

FortiOS V.3.0 MR7
SSL VPN 用户使用手册

FORTINET

www.fortinet.com

介绍

本章向您介绍有关FortiGate设备的SSL(SSL: Secure Sockets Layer)安全层套接VPN技术以及有关Fortinet公开技术说明的补充信息.

本章包括一下内容:

- 有关FortiGate SSL VPN
- 有关该手册
- FortiGate设备技术手册
- 相关文档
- 客户服务与技术支持

有关FortiGate SSL VPN

FortiGate SSL VPN技术使通过互联网进行的业务更为安全。除了加密并保证从web浏览器发送到web服务器的信息安全，FortiGate SSL VPN也可以加密大多数基于互联网的流量。

FortiGate设备内嵌的SSL VPN功能能够保证soho、中型以及大型公司与服务提供商通过互联网传输数据的机密性与完整性。FortiGate设备同样提供加强的验证与对公司网络资源与服务的限制级访问。

SSL VPN有两种操作模式，只能够应用于NAT/路由模式，分别为：

- web-only模式，只能应用于安装web浏览器的瘦远程用户。
- 通道模式，应用于运行各种用户与服务器应用程序的远程计算机设备。

FortiGate设备提供的SSL VPN应用于web-only模式时，远程用户端与FortiGate设备之间通过FortiGate设备的SSL VPN安全功能与远程用户端基于web浏览器的SSL安全功能建立连接。连接建立后，FortiGate设备可以提供通过一个web入口网站，访问所选择的服务与网络资源。

具有对计算机设备完全的管理权限并使用各种应用程序的用户，应用于通道模式的SSL VPN允许远程用户如同直接连接网络般访问本地内部网络。通道模式下，安全SSL连接由FortiGate设备首先发起，并下载SSL VPN用户端软件（ActiveX 插件）到web浏览器。用户安装SSL VPN用户软件后，便可以在SSL连接开放的任何时候与FortiGate设备建立VPN通道。

使用SSL VPN功能时，所有的用户流量都被加密并发送到SSL VPN，包括发送到私网的流量与常规情况下非加密发送的互联网流量。通道分割可以保证该到达私网的流量被发送到SSL VPN网关。互联网流量是通过常规的非加密路由被发送的。这样既保存了带宽也减少了流量瓶颈。通道分割功能默认情况下没有启动。

根据远程计算机设备中安装的应用程序数量以及类型判断使用SSL VPN的模式，只应用于web或通道模式。 任何web模式不支持的对应用的访问，通道模式下均可以实现。有关这些模式操作的详细信息，参见配置FortiGate设备SSL VPN。

关于本手册

本手册就如何使用基于web管理器配置SSL VPN操作进行了说明，包括以下的章节：

- 配置FortiGate SSL VPN功能；描述两种操作模式，建议拓扑结构部署并提供相连接的附属架构信息。有关配置每种模式涉及的高级别的步骤均配合以详细操作说明。本章同时运行支持两种模式所需的基本管理任务进行了说明并有针对每种模式的逐步说明。
- 配置使用web入口；有关web入口的应用以及如何配置使用。 本章节同时也对如何安装ActiveX插件以及通道模式启动后发起VPN通道进行了说明.

注释

以下是本手册中的注释说明：

- 举例说明中，私有IP地址用于私有与公共IP地址。

- 注意与警告标识中的提示较为重要的信息。

  注意：突出□示附件□明□

  警告：□于可能造成意外的不良的□果包括数据丢失或者设备损害等命令或程序发出警告提示。

排版说明

排版□ 明	□ 例
菜□ 命令	□ 入 VPN>IPSEC>□ 段1 并点□ "新建".
□ □ □ 入	在网□ 名称字段□ □ 入□ 程VPN或用□ （例如，Central_office_1）
代□ 范例	Config sys global Set ips-open enable end
CLI命令句法	Config firewall policy edit id_integer set http_retry_count <retry_interer> set natip <address_ipv4mask> end
文档名称	*FortiGate□ □ 管理□ 使用手册*
源文件内容	<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD> <BODY><H4>You must authenticate to use this service.</H4>
程序□ 出	Welcome！
□ 量	<address_ipv4>

FortiGate技术文档

您可以登录Fortinet技术文档网站http://doc.forticare.com，获得最新发布的Fortinet技术文档。

公开以下Fortinet产品技术手册：

FortiGate设备快速启动指南
有关连接与安装Fortinet设备的信息。

FortiGate设备安装手册
如何安装FortiGate设备的描述。包括硬件信息，默认配置信息，安装操作，连接操作以及基本的配置操作。根据产品号选择不同的安装手册。

FortiGate设备管理员使用手册
有关如何配置FortiGate设备的基本信息，包括如何定义FortiGate病毒防护与防火墙策略；

如何应用入侵保护，病毒防护，网页内容过滤以及垃圾邮件过滤以及如何配置 VPN。

FortiGate 设备在线帮助

在线帮助是对 FortiGate 管理员手册的 HTML 格式上下文有关的检索与查询。您可以通过基于 web 的管理其访问在线帮助。

FortiGate 设备 CLI 使用参考手册

有关如何使用 FortiGate CLI（命令行接口）以及所以 FortiGateCLI 命令。

日志信息参考手册

只有在 Fortinet Knowledge Center （Fortinet 知识库）可以获得，FortiGate 日志信息参考对 FortiGate 日志信息的结构与 FortiGate 设备所生成的日志信息有关内容做了描述。

FortiGate 设备 HA 用户指南

深入介绍了 FortiGate 高可用性的性能与 FortiGate 群集协议的信息。

FortiGate 设备配置 IPS 用户指南

对如何配置 FortiGate 入侵检测系统与 FortiGate IPS 是如何处理一些一般的入侵作了描述。

FortiGate 设备配置 IPSec VPN 用户指南

对使用基于 web 的管理器如何配置 IPSec VPN 进行了逐步详细的说明。

FortiGate 设备 SSL VPN 用户指南

对 FortiGate IPSec VPN 与 FortiGate SSL VPN 技术进行比较，并对通过基于 web 的管理器，远程用户怎样配置只适用于网络模式与通道模式 SSL VPN 访问做了描述。

FortiGate 设备配置 PPTP VPN 用户指南

使用基于 web 的管理器如何配置 PPTP VPN。

证书管理用户指南

管理电子证书的程序包括生成电子证书的请求，安装签发的证书，引入

CA 根权威证书与证书撤销名单，以及备份与存储安装的证书信息与私人密钥。

FortiGate 设备配置 VLAN 与 VDOM 用户指南
在 NAT/路由与透明模式下如何配置 VLAN 与 VDOM。

Fortinet知识库

其它有关 Fortinet 技术手册信息都可以从 Fortinet 公司网站（www.fortinet.com）中的知识库板块获得。知识库涵盖涉及 Fortinet 产品故障排除与解释说明性的文章、FAQ 以及技术说明等。

Fortinet 技术文档的建议与意见
如果您在本文档或任何 Fortinet 公司的技术文档中发现错误或疏漏之处，欢迎您将有关信息发送到 techdoc@fortinet.com 。

客户服务与技术支持

Fortinet 公司技术支持将确保您的 Fortinet 系统在您的网络中能够快速启动，轻松配置并能够可靠运行。

敬请访问 Fortinet 技术支持网站 http://support.fortinet.com 获知更多 Fortinet 所提供的技术支持服务。

配置FortiGate SSL VPN

本章的内容有关SSL与IPSec VPN技术比较，以及SSL VPN运行的两种模式说明。针对每种模式的配置涉及的高级操作辅助以详细步骤与过程说明。

本章包括以下内容：

- SSL与IPSec VPN技术比较
- SSL VPN操作模式
- 拓扑结构
- 配置概述
- 配置SSL VPN设置
- 配置用户帐户与SSL VPN用户组
- 配置防火墙策略
- 配置SSL VPN事件日志
- 监控活动的SSL VPN会话
- 配置SSL VPN书签与书签组
- SSL VPN主机OS路径查看
- 设置允许对SSL VPN通道用户组的唯一访问允许
- SSL VPN虚拟接口（ssl.root）
- SSL VPN丢弃连接

SSL与IPSec VPN技术比较

对于同时支持SSL和IPSec VPN技术的设备。这两项技术均可以将加密与VPN网关功能结合建立通过互联网的私有通信通道，从而减少物理网络的成本。同时，这两项技术使您通过单个管理工具定义并部署网络访问与防火墙策略。 另外，它们还支持单个客户端/用户验证程序（包括可选项X509安全证书）。根据您的网络部署自由的选择使用这两项技术。

一般情况下，IPSec VPN对于site－to－site的连接，使用基于装置的防火墙提供网

络防护， 以及经公司批准的用户计算机设备分配到用户使用，这样的情况下使用 IPSec VPN 是不错的选择。 SSL VPN 适用于依靠大范围瘦客户端计算机设备的分散用户从远程访问公司应用和/或资源的情况下使用。

SSL VPN 与 IPSec VPN 通道也可以同时使用。

遗留程序与web启用的程序

IPSec 更适用于基于网络的遗留程序，而不是基于 web 的遗留。作为第三层网络技术，IPSec 在两个主机设备之间建立一个安全通道。IP 数据包被 VPN 用户端封装且运行于主机的服务器软件。SSL 典型的应用于安全的 web 业务，以利用通过 web 启动的 IP 应用的优势。web 浏览器与 web 服务器之间建立一个安全的 HTTP 链接后，应用数据通过通道在被选中的用户端与服务器应用之间直接传输。

验证差别

IPSec 是比较稳定的技术，各项功能使用与实现很成熟，能够支持许多遗留程序，例如 smart card 与 biometric.

SSL 支持登录 web 服务器的前端机，登录后可以访问很多不同企业的应用。Fortinet 公司提供的实施使您可以对 web 服务器分配具体的端口并定制登录页面。

连接性

IPSec 支持到同一个 VPN 通道的多个连接，多个远程 VPN 设备作为同一网络的一部分生效。

SSL 在两个终端形成连接，例如一个远程用户端与企业网络之间。 不支持涉及三方或多方的业务，因为流量只在用户端与服务器应用之间传输。

使用便捷性

虽然管理 IPSec VPN 相对简单，但是对于 SSL VPN 在配置方面更简单。IPSec 协议可能被一些公司，饭店以及其他公共场所屏蔽或限制使用，但 SSL 协议通常不会被限制。

用户端软件要求

在所有的IPSecVPN对等必须安装专门的IPSec VPN软件，且用户端与软件必须配置相兼容的设置。

使用SSL VPN访问服务器端的应用，远程用户必须安装有web浏览器（Internet Explore，Netscape或Mozilla、Firefox），且如果使用了Telnet/RDP，需在Sun Java运行的环境。通道模式下的用户端计算机设备也必须安装ActiveX（IE）或启动Java平台（Mozilla/Firefox）。

访问控制

IPSec VPN只提供安全的网络访问。当访问一个公司的网络资源，可以对具体的IPSec对等和/或用户端启动IPSec VPN。许多应用用户的安全选项被限制。

SSL VPN提供到某些应用的安全访问。web-only模式提供远程用户通过装备了web浏览器的瘦用户端计算机访问服务器程序。通道模式的SSL VPN提供远程用户从笔记本电脑、机场候机亭、Internet吧以及饭店连接到内部网络的功能。通过用户组访问SSL VPN应用是被控制的。

会话续接支持

FortiGate设备HA群集中启动会话续接功能，IPSec VPN通道支持会话续接功能。HA故障恢复后，IPSec VPN通道会话将在不丢失数据的情况下继续。

SSL VPN通道不支持会话续接功能，但是支持SSL VPN用户端与FortiGate设备之间的通信的cookie恢复。也就是说，故障恢复后，SSL VPN用户端可以在不需要验证的情况下重新建立SSL VPN对话。但是，所有SSL VPN通道内的是FortiGate设备之后的所有会话将停止，不得不重新启动。

SSL VPN的操作模式

当远程用户端连接到FortiGate设备，FortiGate设备基于用户名、密码验证用户以及验证域。登录是否成功决定远程用户访问的权力。用户组设置设定是否连接将应用于web－only的模式或通道模式。

您可以启动用户端完整性检查，扫描远程用户端校验被允许访问之前，用户端计算机设备的安全性。用户端计算机设备中记录的安全属性（例如，在windows注册列表中，具体的文件中、或由于运行程序保存在内存中的）将被检测并上传到FortiGate设备。
您可以启动缓存清除程序删除任何敏感数据，否则在会话结束后仍然保留在远程计算机上。例如，所有的缓存条目、浏览器历史记录、cookies、有关用户验证的加密信息与会话从远程计算机删除过程中产生的任何暂时性数据。如果用户的浏览器上不能安装并运行缓存清除程序，用户将不被允许访问ssl－vpn入口。

Web-only模式

Web-only的模式对远程用户从任何装备了web浏览器的瘦用户计算机设备访问服务器应用程序提供快速且高效的方法。web-only模式使用具有内嵌ssl加密与sun Java运行环境的web浏览器提供真正的不记名用户的网络访问。

FortiOS操作系统中支持SSL VPN web-only的模式。该功能包括SSL 后台程序运行于FortiGate设备且，提供用户访问访问网络服务以及资源一个web入口，访问方式包括HTTP/HTTPS，Telnet，FTP，SMB/CIFS，VNC，RDP与SSH。

web－only的模式中，FortiGate设备作为一个安全HTTP/HTTPS网关，验证作为用户组成员之一的远程用户。验证成功后，FortiGate设备重新定向web浏览器倒web入口首页，且用户可以访问FortiGate设备之后的服务器应用程序。

配置FortiGate设备包括在用户组中设置只适用于web的模式并通过SSL VPN配置设置启动该功能。用户组设置可以配置被访问的服务器应用。SSL加密用于确保流量的机密性。

配置只适用于web模式的用户要求

远程用户计算机设备中必须安装以下软件：

- 微软Windows 2000/xp/2003/vista,Linux,MacOS X, UNIX操作系统。
- 微软Internet Explorer 6.0（或以上版本）、Netscape Navigator 7.0 或以上版本）、Mozilla Foundation/Firefox（或以上版本）、或Apple Safari1.3 （或以上版本）。
- 如果使用Telnet/或RDP，Sun Java运行环境1.4 （或以上版本），具有Java applet访问、JavaScript访问，并启动cookie接受。

注意：web 浏览器提供不同的 ssl 安全功能。如果要求支持旧的浏览器，FortiGate 设备提供使用 CLI 配置 ssl v2 的选项。另外，FortiGate 设备支持加密套件用于与各种 web 浏览器协商 SSL 通信。web 浏览器必须至少支持 64bit 加密长度。

通道模式

通道模式提供远程用户从笔记本电脑、机场候机室、饭店商务中心与 Internet 吧这样的传统的基于 web 的方式自由的连接到内部网络。如果您的用户团体对用户端计算机设备上的应用程序的使用不尽相同，您可以对任何远程用户通过起 web 浏览器访问部署一个专门的 ssl vpn 用户。ssl vpn 加密从远程用户计算机设备发出的全部流量并将其通过 ssl vpn 通道以基于 web 浏览器与 FortiGate 设备之间的 HTTPS 链接发送到 FortiGate 设备。同时可用的还有分割通道功能，能够保证只到私网的流量能够发送到 ssl vpn 网关。互联网流量通过常规的非加密路由发送。这样既节约了带宽又减少了带宽瓶颈发生的几率。

通道模式下，远程用户连接到 FortiGate 设备且 web 入口登录页面使用微软 IE、Mozilla Foundation/Firefox、MacOS 或 Linux。FortiGate 设备作为一个安全 HTTPS/HTTP 网关，验证作为用户组成员的远程用户。验证成功后，FortiGate 设备重新定向 web 浏览器到 web 入口首页。用户可以下载 ssl vpn 用户端程序（ActiveX 或 Java 插件）并使用 web 入口页面提供的操作指示安装该程序。

当用户通过 ssl 用户端发起到 FortiGate 设备的 VPN 连接时，FortiGate 设备建立与用户端的通道并从一个保留的地址范围内分配用户端一个虚拟 IP 地址。用户端使用分配的 IP 地址作为连接过程中自身的源地址。通道建立后，用户可以访问 FortiGate 设备之后的网络。配置 FortiGate 设备建立与远程用户端的通道包括在用户组设置中选择通道模式访问并通过 ssl vpn 配置设置启动该功能。FortiGate 设备中的防火墙策略与保护内容表保证向内的流量能够显示并被安全处理。

配置通道模式用户端的要求

远程计算机设备必须安装以下软件：

- 微软 windows2000/XP/2003 或 vista（32 或 64bit）、Macos X

v10.3.9，v10.4“Tiger”、v10.5“leopard”或Linux Distributions RedHat/Fedora，Ubuntu/Debian或Suse.

- 微软IE6.0 （或以上版本），启动了Active X，或启动了Java平台的Mozilla Foundation/Firefox （1.5或该版本以上）。

注：浏览器只是在用户通过WINDOWS浏览器界面建立通道式SSL VPN时使用，使用标准的SSL VPN客户端软件时不需要浏览器。

安装SSL VPN客户端软件时需要有管理员的权限。

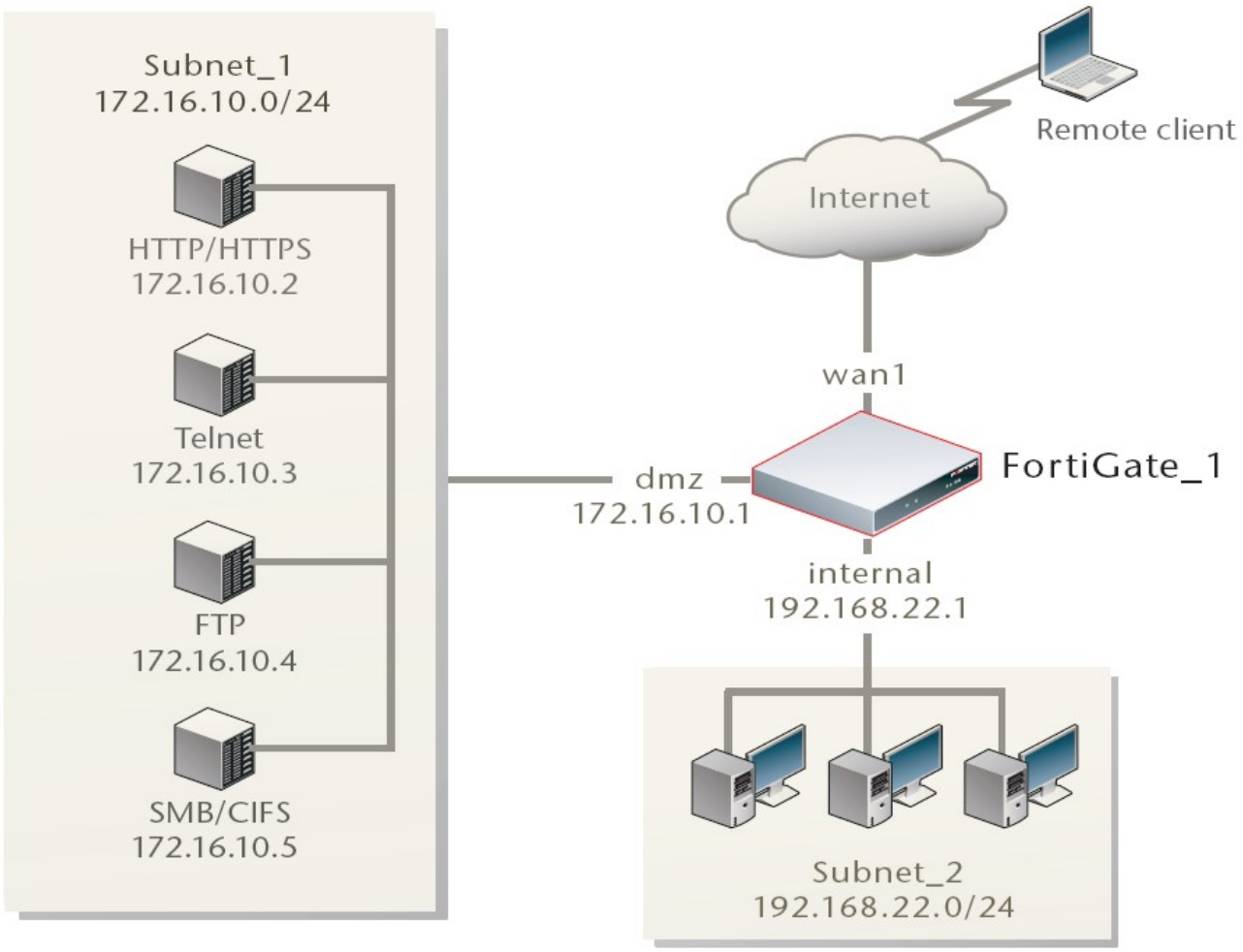
拓扑结构

多数常规的互联网实例应用中，远程用户连接到提供动态IP地址的ISP。ISP将数据包从远程用户端转发到互联网，互联网中这些数据包将被路由到FortiGate设备的公共接口。

FortiGate设备中，您配置用户组以及防火墙策略定义远程用户能够访问的FortiGate设备之后的服务器程序与IP地址范围或网络。

举例说明，图1所示FortiGate网关（FortiGate_1）连接到两个私网，Subnet_1与subnet_2.

图1：SSL VPN配置



提供远程用户从互联网访问 subnet_1 中所有的服务器，您需要配置 FortiGate_1：

- 创建 SSL VPN 用户组并设置将远程用户包括在用户组内。当您创建用户组时，您也可以设定用户是否可以访问 web-only 模式或通道模式的 web 入口。
- 对于通道模式下的用户，定义 FortiGate 设备连接到远程用户时的虚拟 IP 地址。
- 创建防火墙目标 IP 地址为 172.16.10.0/24。
- 创建防火墙策略允许 ssl vpn 用户组成员通过 VPN 连接到 subnet_1.

如果用户团体需要访问 subnet_2，您可以创建第二个防火墙目标 IP 地址 192.168.22.0/24 并创建第二项防火墙策略将相关的远程用户捆绑到 subnet_2 目标地址。

架构要求

- FortiGate 设备必须运行于 NAT/路由模式且具有静态公共 IP 地址。
- ISP 在连接到 FortiGate 设备之前分配 IP 地址到远程用户端。
- 如果远程用户端要求只应用 web 模式的访问，参见上文有关“web-only 模式的用户要

求”。

- 如果远程用户端要求通道模式的访问，参见上文有关“通道模式的用户要求”。

配置概述

开始配置之前，选择在内部网络安装HTTP/HTTPS，telnet，ssh，ftp，smb/cifs，vnc和/或RDP服务器应用程序。作为可选项，这些服务可以通过互联网被远程访问。所有的服务必须运行。用户必须具有单独的用户帐户访问服务器（这些用户帐户与FortiGate用户帐户或FortiGate用户组无关）。

配置FortiGate SSL VPN拓扑，您应该按照以下这些常规步骤进行：

1. 启动SSL VPN连接并设置需要支持ssl vpn配置的基本选项。
2. 如果使用x.509安全证书用于验证，需要下载签发的服务器证书、CA根证书以及证书撤消列表到FortiGate设备，以及个人/用户证书到远程用户端。
3. 对每个远程用户创建一个FortiGate用户帐户并分配用户到ssl vpn类型的用户组。
4. 配置防火墙策略以及其余支持所要求操作模式的参数：
   - 对于web-only的操作模式，参见“配置只适用于web模式的防火墙策略”。
   - 对于通道操作模式，参见“配置通道模式防火墙策略”。
5. 定义ssl vpn事件日志参数。
6. 您也可以监控激活的ssl vpn会话。

配置ssl vpn设置

您可以通过任何运行web浏览器程序的计算机设备通过HTTP（HTTPS）连接配置并管理FortiGate设备。有关如何连接到基于web的管理器信息，参见FortiGate设备安装手册中的“连接到基于web的管理器”章节。

注意：作为另一种选择，您可以适用串口线之间将管理计算机设备连接到Fortigate设备的命令行接口，配置FortiGate设备。从基于web的管理器的管理页面也可以访问CLI。详细信息，参见FortiGate设备CLI使用参考手册中的“连接到FortiGate设备控制台”章节。

参见“FortiGate 设备安装手册”与“FortiGate 设备管理与使用手册”中有关更改密码以及配置 FortiGate 设备接口，与配置基本的操作参数，包括默认网关的内容。

一些对于所有的操作模式都相同的基本管理任务，无论您设置怎样的连接模式，都必须首先被配置。

在“VPN>ssl>配置”页面中包含基本的 ssl vpn 设置，其中包括闲置时间设置以及与各种 web 浏览器相兼容的 ssl 加密方式。您也可以通过 x.509 安全证书启动验证。

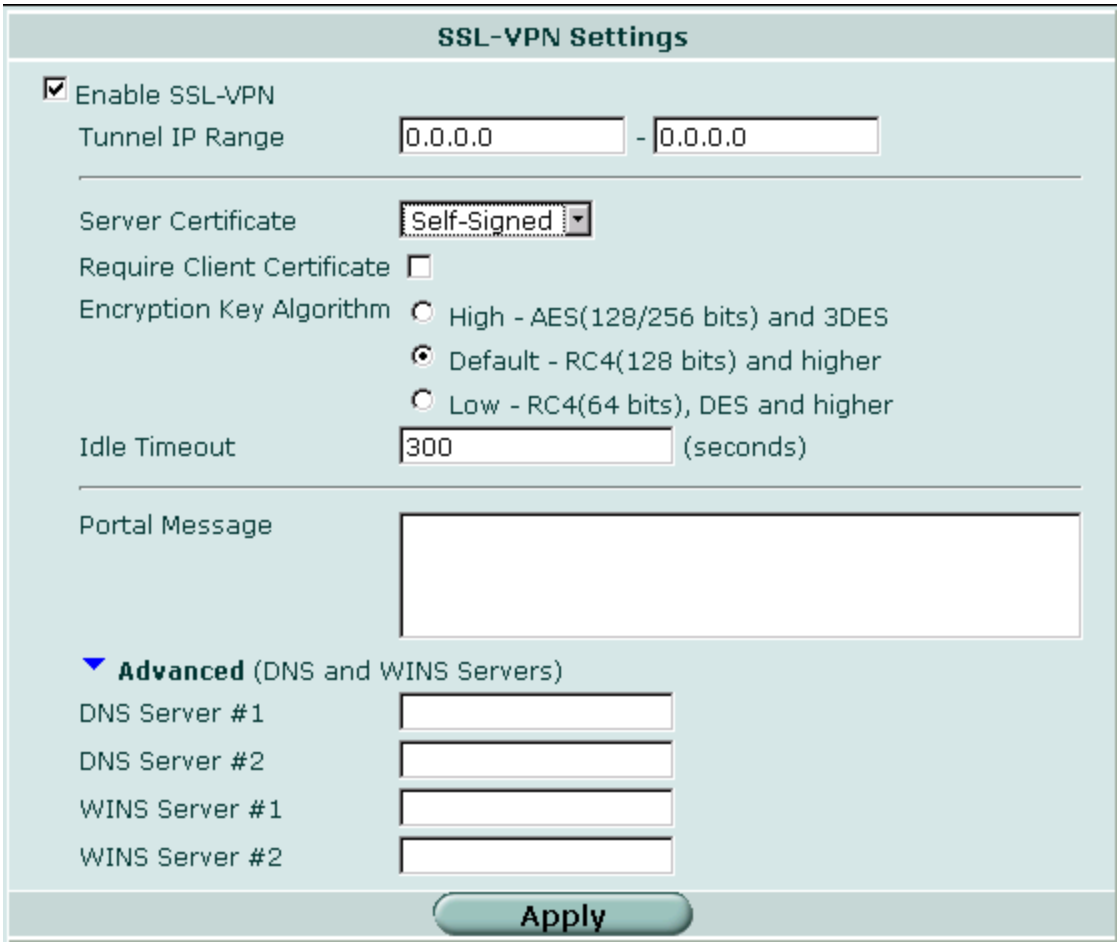
在“VPN>ssl>配置”页面除了配置以上所述设置，您也可以选择修改以下系统设置：

- FortiGate 设备在远程用户端完成验证以及用户成功登录后重新定向 web 浏览器到 web 入口首页。作为一个选项，您可以在对用户组的所有成员弹出的 windows 窗口显示第二个 HTML 页面。详细信息，参见“重新定义用户组到弹出的 window 窗口”。
- 您可以通过替换信息定义 web 入口登录页面的外观。详细信息，参见下文“定义 web 入口登录页面”章节中的信息。

启动ssl vpn连接并编辑ssl vpn设置

进入“VPN>ssl>配置”，启动 ssl vpn 连接并配置或编辑 ssl vpn 设置。FortiGate 设备在没有 ssl vpn 的情况下不接受只应用于 web 模式或通道模式的连接。

图 2：编辑 ssl vpn 设置



启动 SSL VPN	启动 SSL VPN 连接。
通道 IP 范围	设定为通道模式 SSL VPN 用户的 IP 地址范围。在起始与结束字段输入 IP 地址以定义保留 IP 地址范围。
服务器证书	点击设定用于验证使用的签订的服务器证书。如果您保持默认的设置（自签），FortiGate 设备将发送出厂默认的自签证书到连接的远程用户。
要求客户端认证	如果需要使用用户组证书验证远程用户，启动该选项。然后，当远程用户发起连接时，FortiGate 设备切换到用户端的证书作为验证处理的一部份。
加密密钥算法	选择在远程 web 浏览器用户与 FortiGate 设备之间创建安全 SSL 连接的算法。
密钥长度 >=128bit（缺省）	如果远程用户端的 web 浏览器能够匹配 128 位密钥或大于密码套件时，选择该选项。
密钥长度 >128bit（高）	如果远程用户端的 web 浏览器与高级的 SSL 加密相匹配，选择该选项启动密码套件，密码套件即使用多余 128 位密码加密数据。
密钥长度	如果您还不确认远程用户 web 浏览器支持哪个级别的 SSL 加密，

>=64bit（低）	选择该选项启动64位加密或大于64位的密码套件。
闲置超时	在系统要求用户重新登录之前设置保持连接的时间短。设置范围为10到28800秒。该设置应用于SSLVPN会话。在web应用会话或通道处于活动状态时，不会出现闲置超时。
门户信息	如果您想在web门户网站主页顶端显示用户信息，在该栏中键入信息。
高级（DNS与WINS服务器）	
DNS服务器#1	输入提供给用户使用的最多两台DNS服务器。
DNS服务器#2	
WINS服务器#1	输入提供给用户使用的最多两台WINS服务器。
WINS服务器#2	

完成设置后，点击“应用”。

注意：通道IP范围字段只用于配置通道模式访问。如果您配置了只适用于web模式的操作，保留通道IP地址为0.0.0.0.。如果您配置使用通道模式，参见“对通道模式用户设定IP地址范围”。有关通过服务器证书启动基于证书验证于要求用户证书选项的信息，参见FortiGate设备证书管理用户使用手册。

对web入口连接设置端口号

您可以对通过HTTPS链接访问web入口登录页面的用户设定不同的TCP端口号。默认情况下，端口号是10443且用户使用以下默认的url可以访问web入口登录页面：

https：//<Fortigate_ip_address>:10443/remote

<Fortigate_ip_address>是FortiGate设备从远程用户接受连接的接口的IP地址。

注意：请勿选择端口号443作为用户访问web入口登录页面的端口。端口号443保留用于基于web管理器到FortiGate设备的管理连接。

1. 进入“系统>管理>设置”。
2. 在ssl vpn登录端口字段，输入尚未被使用的端口号。
3. 点击“应用”。

对通道模式用户设定IP地址范围

“VPN>ssl>配置”页面中的通道 IP 范围字段可以设定对远程 ssl vpn 用户保留的 IP 地址范围。FortiGate 设备验证通道模式连接的请求，ssl vpn 用户连接到 FortiGate 设备并从该范围中分配得到使用的 IP 地址。之后，FortiGate 设备使用被分配的地址与 ssl vpn 用户通信。

警告：注意避免 IP 地址重叠。不要分配那些已经在私网中被使用的 IP 地址。作为一项防范方法，尽量分配那些不常被使用的地址，例如 10.254.254.0/24。

设置对通道模式用户保留的 IP 地址范围

1. 进入“VPN>ssl>配置”。
2. 在通道 IP 范围字段，输入起始与结束 IP 地址，例如：10.254.254.80 至 10.254.254.100。
3. 点击“应用”。

启动通过安装证书的加强验证

Fortigate 设备支持通过 x.509 安全证书（版本 1 或 3）的加强（双保证）验证。在“VPN>ssl>配置”页面通过设置服务器证书与要求用户证书选项可以对 ssl vpn 用户组配置加强验证。但是，您必须首先保证已安装了所要求的证书。

有关产生证书请求、安装签发的证书、导入 CA 根证书与证书撤消列表以及备份和/或恢复安装的证书以及私有密钥，参见 FortiGate 设备证书管理用户使用手册。

对ssl协商设定加密套件

FortiGate 设备支持的加密套件范围很广，能够与各种 web 浏览器的性能匹配。web 浏览器与 FortiGate 设备在经 ssl 链接传输任何消息之前（例如，用户名与密码）进行密钥套件协商。

1. 进入“VPN>SSL>配置”。
2. 在加密密钥算法字段，选择以下选项之一：
   - 如果远程用户端的 web 浏览器能够匹配 128bit 或更高的密码套件，设置为默认－

RC4（128bit）或更高。

- 如果远程用户端的 web 浏览器能够匹配 ssl 加密更高的密码套件，设置为高－AES（128/256bit）与 3DES。该选项启动后使用大于 128bit 的加密套件加密数据。
- 如果您不确定远程用户端的 web 浏览器支持哪个级别的 ssl 加密，设置低－RC4（64bit），DES 以及更高。web 浏览器必须至少支持 64bit 的密钥长度。

3. 点击“应用”。

设置闲置超时

闲置超时是设置远程用户被系统自动退出之前可以停留的时间。为了提高安全性，保留默认值 300 秒。

1. 进入“VPN>SSL>配置”。
2. 在闲置超时字段，输入整数值。有效范围为 10 到 28800 秒。
3. 点击“应用”。

配置用户验证超时设置

用户验证超时设置是设置经过验证的连接能够保持存活的时间。保持连接的时间超时后，系统要求远程用户重新接受验证。

注意：默认的值为 1500 秒。您只能使用 CLI 命令修改该超时设置值。

举例说明，将验证超时更改为 1800 秒，输入以下命令：

```
config vpn ssl settings
set auth-timeout 1800
end
```

在web入口首页添加自定义标题

您可以在 web 入口首页添加自定义标题（最多 31 个字符）。

添加标题栏

1. 进入“SSL>VPN>配置”。

2. 在门户信息字段，输入标题。

3. 点击“应用”。

对用户添加WINS与DNS服务

您可以设定ssl－vpn用户可用的WINS与DNS服务。

1. 进入“SSL>VPN>配置”。

2. 点击蓝色三角箭头，打开高级选项。

3. 输入对用户提供使用的一个或两个DNS服务器的IP地址。

4. 输入对用户提供使用的一个或两个WINS服务器的IP地址。

重新定向用户组到弹出的窗口

FortiGate设备在验证远程用户且用户登录成功后，将web浏览器重新定向到web网站首页。

作为一个选项，当用户的web浏览器重新定向到web网页时，您可以使FortiGate设备在弹出的窗口显示第二个HTML页面。配置允许该功能的实现，您必须将web浏览器中与internet区域有关的安全设置配置允许弹出窗口。

以下步骤进行的前提是假设已经定义了ssl vpn用户组。基于用户组可以设定不同的弹出窗口。

对用户组显示用户定义的弹出窗口

1. 进入“用户>用户组”。

2. 点击ssl vpn用户组对应的编辑图标。

3. 扩展ssl－vpn用户组选项。

4. 在重新定向url字段，输入在弹出窗口显示的页面的url。

5. 点击OK确认。

自定义web首页登录页面

构成web门户登录页面的HTML代码可以被编辑。编辑之前，将默认的文本拷贝到一个独立的文件中备以保存。之后，如果编辑过程产生意外的结果，您可以重新恢复到原始版本。

编辑 HTML 代码

1. 进入“系统>配置>替换信息”。

2. 扩展 ssl vpn 栏目并定义 ssl vpn 登录页面对应的编辑图标。

3. 编辑 HTML 文本，遵循 FortiGate 设备管理与使用手册中“系统配置”章节中叙述的有关限制说明。

4. 点击 OK 确认。

配置用户帐户与ssl vpn用户组

远程用户在通过 web 门户网站请求服务和/或访问网络资源之前必须被验证。验证操作根据 FortiGate 用户组的定义中规定的选项，使用已建立的验证机制，例如 RADIUS 与 LDAP，验证远程用户。

您可以选择使用纯文本密钥通过 FortiGate 设备（本地域）进行验证，将验证请求转发到一个外部 RADIUS 或 LDAP 服务器， 或使用 PKI 验证。如果密码保护通过 RADIUS 或 LDAP 服务器提供，您必须配置 FortiGate 设备将验证请求转发到 RADIUS 或 LDAP 服务器。如果使用证书验证，您必须安装所要求的证书。

以下步骤显示如何在本地域名中建立用户帐户与用户组。有关如何建立 RADIUS、LDAP 或 PKI 用户帐户的信息，参见 FortiGate 设备管理与使用指南。有关证书验证的信息，参见 FortiGate 设备证书管理用户手册。

在本地域名中创建用户帐户

1. 进入“用户>本地”并点击“新建”。

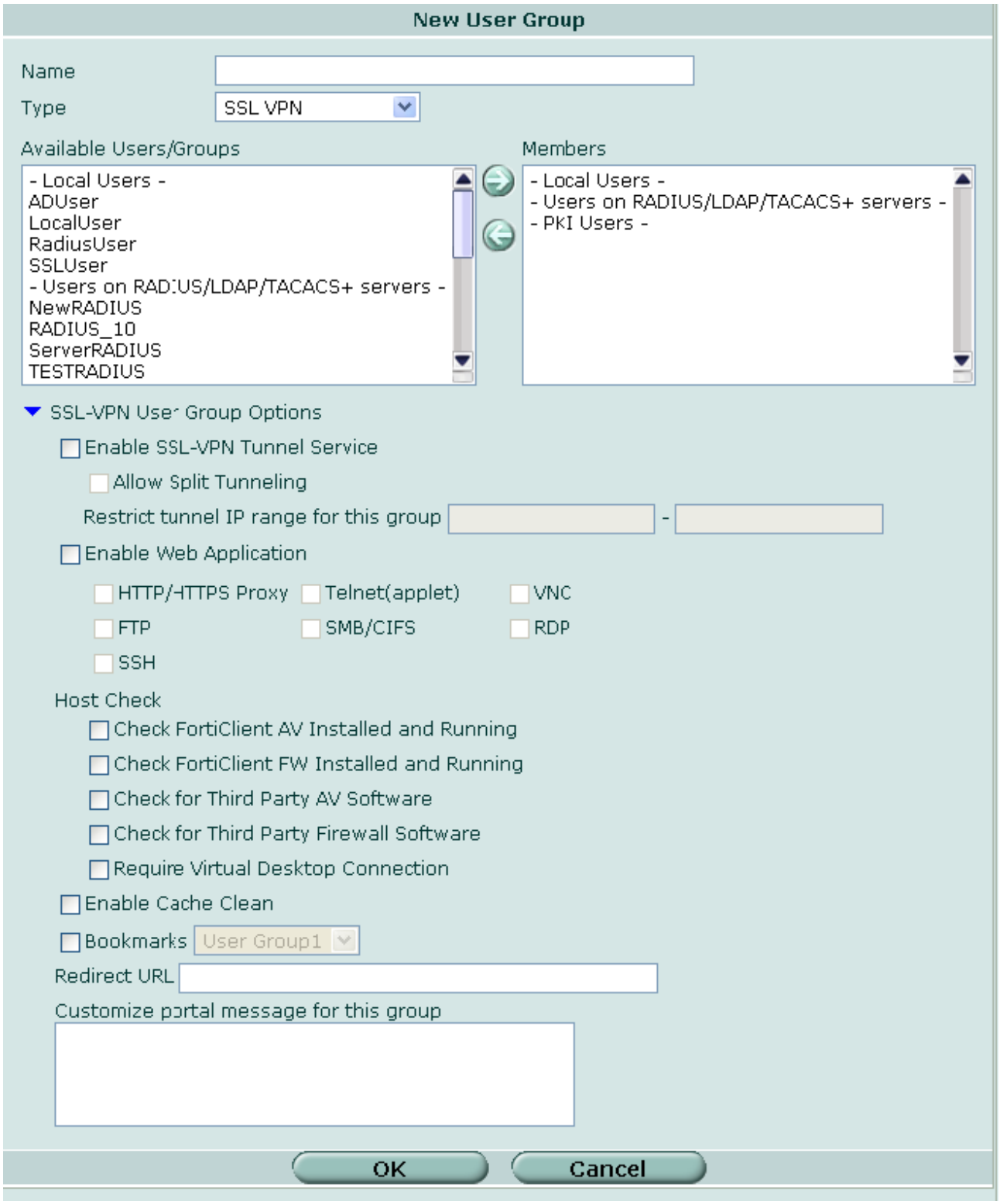
用户名	输入或编辑远程用户名称（例如，User_1）.
撤消	撤消用户接受验证。
密码	使用存储在 ssl vpn 设备中的密码验证该用户。输入或编辑与用户帐户有关的密码。密码应该至少六个字符长度。
LDAP	使用存储在 LDAP 服务器中的密码验证该用户。从下拉菜单中选择 LDAP 服务器。
RADIUS	使用存储在 RADIUS 服务器中的密码验证该用户。从下拉菜单中选择 RADIUS 服务器。

2. 点击“OK”。

3. 重复以上步骤配置每个远程用户。

创建用户组

1. 进入“用户>用户组”，并点击“新建”。



2. 在名称字段，设置用户组的名称。（例如，web－only_group）

3. 从类型下拉列表中，选择 SSL VPN。

4.从用户/组列表中，一次选择一个用户名称；点击向右箭头将其移动到成员列表。

5. 点击蓝色三角箭头扩展 ssl－vpn 用户组选项。

6. 如果与远程用户有关的用户组需要与 FortiGate 设备建立 SSL VPN 通道，启动 SSL－VPN 通道服务。

注意：如果用户已经被配置使用 web－only 的通道模式，当用户登录时，通道将自动激活。通道分割在默认情况下不启动，必须配置启动。

7. 激活通道分割功能，点击“启动通道分割”。通道分割功能能够保证只到达私网的流量被发送到 ssl vpn 网关。互联网流量将通过常规的非加密路由被发送。

8. “VPN>SSL>配置”定义通道 IP 地址范围, 输入起始与结束 IP 地址范围.

注意：如果您配置了用户组并对该组定义了“限制通道 IP 范围”，ssl vpn 配置中将使用组范围。如果您没有定义全局 IP 地址的范围，您必须定义一个组范围。如果您对二者的 IP 地址范围都做了定义，组级别范围将应用到配置。

9. 如果用户组只要求 web-only 模式的访问，点击“启动 web 应用”并选择用户组需要访问的 web 程序和/或网络文件服务。对应服务器应用程序可以运行于 FortiGate 设备之后的网络或通过互联网被远程访问。

10. 启动用户完整性查看选项，选择以下选项：

- 查看 FortiClient Av 的安装与运行
- 查看 FortiClient Fw 的安装与运行
- 查看第三方 AV 软件
- 查看第三方防火墙软件

用户完整性查看是查看在通道建立之前用户端设备是否运行 FortiClient 主机安全应用或其他反病毒/防火墙程序。 主机查看功能由 ActiveX/Java 平台控制程序执行，该执行程序是在用户首次发起 ssl vpn 网页时下载并安装在用户端计算机设备的。

注意：用于在远程计算机端安装 ssl vpn 用户端程序的用户帐户必须具有管理员权限。如果用户帐户不具有管理员权限，安装将失败（windows 下，安装失败不会显示错误信息）。安装 ActiveX/Java 平台控制程序后，用户端计算机设备可以被任何具有管理员权限

的用户使用。

如果用户端计算机上没有安装并启动任何程序，连接将被拒绝。表 1 所列运行 Windows XP SP2 支持用户端的产品名称。所有其他系统必须安装并启动了 Norton（Symantec）反病毒或 McAfee 病毒扫描软件。

表 1：AV/防火墙支持的产品检测

□ 品	AV	防火□
Norton Internet Security 2006	**Y**	**Y**
Trend Micro PC-cillin	**Y**	**Y**
McAfee	**Y**	**Y**
Sophos Anti-virus	**Y**	**N**
Panda Platinum 2006 Internet Security	**Y**	**Y**
F-Secure	**Y**	**Y**
Secure Resolutions	**Y**	**Y**
Cat Computer Servies	**Y**	**Y**
AhnLab	**Y**	**Y**
Kaspersky	**Y**	**Y**
ZoneAlarm	**Y**	**Y**

11. 启动 FortiGate 设备在 ssl vpn 会话结束之前从远程用户端计算机设备删除残留信息（例如，从 web 浏览器的缓存中），点击“启动缓存清除”。该功能启动后，如果用户端的浏览器不能安装并运行缓存清除程序，用户不被允许访问 sll vpn 入口程序。

12. 配置允许 ssl vpn 用户组使用预配置的书签组，启动“书签”并从下拉菜单中选择书签组。

13. 配置显示 web 入口首页时，FortiGate 设备在弹出的窗口中显示第二个 HTML 页面，在重新定向 URL 字段中输入网页的 url。

14. 配置对用户组显示自定义的 web 入口首页，在自定义入口信息字段输入信息。

注意；该自定义信息将取代在“vpn>ssl>配置”中配置的入口信息。

15. 点击 OK 应用。

配置防火墙策略

以下步骤是配置只适用于 web 模式与通道模式操作的步骤说明。步骤说明的前提是假设您已经完成了“配置用户帐户与 ssl vpn 用户组”。

防火墙策略是设定数据包的源地址与预定到达的目标 IP 地址。

通常，配置防火墙策略包括：

- 设定 IP 源与目标地址
- 设定使用的 ssl 加密级别与验证方式
- 将用户组与防火墙策略绑定

注意： 通道模式下，需要创建一项 DENY 防火墙策略遵循 ssl vpn 策略。如果不创建该策略，ssl vpn 通道将使用其他 ACCEPT 防火墙策略。

本章包括以下内容：

- 配置防火墙地址
- 配置通道模式防火墙策略
- 配置 ssl vpn 事件日志
- 监控活动的 ssl vpn 会话

配置防火墙地址

对只适用于 web 与通道模式的连接配置防火墙策略包括设定 IP 源/主机与目标地址：

web－only 模式：

- 对于源地址，设定为防火墙加密策略中的预定义地址“全部”对应 web－only 用户。
- 目标地址对应远程用户需要访问的 IP 地址或地址。目标地址可以对应整个私有网络（FortiGate 设备之后）、私有 IP 地址的一个范围或服务器或主机的私有 IP 地址。

通道模式：

- 源地址对应连接到 FortiGate 设备的公共 IP 地址。该地址用于限制对 FortiGate 设备的访问范围。
- 目标地址对应远程用户需要访问的 IP 地址或地址。目标地址可以对应整个私有网络（FortiGate 设备之后）、私有 IP 地址的一个范围或服务器或主机的私有 IP 地址。

配置web－only防火墙策略

设定目标 IP 地址

1. 进入“防火墙>地址”并点击“新建”。

2. 在地址名称字段，输入表示本地网络、服务器或主机的，发出 IP 数据包的名称。例如 subnet_1。

3. 从类型列表中，选择“子网/IP 范围”。

4. 在“子网/IP 范围”字段，输入对应的 IP 地址与子网掩码（例如 172.16.10.0/24）。

注意：提供到单个主机或服务器的访问，您需要输入一个 IP 地址，如 172.16.10.2/32.设置到两个具有连续 IP 地址的服务器访问，您需要输入 IP 地址范围如 172.16.10『4－5』。

5. 点击 OK 确认。

对 web－only 模式的连接定义防火墙策略

1. 进入“防火墙>地址”并点击“新建”。

2. 特别需要配置以下设置：

源地址	接口/区域 设置从远程用户接受连接的 FortiGate 设备接口。 地址名称 设置为“全部”
目标地址	接口/区域 设置连接到本地私网的 FortiGate 设备接口（例如，dmz）。 地址名称 设置为您之前定义的 IP 目标地址（例如，subnet_1）.
服务	设置为“任何”。
动作	设置为 ssl－vpn。
ssl 用户证书限制	设置允许组（共享）证书的持有者产生的流量，例如，一个用户组包含 PKI 对等/用户。组证书的持有者必须是 ssl vpn 用户组中的一员，且用户组的名称必须在被允许列表中显示。
加密强度	设置以下选项决定使用的 ssl 加密级别。远程用户端计算机设备的浏览器必须能够与您设置的加密强度匹配： ● 设置为“任何”，使用任何加密套件。 ● 设置为“高>=164”，使用 164bit 或更高的加密套件。

	● 设置为“中>=128”，使用 128bit 或更高的加密套件。
用户验证方式	设置为以下选项将用户组与验证方式绑定： ● 如果用户组只包含本地用户，设置为“本地”。 ● 如果远程用户端接受外部 RADIUS 服务器验证，设置为“RADIUS”。 ● 如果远程用户端接受外部 LDAP 服务器验证，设置为“LDAP”。 ● 如果用户组包含本地、RADIUS 与 LDAP 用户，设置为“任何”启动全部的验证方式。先使用“本地”，接着使用“RADIUS”，“LDAP”。
可用用户组	选择要求 ssl vpn 访问的用户组名称，并点击向右箭头移动。除非所选用户组的全部成员都具有相同的访问要求，单独选择用户组。

3.点击 OK 确认。

4. 如果用户组要求访问其他服务器或网络，创建 IP 目标地址并重复该步骤创建所要求的防火墙策略。

5.如需要，对其他用户组创建 IP 目标地址与防火墙策略。

配置通道模式防火墙策略

按照以下所述步骤完成通道模式的配置。以下步骤进行的前提是您已经完成了“配置用户帐户与 ssl vpn 用户组”。

当远程用户发起到 FortiGate 设备的连接时，FortiGate 设备验证用户并判断对用户启用的操作模式。当通道模式启动后，用户可以访问服务器应用以及内部网络中的网络服务，和/或从 web 网页下载以及安装 Active X 插件。ActiveX 插件中包含 ssl vpn 用户端软件。

注意：web 浏览器中，确定互联网区域设置有关的安全设置允许下载并运行 Active X 控件。

当用户在远程用户端的浏览器中安装了 ActiveX 插件后，用户可以启动 ssl vpn 用户端软件发起与 FortiGate 设备的 ssl vpn 通道连接。FortiGate 设备与 ssl 用户端建立通道

并分配用户一个虚拟 IP 地址。至此，ssl 用户在会话期间将该被分配虚拟 ip 地址作为其源地址。

配置 FortiGate 设备支持通道模式的访问，您必须配置 FortiGate 设备：

- 设定 ssl vpn 用户与 FortiGate 设备建立通道时，分配给用户使用的 IP 地址。
- 定义防火墙策略支持通道模式的操作。

防火墙策略设定数据包发出的源地址以及到达的目标网络的 IP 地址。在所述操作中，源地址指远程用户连接 FortiGate 设备的 IP 地址，目标地址是 FortiGate 设备之后的主机、服务器或网络的 IP 地址。

配置防火墙策略包括：

- 设定源与目标 IP 地址。

  源地址是远程用户的 IP 地址。

  目标地址是远程用户需要访问的 IP 地址。目标地址可能是整个私网的地址、私有 IP 地址范围或服务器或主机的私有 IP 地址。
- 设定 ssl 加密的级别与验证方式。
- 将用户组绑定到防火墙策略。

注意：如果通道模式下的目标地址、ssl 加密与用户组设置与 web-only 模式的连接相同，您不需要对通道模式创建防火墙策略。FortiGate 设备将使用 web-only 模式时创建的防火墙策略，但除了源与目标地址范围的设置，这些地址是从通道 IP 范围设置获取的。

设定源 IP 地址

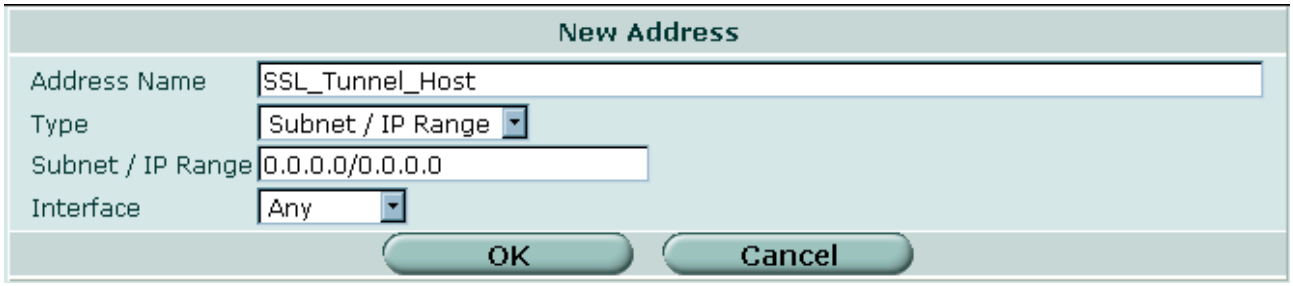
1. 进入“防火墙>地址”并点击“新建”。
2. 在“地址名称字段”，输入被允许建立 ssl vpn 连接的 IP 地址。
3. 从“类型”列表中，选择“子网/IP 范围”。
4. 在“子网/IP 范围”字段，输入 IP 地址与子网掩码（例如，172.16.10.0/24）。如果远程用户的 IP 地址是未知的，子网/IP 范围应该设置为“全部”，也就是 0.0.0.0/0.0.0.0.。

注意：设置到单个主机或服务器的访问，您需要输入 IP 地址如 172.16.10.2/32。到两个具有相邻 IP 地址服务器的访问，您应该输入一个 IP 地址范围，例如 172.16.10.『4－

5』。

5. 在“接口”字段，选择连接到内部（私）网的接口。

6. 点击 OK 确认。



设定目标 IP 地址

1. 进入“防火墙>地址”并点击“新建”。

2. 在“地址名称字段”，输入数据包被传送到的本地网络、服务器或主机的 IP 地址。（例如，subnet_2）。

3. 在“子网/IP 范围”字段，输入 IP 地址（例如，子网地址为 192.168.22.0，或服务器或主机的地址 192.168.22.2），或 IP 地址范围（192.168.22.『10－25』）。

4. 在“接口”字段，选择连接到外部（公）网的接口。

5. 点击 OK 确认。

定义通道模式的防火墙策略

1. 进入“防火墙>地址”并点击“新建”。

2. 配置以下设置：

源地址	接口/区域
	设置从远程用户接受连接的 FortiGate 设备接口（例如，external 外部）。
	地址名称
	设置为远程用户的 IP 地址。
目标地址	接口/区域
	设置连接到本地私有网络的 FortiGate 设备接口（例如，内部 internal 接口）。
	地址名称
	设置为您之前对 FortiGate 设备之后的主机、服务器或网络定义的 IP 目标地址（例如，subnet_2）。

服务	设置为“任何”。
动作	设置为“ssl_vpn”。
ssl 用户证书限制	设置允许组（共享）证书的持有者产生的流量，例如，一个用户组包含 PKI 对等/用户。组证书的持有者必须是 ssl vpn 用户组中的一员，且用户组的名称必须在被允许列表中显示。
加密强度	设置以下选项决定使用的 ssl 加密级别。远程用户端计算机设备的浏览器必须能够与您设置的加密强度匹配： ● 设置为“任何”，使用任何加密套件。 ● 设置为“高>=164”，使用 164bit 或更高的加密套件。 ● 设置为“中>=128”，使用 128bit 或更高的加密套件。
用户验证方式	设置为以下选项将用户组与验证方式绑定： ● 如果用户组只包含本地用户，设置为“本地”。 ● 如果远程用户端接受外部 RADIUS 服务器验证，设置为“RADIUS”。 ● 如果远程用户端接受外部 LDAP 服务器验证，设置为“LDAP”。 ● 如果用户组包含本地、RADIUS 与 LDAP 用户，设置为“任何”启动全部的验证方式。先使用“本地”，接着使用“RADIUS”，“LDAP”。
可用用户组	选择要求 ssl vpn 访问的用户组名称，并点击向右箭头移动。除非所选用户组的全部成员都具有相同的访问要求，单独选择用户组。

3. 点击 OK 确认。

注意：如果您在 ssl vpn 防火墙策略中应用了内容保护表设置，该设置同样将适用与通道模式操作. 见后面的 ssl.root 接口介绍。

4. 如果用户组要求访问其他服务器或网络，创建 IP 目标地址并重复该步骤创建所要求的防火墙策略。

5. 如需要对每个额外的用户组创建另外的 IP 目标地址与防火墙策略。

配置ssl vpn 事件日志

您可以配置 FortiGate 设备记录 ssl vpn 事件日志。有关解析日志的相信信息，参见 FortiGate 设备日志信息参考。

配置记录 ssl vpn 事件

1. 进入“日志&报告>日志配置>日志设置”。
2. 启动将日志存储到以下位置：
   - FortiAnalyzer 设备
   - FortiGate 设备内存
   - 运行 syslog 服务器的远程计算机设备

注意：如果您配置的 FortiGate 设备中有可用的硬盘，您可以启动将日志信息存储到系统硬盘。另外，作为以上列出的可选项之一，您可以配置将日志上传到运行 web trend 防火墙报告服务器的远程计算机设备。有关通过 cli 启动这些选项的详细信息，参见 FortiGate 设备 CLI 使用参考手册。

3. 如果选项是隐藏的，点击每个选项旁边的蓝色三角箭头扩展选项并配置相关设置。
4. 如果日志被写入系统内存，从日志级别列表中，设置级别为“信息”。详细信息，参见 FortiGate 设备管理与使用手册中的“日志与报告”章节。
5. 点击”应用“。

过滤 ssl vpn 事件

1. 进入“日志&报告>日志配置>事件日志”。
2. 选择”启动“并设置以下的一个或多个选项：
   - ssl vpn 用户验证事件
   - ssl vpn 管理事件
   - ssl vpn 会话事件
3. 点击”应用“。

查看 ssl von 事件日志

1. 进入”日志&报告>日志访问“。
2. 如果类型列表中有可用的选项，从硬盘或内存中选择日志文件。

根据您的查看要求，可以在查看日志页面的顶部修改显示设置。符合要求的日志信息将在设置栏的下面显示。

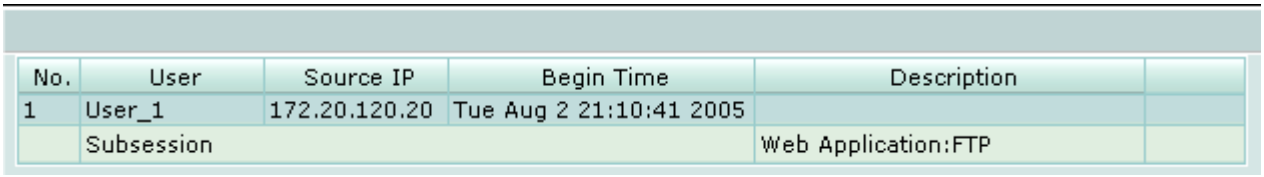


监控活动的ssl vpn会话

您可以配置显示所有活动的 ssl vpn 会话列表。列表中显示远程用户的用户名称、远程客户端的 IP 地址以及连接持续的时间。会话列表还显示提供的服务。参见图 3。

进入”vpn>ssl>监控“，查看活动会话列表。

图 3： 监控列表：web－only 模式连接



No.	User	Source IP	Begin Time	Description
1	User_1	172.20.120.20	Tue Aug 2 21:10:41 2005	
	Subsession			Web Application:FTP

编号（No.） 连接的编号。
用户 所有连接的远程用户的用户名。
源 IP 地址 连接到 FortiGate 设备的主机设备的 IP 地址。
起始时间 每个连接开始的时间。
描述 对提供服务的描述性信息。

当通道模式用户连接时，描述字段显示 FortiGate 设备分配到远程主机的 IP 地址。

图 4：监控列表：通道模式连接



No.	User	Source IP	Begin Time	Description
1	User_4	172.20.120.20	Tue Aug 23 10:26:34 2005	
	Subsession			Web Application:TELNET 10.10.10.10
	Subsession			Tunnel IP:10.10.254.1

如需要，点击连接对应行中的删除图标，可以结束会话/连接。

配置ssl vpn书签与书签组

如果您创建了用户组允许 web－only 访问，您可以对经常访问的服务器程序创建超级链接，那么用户在主页下通过超级连接便可以开始任何会话。FortiGate 设备将用户请求转发到互联网或内部网络中的服务器。配置使用 web 入口程序，您需要在书签列表中添加

url、Ip 地址或服务器应用的名称。当用户启动一个活动的 ssl vpn 会话时，书签也是可用的。

查看ssl vpn书签列表

配置显示 FortiGate 设备创建的所有 ssl vpn 书签列表。列表的信息包括书签的名称、书签的类型以及链接的详细信息。

进入”vpn>ssl>书签“，查看预定义的 ssl vpn 书签列表。

图 5：书签列表



书签名称	链接到远程服务器程序与网络服务器的链接的类型/名称。
链接	书签链接的 url、主机或文件夹。
删除与编辑图标	删除或编辑列表中的条目。

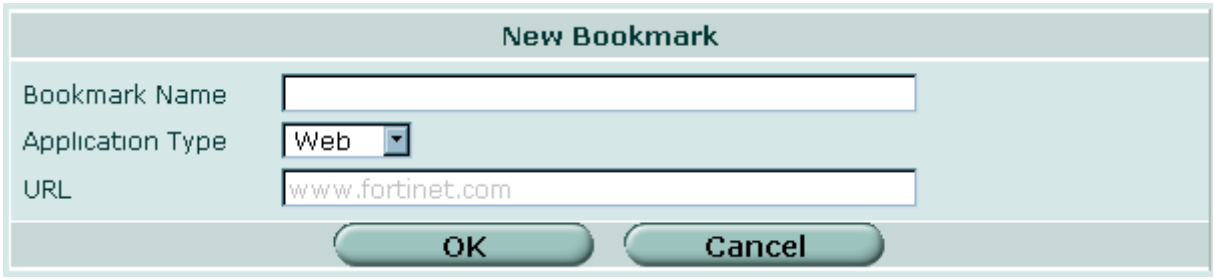
同时参见：

- 配置 ssl vpn 设置
- 监控活动的 ssl vpn 会话
- 配置 ssl vpn 书签与书签组
- 配置 ssl vpn 书签
- 查看 ssl vpn 书签组列表
- 配置 ssl vpn 书签组

配置ssl von书签

进入”vpn>ssl>书签“并点击”新建“创建到经常访问的服务器程序的超级链接。

图 6：新建书签



书签名称	输入超级链接中显示的文本信息，该信息将作为链接的名称显示在书签列表中。
应用类型	从下拉列表中选择缩写的服务器应用名称： • web • Telnet • FTP • SMB/CIFS • VNC • RDP • SSH
URL/主机/文件夹	输入 FortiGate 设备需要将用户端请求转发到正确的服务器应用或网络服务的信息。 • 如果应用类型是 Web，输入 web 服务器的 url（例如，www.fortinet.com）。 • 如果应用类型是 Telnet，输入 Telnet 主机的 IP 地址（例如，10.10.10.10）。 • 如果应用类型是 FTP，输入 FTP 主机的 IP 地址作为根目录/文件夹（例如，//server/folder）。 • 如果应用类型是 SMB/CIFS，输入 SMB 主机的 IP 地址以及与您帐户相关的根目录/文件夹（例如，//server/folder/）。 • 如果应用类型是 VNC，输入主机的 IP 地址（例如，10.10.10.10）。 • 如果应用类型是 RDP，输入 RDP 主机的 IP 地址（例如，10.10.10.10）。 • 如果应用类型是 SSH，输入 SSH 主机的 IP 地址（例如，10.10.10.10）。

同时参见：

- 配置 ssl vpn 设置
- 监控活动的 ssl vpn 会话
- 配置 ssl vpn 书签与书签组
- 配置 ssl vpn 书签
- 查看 ssl vpn 书签组列表
- 配置 ssl vpn 书签组

查看ssl vpn书签组列表

您可以创建具体的书签组包括在 ssl vpn 用户组配置中。

进入“vpn>ssl>书签组”，查看书签组列表。

图 7：书签组列表



组名称	书签组名称。
书签	书签列表在组名称中显示的书签组。
删除与编辑图标	删除或编辑列表中的条目。

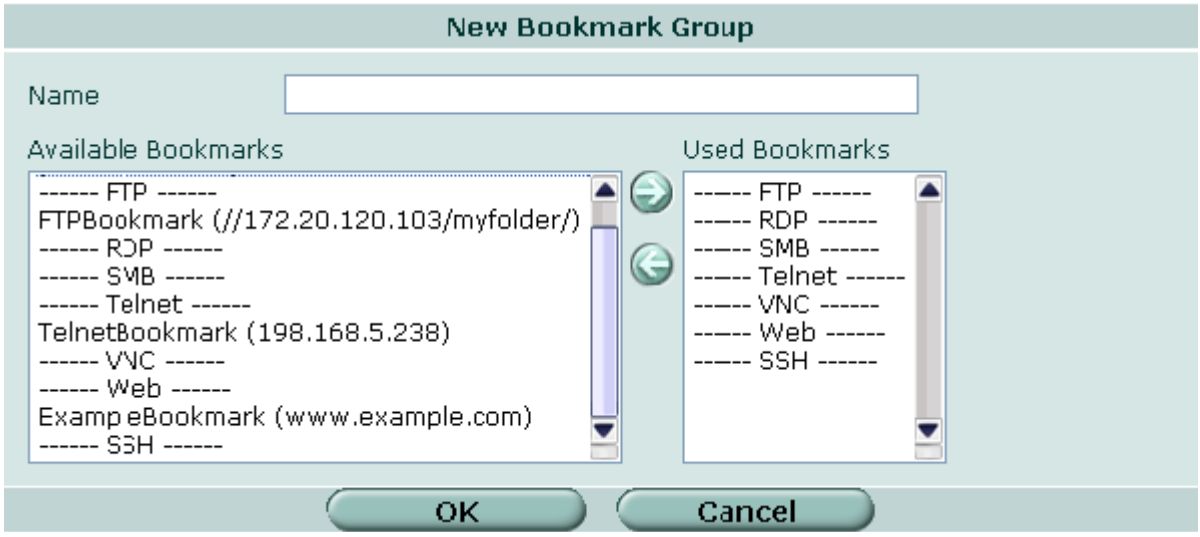
同时参见：

- 配置 ssl vpn 设置
- 监控活动的 ssl vpn 会话
- 配置 ssl vpn 书签与书签组
- 配置 ssl vpn 书签
- 查看 ssl vpn 书签组列表
- 配置 ssl vpn 书签组

配置ssl vpn书签组

进入“vpn>ssl>书签组”并点击“新建”对所选中的书签创建一个组。

图 8：新建书签组



名称	输入书签组的名称。该名称将在书签组列表中显示，并作为 ssl vpn 用户组中的书签列表的选项。
可用书签	可被加入书签组的可用书签列表。所列书签基本类型（FTP，RDP，SMB，Telnet，VNC，Web 或 SSH）。
已用书签	属于书签组的书签列表。
向右箭头	将选中书签添加到已用书签列表。从可用书签列表中选中书签并点击向右箭头将其移动到已用书签列表。
向左箭头	从已用书签列表删除书签。从已用书签列表中选中书签并点击向左箭头将其移动到可用书签列表。
新建	点击在可用书签列表中创建新的书签。

同时参见：

- 配置 ssl vpn 设置
- 监控活动的 ssl vpn 会话
- 配置 ssl vpn 书签与书签组
- 配置 ssl vpn 书签
- 查看 ssl vpn 书签组列表
- 配置 ssl vpn 书签组

对ssl vpn用户分配ssl vpn书签组

进入“用户>用户组”并点击“新建”创建 ssl vpn 用户组，并对用户组分配书签。扩展 ssl－vpn 用户组选项，启动书签并从下拉菜单中选择书签组。当您对 ssl vpn 分配一

个书签组时，这个书签组中的所有书签对于选中的 ssl vpn 用户组都是可用的。

图 9：分配书签组到用户



查看ssl vpn主机os补丁

ssl vpn 用户 os 补丁查看功能配置允许安装具体 os 补丁的用户访问 ssl vpn 服务。主机查看功能只能运行在 windows 平台，也就是说 MacOS/Linux 用户因为不适用补丁查看功能可以一直处于登录状态（该状态的前提是具有正确的用户名与密码）。ssl vpn 用户组设置中定义的选项支持该功能（只能使用 CLI）。

变量	描述
set sslvpn-os-check {disable|enable}	启动或撤消 ssl vpn OS 补丁级别查看功能。默认是撤消的。
config sslvpn-os-check-lish {windows-2000|windows-xp}	配置补丁版本的 OS 查看。将 set sslvpn－os－check 设置为启动时，该功能可用。
set action {allow | check-up-to-date | deny}	设定如何执行补丁版本查看。 ● “允许(allow)”；设置允许任何版本的补丁查看。 ● “查看更新(checkup-to-date)”；设置允许查看的级别。使用 latest－patch－level 与 tolerence 查看。 ● “拒绝(deny)”；os 版本不允许访问。只有当 set sslvpn-os-check 设置为 check-up-to-date 时可用。
set latest-patch-level {disable|0-255}	设定最新被允许的补丁级别。对于 windows2000，默认设置是 4；对于 windows xp，默认设置是 2。该功能只有在 action 设置为 enable 时可用。
set tolerance{tolerance_num}	设定最低允许的补丁版本公差。等于 latest-patch-level 减去 tolerance 的值以及该值以上的版本。对于 windows2000 与 windows xp 的默认值是 0。当 action 设置为

check-up-to-date 时可用。

配置举例

以下配置允许补丁级别为 2（latest-patch-level 减去 tolerance 的值）的 windows2000 用户以及该版本以上的用户，与任何 windows xp 用户访问 vpn 服务。

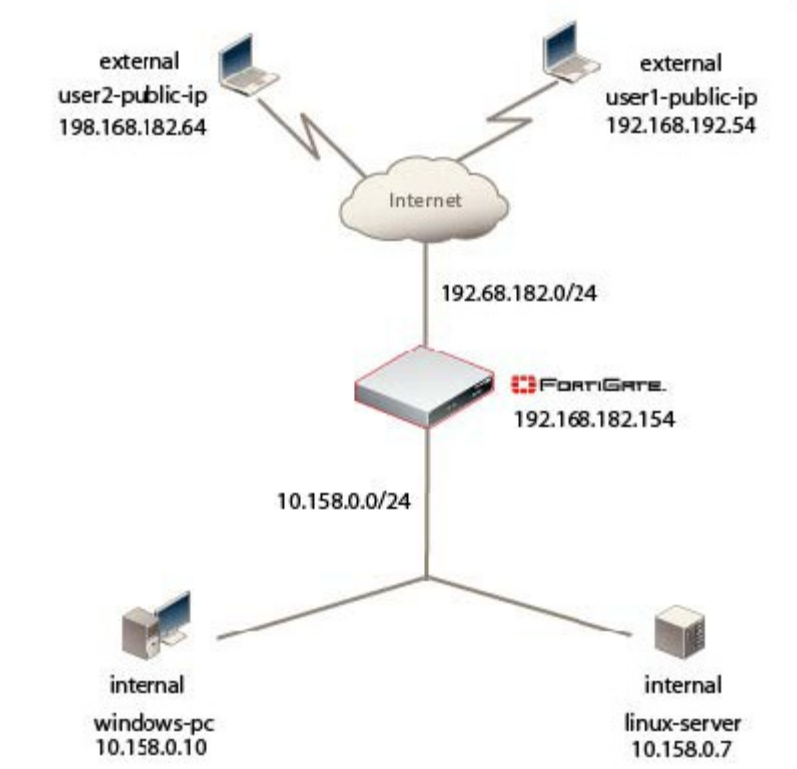
```
config vpn ssl settings
set sslvpn-enable enable
set tunnel-endip 10.1.1.10
set tunnel-startip 10.1.1.1
end
config user group
edit "g1"
set group-type sslvpn
set sslvpn-tunnel enable
set sslvpn-tunnel-startip 10.1.1.1
set sslvpn-tunnel-endip 10.1.1.10
set sslvpn-webapp enable
set sslvpn-os-check enable
config sslvpn-os-check-list "windows-2000"
set action check-up-to-date
set latest-patch-level 3
set tolerance 1
end
config sslvpn-os-check-list "windows-xp"
set action allow
end
set member "u1"
set sslvpn-split-tunneling enable
set sslvpn-http enable
next
end
```

```
config firewall policy
edit 1
set srcintf "internal"
set dstintf "external"
set srcaddr "all"
set dstaddr "172.18.8.0/24"
set action ssl-vpn
set schedule "always"
set service "ANY"
set groups "g1"
next
end
```

对ssl vpn通道用户组设置唯一的访问允许

对于要求不止设置允许一个用户进行通道模式访问的情况中，关键是将IP范围分割成为子ip范围，也就是每个用户组（具有用户成员的组）分配一个专门的ip范围（不重叠的情况下），那么便具有不同的访问权限。

图10：对ssl vpn通道用户组设置唯一的访问允许



对ssl vpn通道用户组设置唯一的访问允许的配置举例

在该配置举例中，有两个用户组，每个用户组均分配了专门的 IP 地址范围。

注意：两项 ssl vpn 防火墙策略的源地址在用户不具有静态公共 IP 的情况下均可以保留为“全部”。

首先，建立通道 IP 范围。

进入“vpn>ssl”，启动 ssl-vpn。

输入通道 IP 范围中用户/用户组可用的 IP 地址范围，在本举例中为 10.1.1.1－10.1.1.100.

图 11：启动 ssl－vpn 设置



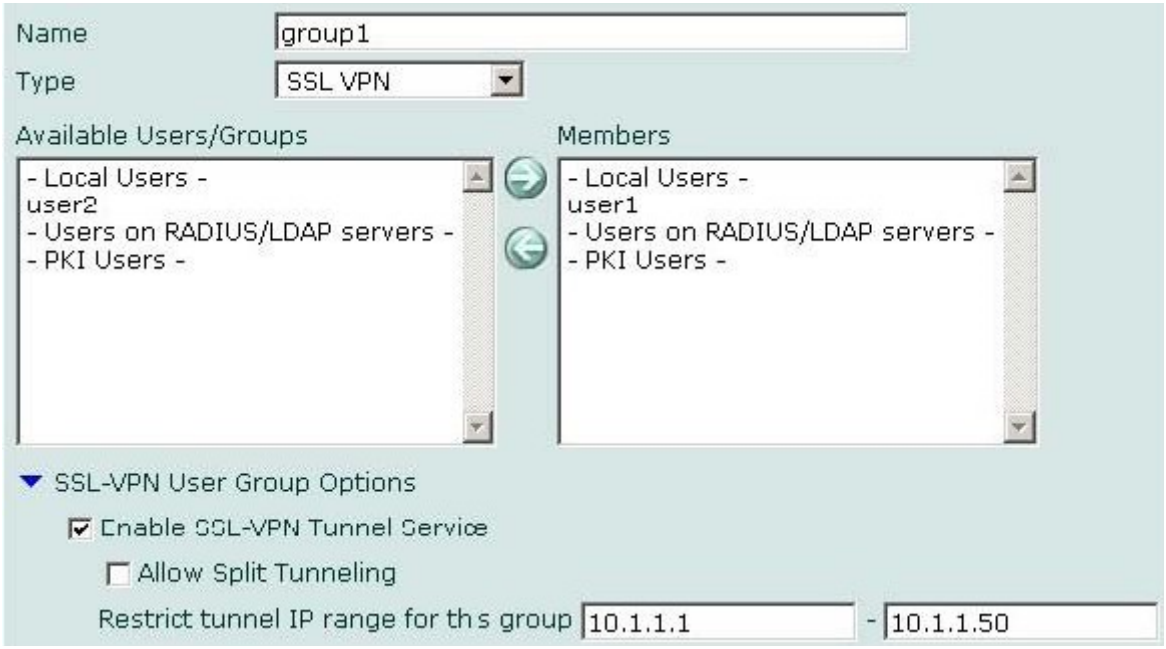
启动 ssl vpn 后，您必须创建用户以及要求 ssl vpn 通道模式访问的用户组。

进入“用户>本地”并创建具有密钥验证的 user1 与 user2。

注意：user1 只具有访问 linux 服务器的权限，user2 只具有访问 windows pc 的权限。您在创建用户之后，必须创建 ssl vpn 用户组。为了对每个用户配置不同的访问权限，您须要创建单独的用户组并对其分配具体的 IP 范围。

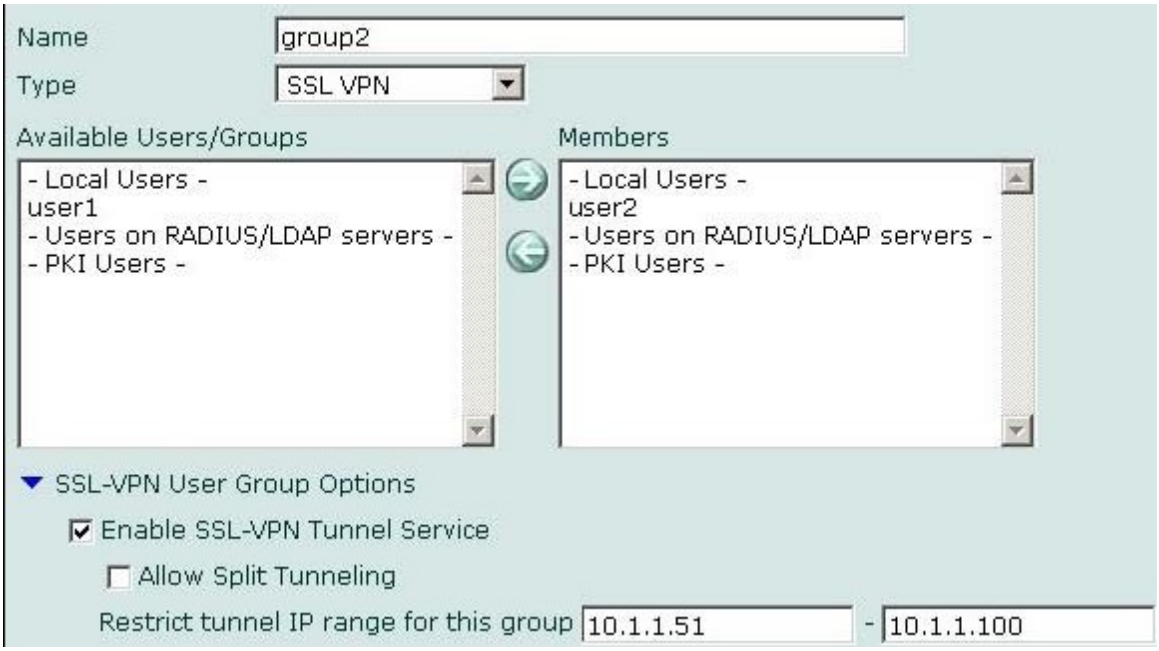
进入“用户>用户组”。创建 group1 作为 ssl vpn 用户组，且 user1 作为其成员，在“限制通道 IP 地址范围”内设置该组专用的地址范围是 10.1.1.1－10.1.1.50。

图 12：group1 用户组属性



创建 group2 作为 ssl vpn 用户组，且 user2 作为其成员，设置 10.1.1.51－10.1.1.100 作为该组的“限制通道 IP 地址范围”。

图 13：group2 用户组属性



在您创建用户组后，您需要定义防火墙策略支持通道模式的操作。

配置防火墙策略设置数据包的源地址与数据包到达的网络中接收端的目标地址。该配置下，源地址对应连接 FortiGate 设备的公共 IP 接口的地址，目标地址对应 FortiGate 设备之后 Linux 服务器/windows PC 的 IP 地址。

创建防火墙策略之前，您必须定义将要作为策略中设置的源与目标地址。

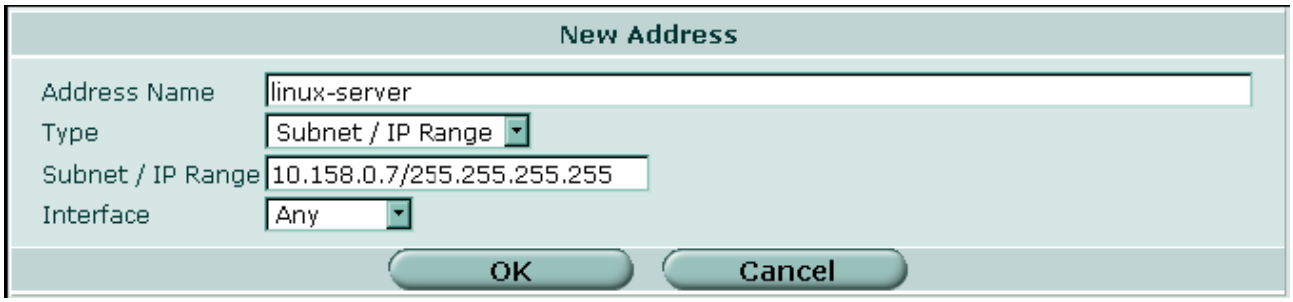
进入“防火墙>地址”，创建源与目标地址。

图 14：源/目标防火墙地址－公共 IP





图 15：源/目标防火墙地址－Linux/windows PC

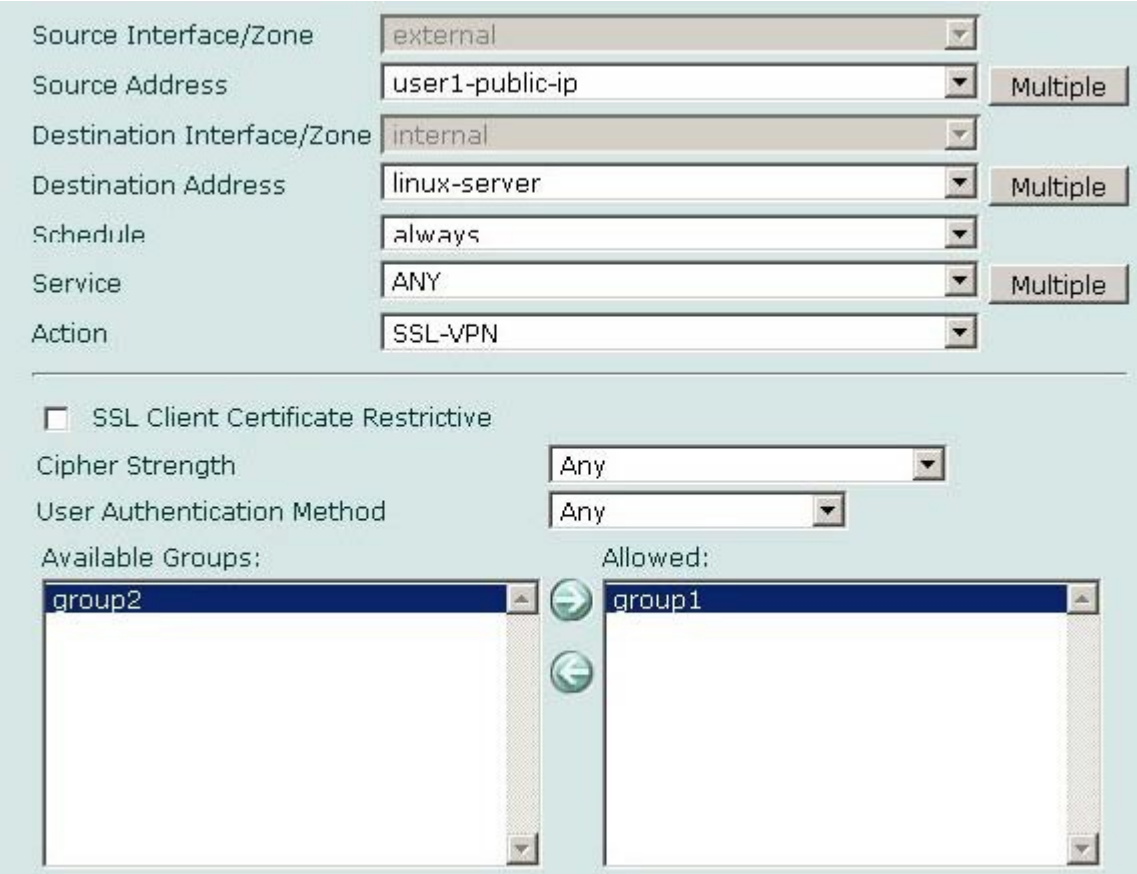




创建源与目标地址后，进入“防火墙>策略”创建防火墙策略。

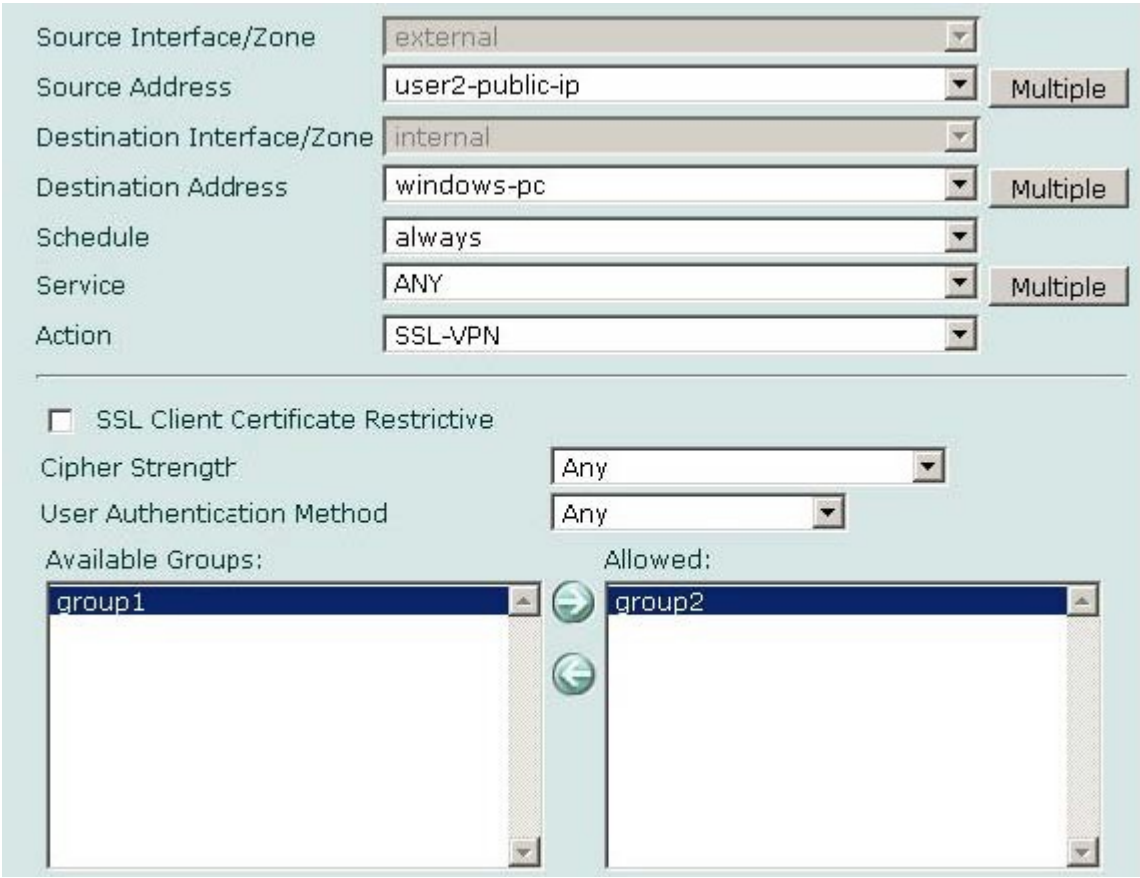
对于 user1 配置的策略是 ssl vpn 防火墙策略，其中包括适用的源与目标地址，以及 group1 作为策略的适用用户组。

图 16：user1 防火墙策略



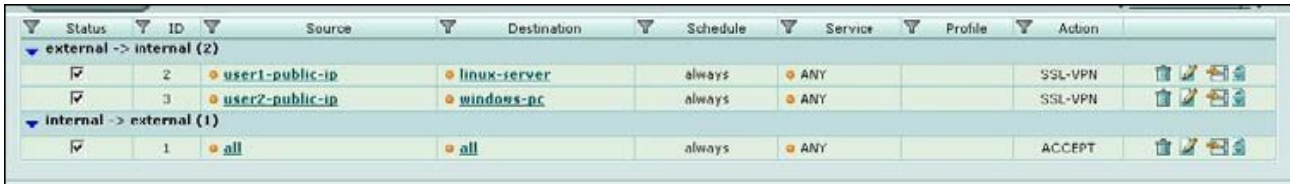
对于 user2 配置的策略是 ssl vpn 防火墙策略，其中包括适用的源与目标地址，以及 group2 作为策略的适用用户组。

图 17：user2 防火墙策略



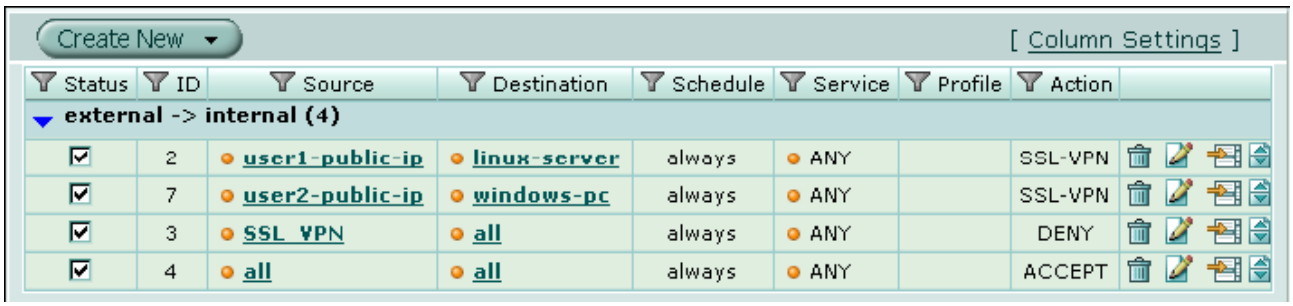
进入“防火墙>策略”，查看 ssl vpn 策略。

图 18：防火墙策略列表



为了避免与其他防火墙地址重叠，在 ssl vpn 策略之下添加 DENY 策略（源地址是 ssl von 通道 IP 范围）。更多信息，参见配置防火墙策略。





ssl vpn虚拟接口（ssl.root）

ssl vpn通道服务配置包括虚拟接口ssl<vdom_name>,提供如同ipsec虚拟接口的功能。在非vdom操作下，该接口显示为ssl.root。ssl.root接口在防火墙策略列表与静态路由列表中显示为ssl.root接口。ssl-root接口允许远程用户到其他网络的访问。例如，接口通过FortiGate设备便于远程用户访问互联网。

ssl vpn通道模式访问要求配置以下防火墙策略：

- external>internal,将动作设置为ssl，且配置ssl 用户组。
- ssl.root>internal，将动作设置为Accept。
- internal>ssl.root，将动作设置为Accept.

同时要求新建一项静态路由且显示如下：

- 目标网络-<ssl 通道模式分配的范围>接口ssl.root.

如果您配置通过ssl vpn通道访问互联网，必须添加以下的配置：

- ssl.root>external,将动作设置为Accept，且启动NAT.

进入“防火墙>策略”，并点击“新建”创建防火墙策略。对于标准配置，创建防火墙策略如下：

验证策略

源	wan1
源地址	全部
目标	internal
目标地址	内部子网
动作	sslvpn
验证	ssl用户组

向内访问策略

源	ssl.root
源地址	远程用户的 ip 地址
目标	internal
目标地址	内部子网
动作	accept
验证	不设置验证

向外访问策略

源	internal
源地址	内部子网
目标	ssl.root
目标地址	ssl 分配的范围
动作	accept
验证	不设置验证

静态路由

目标网络	<ssl 分配的子网>
目标接口	ssl.root

允许用户通过 FortiGate 设备浏览互联网。

互联网浏览策略

源	ssl.root
源地址	ssl 分配的子网
目标	wan1
目标地址	all
动作	accept
启动 NAT	启动
内容保护表	推荐进行设置

允许 ssl 通道用户访问基于策略的 vpn 对等网络：

对等网络策略

源	ssl.root
源地址	ssl 分配的子网
目标	wan1
目标地址	远程 vpn 子网
动作	ipsec
vpn 通道	<vpn 阶段 1 名称>

ssl vpn丢弃连接

当 FortiGate 设备具有多个互联网连接时，sslvpn 用户可以连接到 sslvpn web 入口网站，但是当试图点击“连接”启动通道模式 sslvpn 时，通道将启动几秒后关闭。

这种情况发生在多个接口连接到互联网的情况下，例如，双重 wan 口连接的配置。

升级到 Fortigate 设备至少 3.4MR4 或更过版本的 os 可以解决该问题。

同时也可以使用以下 cli 命令解决该问题：

```
config vpn ssl settings
set route-source-interface enable
end
```

注意：该 cli 命令在 FortiOS 3.0MR4 或更高版本下可用。

在 web 网站下运行

本章介绍 web 入口网站的功能以及如何配置。

包括以下内容：

- 连接到 FortiGate 设备
- web 网站首页的功能
- 发起 web 应用
- 从工具栏启动会话
- 通道模式功能
- 退出
- 在“我的书签”列表中添加书签
- 运行于 ActiveX/java 插件
- 卸载 ActiveX/java 插件
- URL 重写

连接到FortiGate设备

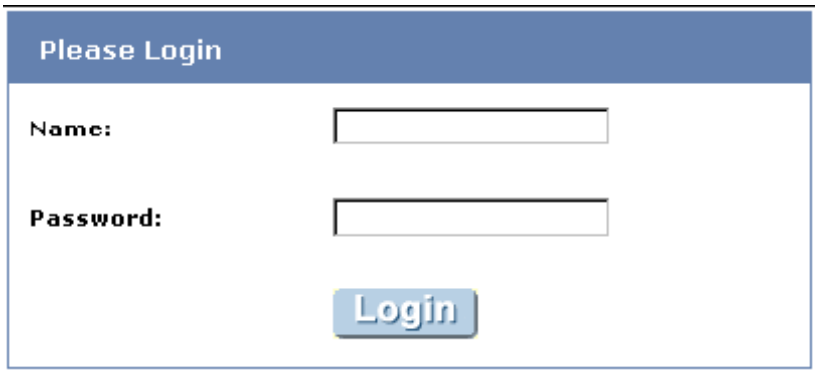
使用 web 浏览器连接到 FortiGate 设备。FortiGate 设备接口的 url 可能在每次的安装下均不同。如需要，可以向 FortiGate 设备管理员要求设备的 URL，并获取用户名与密码。

另外，如果您使用个人或组安全（x.509）证书连接 FortiGate 设备，您的 web 浏览器可能弹出要求证书名称的提示符，您可以向 FortiGate 设备的管理员索取该选择的证书。

登录到 FortiGate 设备安全 HTTP 网关

1. 使用您计算机设备中的 web 浏览器，访问 FortiGate 设备的 URL。（例如，https://<FortiGate_IP_address>:10443/remote）.
2. FortiGate 设备可能呈现可以自签安全证书。如果您执行，点击“是”。
3. 显示的第二项信息通知您 FortiGate 设备证书的著名名称与原始请求不同。只所以显示该信息，是因为 FortiGate 设备试图重新定向您的 web 浏览器的连接。您可以忽略该信息。
4. 提示输入用户名与密码的页面时，在“名称”字段输入您的用户名；在“密码”字段输

入密码。

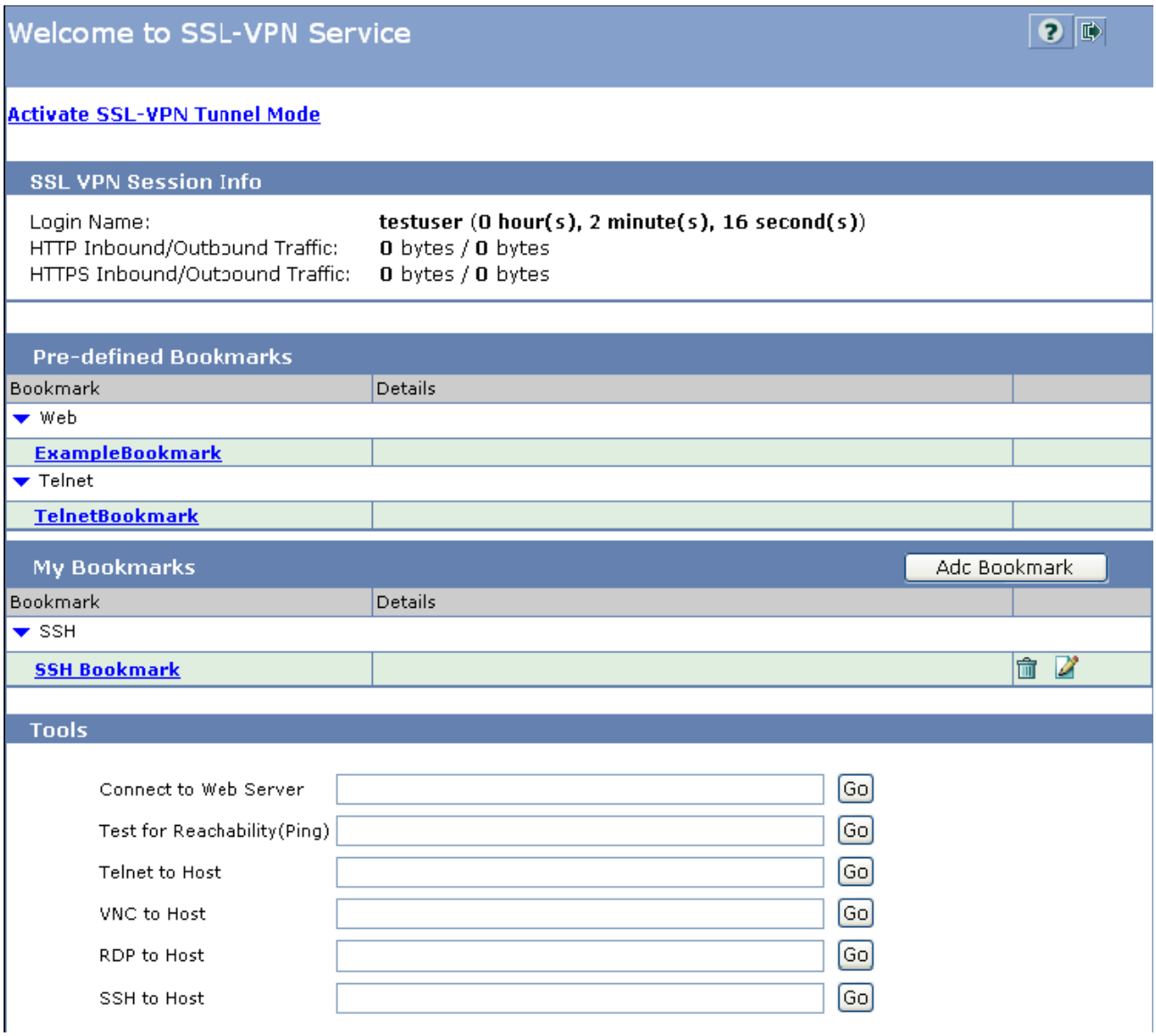


5. 点击“登录”。FortiGate 设备将重新定向您的 web 浏览器自动转到 FortiGate ssl vpn 远程访问页面主页。

Web页面主页功能

您在登录后，显示 FortiGate ssl vpn 远程访问网页主页面。

图 19：FortiGate ssl vpn 远程访问 web 页面


Welcome to SSL-VPN Service
Activate SSL-VPN Tunnel Mode
SSL VPN Session Info
Login Name: testuser (0 hour(s), 2 minute(s), 16 second(s))
HTTP Inbound/Outbound Traffic: 0 bytes / 0 bytes
HTTPS Inbound/Outbound Traffic: 0 bytes / 0 bytes
Pre-defined Bookmarks
Bookmark
Details
Web
ExampleBookmark
Telnet
TelnetBookmark
My Bookmarks
Add Bookmark
Bookmark
Details
SSH
SSH Bookmark
Tools
Connect to Web Server
Go
Test for Reachability(Ping)
Go
Telnet to Host
Go
VNC to Host
Go
RDP to Host
Go
SSH to Host
Go

如果您的用户帐户允许web－only默认访问，且您的管理员已经给您建立了预定义书签，这些书签将在预定义书签列表中显示。点击这些超级链接可以发起任何会话，但是您不能更改这些链接。同时，您可以根据自身需要创建经常访问的服务器应用的超级链接并点击所创建的链接发起任何会话。

如果您的用户帐户允许通道模式连接，您可以安装/卸载FortiNet ssl vpn用户端软件和/或与FortiGate发起ssl vpn通道。查看该主页的顶端部分，点击激活SSL VPN通道模式的链接。

在“工具”栏中，您可以链接到web服务器或启动telnet会话。您页可以查看与FortiGate设备之后网络中的主机或服务器的连接性。

发起web入口应用程序

FortiGate设备将用户请求转发到互联网上的服务器或内部网络。要使用web入口应用，您需要在“我的书签”列表中添加url、ip地址或服务器应用的名称。

注意：如果您在没有在“我的书签”列表中添加书签的情况下访问web服务器或telnet服务器，在“工具”栏下选择合适的字段输入服务器的url或ip地址。

以下服务器应用的一个或多个对于您是可用的，根据服务器管理员安装这些应用的情况：

- web服务器（http/https）下载HTML页面对应web浏览器请求。
- 通过Telnet服务器（TCP/IP终端模拟协议），您可以使用您的计算机设备作为虚拟终端登录到远程主机。
- 通过FTP（文件传输协议），您可以在您的计算机设备与远程主机之间传输文件。
- SMB/CIFS服务器执行SMB协议，以支持您的计算机设备与远程服务器主机之间的文件共享。
- 通过VNC，您可以远程控制其他计算机设备，例如，从您的家中的计算机访问工作的网络。
- RDP服务器具有多通道协议，允许用户连接到运行微软终端服务的计算机设备。
- 通过SSH服务器，您可以使用安全通道在两台计算机设备之间交换数据信息。

注意：windows 通过 SMB/CIFS 支持文件共享是通过共享的文件目录实现的。

当您访问以上任何的服务应用时，服务器可能提示要求输入您的用户名与密码。登录之前必须具有服务器管理员提供您的创建用户帐户的信息。

URL重写

当 FortiGate 设备将用户请求转发到互联网中的服务器或内部网络时，可能会要求在不暴露名称或地址的情况下访问网页。对于 HTTP/HTTPS，FortiGate 设备使用模糊技术将主机名称加密使用 AES－128 随机密钥，对应 hex 值加 Z 将被从开始形成编码的名称时添加。举例说明，url 为 http://test.org/index.html，FortiGate 设备将转换为 http://<sslvpn_host:port>/proxy/http/Z<encrypted hex value>/index.html。

加密密钥只对当前的用户会话有效。一旦用户退出，密钥将不在有效。

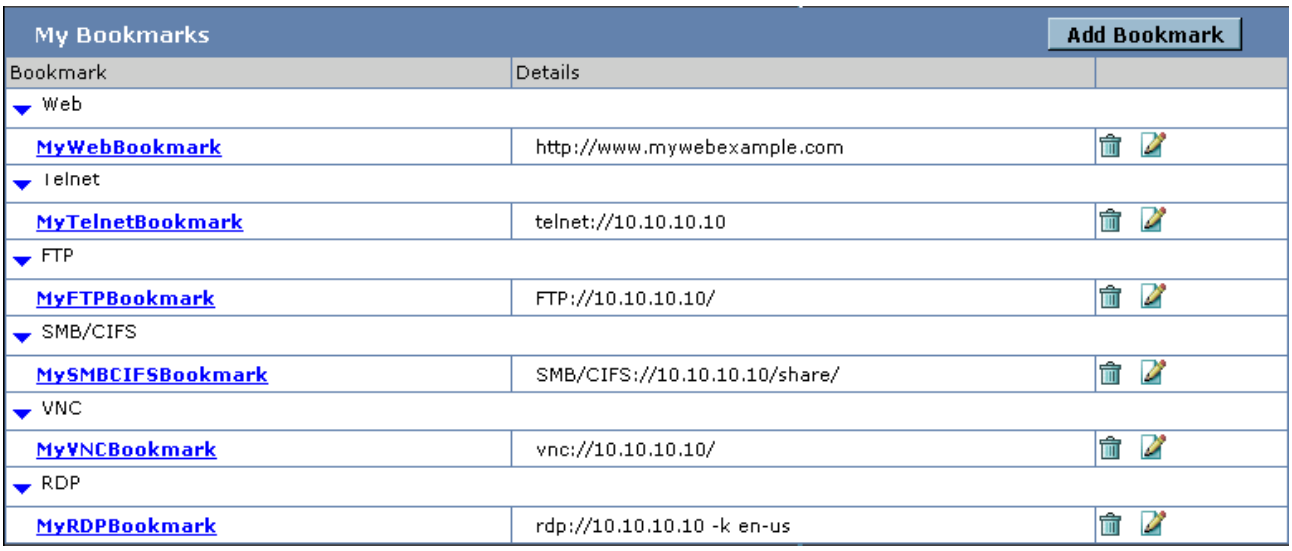
FTP 与 SMB 的情况中，路径/文件名处于内部编码的原因将被转换为 16 进制值。显示真实的主机 IP。不支持其他协议。

有关模糊加密技术的 cli 命令是 config vpn ssl setting 命令下的 url-obscuration。

添加书签到“我的书签”列表

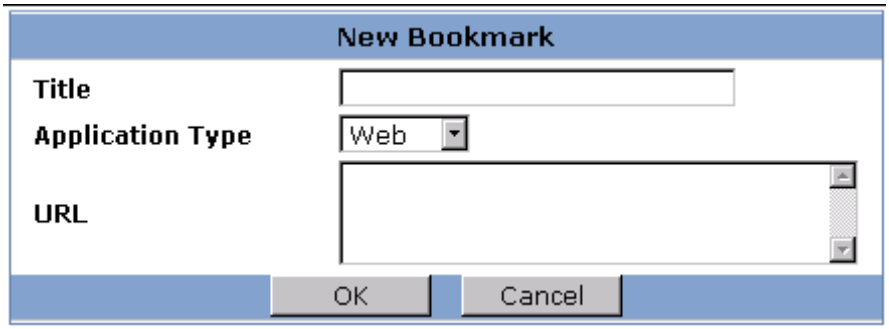
您可以将经常使用的连接添加到 web 入口主页中。那么，从“我的书签”中点击任何一个超级链接便可以发起会话。

图 20：“我的书签”列表中经常使用的链接



添加书签	创建超级链接。
书签	到远程服务器与网络服务的链接名称。
详情	有关 FortiGat 设备将用户请求转发到互联网中的服务器或 FortiGate 设备之后的私网的信息。
删除与编辑图标	删除或编辑列表中的条目。

图 21：新建书签对话框



名称	输入超级链接中显示的文本信息。该名称将在“我的书签”列表中显示。
应用类型	从下拉列表中选择服务器应用或网络服务的缩写名称。 • Web • Telnet • FTP • SMB/CIFS • VNC • RDP

- SSH

URL，主机名称/IP 或共享文件夹 输入 FortiGate 设备需要将用户请求转发到正确的服务器应用或网络服务的信息。

- 如果应用类型是 Web，输入 web 服务器的 url（例如 http://www.google.com 或 http://172.20.120.101）。
- 如果应用类型是 Telnet，输入 telnet 主机的 IP 地址（例如 10.10.10.10）。
- 如果应用类型是 FTP，输入 FTP 主机作为根目录的 IP 地址（例如，//10.10.10.10/share/）。
- 如果应用类型是 SMB/CIFS，输入 SMB 主机的 IP 地址或与您的帐户连接的根目录（例如，//10.10.10.10/share/）。
- 如果应用类型是 RDP，输入 RDP 主机的 IP 地址（例如，10.10.10.10）。
- 如果应用类型是 VNC，输入 VNC 主机的 IP 地址（例如，10.10.10.10）。
- 如果应用类型是 SSH，输入 SSH 主机的 IP 地址（例如，10.10.10.10）。

添加 HTTP 或 HTTPS 连接并访问 web 服务器

1. 点击“添加书签”。
2. 在“名称”字段，输入表示连接的名称。
3. 从“应用类型列表”中选择 web.
4. 在 URL 字段，输入 web 服务器的 url（例如，http://www.mywebexample.com 或 https://172.20.120.101）。



5. 点击 OK 确认。

6. 点击您所创建的超级链接，连接到 web 服务器。

FortiGate 设备使用 http://<FG_IP_address>:<port_no>/proxy/http/<设定的 URL>替换 URL 并显示所请求的页面。

7. 结束会话，关闭浏览器窗口。

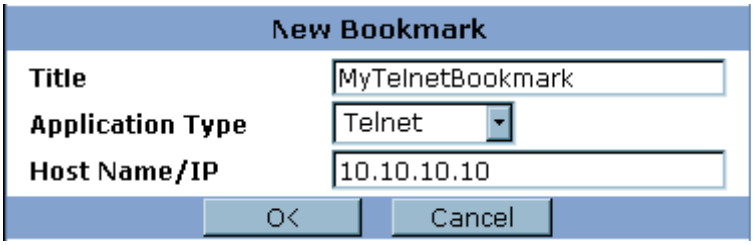
添加 telnet 连接并启动 telnet 会话

1. 点击“添加书签”。

2. 在“名称”字段，输入表示连接的名称。

3. 从“应用类型”列表中，选择 Telnet。

4. 在“主机名称/IP 字段”，输入 Telnet 主机的 IP 地址（例如 10.10.10.10）。



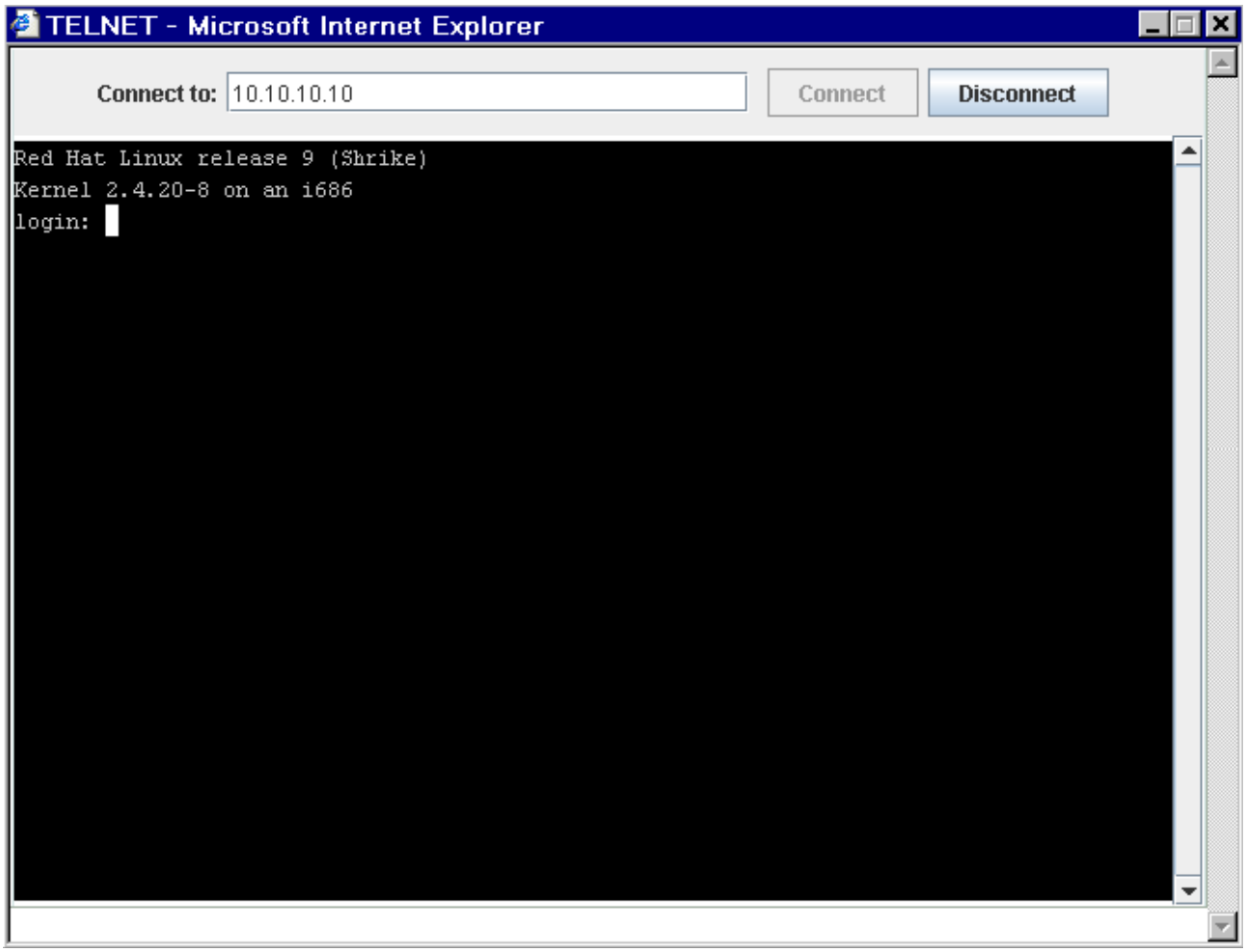
5. 点击 OK 确认。

6. 点击您创建的超级链接，启动 telnet 会话。

注意：FortiGate 设备可能呈现可以自签安全证书。如果您执行，点击“是”。显示的第二项信息通知您主机名称不匹配。只所以显示该信息，是因为 FortiGate 设备试图重新定向您的 web 浏览器的连接。点击“是”执行操作。

7. 点击“连接”。

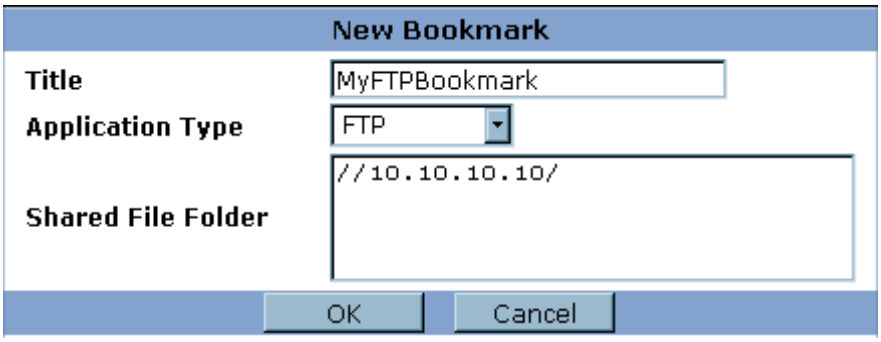
8. Telnet 会话启动且提示您登录远程主机。您必须具有登录的用户帐户。登录后，系统提示符下可以输入一系列有效的 telnet 命令。



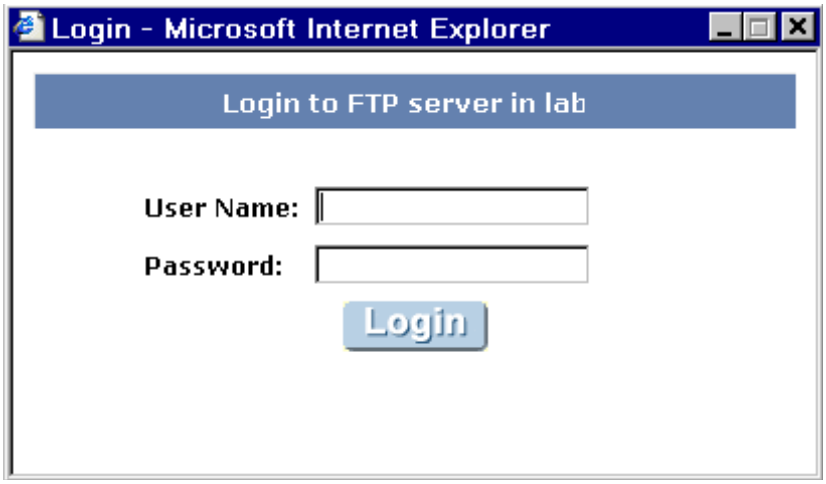
9. 点击“断开连接（或输入 exit）”，断开会话，并关闭 TELNET 连接窗口。

添加 FTP 连接并启动 FTP 会话

1. 点击“添加书签”。
2. 在“名称”字段，输入表示连接的名称。
3. 从“应用类型”列表中，选择 FTPt。
4. 在“主机名称/IP 字段”，输入 FTP 主机的 IP 地址作为根目录（例如，//10.10.10.10/）。

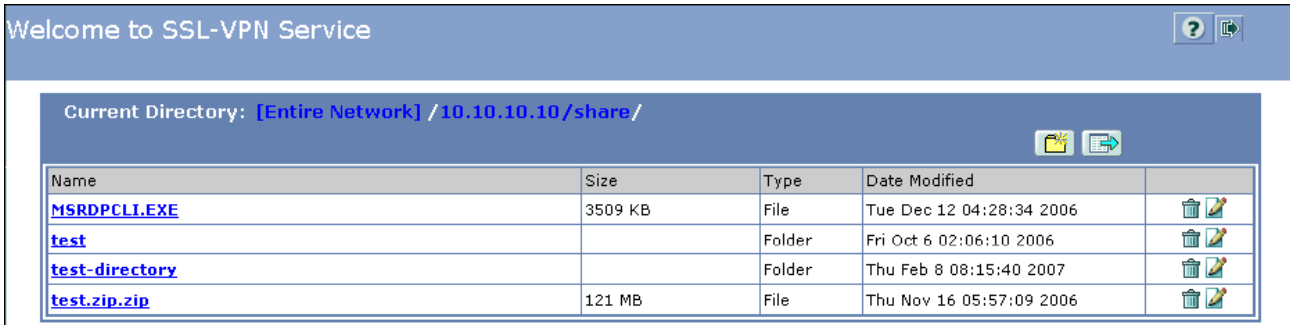


5. 点击 OK 确认。
6. 点击您创建的超级链接，启动 FTP 会话。
7. 提示您登录远程主机时，输入用户名与密码。您必须在登录的远程主机上具有用户帐户。



8. 点击“登录”。

登录后，显示根目录下的文件或子目录。您也可以从根目录切换到子目录。例如，以下镜像显示子目录的名称为“share（共享）”。



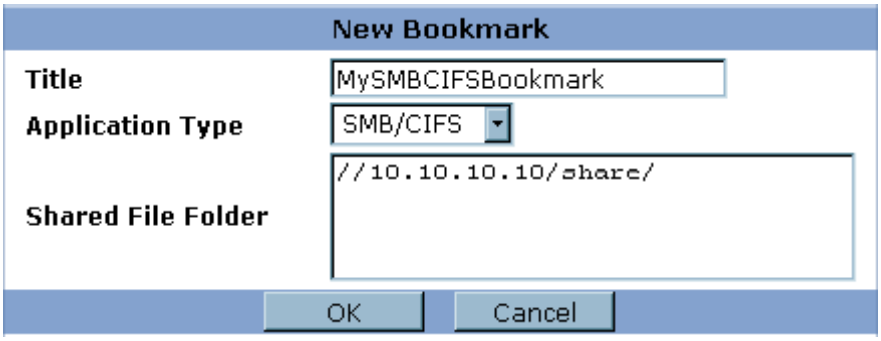
以上的显示页面中，通过以下方法可以对文件系统以及多个文件进行操作：

- 从当前目录中下载文件，从“名称栏”中选择文件链接。
- 点击“新建目录”，在当前的目录下创建子目录。
- 点击“删除”，从当前目录下删除文件或子目录。
- 点击“重命名”，在当前目录中重新命名文件。
- 在“名称”栏中选择文件的链接，从远程目录中选择文件上传到您用户端计算机设备中的当前目录下。
- 在“名称”栏中选择文件的链接，访问子目录。
- 在目前目录是子目录时，点击“上一级（Up）”可以切换到父目录。

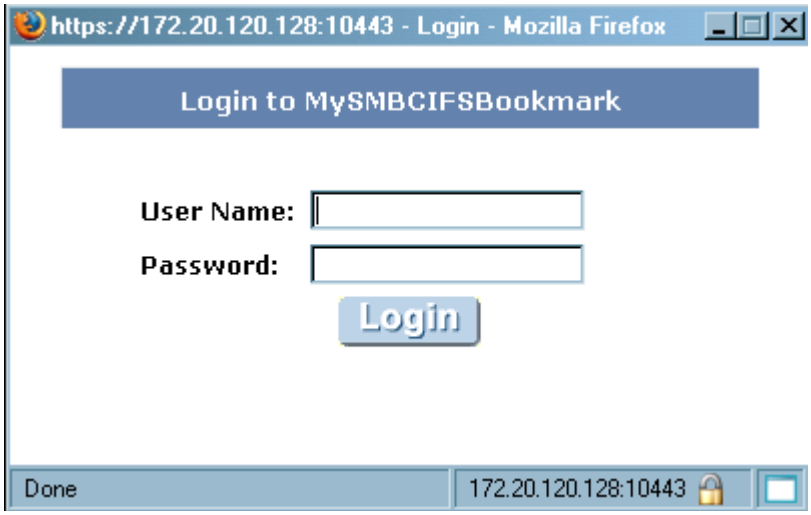
9. 点击“退出”结束 FTP 会话。

添加 SMB/CIFS 链接并启动 SMB 会话

1. 点击“添加书签”。
2. 在“名称”字段，输入表示该连接的名称。
3. 从”应用类型“列表，选择”SMB/CIFS“。
4. 在”共享文件文件夹“字段，输入 SMB 主机的 IP 地址以及与您帐户有关的根目录（例如，//10.10.10.10/share/）。

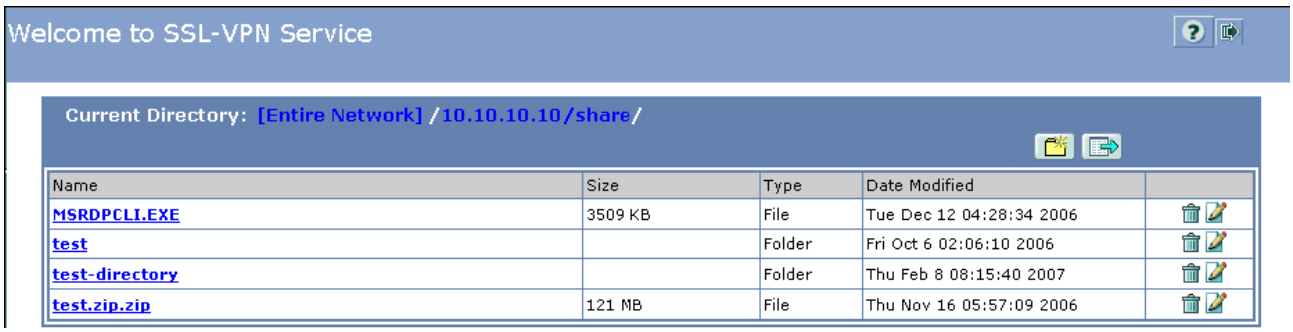


5. 点击 OK 确认。
6. 点击您所创建的超级链接，启动 SMB/CIFS 会话。
7. 提示您登录远程主机时，输入用户名与密码。您必须在登录的远程主机上具有用户帐户。



8. 点击“登录”。

登录后，显示根目录下的文件或子目录。您也可以从根目录切换到子目录。例如，以下镜像显示子目录的名称为“share（共享）”。



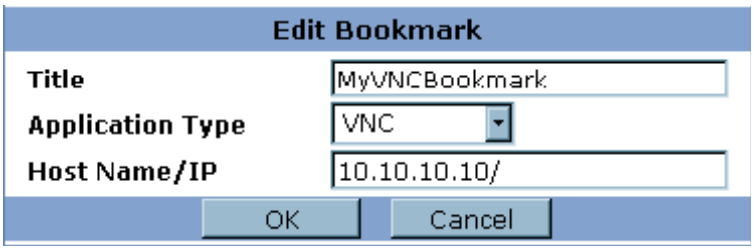
以上的显示页面中，通过以下方法可以对文件系统以及多个文件进行操作：

- 从当前目录中下载文件，从“名称栏”中选择文件链接。
- 点击“新建目录”，在当前的目录下创建子目录。
- 点击“删除”，从当前目录下删除文件或子目录。
- 点击“重命名”，在当前目录中重新命名文件。
- 在“名称”栏中选择文件的链接，从远程目录中选择文件上传到您用户端计算机设备中的当前目录下。
- 在“名称”栏中选择文件的链接，访问子目录。
- 在目前目录是子目录时，点击“上一级（Up）”可以切换到父目录。

9. 点击”退出“，结束 SMB/CIFS 会话。

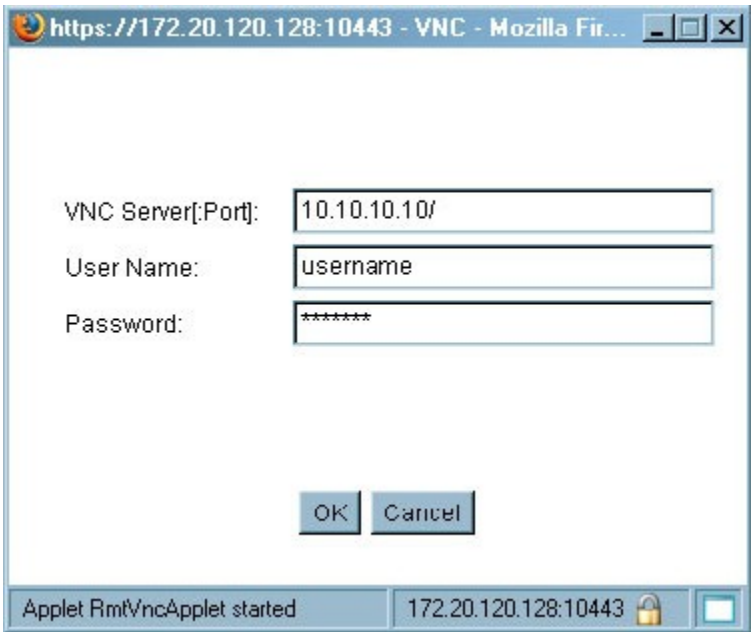
添加 VNC 连接并启动 VNC 会话

1. 点击“添加书签”。
2. 在“名称”字段，输入表示该连接的名称。
3. 从”应用类型“列表，选择”VNC“。
4. 在”共享文件文件夹“字段，输入 SMB 主机的 IP 地址以及与您帐户有关的根目录（例如，10.10.10.10/）。



5. 点击 OK 确认。

6. 点击您所创建的超级链接，启动 VNC 会话。
7. 提示您登录远程主机时，输入用户名与密码。您必须在登录的远程主机上具有用户帐户。



8. 点击“OK”确认。
9. 点击”断开连接“，结束 VNC 会话。

添加 RDP 连接并启动 RDP 会话

注意：建立 RDP 连接时，您可以设定键盘的布局设置作为参数。”RDP 到 Host“设置的格式为：

- ″yourserver.com-m fr″

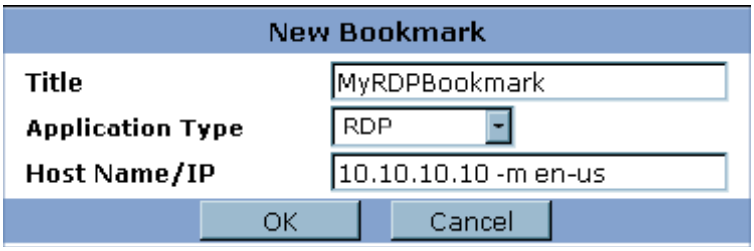
选择“fr”表示法语作为 windows 环境。选择与 windows 本地安装匹配的语言代码，例如，如果您本地设备上安装的是 windows 的土耳其语版本，不管您连接的服务器安装的 window 版本如何，选择“tr”。

以下代码分别表示：

- ar：阿拉伯语
- da：丹麦语
- de：德语
- en-bg:英式英语
- en-us：美式英语

- es:西班牙语
- fi：芬兰语
- fr：法语
- fr-be：比利时法语
- hr:克罗地亚语
- it:意大利语
- ja:日语
- it:立陶宛语
- lv:拉脱维亚语
- mk:马其顿语
- no:挪威语
- pl:波兰语
- pt:葡萄牙语
- pt-br:巴西葡萄牙语
- ru:俄语
- sl:斯洛文尼亚语
- sv:苏丹语
- tk:土库曼语
- tr:土耳其语

1. 点击“添加书签”。
2. 在“名称”字段，输入表示该连接的名称。
3. 从”应用类型“列表，选择”RDP“。
4. 在”共享文件文件夹“字段，输入 SMB 主机的 IP 地址以及与您帐户有关的根目录（例如，10.10.10.10）。

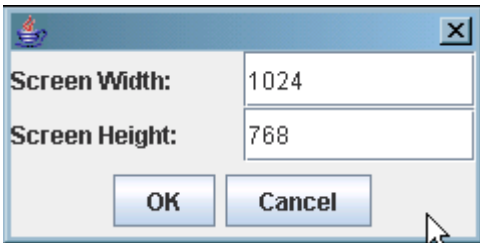


5. 点击 OK 确认。
6. 点击您所创建的超级链接，启动 RDP 会话。

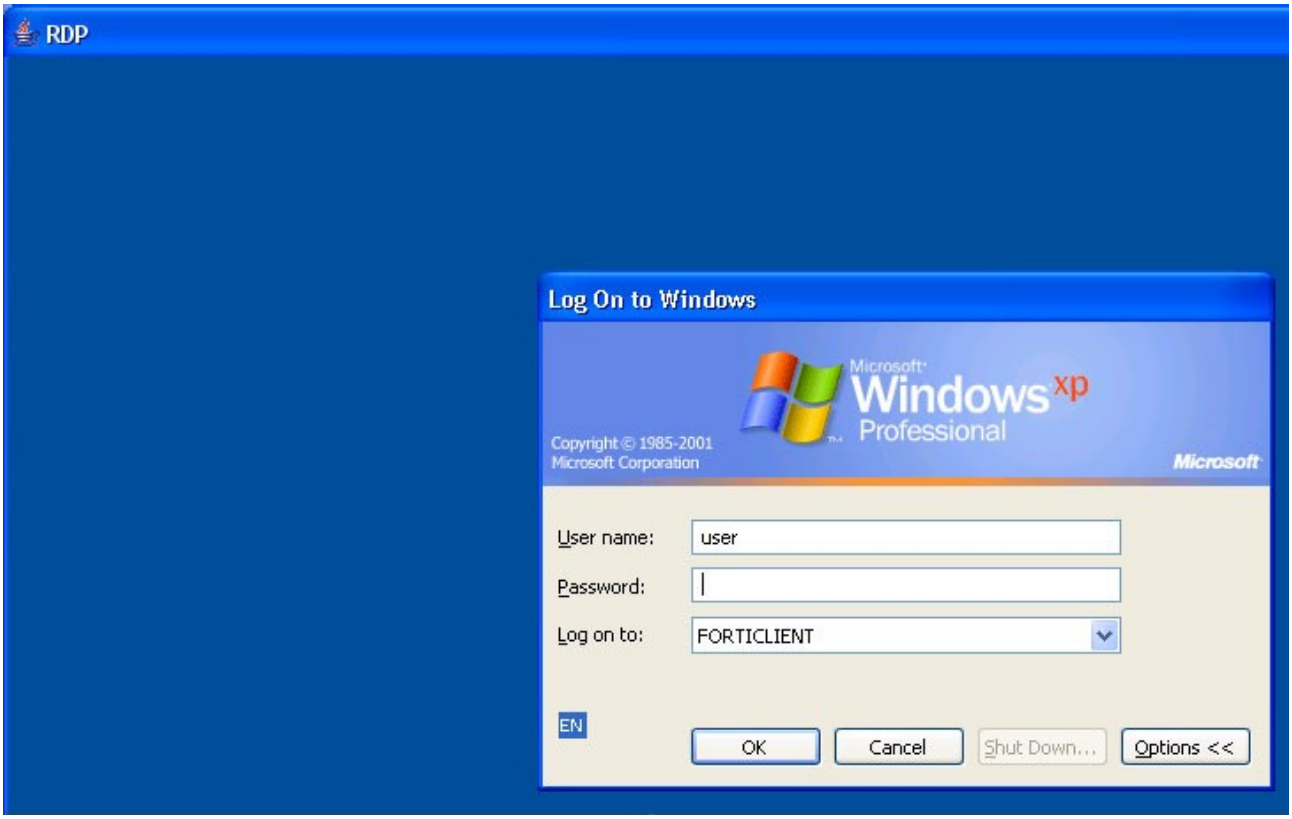
注意：FortiGate 设备可能呈现其自签安全证书。如果您执行，点击“是”。显示的第二项信息通知您主机名称不匹配。只所以显示该信息，是因为 FortiGate 设备试图重新定向您的 web 浏览器的连接。点击“是”执行操作。



7. 弹出屏幕配置对话框时，点击 OK 确认。



8. 提示登录远程主机时，输入用户名与密码。您必须在登录的远程主机上具有用户帐户。



9. 点击“登录”。

10. 点击“退出”，结束 RDP 会话。

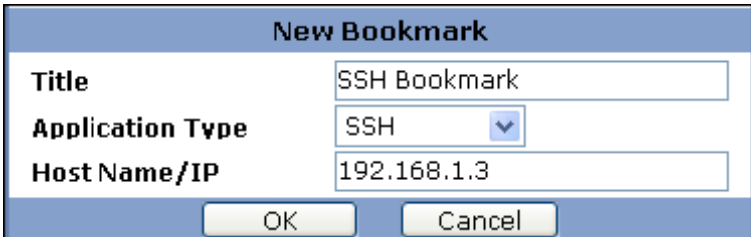
添加 SSH 连接并启动 SSH 会话

1. 点击“添加书签”。

2. 在“名称”字段，输入表示该连接的名称。

3. 从”应用类型“列表，选择”SSH“。

4. 在“主机名称/IP”字段，输入 ssh 主机的 IP 地址（例如，192.168.1.3）。



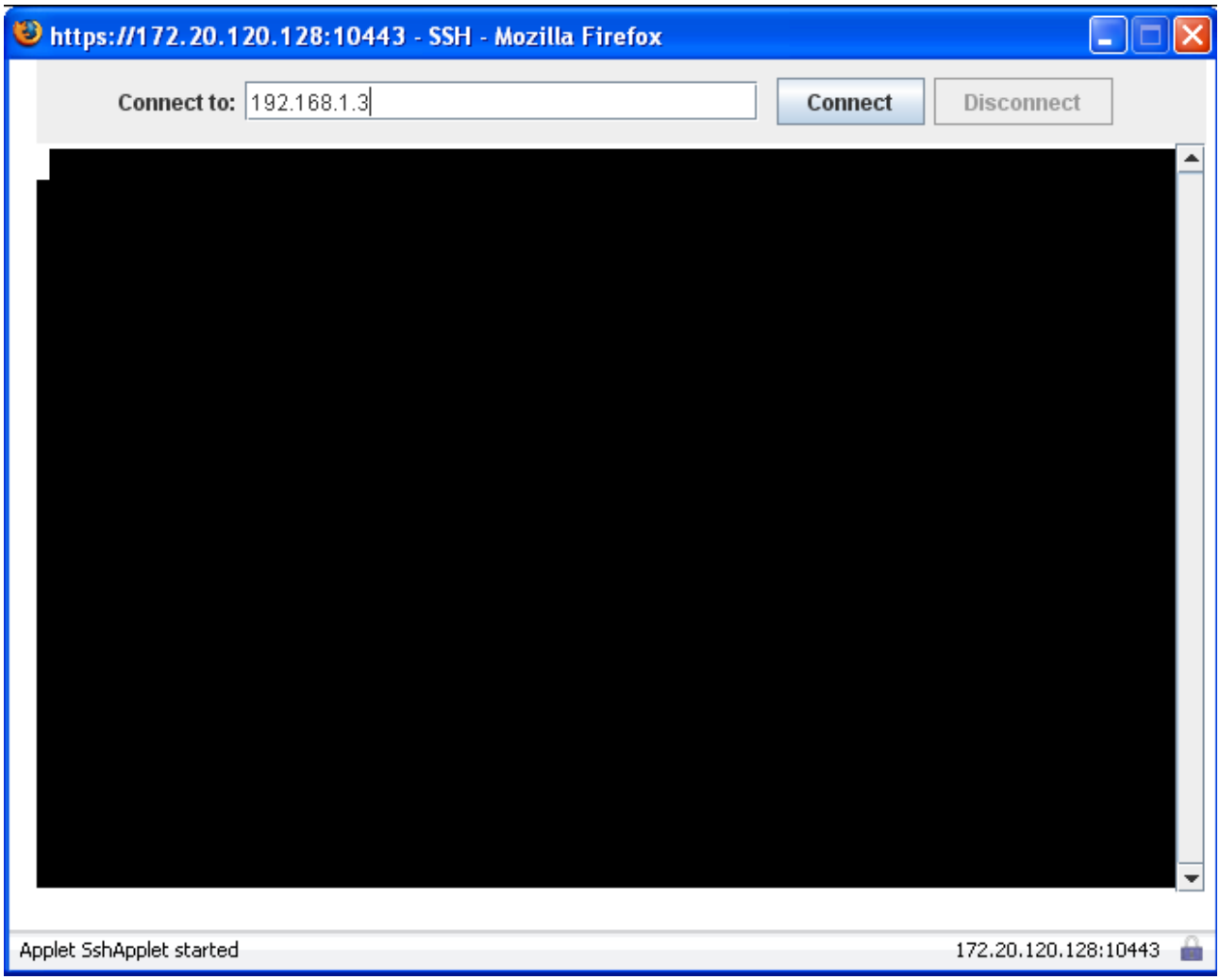
5. 点击 OK 确认。

6. 点击您所创建的超级链接，启动 ssh 会话。

注意：FortiGate 设备可能呈现可以自签安全证书。如果您执行，点击“是”。显示的第二项信息通知您主机名称不匹配。只所以显示该信息，是因为 FortiGate 设备试图重新定向您的 web 浏览器的连接。点击“是”执行操作。

7. 点击“连接”。

8. ssh 会话启动，系统提示登录远程主机。您必须在登录的远程主机上具有用户帐户。登录后，在系统提示符下您可以输入任何有效的命令。





9. 点击“断开连接”（或输入 exit）并关闭 ssh 连接窗口，结束会话。

从“工具”区域启动会话

在不添加任何书签在“我的书签”列表的情况下，您也可以连接到任何 web 服务器或 telnet 服务器。“工具”区域的字段中，您可以设置主机计算机设备的 url 或 ip 地址。如需要，您可以 ping FortiGate 设备之后的主机计算机设备校验与其的连接性。

通过“工具”页面连接到 web 服务器

1. 在“连接到 web 服务器”字段，输入 web 服务器的 url（例如,http://www.mywebexample.com 或 https://172.20.120.101）。
2. 点击“进入”。

FortiGate 设备将 url 替换为 http://<FG_IP_address>:<port_no>/proxy/http/<specified_url>,并显示所请求的页面。

3. 关闭浏览器窗口，结束会话。

Ping FortiGate 设备之后的主机

1. 在“测试可达性”字段，输入您要 ping 的主机或服务器的 IP 地址（例如，192.168.12.22）。
2. 点击“进入”。

显示说明该 IP 地址是否可达。

从“工具”区域启动 telnet 会话

1. 在“Telnet 到主机”字段，输入 telnet 主机的 IP 地址（例如，192.168.5.238）。
2. 点击“进入”。

注意：FortiGate 设备可能呈现可以自签安全证书。如果您执行，点击“是”。显示的第二项信息通知您主机名称不匹配。只所以显示该信息，是因为 FortiGate 设备试图重新定向您的 web 浏览器的连接。点击“是”执行操作。

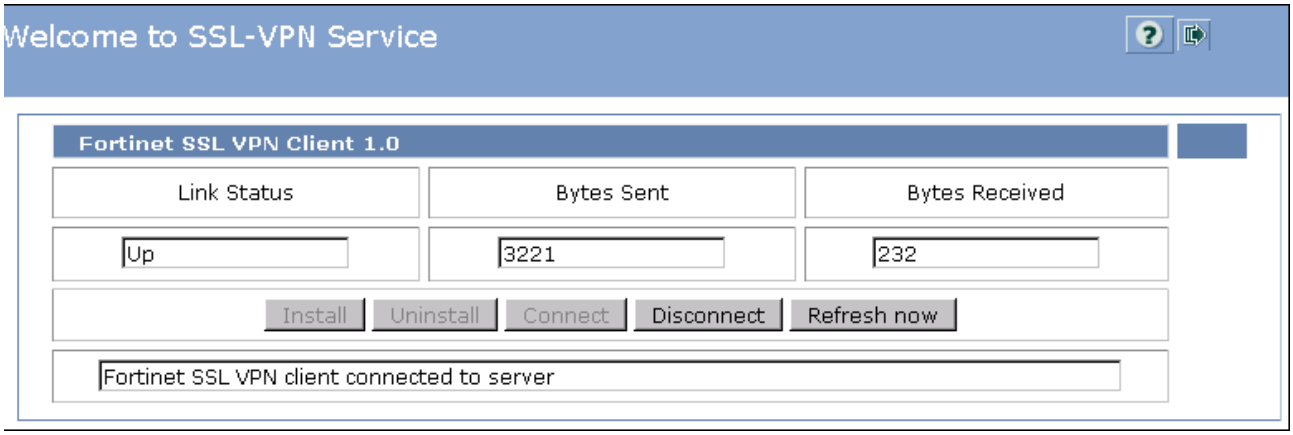
3. 点击“连接”。
4. telnet 会话启动且提示登录远程主机。您必须在登录的远程主机上具有用户帐户。登录后，在系统提示符下您可以输入任何有效的命令。
5. 点击“断开连接”（或输入 exit）并关闭 ssh 连接窗口，结束会话

通道模式功能

您在登录后，FortiGate ssl vpn 远程访问 web 入口网站。在主页中显示“Fortinet ssl vpn 用户”的区域，激活 ssl-vpn 通道模式链接。

如果您的用户帐户允许通道模式的连接，您可以安装/卸载 ssl vpn 用户软件和/或发起与 FortiGate 设备的 ssl vpn 通道连接。

图 22：Fortinet ssl vpn 用户端 1.0 页面（通道模式）



链接状态　　ssl vpn 通道状态：

- 当 ssl vpn 与 FortiGate 设备建立通道后，显示“启动（Up）”。
- 通道连接没有发起时，显示“关闭（Down）”。

发送数据量	自通道建立后，从用户端传输到 FortiGate 设备的数据量（字节）。
接收数据量	自通道建立后，用户端从 fortiGate 设备接收到的数据量（字节）。
安装	通道建立后，从 FortiGate 设备下载 ssl vpn 用户端软件。
卸载	卸载 Active X/Java 平台插件。
断开连接	结束会话并关闭与 FortiGate 设备的通道。
立即刷新	刷新 Fortinet ssl vpn 用户端页面。

安装ActiveX/Java平台插件

ActiveX/Java 平台插件提供用户端计算机设备与 FortiGate 设备建立 ssl vpn 通道所需的软件。在您的计算机设备与 FortiGate 设备建立 vpn 通道之前，需要从 FortiGate 设备下载该插件并将其安装在计算机设备中。有关下载与安装该插件的显示可以从 web 网页中 Fortinet ssl vpn 用户区域查看。

您只需要一次性安装 ActiveX/Java 平台插件。之后，无论何时访问 web 网站，均可以使用 ssl vpn 用户软件发起与 FortiGate 设备的 vpn 通道连接。

注意：在您的 web 浏览器中，查看并确定与互联网区域有关安全设置允许您下载并运行 ActiveX/Java 平台插件。安装 ActiveX/Java 平台插件，您也必须具有管理员的权限。

下载并安装 ActiveX/Java 平台插件

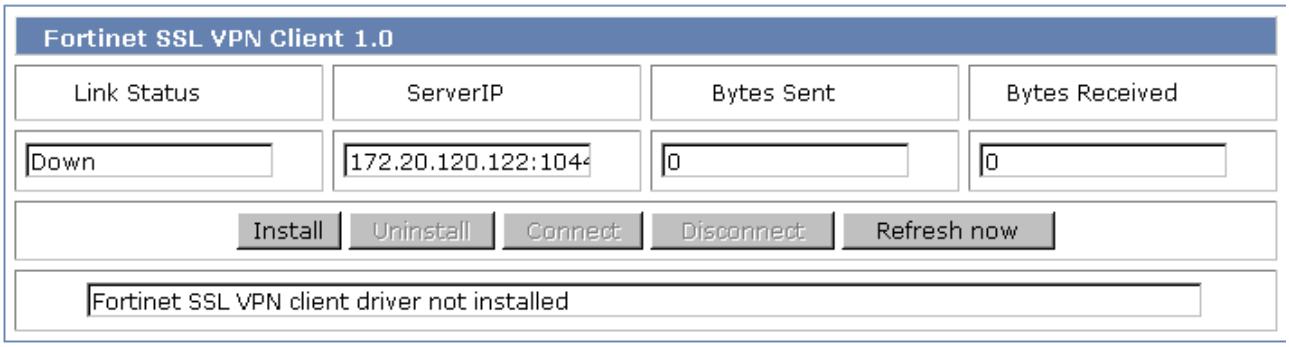
1. 在 web 网站主页面中，点击“激活 ssl vpn 通道模式链接”。



2. FortiGate 设备可能提示您安装 Fortinet ssl vpn 用户端插件。按照提示进行安装。

注意：windows xp Pack2 环境下，在屏幕顶端显示一个黄色的信号条，您必须点击它以表示接受 ActiveX/Java 平台插件的指导步骤。

Fortinet ssl vpn 用户 1.0 页面

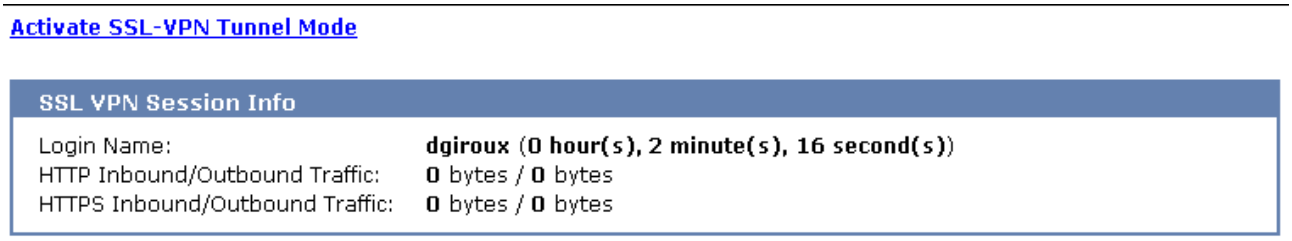


3. 点击“安装”。

发起与 FortiGate 设备建立 vpn 通道

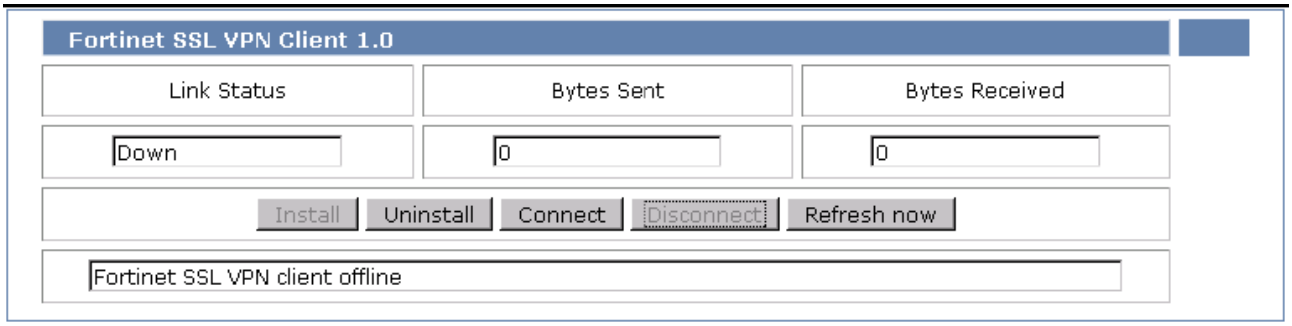
建立 ssl vpn 连接的 FortiGate 设备的公共接口 IP 地址与 TCP 端口号在 Fortinet ssl vpn 用户端软件页面中“服务器 IP 地址”字段中显示。

1. 在 web 网站主页面中，点击“激活 ssl vpn 通道模式链接”。



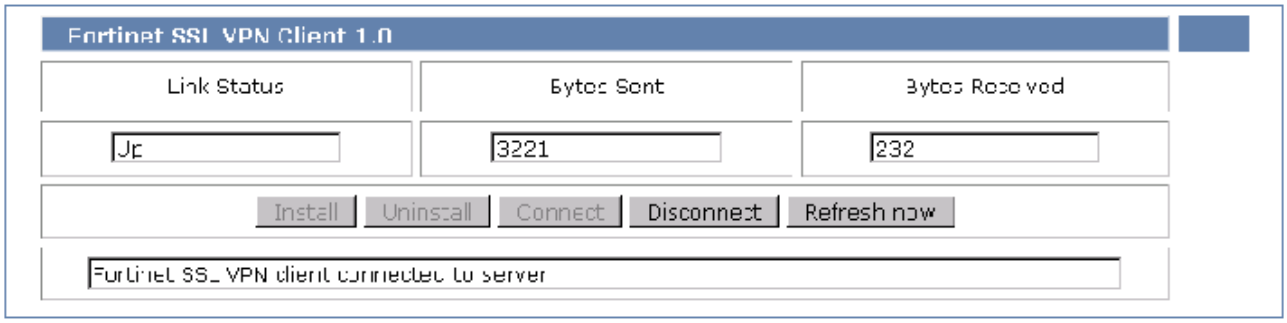
打开 Fortinet ssl vpn 用户端页面。

注意：如果您的帐户配置了用户安全查看，在启动“连接”之前，必须先完成安全查看操作。



2. 点击“连接”。

图 23：通道已建立



显示“Fortinet ssl vpn用户连接到服务器”的信息且在“断开连接”显示为可用时，您可以在FortiGate防火墙策略下直接访问FortiGate设备之后的网络。例如，使用您计算机设备中的用户应用，您可以连接到FortiGate设备之后网络的服务器应用，并下载信息。

点击“断开连接”，可以结束ssl vpn会话并断开与FortiGate的连接。您必须从web网页中退出才能断开与FortiGate设备连接。当然，您可以点击“连接”，重建建立通道的连接。

卸载ActiveX/Java平台插件

卸载ActiveX/Java平台插件

注意：如果您想安装更新后的版本，不需要先卸载ActiveX/Java平台插件。FortiGate设备获得可用的更新ActiveX/Java平台插件版本后，会自动进行安装。

1. 在web网站主页面中，点击“激活ssl vpn通道模式链接”。
2. 点击“卸载”。

退出

点击web主页右上角的“退出（Logout）”图标，退出web页面的登录。

