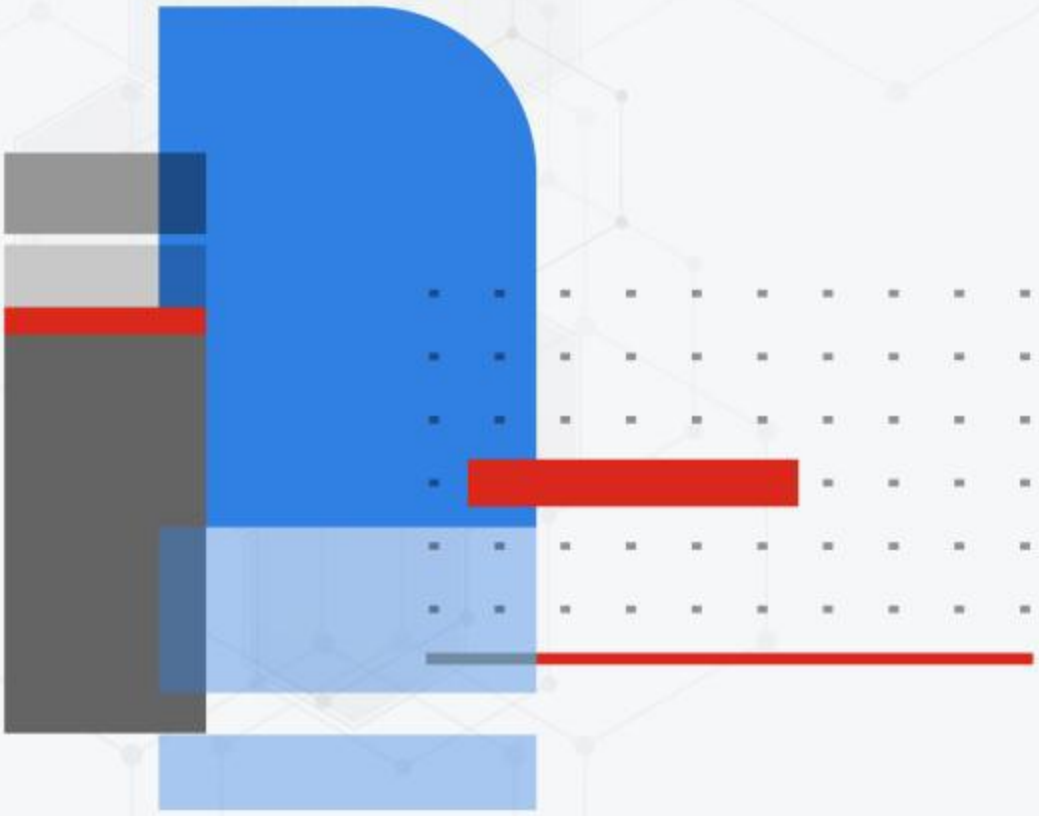
管理指南

FortiProxy 7.4.0



更改日志

日期	变更说明
2023-07-21	初始版本。
2023-08-09	更新了以下主题： 1 第30页的仪表板 1 在第129页创建或编辑策略 1 1
更新了创建或编辑第357页的图像分析个人资料。	
在第475页更新的配置。	
2023-09-01	更新的许可证 在页面上共享 625
更新了以下主题： 1 在第625页上创建或编辑一个 页面上的代理 56 1 显式的web许可证共享	

介绍

FortiProxy提供了一个安全的web网关，通过URL过滤、通过SSL和SSH检查对加密的web流量的可见性和控制，以及粒度web应用程序策略的应用来防止web攻击。灵活的部署模式包括内联、显式和透明的部署。

- 应用程序控制允许您识别和控制网络和端点上的应用程序，而不管使用的端口、协议和IP地址如何。它为您提供了无与伦比的可见性和对应用程序流量的控制，甚至是来自未知应用程序和源的流量。
- SSL和SSH检查允许您确定哪种检查方法将应用于SSH和SSL流量；确定如何处理无效、不受支持或不受信任的SSL证书；并配置哪些网站或网站类别不受SSL检查。
- Web过滤提供了web URL过滤，以阻止访问有害的、不适当的和危险的网站，这些网站可能包含钓鱼/药学攻击，恶意软件，如间谍软件，或可能使您的组织面临的法律责任的不良内容。基于自动研究工具和有针对性的研究分析，实时更新使您能够应用高粒度的策略，过滤基于78个网页内容类别、超过4500万个评级网站和超过20亿个网页的网页访问——所有这些都在不断更新。
- FortiProxy数据泄漏预防（DLP）系统允许您防止敏感数据离开网络。当您定义敏感的数据模式时，匹配这些模式的数据将被阻止或记录，并在通过FortiProxy单元时被允许。您可以通过在DLP传感器中根据文件类型、文件大小、正则表达式、高级规则或复合规则创建单独的过滤器来配置DLP系统，并将该传感器分配给安全策略。虽然DLP特性的主要用途是阻止敏感数据离开网络，但它也可以用于防止不需要的数据进入您的网络，并归档通过FortiProxy单元的部分或全部内容。

FortiProxy单元还提供WAN优化、web缓存和WCCP。FortiProxy WAN优化和web缓存提高了广域网（WAN）位置之间或从互联网到web服务器的流量的性能和安全性。您可以使用FortiProxy单元作为显式的FTP和web代理服务器。此外，您还可以将web缓存添加到任何HTTP会话中，包括WAN优化、显式web代理和其他HTTP会话。

支持的协议

应用层安全性

- SSH
- FTP/FTPS/FTPoHTTP/FTPoHTTP连接
- SMTP/SMTPS
- imap
- 弹出3/弹出3
- CIFS/SMB
- MAPI/MAPIoRPC/MAPIoHTTPS
- DNS

- ICAP/WCCP
- SCP/SFTP

卖主部件编号

- IPsec/SSLVPN

关于此文档

本文档包含以下几部分：

- 第15页上的部署
- 第30页的仪表板
- 第55页上的代理设置
- 第91页的网络
- 在第124页上的策略和对象
- 安全配置文件，请参见第271页
- 内容分析，详见第356页
- 广域网优化图，详见第374页
- 在第383页上的Web缓存
- 第402页的VPN
- 用户和身份验证，详见第428页
- 460页上的系统
- 安全结构，详见第523页
- 第597页的日志和报告
-
-

附录：

- Perl第631页的Perl正则表达式
- 预加载缓存内容，在第633页和web爬虫
- 自动备份到FTP的页面或TFTP服务器
- 在第640页上的自定义签名关键字
-

部署

本节将介绍以下内容：

透明和NAT/路由模式

FortiProxy单元可以在NAT/路由模式或透明模式下运行。

在NAT/路由模式下，FortiProxy单元作为多个网之间，如专用网络和路由器。NAT/路由模式的一个功能是允许FortiProxy使用NAT隐藏专用网络上的IP地址。

FortiProxy在第2层中操作，在路由器、防火墙和交换机等网络设备之间转发流量。例如。它可以在线安装在路由器和交换机之间，以执行安全扫描，而不改变网络拓扑结构或修改IP地址。当您向网络中添加一个处于透明模式的FortiProxy时，它只需要提供一个管理IP地址就可以访问该设备。建议采用专用接口，以透明模式连接到管理网络。透明模式主要用于当需要增加网络保护，但改变网络本身的配置是不切实际的。

更改操作模式将删除大多数配置，包括任何策略和地址对象。要保持配置，请在更改模式之前备份它。

要在GUI中备份您的配置：

1. *单击用户名，并选择“配置>备份”。*
2. 选择存储备份文件、本地PC或USB盘（如果可用）。
3. 可选择启用“加密”并输入密码。
4. 单击确定。

要在CLI中备份您的配置：

```
#执行备份{配置|全配置}{flash|ftp|管理-
      站|sftp|tftp|usb|usb模式}...
```

要从NAT/route模式更改为透明模式：

```
配置系统设置
    设置opmode透明
    设置管理<IP_地址>
    设置网关<网关地址>
最后部分
```

网关设置为可选设置，但操作模式更改后，网关配置为静态路由器设置：

```
配置路由器静态
    编辑<-num>
        设置网关<IP_地址>
    下一个的
最后部分
```

要从透明模式更改为NAT/route模式：

```
配置系统设置
    设置操作模式nat
    设置ip<IP_地址>
    设置设备<接口>
    设置网关<网关地址>
最后部分
```

IP和设备设置是必需的，网关设置是可选的。当操作模式更改后，IP地址配置为接口设置，网关和设备配置为静态路由器设置：

```
配置系统接口
    编辑<接口>
        设置ip<IP_地址>
    下一个的
最后部分
```

```
配置路由器静态
    编辑<-num>
        设置网关<IP_地址>
        设备<接口>
    下一个的
最后部分
```

网络代理

Web代理包括透明代理和显式代理。

本节将涵盖以下主题：

1. Web代理概念
1. 显式web代理概念
1. 透明的web代理概念
1. 显式web代理拓扑
1.

Web代理概念

本节将介绍以下同时适用于透明代理和显式代理的概念：

1. 代理策略
1. 代理身份验证
1. 代理地址
1. Web代理防火墙服务和服务组
1. 学习客户端IP
1.

代理策略

每当启用了使用代理的安全配置文件时，您都需要配置代理选项。安全配置文件中定义的某些检查要求在执行检查时保持代理流量，代理选项定义了将如何处理流量以及将处理流量的级别。以同样的方式，可以有单一类型的多个安全配置文件，也可以有许多唯一的代理选项配置文件，因此，根据策略的需求不同，您也可以为每个单独的策略配置不同的代理选项配置文件，或者可以重复使用一个配置文件。

代理选项支持以下协议：

- l服务程序所用的协议
- l野外终点站平台
- l塞夫斯
- lSSH

每个这些协议的配置都是单独处理的。

代理身份验证

身份验证为基于用户的策略与授权分开。您可以向代理策略添加身份验证，以控制对策略的访问，并识别用户，并对不同的用户应用不同的UTM特性。所描述的身份验证方法适用于显式的web代理和透明的代理。

web代理会话的身份验证使用RFC 2617（HTTP身份验证：基本和摘要访问身份验证）中所述的HTTP基本和摘要身份验证，并提示用户从浏览器获取凭据，允许个人用户通过他们的web浏览器而不是IP地址进行标识。HTTP身份验证允许FortiProxy单元区分从共享IP地址访问服务的多个用户。

身份验证规则表定义了如何标识用户id。它使用了匹配因子：

- l协议
- l源地址

对于一个地址和协议，只有一个身份验证规则。可以为一个地址配置多个身份验证方法。客户端浏览器将从身份验证方法列表中选择一种身份验证方法，但您无法控制浏览器将选择哪种身份验证方法。

代理地址

代理地址同时用于透明的web代理和显式的web代理。

在某些方面，他们可以像FQDN地址，他们指的是一个字母数字字符串分配给一个IP地址，然后他们去额外的粒度通过使用额外的信息和标准进一步指定位置或类型的流量在网站本身。

代理地址组

与IPv4和IPv6地址只能分组一样，代理地址只能与其他代理地址分组。与其他地址组不同，代理地址组被进一步划分为源地址组和目标地址组。

Web代理防火墙服务和服务组

Web代理服务类似于标准的防火墙服务。您可以配置web代理服务，以定义与每个web代理服务关联的一个或多个协议和端口号。Web代理服务也可以分组为Web代理服务组。

web代理服务与防火墙服务不同的一种方式是您可以选择的协议类型。可使用以下协议类型：

- 所有
- 连接/接通
- 野外终点站平台
- 服务程序所用的协议
- 袜子tcp
- 短袜

学习客户端IP

如果在FortiProxy单元和客户端（浏览器）之间有另一个NATing设备，则可以使用此特性来识别真正的客户端，尽管有地址转换。在正在进行授权的情况下，了解实际的客户机是非常必要的。

显式web代理概念

以下是特定于显式代理的信息。web代理通用的任何信息都在第17页的web代理概念中涵盖。

您可以使用FortiProxy显式web代理来在一个或多个FortiProxy接口上启用IPv4和IPv6 HTTP和HTTPS流量的显式代理。显式web代理还支持从web浏览器代理FTP会话和代理自动配置（PAC），以为显式web代理用户提供自动代理配置。从CLI中，您还可以配置显式的web代理，以支持从web浏览器中配置的袜子会话。显式的web和FTP代理可以在同一时间上或在不同的FortiProxy接口上同时操作。

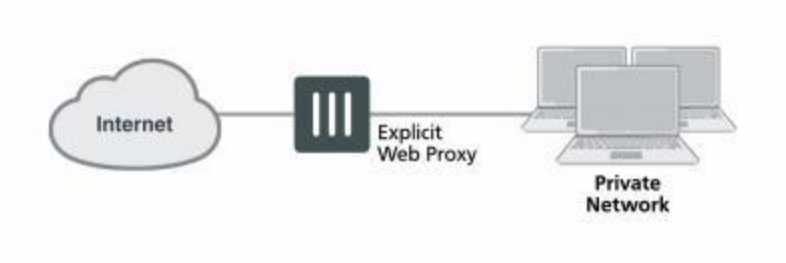
在大多数情况下，通过在连接到该网络的FortiProxy接口上启用显式web代理，您可以为网络上的用户配置显式web代理。网络上的用户将配置他们的web浏览器来使用HTTP和HTTPS、FTP或SOCKS的代理服务器，并将代理服务器的IP地址设置为连接到他们的网络的FortiProxy接口的IP地址。用户还可以将PAC URL输入到他们的web浏览器PAC配置中，以使用存储在FortiProxy单元上的PAC文件自动进行web代理配置。

在一个连接到互联网的接口上启用显式的web代理是一种安全风险，因为任何在互联网上找到该代理的人都可以使用它来隐藏他们的源地址。

如果FortiProxy单元以透明模式运行，用户将将其浏览器配置为使用具有FortiProxy管理IP地址的代理服务器。

web代理接收要在启用显式web代理的forti代理接口上代理的web浏览器会话。web代理使用FortiProxy单元将会话路由到目标接口。在会话离开退出接口之前，显式的web代理会将会话数据包的源地址更改为退出接口的IP地址。当增强代理单元以透明模式运行时，显式的web代理会将源地址更改为管理IP地址。您可以配置显式web代理，以保留原始客户端IP地址。

显式web代理拓扑示例



要允许所有显式web代理流量通过FortiProxy单元，您可以将显式web代理默认防火墙策略操作设置为可接受。但是，在大多数情况下，您可能希望使用安全策略来控制显式的web代理流量，并应用安全功能，如访问控制/身份验证、病毒扫描、web过滤、应用程序控制和流量日志记录。您可以通过将默认的显式web代理安全策略操作保留给DENY，然后添加web代理安全策略来实现这一点。

您还可以将显式的web代理默认安全策略操作更改为接受和添加显式的web代理安全策略。如果这样做，则将根据安全策略设置处理与web代理安全策略相匹配的会话。允许连接到与web代理安全策略不匹配的显式web代理，不需要任何限制或额外的安全处理。注意：不推荐使用此配置，也不是一个最佳实践。

显式的web代理可以接受目标地址的VIP地址。如果外部IP与VIP策略匹配，则IP更改为VIP的映射IP。

Web-proxy策略可以选择性地接受或拒绝流量、应用身份验证、启用流量日志记录以及使用安全配置文件应用病毒扫描、web过滤、IPS、应用程序控制、DLP和SSL/SSH检查到显式的web代理流量。

您不能为显式的web代理流量配置IPsec、SSL VPN或流量整形。Web代理策略只能包括未分配给FortiProxy单元接口或未将接口设置为任何接口的防火墙地址。(在基于web的管理器上，您必须将接口设置为任何接口。在CLI中，您必须取消设置关联的接口。)

显式web代理会话的身份验证使用HTTP身份验证，可以基于用户的源IP地址，也可以基于用户的web浏览器中的Cookie。

要使用显式web代理，必须添加显式web代理所在的FortiProxy接口的IP地址
启用web浏览器的默认8080)代理端口号的代理配置设置。您还可以为显式的web代理会话启用web缓存。

透明的web代理概念

除了显式的web代理之外，FortiProxy单元还支持一个透明的web代理。虽然透明代理没有显式的web代理那么多的特性，但它的优点是不需要在user's系统上做任何操作来将支持的web流量转发给代理。不需要重新配置浏览器或发布PAC文件。所有的东西对最终用户都是透明的，因此得名。这使得将新用户合并到代理部署中变得更容易。

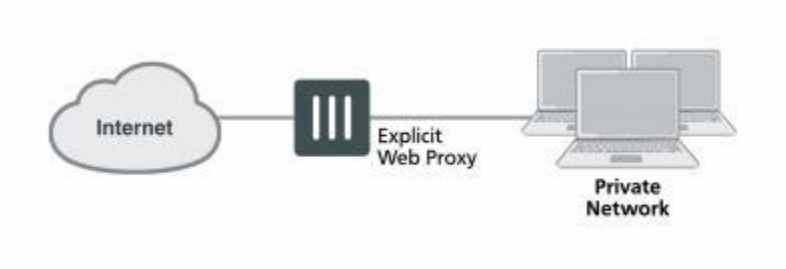
您可以使用透明代理将web身份验证应用于防火墙策略所接受的HTTP流量。

普通的增强代理身份验证是基于ip地址的。用户根据其IP地址进行身份验证，并基于此IP地址允许或拒绝访问。在基于IP地址的身份验证无法工作的网络上，您可以使用透明的web代理来应用基于用户的浏览器而不是基于其IP地址的web身份验证。通过此身份验证方法，即使网络上的多个用户从同一个IP地址连接到FortiProxy单元，您也可以识别单个用户。

显式web代理拓扑

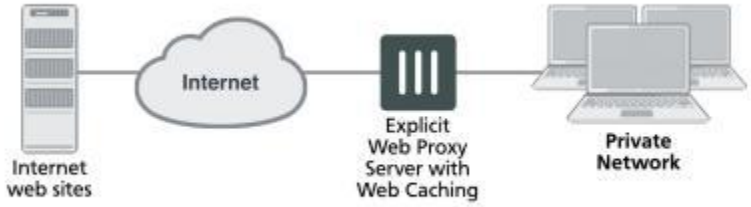
您可以配置一个FortiProxy单元为一个显式的web代理服务器，用于互联网网络浏览IPv4和IPv6网络流量。要使用显式web代理，用户必须将为显式web代理配置的FortiProxy接口的IP地址添加到其web浏览器代理配置中。

显式网络代理拓扑



如果FortiProxy单元支持web缓存，那么您还可以将web缓存添加到接受显式web代理会话的安全策略中。然后，FortiProxy单元将互联网网页缓存在一个硬盘上，以提高网页浏览性能。

具有web缓存拓扑的显式web代理



广域网优化

FortiProxy WAN优化包括许多技术，您可以应用这些技术来提高跨WAN的通信效率。这些技术包括协议优化、字节缓存、web缓存、SSL卸载和安全隧道传输。协议优化可以提高使用CIFS、FTP、HTTP或MAPI协议的流量以及一般TCP流量的效率。字节缓存会在FortiProxy单元上缓存文件和其他数据，以减少通过WAN传输的数据量。Web缓存存储网页o强度代理单元，以减少WAN和Web服务器之间的延迟和延迟。SSL卸载卸载SSL解密和加密从web服务器到FortiProxy SSL加速硬件。安全的隧道隧道保护了它通过广域网时的流量。

根据流量类型，您可以将这些WAN优化技术的不同组合应用到单个流量流中。例如，您可以对任何TCP通信量应用字节缓存和安全隧道传输。对于HTTP和HTTPS流量，您还可以应用协议优化和web缓存。

您可以将FortiProxy单元配置为同时针对IPv4和IPv6流量的显式web代理服务器，以及显式FTP代理服务器。您的内部网络上的用户可以通过显式web代理服务器浏览互联网，也可以通过显式FTP代理服务器连接到FTP服务器。您还可以配置这些代理，以使用反向代理配置来保护对FortiProxy单元后面的web或FTP服务器的访问。

Web缓存可以应用于任何HTTP或HTTPS通信流量，这包括安全策略接受的正常通信流量、显式的Web代理通信流量和WAN优化通信流量。

您还可以配置foroxy单元操作为Web缓存通信协议（WCCP）客户端或服务器。WCCP提供了将web缓存卸载到一个或多个冗余的web缓存服务器的能力。

FortiProxy单元还可以将安全配置文件应用于流量，作为WAN优化、显式web代理、显式FTP代理、web缓存和WCCP配置的一部分。包含任何这些选项的安全策略还可以包括应用FortiProxy单元支持的所有形式的安全配置文件的设置。

要检查为wan优化守护进程（WAD）分配了多少内存，请使用诊断wad内存跟踪[<mem-id>]命令。

WAN优化支持TLS 1.3。

广域网优化透明模式

广域网优化对用户是透明的。这意味着，有了WAN优化，客户端连接到服务器的方式就像不进行WAN优化一样。然而，在WAN优化后接收数据包的服务器会“参见”不同的源地址，这取决于是否选择了透明模式。如果选择了透明模式，WAN优化将保持数据包的原始源地址，因此服务器似乎可以直接接收来自客户端的流量。服务器网络上的路由应配置为将具有客户端源IP地址的通信从服务器端FortiProxy单元路由到服务器，并返回到服务器端FortiProxy单元。

如果没有选择透明模式，某些协议，如CIFS，可能无法按预期运行。在大多数情况下，对于CIFS WAN优化，您应该选择透明模式，并确保服务器网络可以按照所述路由流量以支持透明模式。

如果未选择透明模式，则服务器接收到的数据包的源地址将被更改为发送给服务器的数据包的服务器端增强代理单元接口的地址。因此，服务器似乎会接收来自服务器端增强代理单元的数据包。在这种情况下，服务器网络上的路由更简单，因为不涉及客户端地址。所有的流量似乎都来自服务器端FortiProxy单元，而不是来自单个客户端。

不要混淆广域网优化透明模式和增强代理透明模式。广域网优化透明模式类似于源NAT。增强代理透明模式是一种控制增强代理单元如何处理流量的系统设置。请参见第15页上的透明模式和NAT/路由模式。

WAN优化拓扑

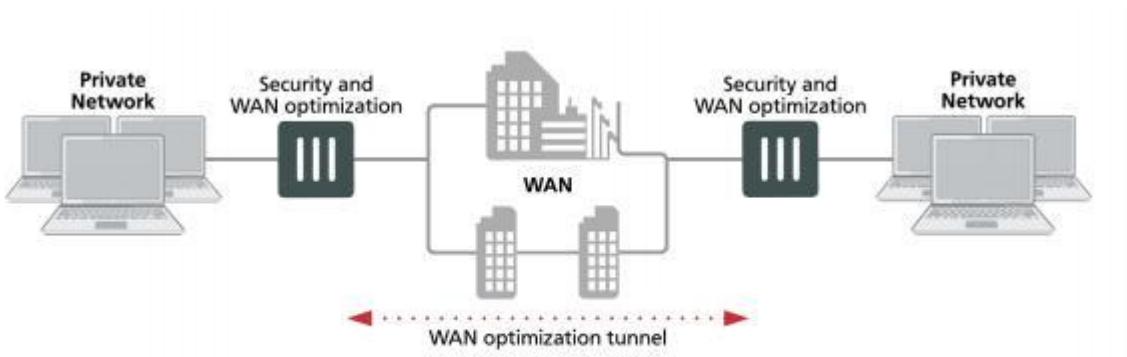
WAN优化拓扑将在以下章节中进行描述：

1. 基本WAN优化拓扑
1. 超路径广域网优化拓扑
1. 多个网络的拓扑结构
1. 广域网优化与web缓存
1.

基本WAN优化拓扑

基本的FortiProxy WAN优化拓扑由两个FortiProxy单元组成，它们作为WAN优化对等点运行，拦截和优化在专用网络之间跨越WAN的流量。

安全设备和广域网优化拓扑结构



FortiProxy单元可以部署为安全设备，以保护连接到广域网的专用网络，并执行广域网优化。在此配置中，FortiProxy单元被配置为专用网络的典型安全设备，并且也被配置为WAN优化。广域网优化配置在通过FortiProxy单元时拦截要进行优化的流量，并使用具有另一个FortiProxy单元的广域网优化隧道来优化穿过广域网的流量。

您还可以在只执行WAN优化的单一用途FortiProxy单元上部署WAN优化。在下面所示的路径广域网优化拓扑中，增强代理单元位于专用网络之外的广域网上。您还可以在专用网络上的安全设备后面安装WAN优化增强代理单元。

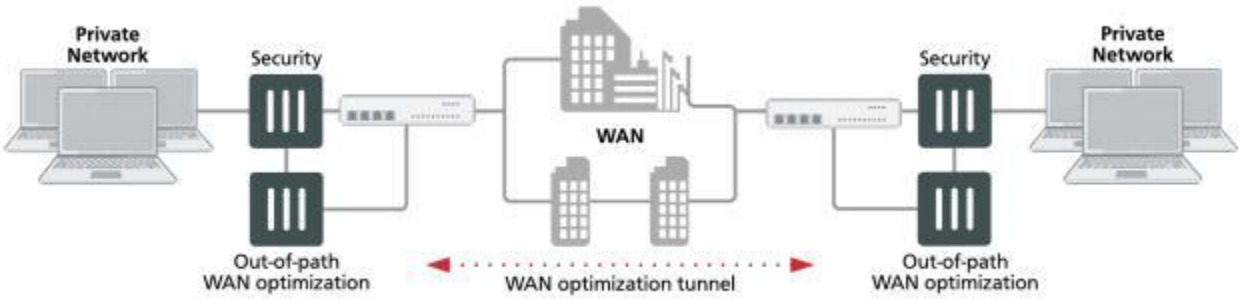
广域网优化配置对于作为安全设备部署的增强代理单元和对于单用途广域网优化增强代理单元的广域网优化配置是相同的。唯一的差异将来自于不同的网络拓扑结构。

超路径广域网优化拓扑

在路径外拓扑中，为WAN优化配置的一个或两个FortiProxy单元并不直接在主数据路径中。相反，超出路径的FortiProxy单元连接到数据路径上的设备，并且该设备被配置为重定向会话以优化到超出路径的FortiProxy单元。

以下非路径的增强代理单元配置为广域网优化，并直接连接到数据路径中的增强代理单元。数据路径中的FortiProxy单元使用策略路由等方法将流量重定向到优化到路径外的FortiProxy单元。路径外的强度代理单元在彼此之间建立一个广域网优化隧道，并优化重定向的流量。

非路径WAN优化



非路径的广域网优化的好处之一是，路径外代理单元只执行广域网优化，而不需要处理其他流量。配置为广域网优化的路径内增强代理单元还必须处理数据路径上的其他未优化的流量。

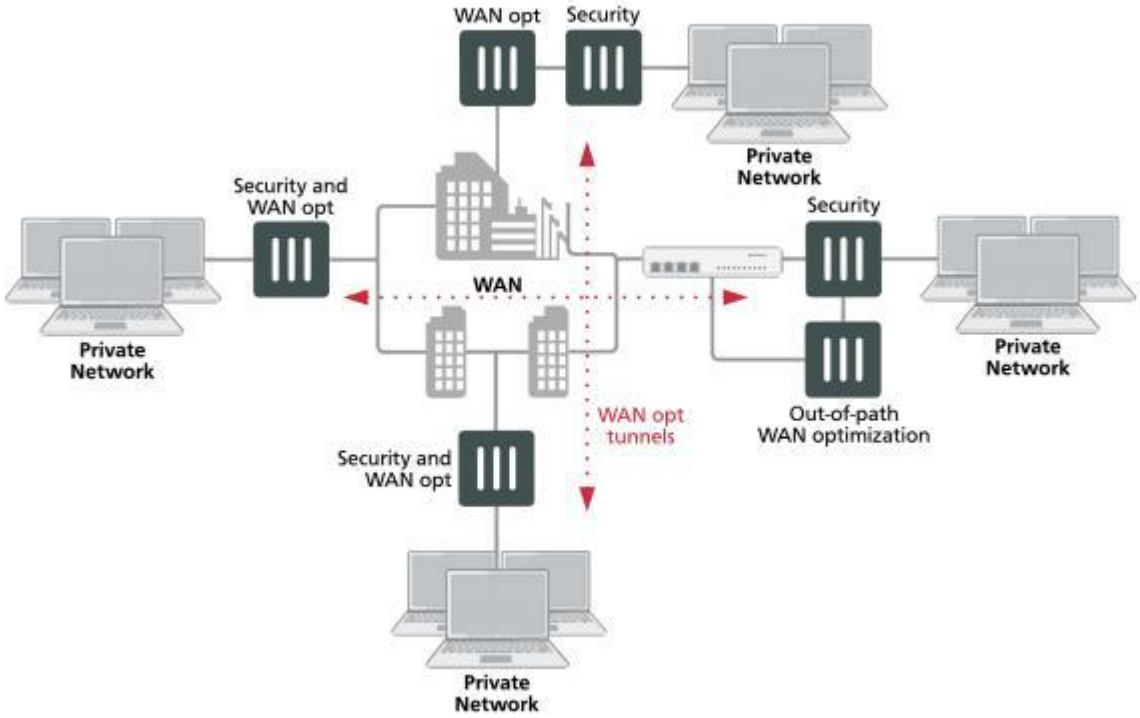
偏离路径的FortiProxy单元可以在NAT/路由或透明模式下运行。

其他的非路径拓扑也是可能的。例如，您可以在专用网络上WAN上安装路径增强单元，而不是。此外，路径外的增强代理单元可以有一个连接到网络，而不是两个。在这样的单臂配置中，必须配置安全策略和路由，以将WAN优化隧道发送出与接收流量的接口相同的接口。

多个网络的拓扑结构

如下图所示，您可以在多个专用网络之间创建多个广域网优化配置。每当广域网优化发生时，它总是在两个增强代理单元之间，但是您可以配置任何增强代理单元，以执行与作为广域网一部分的任何其他增强代理单元之间的广域网优化。

在多个网络之间的广域网优化



您还可以在广域网上具有不同角色的FortiProxy单元之间配置WAN优化。配置为安全设备和广域网优化的FortiProxy单元可以执行广域网优化，就像它们是仅为广域网优化配置的单用途的广域网优化一样。

广域网优化与web缓存

当专用网络上的用户与位于另一个专用网络上的跨WAN上的web服务器进行通信时，您可以将web缓存添加到WAN优化拓扑中。