流量使用 SSL 转发代理和 SSL 协议设置。

如果其他组要求特权访问，则为每个组创建类似的解密策略规则类型。

此外，IT 人员还可以管理数据中心的交换机、路由器和其他设备。如果同一组的 IT 用户管理这些资源，则可以将其添加到目标区域和地址，以便此规则对连接到这些设备管理接口的流量进行解密。如果不同的 IT 用户组管理不同的数据中心资源组，则为每个用户组创建单独的、严格的安全策略规则和相应的解密和身份验证策略规则。

下一个示例展示的是用于 SSH 代理的解密策略规则的用例。您也可以选择不解密流量，而非使用 SSH 代理解密。

		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
IT DC Mgmt-SSH	User to DC BP	IT-Users	it-superusers	IT-Server-Access-DC	IT-Server-Management	decrypt	ssh-proxy	DC BP Decryption	none	false	true

要创建此规则：

- 流量源和目标与前面的 SSL 代理转发用例中的示例规则中的相同。
- 在 Options（选项）选项卡上，将 Action（操作）设置为 **Decrypt**（解密），将解密类型设置为 **SSH Proxy**（**SSH** 解密）。应用数据中心最佳实践解密配置文件，以对流量使用 SSH 代理和 SSL 协议设置。

  此外，IT 人员还可以管理数据中心的交换机、路由器和其他服务。如果同一组的 IT 用户管理这些资源，则可以将其添加到目标区域和地址，以便此规则对连接到这些设备管理接口的流量进行解密。如果不同的 IT 用户组管理不同的数据中心资源组，则为每个用户组创建单独的、严格的安全策略规则和相应的解密和身份验证策略规则。

STEP 4 | 如果法规或合规性规则禁止解密个人敏感信息，则不得解密。

此规则展示如何在需要排除法规或合规性要求之外的流量解密时创建基于策略的解密排除。此示例引用先前创建的安全策略允许规则为每个财务部用户提供财务服务器的访问。如果法规或合规性允许您解密此流量，则进行解密，这样，防火墙可以查看流量，并防御威胁。

		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Finance PCI No Decrypt	User to DC BP	Finance-Users	accounting-users finance-users	Finance-DC-Infra	Fin-Servers	no-decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

要创建此规则：

- 指定与模拟安全策略规则中相同的流量源和目标。在这种情况下，源用户是 **Finance-Users** 区域内的 **accounting-users** 和 **finance-users** 用户组，目标是 **Finance-DC-Infra** 区域内的 **Fin-Servers** 动态地址组内指定的服务器。
- 在 Options（选项）选项卡中，将 Action（操作）设置为 **No Decrypt**（无解密）。应用数据中心最佳实践 No Decryption profile（无解密配置文件）以防止出现证书问题。

不要将“无解密”配置文件应用到 TLSv1.3 流量，因为证书信息经过加密，防火墙无法基于证书信息阻止会话。

定义初始 Internet 到数据中心流量安全策略

与其他数据中心通信流一样，通过应用程序允许安全策略规则严格控制从 Internet 流向数据中心的流量，这样，使用未知或未受约束应用程序的流量不会进入数据中心。此外，将 DoS 保护策略规则（带 DoS 保护配置文件）应用于流向数据中心 Web 服务器层的外部流量，从而保护数据中心 Web 服务器免遭拒绝服务 (DoS) 攻击。

互联网流量给数据中心带来的风险包括从受感染的外部服务器下载恶意软件、下载允许攻击者访问和控制数据中心资产的“调用主页”命令和控制软件，以及无意中允许从互联网访问数据中心。为了减少攻击面，仅允许在数据中心内使用出于业务目的而需要使用的应用程序、用户和服务。解密、检查并记录当地法规、法律和您的业务要求允许的所有流量。此外，遵循 DoS 和区域保护最佳实践，以防止攻击者通过 DoS 攻击破坏数据中心（尤其是 Web 服务器）。

以下部分向您展示允许的流量类型以及如何控制流量、如何解密流量以及如何保护您的数据中心资产免受 DoS 攻击：

- Internet 到数据中心流量安全方法
- 创建 Internet 到数据中心应用程序允许规则
- 创建 Internet 到数据中心 DoS 保护策略规则
- 创建 Internet 到数据中心解密策略规则

Internet 到数据中心流量安全方法

用于保护从 Internet 流入数据中心的数据中心流量的传统旧方法使宝贵的资产面临风险，而最佳实践则保护您的宝贵资产。进入数据中心的流量所携带的最大风险是无意中从受感染的外部服务器下载恶意软件，或是无意中将恶意软件从受攻击的数据中心服务器部署到外部服务器。

传统方法	Risk	最佳实践方法
安装基于端口的安全策略。	恶意应用程序通过端口号欺骗、端口隧道使用、或是使用避免检测的端口跳跃来访问网络。	应用程序允许规则阻止应用程序在非标准端口上运行。记录并监控允许列表违规。

传统方法	Risk	最佳实践方法
		从基于端口的规则转换为基于应用程序的规则时，在数据库中，将基于应用程序的规则置于其将替换的基于端口的规则的上游。重置两个规则的策略规则触发计数器。如果流量到达基于端口的规则，则其策略规则的命中数会增加。调整基于应用程序的规则，直到一段时间内无流量到达基于端口的规则，然后删除基于端口的规则。
入侵防御系统 (IPS) 通常部署为入侵检测系统 (IDS)。	IPS 是一种带内检测和防御系统，而 IDS 是一种带外检测系统。将 IPS 部署为 IDS 就无法在源和目标之间的直接通信路径外部进行入侵检测，这样就不能实时预防，导致威胁可能会进入数据中心。	在防火墙的带内，使用 Palo Alto Networks 的 App-ID、User-ID 和 Content-ID 创建可创建严格控制访问权限的应用程序允许列表安全策略。应用安全配置文件以阻止已知和新威胁。
Web 应用程序防火墙足以保护数据中心。	攻击者将命令和控制 (C2) 软件放置在受攻击的数据中心端点，即可打开网络进行攻击，并可能会在水坑攻击中利用客户端侧的漏洞。	通过将严格的防间谍软件安全配置文件分配给控制流量的安全策略规则，从而防止攻击者将 C2 软件置于数据中心端点。此配置文件是防火墙的附带功能之一，因此，应用此保护时，您无需支付额外的费用。

创建 Internet 到数据中心应用程序允许规则

从 Internet 进入数据中心的流量的最大风险在于无意间从受感染的外部客户端下载恶意软件，或是无意间将恶意软件放置在外部服务器上，但前提是客户端从数据中心的受影响服务器上提取数据。保护从 Internet 进入数据中心的流量，这样，就不会在无意间下载利用服务器漏洞的恶意软件，或是允许客户端从公司某个服务器下载可能会感染合作伙伴、客户的恶意软件，或是下载所在行业内网站上停止使用的恶意软件（服务于水坑攻击）。

确保数据中心的流量源不是源于恶意 IP 地址或是其他潜在风险源，仅允许出于业务目的需要的应用程序。请勿在数据中心内使用不必要（且尤其是未知的）应用程序。要执行这些操作：

- 创建允许规则，以便对外部设备可用于与数据中心进行通信的允许的受约束应用程序进行控制。

  使用预定义的已批准标签标记所有经批准的应用程序。全景图和防火墙认为不带批准标记的应用成为是未批准的应用程序。

- 创建外部动态列表以标识不良 IP 地址，并将其用于阻止访问数据中心。
- 为任何专有应用程序创建自定义应用程序，这样，可以标识应用程序，并对其使用安全。

  如果您有现用的应用程序替代策略，是专门为定义端口集合的自定义会话超时而单独创建的，则将现有的应用程序替代策略转换为基于应用程序的测量，方法为：将基于服务的会话超时配置为维护每个应用的自定义超时，然后迁移基于应用程序的规则管辖的规则。应用程序替代策略基于端口。使用应用程序替代策略维护端口集合的自定义会话超时时，您就无法通过应用程序了解这些流量的情况，所以就无从得知或控制哪些应用程序使用这些端口。基于服务的会话超时达到自定义超时时，同时维护应用程序可见性。

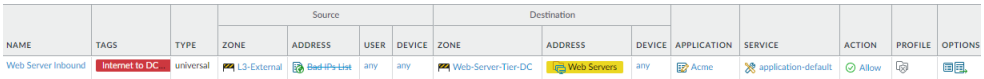
- 应用最佳实践安全配置文件组，其中包括最佳实践安全配置文件以防御恶意软件、漏洞、C2 流量以及已知和未知威胁。
- 在会话结束时记录所有允许的流量，以跟踪和分析违反规则的情况。将日志转发到日志服务器，如果适用，还会将日志电子邮件转发给适当的管理员。

数据中心安全策略规则库排序向您展示如何通过创建用于其他三个数据中心通信流的所有其他规则对这些规则和阻止规则进行排序，这样，就不会出现一个规则屏蔽另一个规则的现象。

要在多个数据中心采用一致的安全策略，则可以重复使用模板和模板堆栈，这样，就可以将相同的策略应用于每个数据中心模板使用变量应用设备特定值，如 *IP* 地址、*FQDN* 等，同时维护全球安全策略并减少您需要管理的模板和模板栈数量。

允许来自供应商、承包商和客户的受约束应用程序流量，仅限于必要的应用程序。

此规则展示如何通过以下方式确保到达数据中心的来自外部源的应用程序流量的安全：严格控制允许的应用程序，只允许其出现在默认端口上，然后通过外部动态列表阻止已知为不良的源，以标识已知的不良 IP 地址。



要创建此规则：

- 防止已知的不良源尝试访问数据中心。使用安全策略规则 **Source Address**（源地址）内的**Negate**（否定） 选项阻止与不良 IP 地址的连接。本示例使用外部动态列表（**Bad IPs List)**（不良 **IP** 列表））标识已知的不良 IP 地址，并予以阻止。（源地址中的删除线文本指示其已被否定，而非允许）。
- 将应用程序限制到仅出于商业目的使用的应用程序，并允许其仅在默认端口上运行（**application-default**（默认应用程序）），从而防止规避的恶意软件尝试在非标准端口上运行。在本示例中，供应商使用名为 **Acme** 的专有应用程序。我们已创建自定义应用程序以标识 **Acme** 专有应用程序，这样，防护期可以对流量进行分类，并使用适当的安全策略。

- 将 **Acme** 应用程序流量的目标限制到**Web-Server-Tier-DC**（**Web** 服务器层 **Dc**）区域内的区域内的 **Web-Servers**（**Web** 服务器）动态地址组。如果目标地址未在 Web 服务器层中，则防火墙丢弃此流量。

通过查看预定义应用程序报告（**Monitor**（监控） > **Reports**（报告） > **Application Reports**（应用程序报告） > **Applications**（应用程序）），验证仅在安全策略规则中明确允许的应用程序正在运行。如果在报告中看到预期以外的应用程序，则查看应用程序允许规则，并对其进行优化，这样，就不会再允许预期以外的应用程序。

创建 Internet 到数据中心解密策略规则

创建解密策略规则，提供对从 Internet 进入数据中心的流量的可见性，这样，才可以将安全策略应用于此流量。当您创建允许访问一组数据中心服务器的安全策略规则时，请创建一个解密策略规则以解密此流量。在创建 Internet 到数据中心应用程序允许规则中，我们创建了允许仅通过使用允许的应用程序从 Internet 访问数据中心 Web 服务器层的安全策略规则。此时，我们会创建解密策略规则（**Policies**（策略） > **Decryption**（解密））以解密这些规则允许的流量。

要解密流量，以便安全策略规则可以对其进行检查，并根据策略允许或阻止它，则解密策略规则必须使用与模拟安全策略规则相同的源区域和用户，以及相同的目标区域和地址（通过由动态地址组进行定义，这样，在添加或删除服务器时，可以更新防火墙，无需执行提交操作）。在安全策略和解密策略中定义的相同源和目标均是适用于相同流量的策略。

解密规则使用数据中心解密配置文件的最佳实践，如创建数据中心解密配置文件的最佳实践所示。

对于每条规则，配置解密日志和日志转发。在防火墙资源允许的范围内记录尽可能多的解密流量。

STEP 1 | 解密从 Internet 到数据中心 Web 服务器的允许流量。

此规则展示如何通过从数据中心外部发起的连接来解密流量。例如，创建的应用程序允许规则允许外部流量仅通过某些应用程序访问数据中心 Web 服务器。要保护数据中心 Web 服务器，请解密流量，以便防火墙对此流量进行检查，并应用威胁防护配置文件。

		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Internet to DC	Internet to DC BP	L3-External	any	Web-Server-Tier-DC	Web Servers	decrypt	ssl-inbound-inspection	DC BP Decryption	Decrypt-LF	true	true

要创建此规则：

- 指定与模拟安全策略规则中相同的源和目标。在这种情况下，源是 **L3-External**（**L3** 外部）区域，目标是 **Web-Server-Tier-DC**（**Web** 服务器层 **Dc**）区域 **Web-Servers**（**Web** 服务器）动态地址组内指定的服务器。
- 在“选项”选项卡上，设置操作为 **Decrypt**（解密），设置解密类型为 **SSL Inbound Inspection**（**SSL** 入站检查）。指定 Web 服务器的服务器证书，并应用数据中心解密配置文件的最佳实践，以在流量上使用 SSL 入站检查和 SSL 协议设置。

STEP 2 | 如果允许此类访问，则为从 Internet 进入任何其他服务器组的流量以及允许的其他应用程序创建类似的解密策略规则。

创建 Internet 到数据中心 DoS 保护策略规则

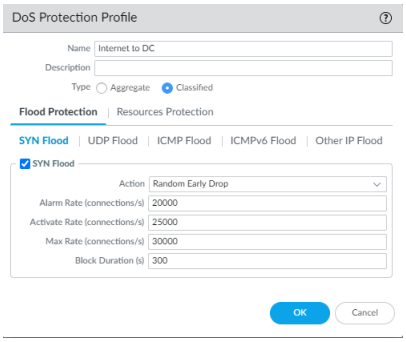
攻击者用来破坏网络的一种方法是拒绝服务(DoS)攻击，即，压制连接到 Internet 的目标系统，并将其关闭，使您所有的合法用户和服务均无法使用该系统。数据中心 Web 服务器是一个很有吸引力的目标，因为将此服务器关闭可阻止大多数对数据中心的合法访问。

要保护数据中心 Web 服务器，可将分类的DoS 保护策略应用于发往这些服务器的 Internet 流量。分类的 DoS 保护策略应用于分类的 DoS 保护配置文件，从而控制策略中规定的流量传入连接数。

此外，可为每个区域配置数据包缓冲区保护，保护防火墙免受单会话 DOS 攻击，否则，此攻击可能会压制防火墙的数据包缓冲区，导致合法流量被丢弃，尤其是在用于保护关键服务的防火墙上。

STEP 1 | 要创建用于保护数据中心 Web 服务器免受 DoS 攻击的分类的 DoS 保护配置文件，可将每秒连接数进行限制，以阻止 SYN 泛滥攻击。

此 DoS 保护配置文件可对附加配置文件的 DoS 保护策略规则中定义的流量每秒连接数 (CPS)予以限制，从而防止 DoS 攻击关闭您的 Web 服务器。配置文件通过设置 CPS 渐进阈值向您发出警报、激活随机早期丢弃 (RED) 数据包丢弃、阻止新连接，并限制新连接保持被阻的持续时间。配置用于保护数据中心 Web 服务器的 CPS 阈值取决于 Web 服务器的容量。



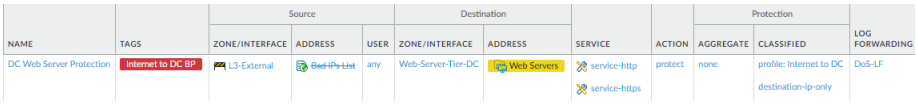
要创建此配置文件：

- 在 **Objects**（对象） > **Security Profiles**（安全配置文件） > **DoS Protection**（**DoS** 保护）中，**Add**（添加）一个分类的 DoS 保护配置文件。
- **Name**（命名）配置文件，选择 **Classified**（已分类）作为配置文件 **Type**（类型），设置用于发出警报（**Alarm Rate**（警报速率））、激活 RED（**Activate Rate**（激活速率）），并开始阻止新会话（**Max Rate**（最大速率））的 CPS 值，然后在 CPS 速率达到 **Max Rate**（最大速率）阈值时设置时间量（以秒为单位）以阻止新会话（**Block Duration**（阻止持续时间））。

如果未使用 *UDP* 等协议或其他 *IP* 协议，则使用安全策略规则组合将其限制到允许应用程序和 Zone Protection Profiles（区域保护配置文件），从而通过将想要阻止的协议的泛滥保护 *CPS* 设置为零数据包来阻止未使用的协议。

STEP 2 | 创建分类的 DoS 保护策略规则，以定义想要保护其免受 DoS 攻击和服务器，然后将 DoS 保护配置文件附加到此规则。

此规则可防止 SYN 泛滥攻击关闭数据中心 Web 服务器层。在本示例中，分类的 DoS 保护配置文件应用于允许连接到 Web 服务器层的外部流量。



		Source			Destination				Protection		
NAME	TAGS	ZONE/INTERFACE	ADDRESS	USER	ZONE/INTERFACE	ADDRESS	SERVICE	ACTION	AGGREGATE	CLASSIFIED	LOG FORWARDING
DC Web Server Protection	Internet to DC BP	L3-External	~~Bad IPs List~~	any	Web-Server-Tier-DC	Web Servers	service-http service-https	protect	none	profile: Internet to DC destination-ip-only	DoS-LF

要创建此规则：

- 要将 DoS 保护应用于发往 Web 服务器层的流量，DoS 保护策略必须用于与允许此流量的安全策略规则相同的流量。在本例中，该 DoS 规则可以保护我们在创建 Internet 到数据中心应用程序允许规则中允许的流量。
- 在选项/保护选项卡中，指定 Web 服务（**service-http** 和 **service-https**），设置操作为 **protect**（保护），以便将 DoS 保护配置文件的 SYN 泛滥阈值应用于此流量，设置日志转发方法（假设您已配置日志转发），然后选择在上一步中为此流量配置的分类的 DoS 保护配置文件（**Internet to DC**（**Internet** 到 **DC**））。

要防止源自内部源的 SYN 泛滥攻击，则创建单独的 DoS 保护策略规则，从而将内部区域指定为源区域，而非 **L3-External**（**L3** 外部）。为外部和内部攻击创建单独的规则，以提供单独的报告，从而使对攻击尝试的调查更容易。

定义初始数据中心到 Internet 流量安全策略

根据数据中心的架构，数据中心的服务器可能会访问 Internet 以检索软件更新，或是检查服务器证书吊销状态。因为安全计划通常集中于用户通信，忽略与 Internet 通信的服务器，因此，数据中心是攻击者最佳藏身之所。当数据中心服务器直接启动与 Internet 的通信时，您需要防范多种安全风险：

- 数据泄露 — 攻击者使用 FTP 或 HTTP 等合法应用程序，或是 DNS 隧道等其他方法窃取数据。创建仅允许用于服务器更新所需的应用程序的应用程序安全策略规则允许列表，这样，所有其他应用程序均被阻止，即使这些应用程序在其他情况下也是合法的应用程序。若应用程序规则变松，则会让攻击者有机可乘。
- 使用合法应用程序的命令和控制 **(C2)** — 如果允许数据中心服务器使用专用于软件更新以外的合法应用程序与 Internet 进行通信，攻击者那些合法的应用程序进行 C2 活动。例如，允许非标准端口上的 Web 浏览可为攻击者创造机会。只允许服务器仅通过软件更新所需的特定应用程序（而非其他应用程序）与 Internet 进行通信，即使是这些其他应用程序是合法的应用程序，且批准用于其他通途。
- 下载其他恶意软件 — 如果攻击者攻击数据中心服务器，则服务器上的恶意软件可能会通过背景连线通讯或其他机制从 Internet 下载更多的恶意软件。严格的允许规则仅允许通过必要的更新应用程序与相应的更新服务器进行通信，从而防止攻击者接触包含恶意软件的网站，避免攻击者泄露数据。此外，在数据中心服务器（及所有端点）上安装 Cortex XDR 客户端可防止已驻留在服务器上的恶意软件执行。
- 数据中心到 Internet 流量安全方法
- 创建数据中心到 Internet 应用程序允许规则
- 创建数据中心到 Internet 解密策略规则

数据中心到 Internet 流量安全方法

用于保护从数据中心流向 Internet 流量的传统旧方法使宝贵的资产面临风险，而最佳实践方法则保护您的宝贵资产。

传统方法	Risk	最佳实践方法
创建基于端口的规则和/或基于 IP 的规则，在可信网络中提供足够的安全。	基于端口和基于 IP 的规则无法控制允许连接到 Internet 的应用程序。如果端口已打开，则任何应用程序都可以使用此端口。	创建严格的基于应用程序的允许规则，仅允许检索更新的数据中心服务器仅使用合法应用程序仅与合法的更新服务器进行通信。记录并监控允许规则违规。

传统方法	Risk	最佳实践方法
		从基于端口的规则转换为基于应用程序的规则时，在数据库中，将基于应用程序的规则置于其将替换的基于端口的规则的上游。重置两个规则的策略规则触发计数器。如果流量到达基于端口的规则，则其策略规则的命中数会增加。调整基于应用程序的规则，直到一段时间内无流量到达基于端口的规则，然后删除基于端口的规则。
数据中心服务器仅接触更新服务器等可信服务器，因此，无需解密此流量。	数据中心已存在的恶意软件或命令和控制软件可能会尝试与外部服务器进行通信，以下载更多的恶意软件或泄露数据。	解密从数据中心流向 Internet 的所有流量。创建自定义 URL 类别，定义数据中心服务器允许联系的 URL，并将其用于安全策略中，以限制对外部服务器的 Internet 访问。在解密策略中使用相同的自定义 URL，以解密流向这些外部服务器的流量。
阻止并警报源自多个供应商的威胁防护配置文件。	各种工具的集合会为攻击者留下安全漏洞，可能无法很好地协同工作。	Palo Alto Networks 通过安全工具的一系列协同合作来阻塞安全漏洞，防止遭受攻击。

创建数据中心到 Internet 应用程序允许规则

启动与 Internet 上外部服务器连接的数据中心服务器的主要用例是更新软件，或是获取证书状态。最大的风险是连接到错误的服务器，尤其是 Linux 更新，因为您可能无意地与很多第三方 URL 相连接。数据中心服务器必须仅使用默认端口上所需的应用程序接收来自合法更新服务器的更新。

为此，请创建严格的应用程序允许规则，以便在连接到外部服务器时限制数据中心服务器连接的外部服务器以及数据中心服务器使用的应用程序。使用预定义的已批准标签标记所有经批准的应用程序。（Panorama 和防火墙将未带有已批准标记的应用程序视为未受约束应用程序）。严格的应用程序允许规则集通过以下方式终止潜在攻击：

- 防止数据中心服务器上已存在的恶意软件连接到受感染的外部服务器（回呼），并下载其他数据，因为允许规则不允许连接到这些服务器。
- 防止攻击者使用 FTP、HTTP 或 DNS 隧道等合法应用程序泄露数据，或是使用非标准端口上的 Web 浏览等合法应用程序执行命令和控制 (C2) 操作，因为允许规则不允许数据中心服务器使用这些应用程序与 Internet 进行通信。另一种有助于防止泄露的方法是使用文件阻止配置文件的 **Direction**（方向）控制来阻止出站更新文件，因此，仅允许下载以用于软件更新文件。

为需要来自不同外部服务器组的软件更新的每个应用程序创建严格的允许规则。在许多情况下，仅 App-ID 不足以保护数据中心服务器。例如，对于 Linux 服务器更新，将流量限制到诸如 *yum* 或 *apt-get* 等更新应用程序是不够的，因为这不能阻止连接到非法服务器。最佳实践是找到数据中心服务器需要连接的 URL，创建指定网站进行使用的自定义 URL 类别（**Objects**（对象）> **Custom Objects**（自定义对象）> **URL Category**（**URL** 类别）），并在安全策略规则中将其与 App-ID 相结合。和自定义 URL 类别的结合，可防止使用非法应用程序，阻止连接到不属于自定义 URL 类别的更新服务器，从而锁定数据中心服务器可以连接的外部服务器。例如，在允许数据中心服务器连接到 CentOS 更新服务器的安全策略规则中，您可以创建一个名为 *CentOS* 更新服务器 的自定义 URL 类别，并添加服务器使用的 CentOS 更新站点到自定义类别。

要找到合法的 *Linux* 更新服务器和其他更新服务器的 *URL*，请与软件工程、开发操作和其他组合作，从而更新软件，了解获取更新的位置。您还可以记录 *Web* 浏览会话，收集开发人员连接到的 *URL*，然后对这些 *URL* 进行工程处理，以筛选用于安全策略的正确 *URL*。

因为您不希望允许所有更新服务器，因此，请勿在安全策略规则中使用用于与 *Internet* 通信的数据中心服务器的 *URL* 筛选配置文件（*PAN-DB URL* 筛选）。对通信进行限制，这样，数据中心服务器仅访问其检索到更新的特定服务器。

此外，所有允许的通信均应发生在每个应用程序的标准端口上。在非标准端口上不得运行任何应用程序。与所有数据中心流量一样，监控允许列表违规，因为此违规表明您需要更新安全策略以允许合法流量，或是攻击者正在或是尝试进入网络。

数据中心安全策略规则库排序向您展示如何通过创建用于其他三个数据中心通信流的所有其他规则对这些规则和阻止规则进行排序，这样，就不会出现一个规则屏蔽另一个规则的现象。

要在多个数据中心采用一致的安全策略，则可以重复使用模板和模板堆栈，这样，就可以将相同的策略应用于每个数据中心模板使用变量应用设备特定值，如 *IP* 地址、*FQDN* 等，同时维护全球安全策略并减少您需要管理的模板和模板栈数量。

以下每一条允许规则：

- 已附加最佳实践安全配置文件组，其中包含最佳实践安全配置文件。使用安全配置文件组，您可以一次性将所有最佳实践配置文件应用到规则，而不是单独指定每个配置文件。利用安全配置文件组可以更快速轻松地配置恶意软件、漏洞、C2 流量以及已知和未知威胁防御。
- 在会话结束时记录流量，以便跟踪和分析违反规则的情况，并且包括日志转发。将日志转发到日志服务器，如果适用，还会将日志电子邮件转发给适当的管理员。

STEP 1 | 允许数据中心服务器访问软件更新服务器。

此规则展示如何限制对 Internet 上软件更新服务器的访问，这样，数据中心服务器仅与已知的合法服务器进行通信，不会与其他外部更新服务器通信。此示例允许工程数据中心服务器访问

CentOS 更新服务器，并将通信限制为仅使用必要的应用程序以建立仅与正确的更新服务器组的连接。

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
CentOS Update	DC to Internet BP	universal	Engineering-DC-Infra	Dev-Servers	any	L3-External	any	yum	application-default	CentOS-Update-Servers	Allow		

要创建此规则：

- 将 CentOS 更新请求源限制到仅需要检索更新的数据中心服务器，在本示例中，为 **Engineering-DC-Infra**（工程 **DC** 基础架构）区域的 **Dev-Servers**（**Dev** 服务器）动态地址组。
- 将数据中心服务器可用于与外部更新服务器进行通信的应用程序限制到仅所需的应用程序，在本示例中，为用于 CentOS 更新的 **yum**。仅允许应用程序在默认端口上运行，可防止规避的恶意软件尝试使用非标准端口。
- 创建自定义 URL 类别以定义数据中心服务器可以连接的更新服务器的 URL。在本示例中，**CentOS-Update-Servers**（**CentOS** 更新服务器）自定义 URL 类别可定义数据中心服务器可以访问的更新服务器 URL。

这种限制组合还可以阻止已损害数据中心服务器的攻击者访问其他目标，并使用其他应用程序泄露数据或是下载其他恶意软件。

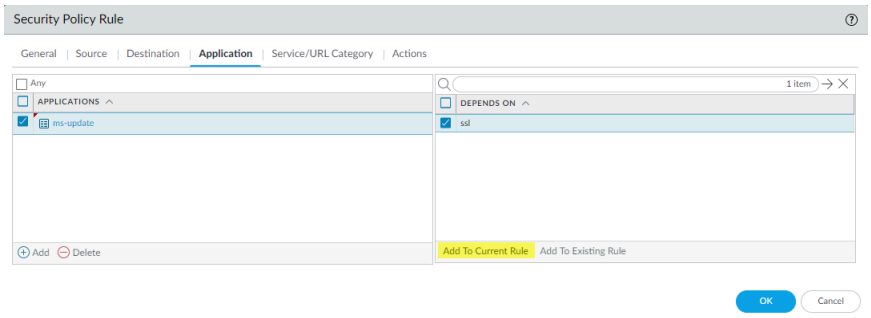
同样，允许相同服务器与 Microsoft Windows 更新服务器进行通信的规则也所使用相同的结构。

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
Windows Update	DC to Internet BP	universal	Engineering-DC-Infra	Dev-Servers	any	L3-External	any	ms-update ssl	application-default	Win-Update-Servers	Allow		

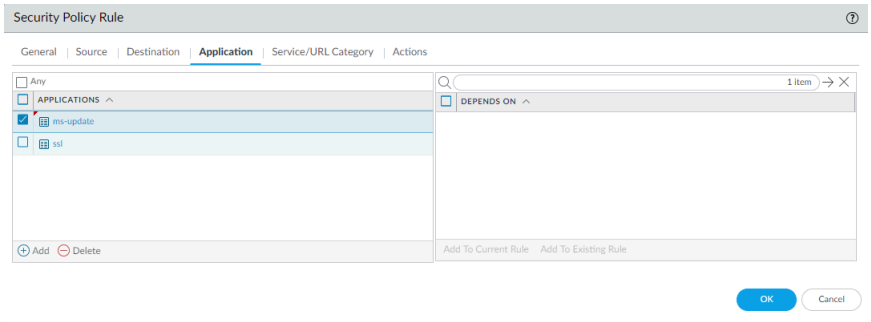
源区域和地址与之前的 CentOS 更新规则相同。区别为：

- 自定义 URL 类别（**Win-Update-Servers**（**Win** 更新服务器））包含用于 Windows 更新的 URL，这样，与其他 URL 的接触将被拒绝。
- 应用程序与 Microsoft 更新相关。除了 **ms-update**应用程序，Microsoft 更新还需要 **ssl**应用程序，因为 ms-update 取决于 SSL。与 CentOS 更新规则一样，仅标准端口有效。

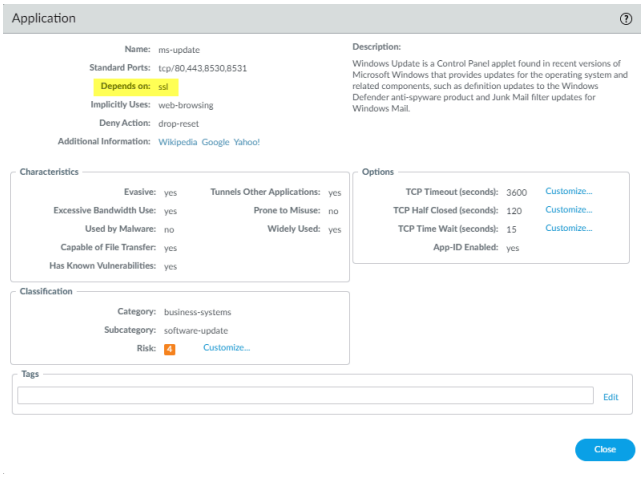
  某些应用程序取决于其他应用程序。对于给定的应用程序，必须允许所有相关应用程序或是应用程序不起作用。当您创建安全策略规则时，用户界面会显示应用程序的依赖性。例如，当您在规则中指定 ms-update 应用程序时，界面会显示 ms-update 也依赖于允许 SSL：



  单击 **Add to Current Rule**（添加到当前规则）可将所选应用程序添加到规则。



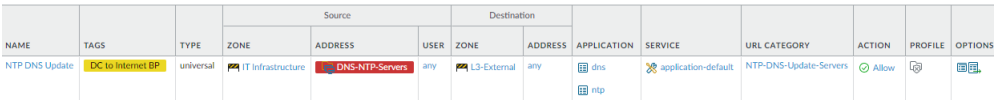
您还可以使用搜索功能（***Objects***（对象） > ***Applications***（应用程序））查找应用程序依赖性。例如，为了找到 *ms-update* 应用程序的依赖性，请搜索 ***ms-update***，在结果应用程序列表中单击***ms-update*** 应用程序，然后检查 ***Depends on:***（依赖于：）字段。



STEP 2 | 允许数据中心服务器访问 DNS 和 NTP 更新服务器。

此规则展示如何限制对 Internet 上 DNS 和 NTP 更新服务器的访问，这样，数据中心服务器仅与已知的合法服务器进行通信。此示例允许 IT 数据中心服务器访问 DNS 和 NTP 更新服务器，并将通信限制为仅使用必要的应用程序以建立仅与正确的更新服务器组的连接。

仅允许流量流向批准的 *DNS* 服务器。使用 DNS 安全服务阻止恶意 *DNS* 服务器连接。



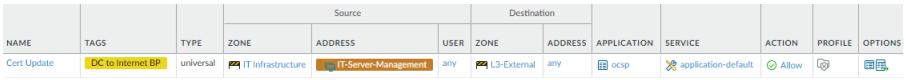
NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
NTP DNS Update	DC to Internet BP	universal	IT Infrastructure	DNS-NTP-Servers	any	L3-External	any	dns ntp	application-default	NTP-DNS-Update-Servers	Allow		

要创建此规则：

- 将 DNS 和 NTP 更新请求源限制到仅需要检索更新的数据中心服务器，在本示例中，为 **Engineering-DC-Infra**（工程 **DC** 基础架构）区域的 **DNS-NTP-Servers**（**DNS-NTP** 服务器）动态地址组。
- 将数据中心服务器可用于与这些外部更新服务器进行通信的应用程序限制到仅所需的应用程序，在本示例中，为 **dns** 和 **ntp**。仅允许应用程序在默认端口上运行，可防止规避的恶意软件尝试使用非标准端口。
- 创建自定义 URL 类别以定义数据中心服务器可以连接的更新服务器的 URL。在本示例中，**NTP-DNS-Update-Servers**（**NTP-DNS** 更新服务器）自定义 URL 类别可定义数据中心服务器可以访问的更新服务器 URL。

STEP 3 | 允许数据中心服务器访问证书颁发机构服务器，以获取数字证书的吊销状态，确保其有效性。

通过此规则，数据中心服务器可以连接到 Internet 上的在线证书状态协议 (OCSP) 响应器（服务器），以检查验证证书的吊销状态。与浏览器证书吊销列表 (CRL) 更新相比，OCSP 响应器提供最新的证书状态，这取决于要跟上证书吊销的 CRL 浏览器更新的频率。在防火墙上配置证书配置文件时，如果 OCSP 响应器无法访问，则可以设置 CRL 证书验证为 OSCP 的回退方法。



NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Cert Update	DC to Internet BP	universal	IT Infrastructure	IT-Server-Management	any	L3-External	any	ocsp	application-default	Allow		

要创建此规则：

- 将证书吊销检查请求源限制到仅需要检查证书验证的数据中心服务器，在本示例中，为 **IT-Infrastructure**（**IT** 基础架构）区域的**IT-Server-Management**（**IT** 服务器管理）动态地址组。
- 将数据中心服务器可用于与外部证书吊销服务器进行通信的应用程序限制到仅所需的应用程序。本示例可确保数据中心服务器和 OCSP 响应器之间的连接安全，因此，指定的应用程序应仅为 **ocsp**。仅允许应用程序在默认端口上运行，可防止规避的恶意软件尝试使用非标准端口。

通过查看预定义应用程序报告（**Monitor**（监控） > **Reports**（报告） > **Application Reports**（应用程序报告） > **Applications**（应用程序））确认仅在安全策略规则中明确列入允许列表的应用程序正在运行。如果在报告中看到预期以外的应用程序，则查看应用程序允许规则，并对其进行优化，这样，就不会再允许预期以外的应用程序。

创建数据中心到 Internet 解密策略规则

创建解密策略规则以提供从数据中心服务器到 Internet 的流量可见性。解密所有从数据中心服务器到 Internet 的流量。启动从数据中心内部到 Internet 的连接的唯一账户是服务账户，且其大部分流量均与软件更新相关，因此，无需考虑隐私问题。解密并检查此流量非常重要，因为如果更新服务器受感染，则数据中心服务器可能会下载恶意软件，并通过软件更新过程进行传播。检查流量并应用威胁防护配置文件的最佳实践可以保护您的数据中心免受可能使用合法应用程序从合法更新服务器下载的恶意软件的影响。

在创建数据中心到 Internet 应用程序允许规则中，我们已创建允许数据中心服务器启动与 Internet 更新服务器连接的安全策略规则，以更新操作系统软件、DNS 和 NTP，并检查证书。此时，我们创建模拟解密策略规则以解密更新安全策略规则允许的流量。

请勿解密证书吊销服务器（在线响应器）的流量。在线证书状态协议 *(OCSP)* 流量通常使用 *HTTP*，因此，此流量是未加密的明文流量。此外，*SSL* 转发代理解密可能会破解更新过程，因为防火墙充当的是中间人代理，并采用 *OSCP* 响应器可能视为无效的代理证书替换客户端证书。

就这些通信流而言，解密策略规则共享一些共同元素：

- 创建解密策略规则时，目标是解密流量，因此，安全策略规则可以对其进行检查，并根据策略允许或阻止它。要实现这一点，解密策略规则必须使用与模拟安全策略规则相同的源区域和用户，以及相同的目标区域和地址（通过由动态地址组进行定义，这样，在添加或删除服务器时，可以更新防火墙，无需执行提交操作）。在安全策略和解密策略中定义的相同源和目标均是适用于相同流量的策略。
- 所有这些规则的操作均属解密。
- 对于每条规则，配置解密日志和日志转发。在防火墙资源允许的范围内记录尽可能多的解密流量。
- 所有这些解密规则均会使用数据中心最佳实践解密配置文件，如创建数据中心最佳实践解密配置文件所示。

在很多情况下，解密策略规则示例包括自定义 URL 类别（**Objects**（对象） > **Custom Objects**（自定义对象） > **URL Category**（**URL** 类别）），以缩小解密的流量范围。每个解密策略规则均使用与模拟安全策略规则相同的自定义 URL 类别（以及源和目标），因此，解密和安全策略均完全适用于相同的流量。App-ID 和自定义 URL 类别的组合，可使防火墙仅解密规则允许的流量，而不解密防火墙阻止的流量，从而节省处理时间。（解密必须发生在安全策略规则评估之前。）

STEP 1 | 解密 Internet 上数据中心服务器和软件更新服务器之间的流量。

此规则展示如何解密数据中心服务器的软件更新流量，从而提供对可能出现在 Internet 更新服务器上的威胁的可见性，这样，方便防火墙进行阻止。本示例基于在创建数据中心到 Internet 应用

程序允许规则创建的模拟应用程序允许规则对 Internet 上数据中心服务器和 CentOS 更新服务器之间的允许流量进行解密。

		Source		Destination			Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	ZONE	ADDRESS	URL CATEGORY	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
CentOS Update Decrypt	DC to Internet BP	Engineering-DC-Infra	Dev-Servers	L3-External	any	CentOS-Update-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

要创建此规则：

- 指定与模拟安全策略规则中相同的源和目标。在这种情况下，源是 **Engineering-DC-Infra**（工程 **DC** 基础架构）区域中 **Dev-Servers** 动态地址组，而目标是 Internet（**L3-External**（**L3** 外部）区域）。
- 指定与模拟安全策略规则中相同的自定义 URL 类别（**CentOS-Update-Servers**（**CentOS** 更新服务器）），以将解密范围缩小到仅解密规则允许的流量，以免防火墙浪费周期来解密将丢弃的流量。
- 在 Options（选项）选项卡上，将 Action（操作）设置为 **Decrypt**（解密），将解密类型设置为 **SSL Forward Proxy**（**SSL** 转发代理）。应用数据中心最佳实践解密配置文件，以对流量使用 SSL 转发代理和 SSL 协议设置。

根据与模拟安全策略规则中相同的源和目标、以及相同的自定义 URL 类别，为需要连接到 Internet 更新服务器的每组数据中心服务器的数据中心允许流量创建类似的解密策略规则。例如，根据模拟安全策略规则，用于需要与 Microsoft Windows 更新服务器通信的数据中心服务器的解密策略规则正是此类示例：

		Source		Destination			Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	ZONE	ADDRESS	URL CATEGORY	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Win Update Decrypt	DC to Internet BP	Engineering-DC-Infra	Dev-Servers	L3-External	any	Win-Update-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

STEP 2 | 解密 Internet 上数据中心服务器和 NTP 和 DNS 之间的流量。

此规则展示如何解密数据中心服务器的 NTP 和 DNS 更新流量，从而提供对可能出现在 Internet 更新服务器上的威胁的可见性，这样，方便防火墙进行阻止。本示例基于在创建数据中心到 Internet 应用程序允许规则中创建的模拟应用程序允许规则对允许流量进行解密。

		Source		Destination			Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	ZONE	ADDRESS	URL CATEGORY	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
DNS-NTP Update Decrypt	DC to Internet BP	IT Infrastructure	DNS-NTP-Servers	L3-External	any	NTP-DNS-Update-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

要创建此规则：

- 指定与模拟安全策略规则中相同的源和目标。在这种情况下，源是**IT Infrastructure**（**IT** 基础架构） 区域中的**DNS-NTP-Servers**（**DNS- NTP** 服务器） 动态地址组，而目标是 Internet（**L3-External**（**L3** 外部）区域）。
- 指定与模拟安全策略规则中相同的自定义 URL 类别（**NTP-DNS-Update-Servers**（**NTP-DNS** 更新服务器）），以将解密范围缩小到仅解密规则允许的流量。
- 在 Options（选项）选项卡上，将 Action（操作）设置为 **Decrypt**（解密），将解密类型设置为 **SSL Forward Proxy**（**SSL** 转发代理）。应用数据中心最佳实践解密配置文件，以对流量使用 SSL 转发代理和 SSL 协议设置。

定义初始数据中心内部流量安全策略

数据中心内部流量在数据中心服务器和应用程序层之间流动。您可以认为，数据中心外围内部的所有流量均为可信流量，无需进行检测。但是，如果攻击者攻击数据中心服务器，且应用程序层之间的流量不流进防火墙，则攻击者可以从数据中心横向移动到关键服务器，下载更多的恶意软件，重新利用服务器，并使用数据中心不存在的合法应用程序泄露数据，就像在过去几年中曾发生过的几起重大攻击事件一样。

要想防止恶意软件在数据中心站稳脚，最佳做法是采用严格的特定应用程序允许规则来保护流量安全，并使用在应用程序层之间部署的下一代防火墙对流量进行检测。

此外，数据中心不允许存在未知应用程序。未知应用程序可能表示，攻击者已获得数据中心的访问权限。为内部专有应用程序创建自定义应用程序，这样，可以采用 App-ID 对其进行标识，并应用安全策略。如果未给专有应用程序创建自定义应用程序，则防火墙会将其视为未知 tcp 或未知 udp 流量。问题是防火墙会采用处理未知应用程序相同的方法处理这些专有应用程序，而您则会阻止未知应用程序，因为他们可能是攻击者的工具。如果允许数据中心的未知应用程序，则可能将资产王国的钥匙亲手交给攻击者。

对于未知商业应用程序，可以提交请求到 *Palo Alto Networks*，以创建 *App-ID*。

如果您有现用的应用程序替代策略，是专门为定义端口集合的自定义会话超时而单独创建的，则将现有的应用程序替代策略转换为基于应用程序的测量，方法为：将基于服务的会话超时配置为维护每个应用的自定义超时，然后迁移基于应用程序的规则管辖的规则。应用程序替代策略基于端口。使用应用程序替代策略维护端口集合的自定义会话超时时，您就无法通过应用程序了解这些流量的情况，所以就无从得知或控制哪些应用程序使用这些端口。基于服务的会话超时达到自定义超时时，同时维护应用程序可见性。

- 数据中心内部流量安全方法
- 创建数据中心内应用程序允许规则
- 创建数据中心内部解密策略规则

数据中心内部流量安全方法

用于保护数据中心服务器之间东西流量的传统旧方法使宝贵资产面临风险，而最佳实践方法则能保护您的宝贵资产。

传统方法	Risk	最佳实践方法
您无需对不经过数据中心外围的流量进行分段，因此，应用程序层之间的流量无需通过安全基础架构。	攻击任何数据中心服务器的攻击者可以横向移动至关键的数据中心服务器，并重新利用他们。数据中心内部的攻击者可	使用严格的允许规则对应用程序层之间的流量进行分段，防止不必要的通信，减少攻击面，并且有助于防止攻击者在

传统方法	Risk	最佳实践方法
	以随意移动，不会担心被发现。	数据中心横向移动。记录并监控允许列表违规。
可信网络内的数据中心很安全，因此，不必急于快速修复数据中心服务器。	漏洞会打开很长一段时间，成为攻击者发动攻击的媒介。	及时在数据中心服务器上安装修补程序，以关闭漏洞。创建允许列表安全策略规则，帮助您了解正在数据中心上运行的内容以及未修复服务正在运行的位置。
阻止并警报源自多个供应商的威胁防护配置文件。	各种工具的集合会为攻击者留下安全漏洞，可能无法很好地协同工作。	Palo Alto Networks 协作安全工具套件可协同工作，以填补安全漏洞、阻止攻击、并标识尝试在数据中心服务器上传播的未知恶意软件。

此外：

- 为每个功能创建一个唯一的服务账户。例如，仅允许特定服务账户复制 Exchange 邮箱，仅允许 Web 服务器上的特定服务账户查询 MySQL 数据库。请勿为这两个功能使用同一个服务账户。
- 监控服务账户。
- 不允许在数据中心使用常规用户账户。

从基于端口的规则转换为基于应用程序的规则时，在数据库中，将基于应用程序的规则置于其将替换的基于端口的规则的上游。重置两个规则的策略规则触发计数器。如果流量到达基于端口的规则，则其策略规则的命中数会增加。调整基于应用程序的规则，直到一段时间内无流量到达基于端口的规则，然后删除基于端口的规则。

创建数据中心内应用程序允许规则

数据中心流量通常由多层应用程序流量组成，这些应用程序流量在不同的服务器层之间流动，为 SharePoint、WordPress、内部专有应用程序等应用程序提供服务。最常见的多层应用程序体系结构由 Web 服务器（表示层）、应用程序服务器（应用层）和数据库服务器（数据层）组成。创建数据中心分段策略可提供有关如何在应用程序层之间防止防火墙以及如何对数据中心进行分段的指南。

数据中心服务器之间流量的处理方式由该流量决定。对于大多数应用程序流量，添加威胁防护配置文件到安全策略允许列表，以检查流量。例如，使用采用安全配置文件的最佳实践来保护财务应用程序和工程开发应用程序等的 Web、应用程序和服务层之间的流量。应用威胁防护配置文件的例外是针对诸如邮箱复制和备份流量等大容量的低价值应用程序。您仍可以通过允许访问这些应用程序，但是，由于防火墙已在复制前对流量进行检查，因此，应用威胁防护配置文件会消耗防火墙的 CPU 周期，而不会提供额外的价值。

WildFire 安全配置文件可标识尝试在数据中心服务器之间进行传播的未知恶意软件，以防止在发现恶意软件损坏系统之前泄露数据。如果不能使用WildFire 全局云，则可以部署 WildFire 专有云或 WildFire 混合云。

本节中的安全策略规则示例显示了如何为 Web 服务器、应用程序服务器和数据库服务器层允许需要的多层数据中心财务应用程序流量，从而为应用程序提供服务。此示例包含两个已为其创建自定义应用程序的内部专用应用程序：（**Billing-App**（计费应用程序）和 **Payment-App**（支付应用程序））序配置允许流量在应用程序服务器层之间流动的规则。为这些应用程序创建自定义 App-ID 后，防火墙可以对其进行标识、控制，并使用安全策略。因为未知应用程序无法标识，无法应用安全，可能表示数据中心存在攻击，因此，请勿在数据中心允许此类应用程序。每个数据中心应用程序均应拥有一个 App-ID。

仅允许其标准（***application-default***（默认应用程序））端口上的应用程序。在某些情况下，出于业务要求，可能需要作出例外，允许应用程序使用特定客户端和服务器之间的非标准端口。在这些情况下，请注意在非标准端口上正在运行的应用程序流量，确保您知道非标准端口上正在运行的每个应用程序实例。非标准端口上运行的尚未作出明确（已知）例外的应用程序可能表示存在规避的恶意软件。

使用预定义的已批准标签标记所有经批准的应用程序。全景图和防火墙认为不带批准标记的应用成为是未批准的应用程序。

数据中心安全策略规则库排序向您展示如何通过创建用于其他三个数据中心通信流的所有其他规则对这些规则和阻止规则进行排序，这样，就不会出现一个规则屏蔽另一个规则的现象。

要在多个数据中心采用一致的安全策略，则可以重复使用模板和模板堆栈，这样，就可以将相同的策略应用于每个数据中心模板使用变量应用设备特定值，如 *IP* 地址、*FQDN* 等，同时维护全球安全策略并减少您需要管理的模板和模板栈数量。

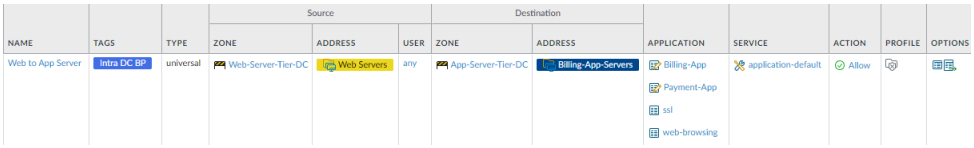
以下每一条允许规则：

- 已附加最佳实践安全配置文件组，其中包含最佳实践安全配置文件。使用安全配置文件组，您可以一次性将所有最佳实践配置文件应用到规则，而不是单独指定每个配置文件。利用安全配置文件组可以更快速轻松地配置恶意软件、漏洞、C2 流量以及已知和未知威胁防御。
- 在会话结束时记录流量，以便跟踪和分析违反规则的情况，并且包括日志转发。将日志转发到日志服务器，如果适用，还会将日志电子邮件转发给适当的管理员。

STEP 1 | 允许 Web 服务器层和应用程序服务器层之间的财务应用程序流量。

此规则限制可以在用于财务部计费服务器的 Web 服务器层和应用程序服务器之间流动的流量，这样，仅合法应用程序的流量可以访问计费服务器。（在创建用户到数据中心应用程序允许规则时，我们还创建一个用于限制财务部用户访问数据中心的规则，这样，仅适当财务部用户才能访问数据中心。）此规则使用动态地址组指定每个应用程序层中的服务器 — **Billing-App-**

Servers（计费应用程序服务器）指定应用程序服务器层中的服务器地址，**DB2-Servers**（**DB2** 服务器）指定财务部数据库服务器层中的服务器地址。



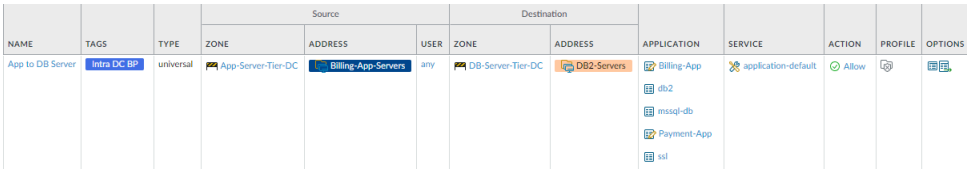
要创建此规则：

- 在 **Web-Server-Tier-DC**（**Web** 服务器层 **DC**）中限制用于 Web 服务器（**Web-Servers**（**Web** 服务器））的财务应用程序流量源。
- 在 **App-Server-Tier-DC**（应用程序服务器层 **DC**）中限制用于计费服务器（**Billing-App-Servers**（计费应用程序服务器））的财务应用程序目标。
- 限制 Web 服务器可以用于访问计费应用程序服务器的应用程序，仅允许其默认端口上的应用程序。在本示例中，应用程序包括两个自定义应用程序：**Billing-App**（计费应用程序） 和 **Payment-App**（支付应用程序），针对每个应用程序，均在创建时指定了端口。财务部将采用这些用于计费和支付服务的专用应用程序。

创建类似规则，以控制 Web 服务器层和其他应用程序服务器层之间的应用程序和流量。

STEP 2 | 允许应用程序服务器层和数据库服务器层之间的财务应用程序流量。

此规则用于限制在可以用于财务部计费服务器的应用程序服务器层和数据库服务器层之间流动的流量，这样，仅使用合法应用程序的流量可以在计费应用程序服务器和积分数据库服务器之间流动。此规则使用动态地址组指定每个应用程序层中的服务器 — **Billing-App-Servers**（计费应用程序服务器）指定应用程序服务器层中的服务器地址，**DB2-Servers**（**DB2** 服务器）指定财务部数据库服务器层中的服务器地址。



要创建此规则：

- 在 **App-Server-Tier-DC**（应用程序服务器层 **DC**）中限制用于计费应用程序服务器（**Billing-App-Servers**（计费应用程序服务器））的财务应用程序源。
- 在 **DB-Server-Tier-DC**（**DB** 服务器层 **DC**）中限制用于数据库服务器（**DB2-Servers**（**DB2** 服务器））的财务应用程序目标。
- 限制计费应用程序服务器可以用于访问数据库服务器的应用程序，仅允许默认端口或其已知非默认端口上的应用程序。

创建类似规则，以控制应用程序服务器层和其他应用程序的数据库服务器层之间的应用程序和流量。

通过查看预定义应用程序报告（**Monitor**（监控） > **Reports**（报告） > **Application Reports**（应用程序报告） > **Applications**（应用程序）），验证仅在安全策略规则中明确允许的应用程序正在运行。如果在报告中看到预期以外的应用程序，则查看应用程序允许规则，并对其进行优化，这样，就不会再允许预期以外的应用程序。

创建数据中心内部解密策略规则

为什么在数据中心内部解密流量？毕竟，这里没有用户，数据中心是安全网络内部深处一个安全的环境。但事实并非如此。因为很多人认为，数据中心很安全，无需进行查看，因此，数据中心成为攻击者实现精确藏身的最佳位置。但是，网络其余部分存在的相同的基本原则在数据中心也是成立的：您无法保护自己免受看不见的东西的损害。对加密的数据中心流量进行解密，从而方便防火墙检查流量、控制访问、提供威胁可见性，从而保护您的宝贵资产。

有一些数据中心流量未加密（明文）。不得在明文流量上启用解密，因为这里无密可解。

在创建数据中心内应用程序允许规则中，我们创建了安全策略规则，允许位于不同应用程序层的财务部应用程序相关的服务器相互进行通信。此时，我们创建模拟解密策略规则来解密这些规则允许的流量。

对于每条规则，配置解密日志和日志转发。在防火墙资源允许的范围内记录尽可能多的解密流量。

STEP 1 | 解密 Web 服务器层和应用程序服务器层之间的财务应用程序流量。

此规则解密用于财务部计费服务器的 Web 服务器层和应用程序服务器层之间流动的流量，这样，防火墙就可以看到流量，并保护每层中的服务器免受潜在威胁的影响。

		Source			Destination		Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Web to App	Intra DC BP	Web-Server-Tier-DC	Web Servers	any	App-Server-Tier-DC	Billing-App-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

要创建此规则：

- 指定与模拟安全策略规则中相同的源和目标。在本示例中，源是**Web-Server-Tier-DC**（**Web** 服务器层 **Dc**）区域中的区域中的 **Web-Servers**（**Web** 服务器）动态地址组，而目标是 **App-Server-Tier-DC**（应用程序服务器层 **Dc**）区域中的区域中的 **Billing-App-Servers**（计费应用程序服务器）。
- 在 Options（选项）选项卡上，将 Action（操作）设置为 **Decrypt**（解密），将解密类型设置为 **SSL Forward Proxy**（**SSL** 转发代理）。应用数据中心最佳实践解密配置文件，以对流量使用 SSL 转发代理和 SSL 协议设置。

STEP 2 | 解密应用程序服务器层和数据库服务器层之间的财务应用程序流量。

此规则解密用于财务部计费服务器的应用程序服务器层和数据库服务器层之间流动的流量，这样，防火墙可以看到流量，并保护每层中的服务器免受潜在威胁的影响。

		Source			Destination		Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
App to DB	Intra DC BP	App-Server-Tier-DC	Billing-App-Servers	any	DB-Server-Tier-DC	DB2-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

要创建此规则：

- 指定与模拟安全策略规则中相同的源和目标。在本示例中，源是 **App-Server-Tier-DC**（应用程序服务器层 **Dc**）区域中的区域中的 **Billing-App-Servers**（计费应用程序服务器）动态地址组，而目标是 **DB-Server-Tier-DC**（**DB** 服务器层 **Dc**）区域中的区域中的 **DB2-Servers**（**DB2** 服务器）。
- 在 Options（选项）选项卡上，将 Action（操作）设置为 **Decrypt**（解密），将解密类型设置为 **SSL Forward Proxy**（**SSL** 转发代理）。应用数据中心最佳实践解密配置文件，以对流量使用 SSL 转发代理和 SSL 协议设置。

数据中心安全策略规则库排序

本主题提供示例安全策略规则库的概述，其中展示了四个数据中心流量的规则排序。前面的部分详细讨论了每个安全策略规则和解密策略规则，若有需要，还将讨论身份验证策略和 DoS 保护策略规则。

安全策略规则的顺序至关重要。一个规则不应屏蔽另一个规则。例如，阻止规则不得阻止您想允许的流量，因此，必须将允许规则放置在阻止流量的规则生效之前。此外，允许规则不得允许想要阻止的流量。通过创建非常具体的允许规则，您可以严格控制允许的应用程序以及谁可以/不可以使用它们。

规则 **1-7**：前两条规则阻止 QUIC 应用程序，以防止它阻止流量或阻止解密。接下来五条规则为用户允许 DNS 访问，并为特定的用户组允许特定应用程序和服务器访问。这些规则在创建用户到数据中心应用程序允许规则中配置。

			Source			Destination						
	NAME	TAGS	ZONE	ADDRESS	USER	ZONE	ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
1	Block QUIC UDP	none	any	any	any	L3-External	any	any	quic_udp_ports	Deny	none	
2	Block QUIC	none	any	any	any	L3-External	any	quic	application-default	Deny	none	
3	DNS Services	User to DC BP	any	any	any	IT Infrastructure	DNS-Servers	dns	application-default	Allow		
4	IT DC Server Management	User to DC BP	IT-Users	any	it-superusers	IT-Server-Access-DC	IT-Server-Management	ms-rdp ssh ssl	Custom-IT-Ports	Allow		
5	Engineering Resources	User to DC BP	Engineering-Users	any	api-users engg-users	Engineering-DC-Infra	Dev-Servers	oracle-bi perforce profinet qlikview	application-default	Allow		
6	Finance to DC	User to DC BP	Finance-Users	any	accounting-users finance-users	Finance-DC-Infra	Fin-Servers	netsuite oracle oracle-crm-ondemand oracle-forms	application-default	Allow		
7	SAP-Contractors	User to DC BP	Contractors	any	sap-contractors	SAP-Infra	SAP DB Servers	ms-sql-analysis-service mssql-db mssql-mon sap	application-default	Allow		

图 **1:** 数据中心规则 **1-7**

仅特定用户才能使用其默认端口上的特定应用程序来访问数据中心特定的目标服务器（地址）。安全配置文件保护所有这些允许规则免受威胁的影响。这些规则非常具体，因此将比阻止规则先发现网络上的未知用户和应用程序，从而阻止已批准的用户和应用程序与规则库中更多较低级别的一般规则进行匹配。

规则 **8-9**：虽然之前的规则允许批准的应用程序，但在创建数据中心阻止规则中创建的后两条规则可以发现和阻止标准端口上用户的非预期应用程序，并阻止非标准端口上的所有应用程序。（您的部署可能包含比示例中更多的用户区域。）

			Source			Destination						
	NAME	TAGS	ZONE	ADDRESS	USER	ZONE	ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
8	Unexpected-App-from-User-Zone	User to DC BP	Contractors Engineering-Users Finance-Users IT-Users	any	any	Web-Server-Tier-DC	any	any	application-default	Drop	none	
9	Unexpected-User-App-Any-Port	User to DC BP	Contractors Engineering-Users Finance-Users IT-Users	any	any	Web-Server-Tier-DC	any	any	any	Drop	none	

图 **2:** 数据中心规则 **8-9**

非用户区域的流量不符合这些规则。将这些规则置于应用程序阻止规则（规则 18 和 19）的上游，否则将会这些后者会屏蔽前者。（与这两个规则匹配的流量可以与更多的一般应用程序阻止规则匹配。如果应用程序阻止规则排在第一位，且匹配的流量与这些规则也匹配，则此流量将不会触犯这些规则，也不会单独记录，因此，这些规则就不会产生作用，无法将员工用户活动导致的阻止与其他区域活动导致的阻止区分开来。

规则 **10-16**：后七条规则允许数据中心与 Internet 之间以及数据中心内部的流量（在创建 Internet 到数据中心应用程序允许规则、创建数据中心到 Internet 应用程序允许规则和创建数据中心内应用程序允许规则中创建）。安全配置文件保护所有这些允许规则免受威胁的影响。

	NAME	TAGS	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
10	Web Server Inbound	Internet to DC BP	L3-External	~~Bad IPs List~~	any	Web-Server-Tier-DC	Web Servers	Acme	application-default	any	Allow		
11	NTP DNS Update	DC to Internet BP	IT Infrastructure	DNS-NTP-Servers	any	L3-External	any	dns ntp	application-default	NTP-DNS-Update-Servers	Allow		
12	CentOS Update	DC to Internet BP	Engineering-DC-Infra	Dev-Servers	any	L3-External	any	yum	application-default	CentOS-Update-Servers	Allow		
13	Windows Update	DC to Internet BP	Engineering-DC-Infra	Dev-Servers	any	L3-External	any	ms-update ssl	application-default	Win-Update-Servers	Allow		
14	Cert Update	DC to Internet BP	IT Infrastructure	IT-Server-Management	any	L3-External	any	ocsp	application-default	any	Allow		
15	App to DB Server	Intra DC BP	App-Server-Tier-DC	Billing-App-Servers	any	DB-Server-Tier-DC	DB2-Servers	Billing-App db2 mssql-db Payment-App ssl	application-default	any	Allow		
16	Web to App Server	Intra DC BP	Web-Server-Tier-DC	Web Servers	any	App-Server-Tier-DC	Billing-App-Servers	Billing-App Payment-App ssl web-browsing	application-default	any	Allow		

图 **3:** 数据中心规则 **10-16**

规则 **17-20**：最后四条规则在创建数据中心流量阻止规则时创建，用于阻止您不希望出现在数据中心的应用程序和非预期的应用程序，并发现网络上的未知用户。

	NAME	Source ZO...	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
17	Block-Bad-Apps	any	any	any	App-Server-Tier-DC DB-Server-Tier-DC Engineering-DC-Infra Finance-DC-Infra IT Infrastructure SAP-Infra Web-Server-Tier-DC	any	Encrypted-Tunnels File-Sharing Remote-Access	any	Drop	none	
18	Unexpected-App-from-Any-Zone	any	any	any	Web-Server-Tier-DC	any	any	application-default	Drop	none	
19	Unexpected-App-Any-Port	any	any	any	Web-Server-Tier-DC	any	any	any	Drop	none	
20	Discover-Unknown-Users	any	any	unknown	any	any	any	any	Deny	none	

规则 17 阻止您不希望出现在数据中心的应用程序。该规则位于应用程序允许规则之后，从而支持例外访问权限。例如，您可能批准置于此阻止规则上游的应用程序允许规则中的一至两个文件共享应用程序，然后，此规则中的应用程序筛选器将会阻止此应用程序类别中的其他应用程序，从而阻止使用未批准的文件共享应用程序。如果网络上出现您从不希望出现的应用程序组或单个应用程序组，并且没有例外，例如 BitTorrent，则可以创建特定的允许规则以仅阻止这些应用程序，并将其置于规则库的顶部，即应用程序允许规则的上游。但是，如果这样操作，则必须确保阻止的应用程序没有合法的业务用途，因为用户将无法访问这些应用程序。

规则 18 和 19 与规则 8 和 9 相似，后两者用于发现来自用户的非预期应用程序（这些规则允许的流量仅来自用户区域）。规则 18 和 19 用于发现所有其他区域的非预期应用程序。若具有单独的规则，则可以记录更高粒度的阻止规则匹配。

规则 20 用于发现未知用户，从而让您单独记录这些访问尝试，以便进行调查。

与所有安全策略规则库一样，最后两条规则是用于区域内流量（允许）和区域间流量（拒绝）的 Palo Alto Networks 默认规则。

记录并监控数据中心流量

防火墙的日志记录和监控工具可揭示网络上的应用程序、用户和流量模式，包括您可能不知道已在此处存在的应用程序和用户。记录和监控功能可为转换到数据中心最佳实践安全策略以及该安全策略维护的所有阶段提供有用的信息，因为，它可以揭示未知用户（未通过 User-ID 标识）、未知应用程序和预期之外端口上的流量,所有这些都表明未正确构建安全策略规则，或构建不严格。所有这些都表明未正确构建安全策略规则，或构建不严格。记录和监控信息有助于您确定允许哪些应用程序以及允许哪些用户访问哪些应用程序和设备，同时还帮助您调查潜在的安全问题。

访问数据中心时，可以捕获基准测量。定期将这些基准测量与当前测量进行对比，以评估进度、确定变化，并在实施数据中心最佳实践安全策略时找出需要改进的地方。

如果使用 *Panorama* 管理防火墙，则可以检测防火墙的健康，以便对比设备的基线性能，以及将设备对比来确定与正常行为的偏差。

配置从防火墙到 Panorama、到 SNMP 陷阱服务器等外部服务器、或是到 syslog 服务器的日志转发，以集中多个防火墙的日志，从而使查看和分析更便捷（防火墙仅可以显示本地日志和报告，而不是来自其他防火墙的日志和报告）。配置日志转发时，应配置发送通知以验证配置的日志目标是否正在接收防火墙日志。

数据中心日志记录和监控的最佳实践包括：

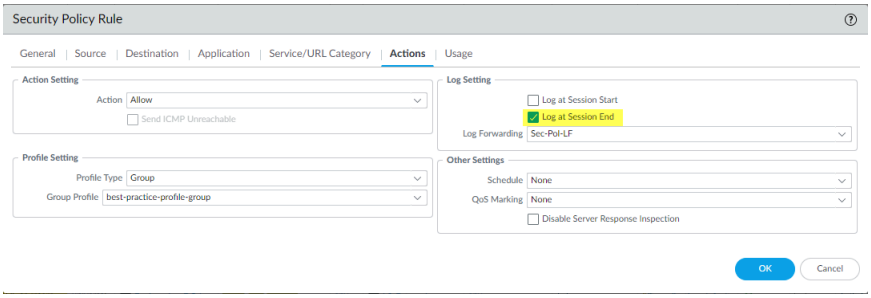
- 记录并监控的数据中心流量
- 监控数据中心阻止规则并调整规则库
- 记录与区域间规则不匹配的数据中心流量
- 记录与区域间允许规则匹配的数据中心内部流量

记录并监控的数据中心流量

Palo Alto Networks 下一代防火墙默认会创建一些日志，而您则需要为其他流量配置日志记录。最佳做法是记录数据中心的所有流量，并监控用于记录预期之外应用程序、用户、流量和行为的日志。

默认情况下，防火墙会记录与明确配置的安全策略规则匹配的流量，不会记录与规则库底部的预定义区域内默认（允许具有同一源和目标的流量在同一区域内存在）和区域间默认（规则库中的最后一个规则，拒绝与之前规则不匹配的流量）规则匹配的流量。

创建安全策略规则时，在默认情况下，防火墙会记录会话结束时的流量：



但默认情况下，防火墙不会转发日志，也不会应用安全配置文件。前面的示例展示了将日志转发到适当日志服务器和管理员，以及应用最佳实践安全配置文件的最佳实践。

对于大多数流量，最佳做法是 **Log at Session End**（在会话结束时记录），原因在于应用程序通常会在整个会话期间发生变化。例如，会话的初始 App-ID 可能是 Web 浏览，但在防火墙处理几个数据包之后，防火墙找到了该应用程序的更具体的 App-ID，从而更改 App-ID。在会话开始时记录流量有几种用例，包括长时间隧道会话，例如 GRE 隧道（除非您同时启用 **Log At Session Start**（在会话开始时记录）和 **Log At Session End**（在会话结束时记录），否则无法在 ACC 中查看活跃的会话），当您需要在会话开始时获取信息以进行故障排除时，以及为了获取对运营技术/工业控制系统 (OT/ICS) 会话的可见性（这也是长时间会话）。

流量记录功能将记录关于规则允许以及规则拒绝或丢弃（违规）的流量信息，因此无论怎样处理流量，防火墙都会提供有价值的信息。违规活动将指示潜在攻击或需要进行调整（以允许合法的业务应用程序）的允许规则。

在检查日志中的已阻止流量时，请将防火墙在任何系统遭到攻击之前为实施保护而阻止的流量（例如，阻止未允许的应用程序）与防火墙在攻击后阻止的流量（例如，已存在于数据中心服务器上的恶意软件尝试联系外部服务器，以下载更多恶意软件或泄露数据）区分开来。

防火墙提供了大量用于网络监控的监控工具、日志和日志报告：

- **Monitor**（监控） > **Logs**（日志）提供了流量、威胁、User-ID 和许多其他日志类型，包括可在同一个屏幕上显示多个日志类型的 **Unified**（统一）日志，因此，您无需单独查看不同类型的日志。当摘要部分出现放大镜图标时，您可以点击它以查看详细的日志条目。
- **Monitor**（监控） > **PDF Reports**（**PDF** 报告）提供可以查看的预定义报告以及用于创建由预定义和自定义报告所组成报告组的功能。例如，您可以查看流量活动或是进行基线测量，以按区域或接口了解数据中心每个分段的带宽使用情况和流量。
- **Monitor**（监控） > **Manage Custom Reports**（管理自定义报告）提供了创建自定义报告 的功能，您可以通过此功能查看阻止规则、允许规则或是任何其他相关主题的信息。
- **Monitor**（监控） > **Packet Capture**（数据包捕获）可让您对流经防火墙管理接口和网络接口的流量实施数据包捕获。
- 应用程序命令中心 **(ACC)** 提供的小组件可显示应用程序、用户、URL、威胁和流经网络的内容的交互式图形摘要。例如，您可以查看并评估网络上的应用程序（**ACC** > **Network Activity**（网络活动） > **Application Usage**（应用程序使用情况） > **Threats**（威胁）），以检查应用程序是

否有任何变化，或是应用程序是否存在威胁行为。如果在列表内看到预期以外的应用程序，则对如何处理这些应用程序进行评估。

ACC 信息的另一个用途是帮助识别受攻击的用户帐户和主机系统。使用**ACC** > **Network Activity**（网络活动） > **User Activity**（用户活动） > **Threats**（威胁）小组件对威胁和与威胁相关的用户名进行分析，然后使用威胁日志将具体的问题隔离。

- 仪表板（**Dashboard**（仪表板））提供的小组件可显示防火墙的一般信息以及威胁、配置和系统日志中最多 10 个最新条目。
- 使用 Panorama 监控防火墙健康状况并对新设备进行基线测量，比较性能指标，并在提交、软件更新、内容更新、规则更改和新应用程序添加等事件后跟踪防火墙的性能。如果性能偏离设备基线，则可以手动查看并排除故障，或是自动开出票证以进行调查。
- 在 Panorama 或单个防火墙上，使用策略规则触发计数器分析规则库的变化。例如，添加新应用程序时，先将允许规则添加至规则库，再允许应用程序的网络流量。如果流量触发规则，且计数器递增，这表示，即使您尚未激活此应用程序，与规则匹配的流量也已存在于网络上，或是您需要调整此规则。另一个示例是使用基于应用程序的规则替换基于端口的规则，方式如下：将基于应用程序的规则置于基于端口的规则上游，并记录是否有任何流量触发了此基于端口的规则。如果有，则需要调整基于应用程序的规则，以捕获此流量。

  结合策略规则触发计数器，检查 **ACC** > **Threat Activity**（威胁活动） > **Applications Using Non Standard Ports**（使用非标准端口的应用程序）和 **ACC** > **Threat Activity**（威胁活动） > **Rules Allowing Apps On Non Standard Ports**（允许非标准端口上应用程序的规则）小组件，以查看非标准端口上的流量是否导致了非预期的规则触发。

使用策略规则计数器的关键在于执行更改时重置计数器，如引入新应用程序或更改规则的定义。重置计数器时确保您看到更改后的结果，结果不包括更改前所做的更改和发生的事件。

监控数据中心阻止规则并调整规则库

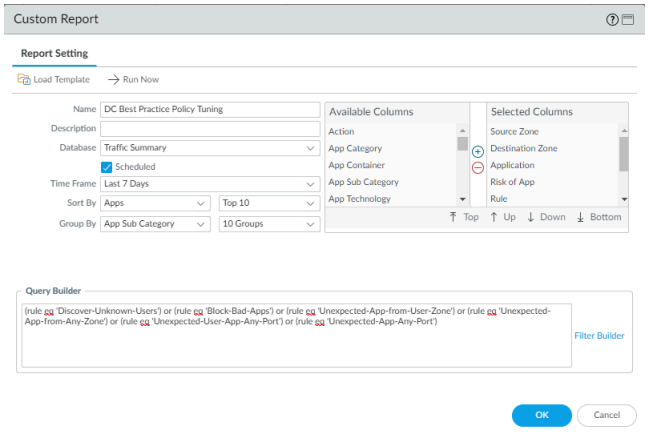
制定最佳实践安全策略是一个迭代过程。一旦创建数据中心流量阻止规则，就开始监控与旨在识别策略缺口、预期之外行为和潜在攻击的阻止规则匹配的流量。调整应用程序允许规则，以纳入与阻止规则匹配但应被允许的流量，并对可能表明存在攻击的流量进行调查。

已阻止流量的报告中包含了可用于调查潜在问题的有价值信息。保留规则库中的阻止规则，以保护宝贵的数据中心资产，并在流量匹配阻止规则时提供此信息。

按照内容更新最佳实践，使您的防火墙保护保持最新。维护数据中心最佳实践规则库包含数据中心防火墙的特定最佳实践。

STEP 1 | 创建自定义报告，以监控与旨在标识策略缺口和潜在攻击的阻止规则匹配的流量。

1. 选择 **Monitor**（监控） > **Manage Custom Reports**（管理自定义报告）。
2. **Add**（添加）报告，并为其指定一个用于描述此报告用途的 **Name**（名称）。在本示例中，为 **DC Best Practice Policy Tuning**（数据中心最佳实践策略调整）。
3. 将 **Database**（数据库）设为 **Traffic Summary**（流量统计）。这还会更改 **Available Columns**（可用列）选项。
4. 从 **Available Columns**（可用列）中，将 **Source Zone**（源区域）、**Destination Zone**（目标区域）、**Sessions**（会话）、**Bytes**（字节数）、**Application**（应用程序）、**Risk of App**（应用风险）、**Rule**（规则）和 **Threat**（威胁）添加到 **Selected Columns**（所选列）列表。如果想要监控其他类型的信息，则同时选中这些信息。
5. 选中 **Scheduled**（已调度）框。
6. 设置所需的 **Time Frame**（时间框架）、**Sort By**（排序方式）和 **Group By**（分组方式）值。在本例中，我们将 **Time Frame**（时间范围）设置为 **Last 7 Days**（过去 7 天），将 **Sort By**（排序方式）设置为 **Apps**（应用程序），并将 **Group By**（分组方式）设置为 **App Sub Category**（应用子类别）。
7. 定义查询，以匹配触犯了用于查找策略缺口和潜在攻击的规则的流量。您可以使用 **or**（或）运算符为匹配任何规则的流量创建单个报告，或是创建单个报告以监控每个规则。在 **Query Builder**（查询生成器）中，指定想要在报告中包含的每个规则名称。本示例使用六个阻止规则，并使用 **Or**（或）运算符包含与任何规则匹配的流量的相关信息：
   - `(rule eq 'Discover-Unknown-Users')`
   - `(rule eq 'Block-Bad-Apps')`
   - `(rule eq 'Unexpected-App-from-User-Zone')`
   - `(rule eq 'Unexpected-App-from-Any-Zone')`
   - `(rule eq 'Unexpected-User-App-Any-Port')`
   - `(rule eq 'Unexpected-App-Any-Port')`



STEP 2 | 定期回顾报告，确保您能了解流量为何会匹配每个阻止规则，或者升级策略，将合法的应用程序和用户包含在内，或者用报告中的信息评估匹配规则的流量的风险。

记录与区域间允许规则匹配的数据中心内部流量

默认情况下，允许所有区域间流量（同一区域内的源和目标）。防火墙对安全策略进行评估后，要么会允许应用程序允许列表规则控制的流量，拒绝阻止规则控制的流量，或是，如果区域间流量与规则不匹配，则防火墙默认允许所有流量。（防火墙默认阻止区域内流量）。因为数据中心存在宝贵的资产，因此最佳做法是监控数据中心服务器之间的所有数据中心内部流量，包括区域间默认允许规则允许的流量。

要获得对此流量的可见性，则在将区域间默认规则应用至数据中心区域内的流量时，在其上启用日志记录。您可通过此流量的日志记录检查未明确允许的访问，以及您可能想要通过修改允许规则而明确允许或明确阻止的访问。

在定义初始数据中心内部流量安全策略时，我们会在数据中心内部使用三个示例区域：Web 服务器层 DC、应用程序服务器层 DC、以及 DB 服务器层 DC。在本示例中，我们创建了一个自定义报告来收集与数据中心这三个内部区域中的数据中心区域内流量相关的日志信息。

STEP 1 | 在规则库中选择区域内默认列，然后点击 **Override**（替代）以启用规则编辑。

STEP 2 | 选择 **intrazone-default**（区域内默认）规则名称，以编辑此规则。

STEP 3 | 在 Actions（操作）选项卡中，选择 **Log at Session End**（结束时记录），然后点击 **OK**（确定）。

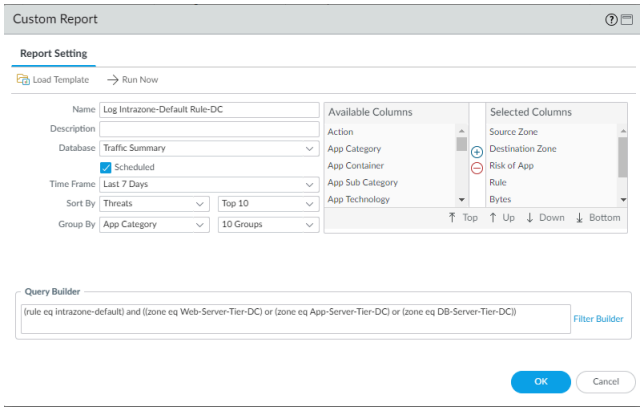
STEP 4 | 创建自定义报告，为数据中心内部区域监控触犯该规则的流量。

1. 选择 **Monitor**（监控） > **Manage Custom Reports**（管理自定义报告）。
2. **Add**（添加）一个报告，并为其指定描述性 **Name**（名称）。在本示例中，为 **Log Intrazone-Default Rule-DC**（记录数据中心区域内默认规则）。
3. 将 **Database**（数据库）设为 **Traffic Summary**（流量统计）。
4. 从 **Available Columns**（可用列）中，将 **Source Zone**（源区域）、**Destination Zone**（目标区域）、**Sessions**（会话）、**Bytes**（字节数）、**Application**（应用程序）、**Risk of App**（应用风险）、**Rule**（规则）和 **Threat**（威胁）添加到 **Selected Columns**（所选列）列表。如果想要监控其他类型的信息，则同时选中这些信息。
5. 选中 **Scheduled**（已调度）框。
6. 设置所需的 **Time Frame**（时间框架）、**Sort By**（排序方式）和 **Group By**（分组方式）值。在本示例中，选中的值分别为 **Threats**（威胁）和 **App Category**（应用程序类别）。
7. 定义查询，匹配与用于数据中心区域的区域内默认规则匹配的流量：

```
(rule eq intrazone-default) 和（(zone eq Web-Server-Tier-DC) 或
 (zone eq App-Server-Tier-DC) 或 (zone eq DB-Server-Tier-DC)）
```

此查询可筛选与区域内默认规则匹配的流量，并与定义的三个内部数据中心区域中的任何一个匹配。因为默认 **Selected Columns**（选中列）包含有区域，因此，此报告可显示每个会话

的区域。在实际的数据中心中，可能会有更多的区域，您可以将每个区域添加到查询中。最终的自定义报告设置如下所示：



8. **Commit**（提交）更改。

记录与区域间规则不匹配的数据中心流量

与配置的任何安全策略规则都不匹配的流量将与数据库底部的预定义区域间默认阻止规则进行匹配，并且会被拒绝。要获得对与您明确配置的规则不匹配的流量的可见性，请在区域间默认规则上启用日志记录。记录此流量可以让您检查未明确允许的访问尝试，从而识别攻击尝试或您想要修改允许规则的流量。

STEP 1 | 在规则库中选择区域间默认列，然后点击 **Override**（替代）以启用规则编辑。

STEP 2 | 选择 **interzone-default**（区域间默认）规则名称，以编辑此规则。

STEP 3 | 在 Actions（操作）选项卡中，选择 **Log at Session End**（结束时记录），然后点击 **OK**（确定）。

STEP 4 | 创建自定义报告，监控触犯该规则的流量。

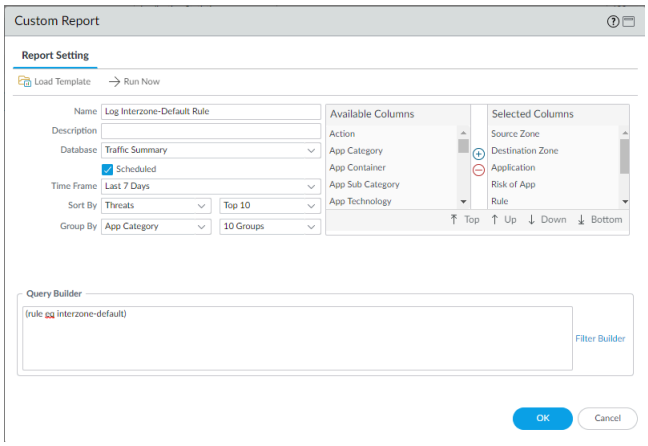
1. 选择 **Monitor**（监控）> **Manage Custom Reports**（管理自定义报告）。
2. **Add**（添加）一个报告，并为其指定描述性 **Name**（名称）。在本示例中，为 **Log Interzone-Default Rule**（记录数据中心区域内默认规则）。
3. 将 **Database**（数据库）设为 **Traffic Summary**（流量统计）。
4. 从 **Available Columns**（可用列）中，将 **Source Zone**（源区域）、**Destination Zone**（目标区域）、**Sessions**（会话）、**Bytes**（字节数）、**Application**（应用程序）、**Risk of App**（应用

风险）、**Rule**（规则）和 **Threat**（威胁）添加到 **Selected Columns**（所选列）列表。如果想要监控其他类型的信息，则同时选中这些信息。

5. 选中 **Scheduled**（已调度）框。
6. 设置所需的 **Time Frame**（时间框架）、**Sort By**（排序方式）和 **Group By**（分组方式）值。在本示例中，选中的值分别为 **Last 7 Days**（过去 7 天）、**Threats**（威胁）和 **App Category**（应用类别）。
7. 定义查询，以匹配与区域间默认规则匹配的流量：

```
(rule eq interzone-default)
```

最终的自定义报告设置如下所示：



8. **Commit**（提交）更改。

维护数据中心最佳实践规则库

应用程序在不断发展，因此，应用程序允许列表也需要同步改进。由于最佳实践规则利用策略对象来简化管理，为新的应用程序添加支持，或者从允许列表中删除应用程序，通常意味着修改对应的应用程序组或应用程序筛选器。

Palo Alto Networks 发送您应该自动下载并尽快在防火墙上安排安装的内容更新。大部分内容更新可能包含威胁内容安全的更新（防病毒、漏洞、反间谍软件等），还可能包含 ID 被修改的应用程序。每个月的第三个星期二的内容更新也包含新 App-ID。您可以设置单独的阈值延迟安装常规内容更新和每月一次的更新，后者包括在下载后特定期限内的新 App-ID。延迟安装可让您安装不包括新 App-ID 的内容更新，以便尽快获取最新的威胁签名，同时还能预留更多时间在安装前检查新 App-ID。

每个月第三个星期二的内容更新包含新 App-ID 时，则可能导致安全政策实施方法发生改变。安装新的或修改的 App-ID 前，请检查对策略的影响，阶段更新对测试的影响，并视需要修改现有的安全策略。控制在防火墙上下载和安装内容更新最有效的方法是，（如果您使用 Panorama），在 Panorama 加载内容更新并获取内容更新的推送。

遵循一般的内容更新最佳实践，但请记住，数据中心的可用性通常是关键，因此您可能不会选择像在面向 Internet 的防火墙上一样，在数据中心快速推出内容更新：

- 在网络的安全区域中对内容更新进行快速测试，然后将其安装到数据中心。
- 对于不包含新 App-ID 的内容更新，则在自动下载后设置安装阈值为不超过八小时，并在该时间段内进行测试。
- 对于包含新 App-ID 的内容更新，则在自动下载后设置安装阈值为不超过八天，并在该时间段内进行测试。
- 配置所有内容更新的日志转发。

STEP 1 | 安装新的内容更新之前，检查新的和修改的 App-ID，确定是否有策略上的影响。

STEP 2 | 如有必要，修改现有的安全策略规则，以适应 App-ID 的更改。

如果有些 App-ID 要求执行更多测试并安装剩下的新 App-ID，您可以禁用选择的 App-ID。在下一个月带新 App-ID 的内容更新发布之前（每个月的第三个星期二），请完成对任何必要的策略修改的测试，以避免重叠。

随着时间的推移，数据中心使用的应用程序列表通常会稳定下来，因此，相关的新 *App-ID* 会越来越少。（大多数新 *App-ID* 与面向 *Internet* 的应用程序相关）来这可以降低新 *App-ID* 在数据中心制造问题的风险，并让您能够更快安装带新 *App-ID* 的内容更新。

STEP 3 | 准备策略更新，以便解释内容更新中包含的 App-ID 更改，将新的经批准的应用程序添加至允许列表规则，或者从允许列表规则移除应用程序。

维护最佳实践规则库的其他方法包括：

- 使用 Palo Alto Networks 评估和检查工具识别安全覆盖中的缺口。

- 用户反馈其再也无法访问应用程序，这说明规则库存在缺口，或者在积极执行阻止使用这些应用程序之前，网络上使用了存在风险的应用程序。
- 将对数据中心评估时创建的资产清单列表与资产本身进行比较，确保这些资产得到正确保护。
- 使用 应用程序命令中心 (ACC) 等 Palo Alto Networks 记录和监控工具查找并调查可能表示配置错误或规则缺失的预期以外的活动定期运行报告，检查是否已应用您想要应用的安全等级

如果使用 *Panorama* 管理防火墙，则可以检测防火墙的健康，以便对比设备的基线性能，以及将设备对比来确定与正常行为的偏差。

使用 Palo Alto Networks 评估和检查工具

Palo Alto Networks 的客户成功团队开发出了一种预防架构，其中包含的工具和资源有助于您查看并评估网络安全风险，以及如何利用防火墙和其他工具保护您的网络。联系您的 Palo Alto Networks 代表安排评估和审查（Palo Alto Networks 销售工程师负责实施审查，并提供网络安全状况评估方面的专业知识）。截至发布时止，可用的安全风险预防工具包括：

- 防御状态评估 **(PPA)** — PPA 是一组调查问卷，有助于揭示网络和安全架构所有区域中安全风险预防缺口。它不仅可以帮助您标识所有安全风险，还能提供如何预防这些风险和关闭缺口的详细建议。此评估在 Palo Alto Networks 经验丰富的销售工程师的指导下，可有助于确定应重点关注预防活动的最具风险的区域。您可以在防火墙和 Panorama 上运行 PPA。
- 最佳实践评估 **(BPA)** 工具 — 用于下一代防火墙和 Panorama 的 BPA 可以评估设备配置情况，方式如下：测量功能的使用情况，验证策略是否符合最佳实践，并提供关于如何修复最佳实践检查失败问题的建议和说明。

  安全策略采用热图组件将按设备组、序列号、区域、架构区域和其他类别筛选信息。结果包括趋势数据，显示在采用新功能、修复缺口以及朝向零信任网络发展时的安全性提升速率。

  BPA 组件对防火墙或 Panorama 配置执行超过 200 次的安全检查，并为每次检查提供通过/失败分数。每次检查都是 Palo Alto Networks 安全专家确定的一次最佳实践。如果检查返回失败分数，则此工具将提供给出此分数的理由，以及如何修复该问题。

Palo Alto Networks 将继续开发新工具，并改进现有工具。请联系您的 Palo Alto Networks 代表，了解最新工具可为提高数据中心网络安全做些什么。