

V3.0 FortiGate 设备 VLAN 与 VDOM 用户使用与配置手册

FORTINET

目录

FortiGate设备VLAN与VDOM配置简介 6
VLAN概述 6
Layer-2 VLAN的数据交换 7
Layer-2 VLAN应用示例 7
Layer-3 中VLAN的路由应用 9
Layer-3 中应用VLAN的示例 9
VLAN ID设置规则 10
虚拟域概述 11
VDOM的最大设置数量 11
VDOM间的路由 11
管理虚拟域 12
虚拟域的管理 12
全局配置与虚拟域设置 12
详细信息 15
NAT/路由模式下使用VLAN 16
概述 16
NAT/路由模式下配置FortiGate设备 16
添加VLAN子接口 17
添加防火墙策略 17
配置路由 18
NAT/路由模式下的VLAN配置举例（简单配置） 18
常规配置步骤 19
配置FortiGate-800 设备 20
配置外部接口 20
添加VLAN子接口 21
添加防火墙地址 22
添加防火墙策略 24
配置Cisco交换机支持VLAN标签 28
测试配置 29
运行NAT/路由模式下的配置举例（复杂） 31
常规配置步骤 33
配置FortiGate-800 设备 33
添加VLAN子接口 33
添加默认路由 36
添加防火墙地址 37
添加防火墙策略 38
配置FortiGate-800 设备的IPSec通道与加密策略 44
配置VPN网关 44
配置VPN通道 45
定义VPN用户IP地址 47

添加加密策略.....47
配置VPN用户端.....49
配置内部Cisco交换机.....51
配置外部交换机.....52
测试配置.....53
NAT/路由模式下使用VDOM.....55
概述.....55
启动虚拟域.....55
启动虚拟域配置.....55
创建虚拟域.....56
创建虚拟域.....56
获得VDOM许可证密钥.....56
创建虚拟域的管理员.....57
访问并配置虚拟域.....57
配置虚拟域.....58
更改管理虚拟域.....58
对虚拟域添加接口与VLAN子接口.....59
对虚拟域配置路由.....60
对虚拟域配置防火墙策略.....60
对虚拟域配置VPN.....61
NAT/路由模式下配置虚拟域举例（简单）.....61
常规配置步骤.....62
创建虚拟域.....63
配置FortiGate-800 设备的外部与DMZ接口.....63
配置外部接口.....64
配置DMZ接口.....64
配置ABC虚拟域.....65
添加VLAN子接口.....65
添加ABC虚拟域防火墙地址.....67
添加ABC虚拟域的防火墙策略.....68
添加默认路由.....69
配置DEF虚拟域.....70
添加VLAN子接口.....70
添加DEF虚拟域防火墙地址.....71
添加DEF虚拟域的防火墙策略.....72
添加默认路由.....74
配置Cisco交换机.....75
测试配置.....75
测试VLAN100 到外部网络的流量.....76
测试从VLAN200 到DMZ网络的流量.....76
运行于NAT/路由模式下的虚拟域配置（复杂）.....77
常规配置步骤.....79
创建虚拟域.....79
配置ABC虚拟域.....80

选择ABC虚拟域 80
添加VLAN子接口 80
添加默认路由 83
添加防火墙地址 84
添加防火墙策略 85
配置Commercial虚拟域 89
选择Commercial虚拟域 89
添加VLAN子接口 89
添加默认路由 92
添加防火墙地址 94
添加防火墙策略 95
配置Cisco交换机 102
测试配置 104
其它测试 105
透明模式下应用VLAN与VDOM 106
概述 106
VLAN与虚拟域 106
配置运行于透明模式下的FortiGate设备 107
添加VLAN子接口 107
创建防火墙策略 108
透明模式下配置举例（简单） 108
常规配置步骤 109
配置FortiGate-800 设备 110
添加VLAN子接口 110
添加防火墙策略 112
配置Cisco交换机 116
配置VLAN子接口与trunk接口 116
配置Cisco路由器 117
配置VLAN子接口与trunk接口 117
测试配置 118
测试VLAN100 到VLAN200 的流量 118
透明模式下配置多个虚拟域举例 119
配置全局设置项 119
创建时间表 119
创建内容保护内容列表 120
创建虚拟域 123
配置ABC虚拟域 124
添加VLAN子接口 124
进入ABC虚拟域配置页面 125
创建服务组 126
配置ABC虚拟域的防火墙地址 126
配置ABC虚拟域的防火墙策略 127
配置DEF虚拟域 130
添加VLAN子接口 130

进入DEF虚拟域配置页面 131
创建服务组 131
配置DEF虚拟域的防火墙地址 132
配置DEF虚拟域的防火墙策略 132
配置XYZ虚拟域 136
添加VLAN子接口 136
进入XYZ 虚拟域配置页面 138
创建服务组 138
配置XYZ虚拟域的防火墙地址 139
配置XYZ虚拟域的防火墙策略 139
配置Cisco交换机 142
配置交换机 1 142
配置交换机 2 143
测试配置 143
测试VLAN100 到互联网的流量 143
VDOM间的路由 145
概述 145
实现VDOM间路由的好处 145
解放了物理接口 145
传输速度比物理接口快 146
仍然能够使用安全的防护墙策略 146
更多的配置灵活性 146
开始配置VDOM间路由 147
高级VDOM间路由的有关问题 148
VDOM间的高级路由 148
HA虚拟群集与VDOM间的链接 148
FortiManager与VDOM间的路由 149
使用FortiManager配置VDOM间的路由 149
VDOM间的路由配置 150
单个VDOM配置 150
独立的VDOM配置 151
管理VDOM的配置 151
网状VDOM配置 152
VDOM间的路由规划 153
避免使用VLAN带来的问题 153
不均衡的路由 153
Layer-2 流量 154
ARP流量 154
多个VDOM的解决方案 155
转发域的解决方案 155
NetBIOS 156
STP转发 156
太多的VLAN接口 157

FortiGate 设备 VLAN 与 VDOM 配置简介

虚拟本地局域网络（VLAN: Virtual Local Area Networks）与虚拟域（VDOM:Virtual Domains）配置增强了 FortiGate 设备性能。VLAN 应用对网络中传输的数据包标记 ID 的功能，增加了除 FortiGate 设备物理接口以外的网络接口数量。VDOM 的配置可以使 FortiGate 设备作为多个独立运行的安全设备执行常规的管理功能。VLAN 与 VDOM 均可以增强网络的安全性。

应用 VLAN，单个 FortiGate 设备可以在多个安全域之间提供安全服务并控制连接。VDOM 可以使单个的 FortiGate 设备服务于多个公司，提供独立的防火墙策略，并且在 NAT/路由模式下，对每个服务对象提供完全独立的路由与 VPN 配置。

本手册就如何将运行于 NAT/路由模式与透明模式下的 FortiGate 设备应用 IEEE 802.1Q 虚拟 LAN（VLAN）技术进行说明。并适用配置范例示出 VLAN 是如何在 FortiGate 设备与其他 802.1Q 兼容的设备如 Cisco 交换机与路由器之间应用实施的。本手册还将如何应用虚拟域（VDOM）以及示范如何在 FortiGate 设备中配置 VDOM。

本手册中所述内容可以应用于全部 FortiGate 设备。所有型号的 FortiGate 设备均支持 VLAN 与 VDOM。本章包括以下内容：

- VLAN 概述
- VDOM 概述
- NAT/路由模式下使用 VLAN
- NAT/路由模式下使用 VDOM
- 透明模式下使用 VLAN 与 VDOM
- VDOM 间的路由
- VLAN 使用中应避免的问题

详细信息以及配置示例参见每章中的具体内容。

VLAN 概述

一个 LAN 是由网络广播域组成的。一个网络广播域包括在广播域中从任何计算机设备接收数据包广播的所有计算机。交换机自动将数据包转发到所有与交换机连接的接口，但是分离广播域的默认路由器不自动转发数据包。如果一个网络中只有交换机没有路由器，那么不管该网络覆盖的范围多大，都被作为一个广播域来考虑。

虚拟 LAN（VLAN）使用 ID 标签将一个 LAN 中从逻辑上划分为更小的广

播域。每个 VLAN 是一个独立的广播域。较小的广播域分流并减少了流量，增强了网络的安全性。IEEE 802.1Q 标准中定义了 VLAN。网络中第二与第三层的设备必须兼容 802.1Q 以便支持 VLAN 的应用。

VLAN 通过只对属于各自 VLAN 的端口或其主干网络转发数据包从而缩小了广播域的范围。主干网络是指交换机与交换机，或交换机与路由器之间的连接，并转发全部的 VLAN 流量。这样，一个 VLAN 可以包含逻辑上属于同一网络但是物理距离相差很远的设备。

任何虚拟域在 NAT 或 TP 模式下最多可以配置 255 个接口，包括 VLAN、其他虚拟接口与物理接口。如果需要配置多于 255 个接口时，您需要设置添加多个 VDOM，并在每个 VDOM 中配置多个接口。

VDOM 典型的应用举例是在一个公司的会计部分。会计用计算机设备可以安置在不同的办公地点（总公司或分公司）。实际情况是会计部分的计算机设备之间需要实现相互通信并且能在足够安全的环境下进行。VLAN 的应用能够实现会计数据只在会计部门的网络计算机内传播，即使是不在相同物理位置的属于会计部门的计算机网络内传播。

用于定义 VLAN 的 ID 标签是一个 4 比特的域扩展，应用于经由交换机与路由器之间的 VLAN 中各设备发送与接收的数据包。工作站与桌面计算机设备均不是 VLAN 操作过程中的参与部分---也就是说所有加上与去除 VLAN ID 标签的操作都是在数据包离开计算机设备后完成的。

**注意：**本手册所指数据包是网络第二与第三层中传递的数据包。

Layer-2 VLAN的数据交换

交换机通常情况下兼容 802.1Q---它们是第二层（Layer-2）的网络设备。Layer-2 指 OSI 网络模型中的第二层---数据链路层。当 FortiGate 设备运行于透明模式下时作为第二层的交换机，只执行标记 VLAN ID 标签并转发 VLAN 数据量或移出标签的操作。

一个 VLAN 可以被分配应用很多物理接口。物理接口可以被分配到多个 VLAN 中。通常情况下，一个 VLAN 可以配置很多物理接口，但至少要分配两个物理接口---至少一个用于接收数据，另一个用于发送数据。FortiGate 设备可以配置使用多个 VLAN，包括主干链路。

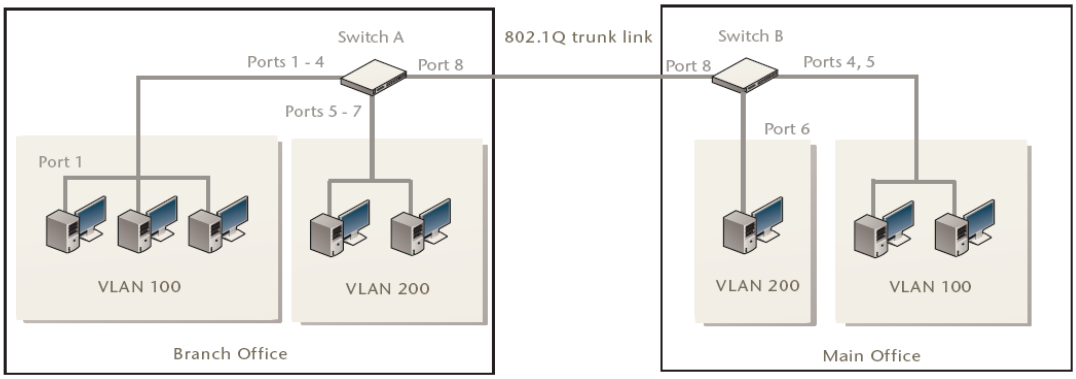
主干链路是指通过所有 VLAN 流量中交换机与路由器之间的连接，通过这些连接数据包才可以到达网络的其它部分。交换机与路由器只是起传递 VLAN 流量到指定目的地的作用，并不能引起网络溢流。

Layer-2 VLAN 应用示例

为了更好的理解 VLAN 的操作，参见以下在网络中应用 VLAN 的举例。

两个 8 个端口的交换机配置在网络中支持应用两个 VLAN。子网 1 连接到交换机 A，子网 2 连接到交换机 B。交换机 A 中，端口 1 到 4 是 VLAN100 的一部分。两个交换机的端口 8 都连接着 8.02.1Q 主干链路。交换机 A 的其它端口（端口 5 到 7）属于 VLAN200。交换机 B 中，端口 4 与 5 是 VLAN100 的一部分，端口 6 属于 VLAN200。交换机 B 中还存在没有分配使用的端口。

图 1：VLAN 在 Layer-2 的配置示例



让我们从子网 1 中计算机发送的数据讲起，子网 1 是 VLAN100 的一部分。

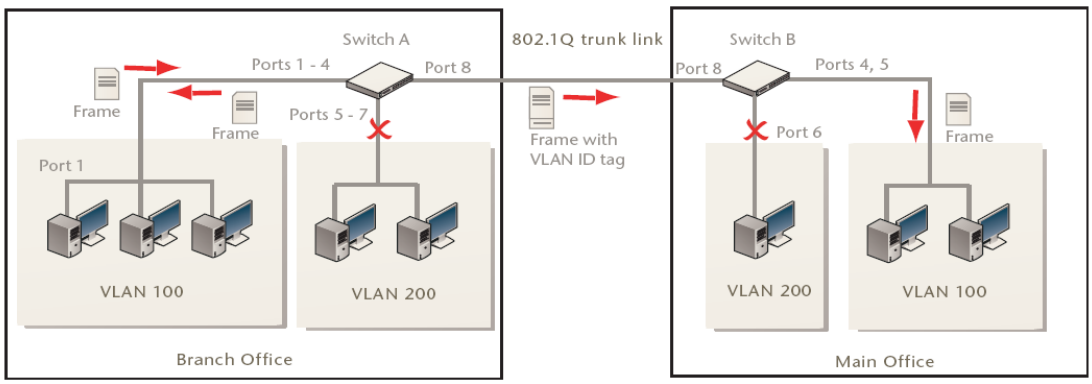
连接交换机 A 端口 1 的计算机设备发送了数据流。因为端口 1 属于 VLAN100，交换机 A 在数据到达时对其标记上 VLAN100 ID 标签。然后将标记的数据转发到其它 VLAN100 端口（端口 2 到 4），同时也将数据转发到 802.1Q 主干链路（端口 8），那么属于 VLAN100 组的其他网络部分将接收到名为 VLAN 100 的数据流量。

该数据将不会被转发到交换机 A 的其它端口，因为这些端口并不属于 VLAN100。这样便增强了网络的安全性并减少了网络数据流。

交换机 B 通过主干链路接收到数据。交换机 B 的端口 4 与 5 属于 VLAN100，所以数据也将转发到这些端口。即使通过交换机 A，数据也不会转发到 VLAN200。

如果交换机 B 中没有属于 VLAN100 的端口，交换机将不转发这些数据，那么数据将停滞在那。

图 2：VLAN 在第二层网络结构中应用时数据包的传输示例



在一台交换机将数据包转发到目的地之前，数据包的 VLAN 的 ID 标签将被删除。数据包的发送端与接收端将不会对这样的删除动作有任何的察觉与反应。也就是说，任何目的地计算机接收到的数据包是正常形式的。

Layer-3中VLAN的路由应用

路由器是第三层（Layer-3）网络中的设备。Layer-3 是指 OSI 网络模型中的第三层---网络层。运行于 NAT/路由模式的 FortiGate 设备可以作为第三层网络设备。与链路层相比，FortiGate 设备作为 Layer-3 设备也是兼容 802.1Q 的。

Layer-2 与 Layer-3 层设备的主要不同在于怎样处理 VLAN 标签。Layer-2 交换机只是添加、读取以及删除标签，并不进行更改标签或进行更高级别的动作。Layer-3 设备并不执行添加、读取以及删除标签动作，但是可以进行数据包及其内容的分析。这样的分析动作便允许 Layer-3 路由器在适当情况下更改 VLAN 标签后将数据包发送到不同的 VLAN。

在 Layer-3 网络环境中，兼容 802.1Q 的路由器接收数据包并分配标记 VLAN ID。路由器然后将数据包转发到其它具有相同 VLAN 广播域的成员。广播域可以包括本地端口、Layer-2 与 Layer-3 层的设备如路由器与防火墙设备。当一个 Layer-3 的设备接收到数据包时，该设备将数据包的 VLAN 标签删除并查看其内容，决定如何处理数据包。Layer-3 设备将查看数据包的以下方面：

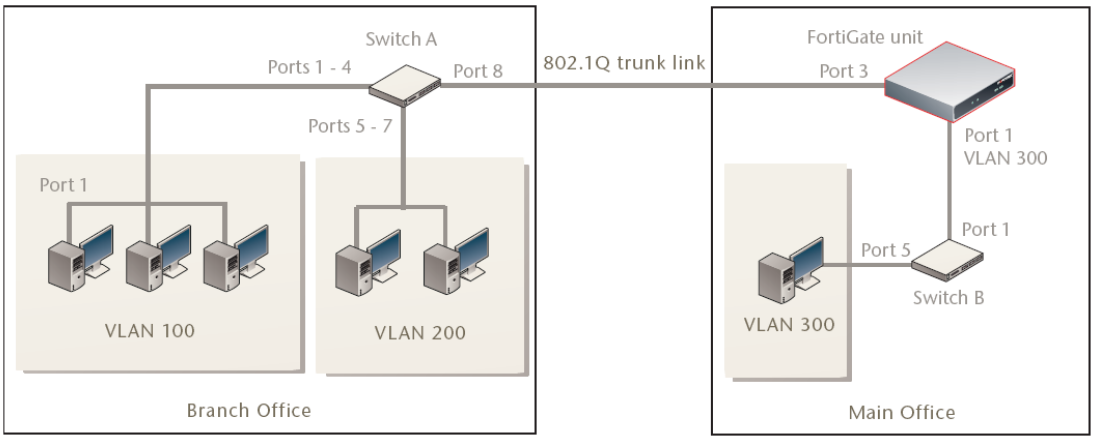
- 源与目标地址
- 传输协议
- 传输端口

经过以上动作，数据包也许会转发到其它 VLAN，发送到常规非标记 VLAN ID 的网络或只是转发到与 Layer-2 的交换机相同的 VLAN。

Layer-3 中应用 VLAN 的示例

在该配置举例中，子网 1 与之前 layer-2 中的相同。在子网 2 中，交换机 B 的端口 5 与 VLAN300 连接。FortiGate 设备的端口 1 连接着交换机 B，端口 3 与交换机 A 连接，连接着主干链路。交换机 B 中的其它端口没有进行分配。该配置如下图 3 所示：

图 3：VLAN 在 layer-3 中的路由应用



该示例说明了从VLAN100中发出的数据如何到达VLAN300中的目标地址。Layer-2 交换机单独并不能完成该过程，但是 layer-3 中的路由器可以实现这样的操作。我们使用分公司网络中 VLAN100 发送的数据包如何到达主办公区中的VLAN300 来说明。

在 layer-2 的举例中，VLAN100 中的计算机设备发送数据包到交换机 A，并被添加了 VLAN 100 标签。交换机 A 将标记过的数据包通过主干链路转发到FortiGate 设备。FortiGate 设备删除 VLAN100 标签并根据数据包的内容选择正确的防火墙策略。

在该示例中，FortiGate 设备的防火墙策略将允许数据包继续传输到VLAN300。该数据包将到达 VLAN300 的全部接口，但是在示例中只列出了FortiGate 设备的一个端口，端口 1。在数据包离开 FortiGate 设备之前，VLAN子接口将对数据包添加一个 VLAN ID300 的标签。

然后，FortiGate 设备将数据包转发到交换机 B。因为交换机 B 将是路由的最后一跳，数据包的 VLAN 1D300 标签将被删除然后被发送到计算机端口 5。

在该示例中，数据包在到达 FortiGate 设备时仍然标记着 VLAN100 的标签，在设备对其内容进行查看后，解除标记并发送到 VLAN300。数据包从 VLAN100到 VLAN300 的传输过程中，数据包的标记与解除需要 layer-3 路由设备来执行，layer-2 中的交换机设备不能执行该更改数据包标签更改的操作。

VLAN ID设置规则

Layer-2 中的交换机设备与 Layer-3 的设备在数据包到达时添加 VLAN ID 标签操作，并在数据包传输到目标地址之前删除 VLAN ID 标签。网络中的其它设备，如 PC 机与服务器对于 VLAN 的应用不需要进行任何特殊的配置。

对于 Layer-2 的交换机，您可以只在每个物理接口中配置一个 VLAN 子接口，除非该接口将配置作为一个主干链路接口。主干链路可以传输不止一项 VLAN数据包到网络的其它部分。

一台 FortiGate 设备中，对于同一个物理接口可以应用到多个 VLAN。但是，添加到同一物理接口的两个 VLAN 子接口不能拥有相同的 VLAN ID 或相同子网的 IP 地址。您可以在不同的物理接口上添加两个或更多的 VLAN 子接口使用相

同的 VLAN ID。

使用相同的 VLAN ID 创建的 VLAN 子接口之间不能建立任何的内部连接。例如，创建端口 1 中的 VLAN ID300 与端口 2 中的 VLAN ID300 是允许的，但是它们之间不能够存在连接，他们之间的关系与任何两个 FortiGate 网络接口之间的关系相同。

虚拟域概述

虚拟域的应用可以将 FortiGate 设备配置作为多个独立的设备。您可以单独扩展并管理每个虚拟域的接口、VLAN 子接口、区域、防火墙策略、路由以及 VPN 配置。虚拟域的设置简化了管理配置，您不需要一次性管理许多的路由与防火墙策略。

应用虚拟域的功能之一，便是使用一台 FortiGate 设备对几个对象的网络提供路由与网络防护功能。每个对象都有属于自己的网络接口（物理接口或虚拟接口）、路由要求与网络防护规则。默认的情况下，这些机构之间的通信只有在其相互都允许要外部网络（如互联网）访问的情况下才能够实现。在本章中“在 NAT/路由模式下使用 VDOM”一节的叙述中举例说明了以上情况。

当一个数据包进入 FortiGate 设备中的某个虚拟域时， 它将被限制在这个虚拟域中。在一个给定的域中，您只能够对 VLAN 子接口与区域之间的连接创建防火墙策略。数据包不能够跨越域的边界。

VDOM的最大设置数量

如果 FortiGate 设备中启动了虚拟域配置，您可以使用默认的 admin 管理员登录，访问“系统>状态”在“许可证信息”项目栏中查看 FortiGate 设备所支持的允许配置虚拟域的最大数量。默认情况下，不管是运行于 NAT/路由还是透明模式的 FortiGate 设备支持最大设置 10 个虚拟域。对于 FortiGate-3000 或更高型号的 FortiGate 设备，您可以购买许可证密钥将 VDOM 的设置数量增加到 25，50，100 或 250 个。详细信息，参见“创建虚拟域”。

VDOM间的路由

FortiOS v3.0MR1 开始增加了一项有关虚拟域设置的新功能，名为“VDOM 间的路由”。配置了该功能后，VDOM 之间可以相互通信，并不像之前如果要实现 VDOM 之间的路由，流量必须从 FortiGate 设备的一个物理接口发送并通过不同的物理接口返回。VDOM 间的路由功能可以使您分辨限于两个 VDOM 的相互连接与所有 VDOM 均参与的连接。VDOM 之间的所有流量是通过外部接口的连接，所以必须通过防火墙策略。

配置该功能的命令，称为 vdom-link，只有在 CLI 中可用。使用基于 web 的管理器不能配置 VDOM 之间的通信。详细信息参见 FortiGate 设备 CLI 使用参考手册。

管理虚拟域

FortiGate 设备所有的管理流量均要通过管理虚拟域。包括所有的外部连接、远程管理与其它 Fortinet 的服务。默认情况下，管理虚拟域是 root（根）虚拟域。您也可以更改该管理域为其他的 VDOM，那么所有的流量都要先通过所更改的新的管理 VDOM。

虚拟域的管理

您可以使用一个常规管理员或对每个 VDOM 设置的多个独立的管理员管理虚拟域。

FortiGate 设备默认的管理员帐户为 admin 帐户。该帐户是常规管理员帐户能够访问 FortiGate 设备中所有的虚拟域。Admin 管理帐户不可以删除。

您可以登录 admin 管理帐户创建常规管理员帐户并将其分配到 VDOM 中。每个常规管理员只能够配置属于其的 VDOM。全局配置影响全部的 VDOM。只有使用 admin 帐户才能够配置全局属性。

管理员的访问权限可以配置为只读或读/写皆可的。管理员可以访问：

- 系统配置
- 安全策略
- 管理员配置
- 配置备份/恢复
- 日志与报告
- 用户验证
- FortiGuard 更新

那么，每个 VDOM 虚拟域的管理员便可以对不同的服务进行管理。例如，您可以设置管理员在一个 VDOM 中负责日志记录与报告，其他的管理员在同一个 VDOM 中负责安全策略。

当您使用 admin 帐户配置 VDOM 时，基于 web 的管理器 GUI 中左下角将显示您所编辑的 VDOM。如果您在配置全局属性，将没有标记可显示。

全局配置与虚拟域设置

配置使用虚拟域后，需要记住哪些设置是需要对单个 VDOM 配置，哪些是可以通过全局配置进行设置。

以下配置虚拟域配置中唯一性的设置，不能够在不同的虚拟域之间共享。

系统设置

- 区域
- DHCP 服务
- 操作模式（NAT/路由模式或透明模式）
- 管理 IP（透明模式）

路由配置

- 全部

防火墙设置

- 策略
- 地址
- 服务组与用户定义服务
- 时间表
- 虚拟 IP
- IP 池

用户设置

- 用户
- 用户组
- RADIUS 与 LDAP 服务器

VPN

- IPSec
- PPTP
- SSL
- L2TP
- 策略下载

IM 设置

- 统计表
- 用户列表与策略

共享配置设置：

所有的虚拟域共享以下配置设置。即使您配置了多重虚拟域，配置以下设置的方法是不变的：

系统设置

- 物理接口与 VLAN 子接口（每个物理接口或 VLAN 子接口只属于一个 VDOM。每个 VDOM 可以使用或配置属于其的接口。）
- DNS 设置
- 主机名称
- 系统时间
- 固件版本
- 闲置与验证超时
- web 管理器的语言设置
- 失效网关检测
- HA 配置
- SNMP 配置
- 替换信息
- 管理员
- 访问权限
- FortiManager 配置
- 配置备份与恢复
- FDN 更新配置
- Bug 报告

防火墙设置

- 预定义服务
- 保护内容表

IPS 设置

- 全部

反病毒设置

- 全部

Web 过滤配置

- 全部

垃圾邮件过滤配置

- 全部

日志配置与日志报告

- 全部

详细信息

有关虚拟域的详细信息与操作，参见“在 NAT/路由模式下使用 VDOM”与“在透明模式下使用 VDOM”。

NAT/路由模式下使用 VLAN

概述

NAT/路由模式下，FortiGate 作为 3 层设备控制多个 VLAN 之间的数据包流。FortiGate 设备也可以删除向内的 VLAN 数据包的 VLAN 标签，也可以将没有标签的数据包转发到其它网络，如互联网。

NAT/路由模式下，FortiGate 设备支持 IEEE 802.1Q 交换机（或路由器）与 FortiGate 设备之间创建 VLAN trunk。主干链路在物理子网或网络之间传送被标记的 VLAN 数据包。当您在 FortiGate 设备的物理接口添加 VLAN 子接口时，VLAN 子接口发出的数据包便具有了与主干链路中的数据包的 VLAN ID 相匹配的 ID。FortiGate 设备将与子接口 ID 匹配的数据包发送。

通常情况下，FortiGate 设备的内部接口连接着一个 VLAN trunk，外部接口连接着一个不执行标注功能的互联网路由器。这样的配置下，FortiGate 设备可以对与内部接口连接着每个 VLAN 的流量应用不同的防火墙策略。

您可以在 FortiGate 设备所有的接口上定义 VLAN 子接口。 但是，如果在 FortiGate 设备上配置了多个虚拟域，您只能访问您所在虚拟域的物理接口。FortiGate 设备可以对通过 VLAN 子接口的数据包上添加 VLAN 标签，或从流入的数据包中删除 VLAN 标签并同时在流出的数据包上添加不同的 VLAN 标签。

NAT/路由模式下配置 FortiGate 设备

您可以通过与 FortiGate 设备接口连接的支持 web 浏览器的管理计算机上访问 FortiGate 设备基于 web 管理器。该接口必须配置了管理访问。使用 HTTPS 访问接口的地址。默认情况下，所有的设备接口都启动了管理访问设置。下文所举的例子中，默认接口的地址为：192.168.1.99。

本章，我们假设您的 FortiGate 设备还没有启动虚拟域配置。如果已经启动了虚拟域配置，在进行以下操作之前，将被直接切换到全局与 VDOM 配置页面。

本手册中将不对如何配置病毒扫描，web 过滤与垃圾邮件过滤进行说明。

配置 FortiGate 设备的 VLAN 几项必需的步骤：

- 添加 VLAN 子接口
- 创建防火墙策略
- 配置路由

添加VLAN子接口

在 FortiGate 设备的物理接口添加 VLAN 子接口，使其能够接收 VLAN 标签的数据包。

FortiGate 设备接口的 IP 地址不能重叠。也就是说，所有接口的 IP 地址必须在不同的子网。该规则对物理接口与 VLAN 子接口同样适用。

**注意**：如果您不能更改现有的配置避免 IP 地址的重叠，使用 CLI 输入命令 config global 与 set ip-overlap enable 允许 IP 地址的重叠。使用该命令后，多个 VLAN 接口可以具有其它接口使用子网中的 IP 地址。建议高级用户使用该命令。

每个 VLAN 子接口必须配置其自己的 IP 地址与掩码。子接口的 VLAN ID 必须与 IEEE 802.1Q 路由器添加 VLAN ID 相匹配。VLAN ID 可以为 1 到 4096 之间任何的数字。如果 VLAN ID 不匹配，子接口接收不到 VLAN 标签的流量。

NAT/路由模式下添加 VLAN 子接口

1. 如果启动了 VDOM，并且您不在根 VDOM 下，点击进入“全局”。
2. 进入“系统管理>网络配置>接口”。
3. 点击“新建”添加 VLAN 接口。
4. 输入能够识别 VLAN 接口的名称。
5. 从接口列表中，选择通过该 VLAN 子接口接收 VLAN 数据包的物理接口。
6. 输入与该 VLAN 子接口接收到的数据包的 VLAN ID 相匹配的 VLAN ID。
7. 使用配置任何 FortiGate 接口的方法配置 VLAN 子接口的设置。
8. 点击 OK 保存配置更改。

FortiGate 设备根据您在步骤 5 的选择添加新的 VLAN 子接口。

点击物理接口旁边的蓝色箭头，扩展查看添加的 VLAN 子接口。如果物理接口旁没有蓝色箭头显示，表示该接口没有子接口存在。

添加防火墙策略

防火墙策略是根据 FortiGate 设备网络接口的源与目标地址控制其流量。或者，通过防火墙策略，您可以对流量限制时间或控制一些服务。

您需要对通过 FortiGate 设备 VLAN 接口的数据包添加防火墙策略配置数据包的进入接口与流出接口。对于每个 VLAN 创建一项防火墙策略以允许 VLAN 应用的以下连接：

- 从 VLAN 到外部网络的连接

- 从外部网络到 VLAN 的连接
- FortiGate 设备中相同的域中一个 VLAN 到其它 VLAN 的连接
- FortiGate 设备中相同的域中从其它 VLAN 到一个 VLAN 的连接

通过每个 VLAN 的数据包要经过反病毒与垃圾邮件的扫描。

对 VLAN 子接口添加防火墙策略

1. 进入“防火墙>地址”。
2. 点击“新建”添加与 VLAN 数据包的源及目标地址相匹配的防火墙地址。
3. 进入“防火墙>策略”。
4. 根据需要添加防火墙策略。

配置路由

在较简单的网络情况下，您需要对具有外部目标地址的、需要到达外部网络网关的数据包配置默认的路由。在较为复杂的网络情况下，您需要根据数据包的源与目标地址配置不同的路由。

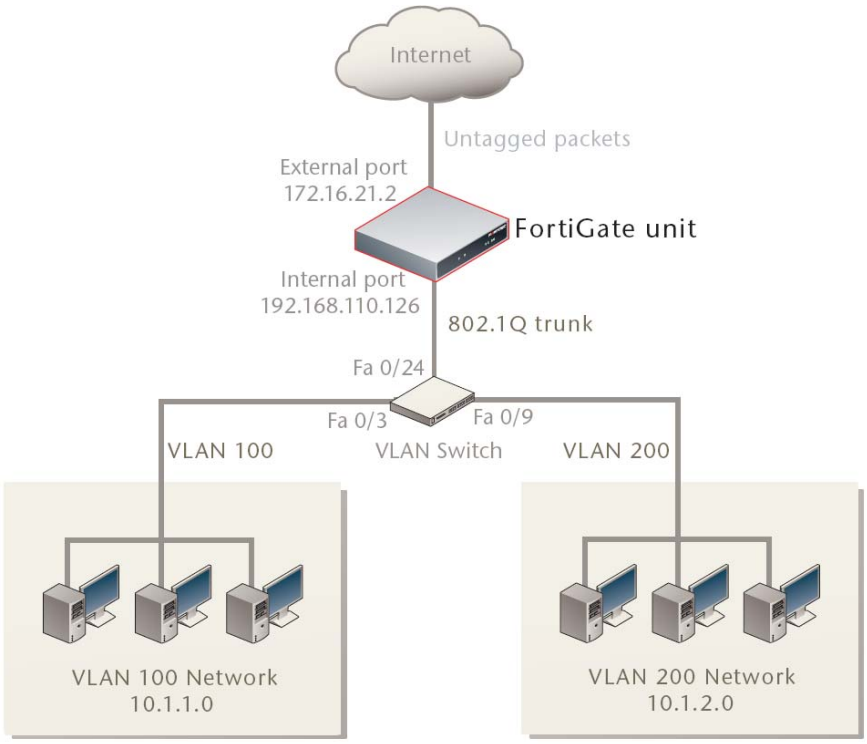
同样，在防火墙的作用下，您需要对 VLAN 配置路由。对 VLAN 配置路由与网关后，才能够从本地子网之外的网络发送与接收数据包。根据所连接的网络，可以配置静态或动态路由。动态路由可以使用 RIP，BPG，OSPF 或多播。

如果您在 VLAN 中启动了 SSH，PING，TELNET 或 HTTPS 协议，您可以使用这些协议确认路由配置是否正确。在接口启动日志记录功能也可以帮助诊断可能发生的事件。

NAT/路由模式下的 VLAN 配置举例（简单配置）

图 4 所示是简化的 NAT/路由模式 VLAN 配置。该示例中，FortiGate 内部接口通过 802.1Q trunk 与 Cisco2950 VLAN 交换机连接与并配置了两个 VLAN 子接口（VLAN100 与 VLAN200）。外部接口与互联网连接。外部接口不配置 VLAN 子接口。

图 4：NAT/路由模式下的 FortiGate 设备



当Cisco交换机从VLAN100与VLAN200接收被标记了VLAN ID的数据包，并将这些数据包转发到本地端口，然后数据包通过主干链路到达 FortiGate 设备。FortiGate 配置使用了策略允许通过 VLAN 之间的数据流以及从 VLAN 到外部网络的数据传输。

以上的网络拓扑结构举例中使用了 FortiGate-800 设备与 Cisco Catalyst2950 交换机设备。该配置中的 Cisco 交换机使用 ISO 命令。举例中假设已经安装并连接了 FortiGate-800 与 Cisco Catalyst 2950，那么基本设置就算完成了。在交换机的设置中，您需要连接到 CLI 能够输入命令。关于各个设备的使用，参见各自的使用说明手册。

常规配置步骤

根据以上的配置举例，对硬件设备的配置使用与测试进行说明：

1. 配置 FortiGate-800 设备
   - 配置外部接口
   - 在内部网络接口添加两个 VLAN 子接口
   - 对内部与外部网络添加防火墙地址与地址范围
   - 添加防火墙策略允许以下的流量：
     i. VLAN 之间的相互访问
     ii. VLAN 网络到外部网络的访问
2. 配置 Cisco 交换机支持数据包标签

3. 测试配置

配置 FortiGate-800 设备

使用 FortiGate 设备的 web 管理器进行设备配置，也可以使用 CLI。

配置 FortiGate 设备的以下设置：

- 配置外部接口
- 添加 VLAN 子接口
- 添加防火墙地址
- 添加防火墙策略

配置外部接口

FortiGate 设备的外部接口是互联网与您的网络之间的通信通道。

使用基于 web 的管理器与 CLI 均可以配置外部接口。

使用基于 web 的管理器配置外部接口

1. 如果启动 VDOM，且您不在根 VDOM 中，点击“全局”。
2. 进入“系统>网络>接口”。
3. 点击外部接口的编辑图标。
4. 输入外部接口需要设置的以下信息，并点击“OK”。

寻址模式	手工
IP/掩码	172.16.21.2/255.255.255.0
根据需要配置其它字段。	

使用 CLI 配置外部接口

```
config system interface
edit external
set mode static
set ip 172.16.21.2    255.255.255.0
end
```

添加 VLAN 子接口

该步骤是在 FortiGate 设备的物理接口创建 VLAN。示例中其余的部分是在设备上配置 VLAN，并配置交换机像 FortiGate 设备对待 VLAN 一样以及测试所做的设置是正确的。

以下是使用基于 web 的管理器或 CLI 在 FortiGate 设备的物理接口添加 VLAN 接口的说明。

使用基于 web 的管理器添加 VLAN 子接口

1. 如果启动 VDOM，且您不在根 VDOM 中，点击“全局”。
2. 进入“系统>网络>接口”。
3. 点击“新建”。
4. 设置 VLAN_100 的以下信息，并点击 OK。

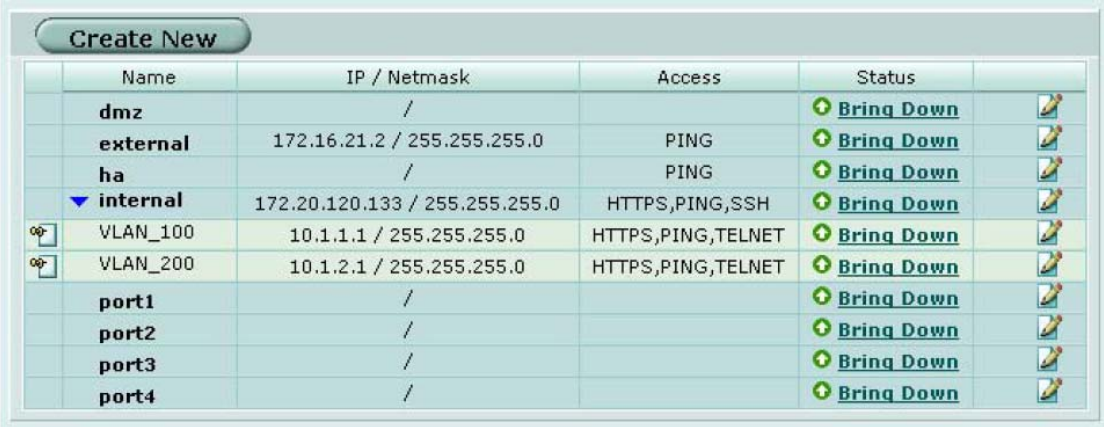
名称	VLAN_100
接口	内部接口
VLAN ID	100
寻址模式	手工
IP/掩码	10.1.1.1/255.255.255.0
管理访问	HTTPS PING TELNET
根据需要配置其它字段。	

5. 点击“新建”。
6. 设置 VLAN_200 的以下信息，并点击 OK。

名称	VLAN_200
接口	内部接口
VLAN ID	200
寻址模式	手工
IP/掩码	10.1.2.1/255.255.255.0

管理访问	HTTPS PING TELNET
根据需要配置其它字段。	

图 5：VLAN 子接口



使用 CLI 添加 VLAN 子接口

config system interface

edit VLAN_100

set interface internal

set vlanid 100

set mode static

set ip 10.1.1.1 255.255.255.0

set allowaccess https ping telnet

next

edit VLAN_200

set interface internal

set vlanid 200 set mode static

set ip 10.1.2.1 255.255.255.0

set allowaccess https ping telnet

end

添加防火墙地址

您需要在防火墙策略选项中定义 VLAN 子网的地址。FortiGate 设备中默认

的地址是“全部（all）”，也就是说，对通过防火墙的所有地址，源或目标地址的数据包应用同一项防火墙策略。

以下举例中，“_Net”是地址名称的一部分表示地址的范围，而不是唯一的地址。设置防火墙地址时以明确、唯一并简短为原则。您可以使用基于 web 的管理器或 CLI 添加防火墙地址。

使用基于 web 的管理器添加防火墙地址

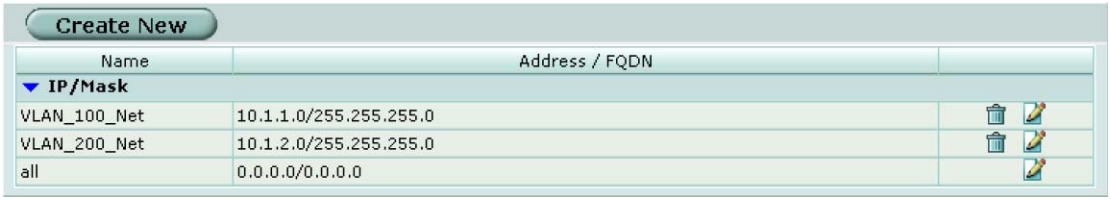
1. 进入“防火墙>地址”。
2. 点击“新建”。
3. 输入以下信息并点击 OK：

地址名称	VLAN _100_Net
类型	子网/IP 地址范围
子网/IP 范围	10.1.1.0/255.255.255.0

4. 点击“新建”。
5. 输入以下信息并点击 OK：

地址名称	VLAN _200_Net
类型	子网/IP 地址范围
子网/IP 范围	10.1.2.0/255.255.255.0

图 6：防火墙地址



使用 CLI 配置防火墙地址

config firewall address

edit VLAN_100_Net

set type ipmask set subnet 10.1.1.0 255.255.255.0

next

edit VLAN_200_Net

set type ipmask set subnet 10.1.2.0 255.255.255.0

end

添加防火墙策略

对 VLAN 分配了地址后，您需要使用基于 web 的管理器或 CLI 对 VLAN 配置防火墙策略。也就是设置策略允许数据包在 VLAN 之间以及到外部互联网的传输。

如果您不希望在一个 VLAN 中允许全部的服务，您可以只对允许的服务创建策略。以下的举例是允许应用全部的服务。

使用基于 web 的管理起添加防火墙策略

1. 进入“防火墙>策略”。
2. 点击“新建”。
3. 输入以下信息，并点击“OK”：

源地址		
	接口/区域	VLAN_100
	地址名称	VLAN_100_Net
目标地址		
	接口/区域	VLAN_200
	地址名称	VLAN_200_Net
时间表		总是 （Always）
服务		ANY
动作		ACCEPT
NAT		点击选择
根据需要配置其它字段。		

4. 点击“新建”。
5. 输入以下信息并点击 OK 确认。

源地址		
	接口/区域	VLAN_200
	地址名称	VLAN_200_Net
目标地址		
	接口/区域	VLAN_100
	地址名称	VLAN_100_Net
时间表		总是 （Always）
服务		ANY
动作		ACCEPT
NAT		点击选择
根据需要配置其它字段。		

6. 点击“新建”。

7. 输入以下信息并点击 OK 确认。

源地址		
	接口/区域	VLAN_100
	地址名称	VLAN_100_Net
目标地址		
	接口/区域	外部接口
	地址名称	全部
时间表		总是 （Always）
服务		ANY
动作		ACCEPT

NAT	点击选择
根据需要配置其它字段。	

8. 点击“新建”。

9. 输入以下信息并点击 OK 确认：

源地址		
	接口/区域	VLAN_200
	地址名称	VLAN_200_Net
目标地址		
	接口/区域	外部接口
	地址名称	全部
时间表		总是 （Always）
服务		ANY
动作		ACCEPT
NAT		点击选择
根据需要配置其它字段。		

使用 CLI 添加防火墙策略

config firewall policy

edit 1

set srcintf VLAN_100

set dstintf VLAN_200

set srcaddr VLAN_100_Net

set dstaddr VLAN_200_Net

set schedule always

set service ANY

set action accept

set nat enable

set status enable

next

edit 2

set srcintf VLAN_200

set dstintf VLAN_100

set srcaddr VLAN_200_Net

set dstaddr VLAN_100_Net

set schedule always

set service ANY

set action accept

set nat enable

set status enable

next

edit 3

set srcintf VLAN_100

set dstintf external

set srcaddr VLAN_100_Net

set dstaddr all

set schedule always

set service ANY

set action accept

set nat enable s

et status enable

next

edit 4

set srcintf VLAN_200

set dstintf external

set srcaddr VLAN_200_Net

set dstaddr all

set schedule always

set service ANY

set action accept

set nat enable

set status enable

end

配置 Cisco 交换机支持 VLAN 标签

在 Cisco Catalyst 2950 以太网交换机中，您需要在 VLAN 数据库中定义 VLAN 100 与 VLAN200，然后添加配置文件以定义 VLAN 子接口与 802.1Q trunk 接口。

配置 Cisco 交换机的方法之一是通过串行连接到设备的控制台 console 端口，使用 CLI 输入配置命令。另一种方法是在交换机分配一个接口作为管理接口，通过该接口使用 web 浏览器连接到交换机的用户图形界面。有关连接与配置交换机的详细信息，参见交换机的使用说明手册。

以上配置举例使用的是 Cisco Catalyst 2950 交换机，配置交换机的命令是 IOS 命令，详细信息参见交换机的使用说明。

配置 VLAN 子接口与 trunk 接口

在 Cisco 交换机中添加以下命令：

!

interface FastEthernet0/3

switchport access vlan 100

!

interface FastEthernet0/9

switchport access vlan 200

!

interface FastEthernet0/24

switchport trunk encapsulation dot1q

switchport mode trunk

!

交换机具有以下配置：

端口 0/3	VLAN ID 100
端口 0/9	VLAN ID 200
端口 0/24	802.1Q trunk

**注意**：在应用 VLAN 之前还有配置 VLAN 的默认网关。VALN100 的默认网关是 FortiGate VLAN100 子接口。VALN200 的默认网关是 FortiGate VLAN200 子接口。

测试配置

使用诊断命令（tracert,ping）测试 FortiGate 设备与 Cisco 交换机之间的路由流量。测试操作包括：

- 测试 VLAN100 到 VLAN200 之间的流量
- 测试从 VLAN 到外部网络的流量

测试 VLAN100 到 VLAN200 之间的流量

以下测试举例中，是对两个内部网络之间的路由设置跟踪的。路由目标是 VLAN200 上一个主机。

从 VLAN100，在命令提示符下输入：

C:\>tracert 10.1.2.2

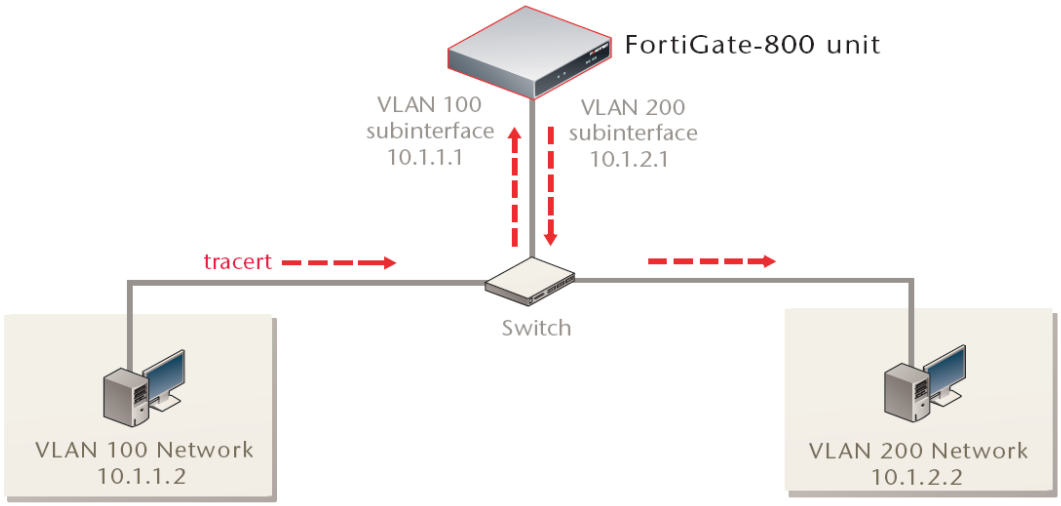
Tracing route to 10.1.2.2 over a maximum of 30 hops:

1 <10 ms <10 ms <10 ms 10.1.1.1

2 <10 ms <10 ms <10 ms 10.1.2.2

Trace complete.

图 7：从 VLAN100 到 VLAN200 的路由跟踪



测试从 VLAN 到外部网络的流量

以下测试举例中，是对内部网络到外部网络的路由设置跟踪的。路由目标是 FortiGate-800 设备的外部网络接口。

从 VLAN100，在命令提示符下输入：

C:\>tracert 172.16.21.2

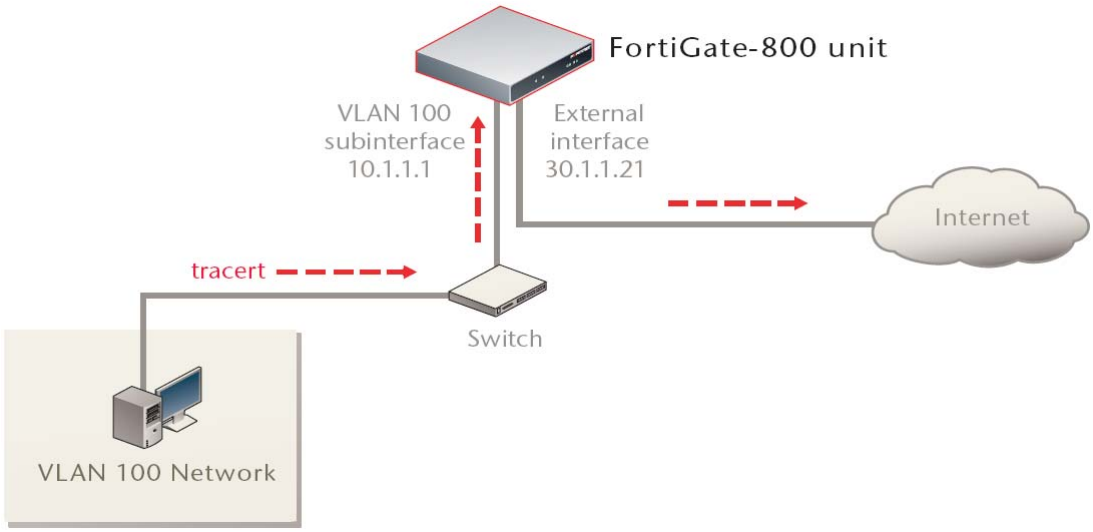
Tracing route to 172.16.83.1 over a maximum of 30 hops:

1 <10 ms <10 ms <10 ms 10.1.1.1

2 <10 ms <10 ms <10 ms 172.16.21.2

Trace complete.

图 8：从 VLAN100 到外部网络的路由跟踪



运行 NAT/路由模式下的配置举例（复杂）

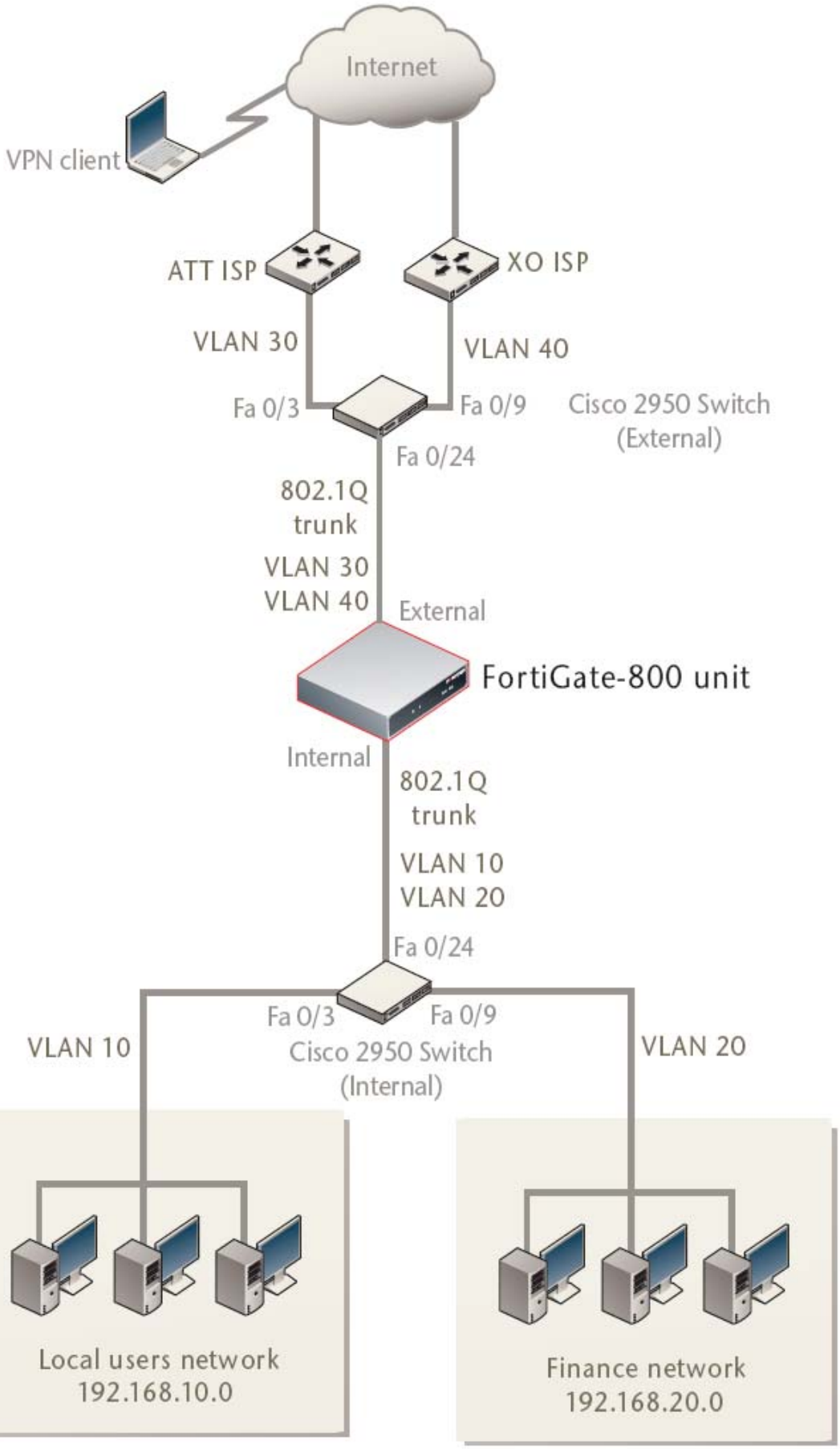
在以下举例中，FortiGate-800 设备运行于 NAT/路由模式，设备的网络接口配置如下：

- 内部接口配置了两个 VLAN 子接口：VLAN10 作为本地用户网络的接口，VLAN20 作为财务网络接口。内部接口通过 80.1Q trunk 与 Cisco 2950 交换机连接。
- 外部接口配置了两个 VLAN 子接口：VLAN30 作为 ATT ISP 网络的接口，VLAN40 作为 XO ISP 接口。内部接口同时 80.1Q trunk 与 Cisco 2950 交换机连接。

FortiGate-800 配置了防火墙策略以控制网络之间的流量。财务网络是最为安全的网络，该网络中允许向外到所有其它网络的流量，但是限制进入该网络的流量。本地用户网络允许传输到外部网络（ATT ISP 与 XO ISP）的流量，从财务网络发出的流量以及从 ATT ISP 网络中一个 VPN 用户的连接。

配置 FortiGate-800 与两台兼容 802.1Q 的交换机应用图 9 所示的网络拓扑结构。

图 9：VLAN 拓扑结构（运行于 NAT/路由模式的 FortiGate 设备）


Internet
VPN client
ATT ISP
XO ISP
VLAN 30
VLAN 40
Fa 0/3
Fa 0/9
Cisco 2950 Switch
(External)
Fa 0/24
802.1Q
trunk
VLAN 30
VLAN 40
External
FortiGate-800 unit
Internal
802.1Q
trunk
VLAN 10
VLAN 20
Fa 0/24
Fa 0/3
Fa 0/9
VLAN 10
Cisco 2950 Switch
(Internal)
VLAN 20
Local users network
192.168.10.0
Finance network
192.168.20.0

常规配置步骤

以下的说明将复杂的配置步骤拆分为不同的配置阶段：

1. 配置 FortiGate-800 设备
2. 配置 FortiGate-800 设备 IPSec VPN 通道与加密策略
3. 配置 VPN 用户端
4. 配置内部 Cisco 交换机
5. 配置外部 Cisco 交换机
6. 测试配置

配置 FortiGate-800 设备

使用基于 web 的管理器或 CLI 均可以配置 FortiGate-800 设备。需要对 FortiGate 设备配置以下选项：

- 添加 VLAN 子接口到本地 LAN，ATT-ISP 与 XO-ISP 网络
- 添加默认路由
- 添加防火墙地址
- 添加防火墙策略

添加 VLAN 子接口

使用基于 web 的管理器或 CLI 添加 VLAN 子接口。

使用基于 web 的管理器添加 VLAN 子接口

1. 如果启动了 VDOM 且不在根 VDOM，退回到“全局”配置。
2. 进入“系统>网络>接口”。
3. 点击“新建”。
4. 对本地用户网络输入以下信息并点击 OK 确认：

名称	Local_LAN
接口	内部接口
VLAN ID	10
寻址模式	手工

IP/掩码	192.168.10.1/255.255.255.0
管理访问	HTTPS, PING, TENET

5．点击“新建”。

6. 对财务网络输入以下信息并点击 OK 确认：

名称	Finance
接口	内部接口
VLAN ID	20
寻址模式	手工
IP/掩码	192.168.20.1/255.255.255.0
管理访问	HTTPS, PING, TENET

7. 点击“新建”。

8. 对 ATT ISP 网络输入以下信息并点击 OK 确认：

名称	ATT-ISP
接口	外部接口
VLAN ID	30
寻址模式	手工
IP/掩码	30.1.1.1/255.255.255.0
管理访问	HTTPS, PING, TENET

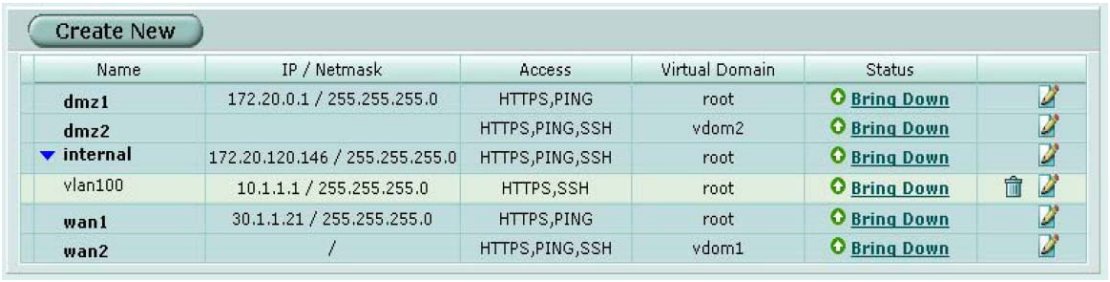
9. 点击“新建”。

10. 对 XO ISP 网络输入以下信息并点击 OK 确认：

名称	XO-ISP
接口	外部接口

VLAN ID	40
寻址模式	手工
IP/掩码	40.1.1.1/255.255.255.0
访问	HTTPS, PING, TENET

图 10：VLAN 子接口



使用 CLI 添加 VLAN 子接口

config system interface

edit Local-LAN

set interface internal

set vlanid 10

set mode static

set ip 192.168.10.1 255.255.255.0

set allowaccess https ping telnet

next

edit Finance

set interface internal

set vlanid 20

set mode static

set ip 192.168.20.1 255.255.255.0

set allowaccess https ping telnet

next

edit ATT-ISP

set interface external

set vlanid 30

set mode static

set ip 30.1.1.1 255.255.255.0

set allowaccess https ping telnet

next

edit XO-ISP

set interface external

set vlanid 40

set mode static

set ip 40.1.1.1 255.255.255.0

set allowaccess https ping telnet

end

添加默认路由

到 ISP 的连接需要添加默认的路由。这些路由是根据距离向量的不同来衡量的。也就是说默认情况下流量将通过 ATT-ISP 传输。

**注意：**如果您想交替使用两个 ISP，例如，设置会话的负载平衡，那么必须设置三个项目：相同的距离向量，相同的优先级以及启动负载平衡设置。有关这些设置的详细信息，参见 FortiGate 设备 CLI 使用参考手册。

使用基于 web 的管理器或 CLI 配置路由

使用基于 web 的管理器添加路由

1. 进入“路由>静态>静态路由”。
2. 点击“新建”，添加新的路由。
3. 输入以下信息将默认的路由添加到 ATT-ISP 网络，并点击 OK：

目标 IP/掩码	0.0.0.0/0.0.0.0
网关	30.1.1.2
设备	ATT-ISP
距离	10

4. 输入以下信息对 XO-ISP 添加二级默认路由，设置流量从外部接口离开，点击 OK 确认：

目标 IP/掩码	0.0.0.0/0.0.0.0
网关	40.1.1.2
设备	XO-ISP
距离	20

使用 CLI 添加路由

config router static

edit 1

set device ATT-ISP

set gateway 30.1.1.2

set distance 10

next

edit 2

set device XO-ISP

set gateway 40.1.1.2

set distance 20

end

添加防火墙地址

在配置防火墙策略控制 VLAN 之间与 VLAN 与互联网之间的网络流量时，您需要先配置防火墙地址。所定义的这些子网将是防火墙策略应用的地方。

使用基于 web 的管理器与 CLI 都可以添加防火墙地址。

使用基于 web 的管理器添加防火墙地址

1. 进入“防火墙>地址”。
2. 点击“新建”。
3. 输入以下信息并点击 OK 确认：

地址名称	Local_users

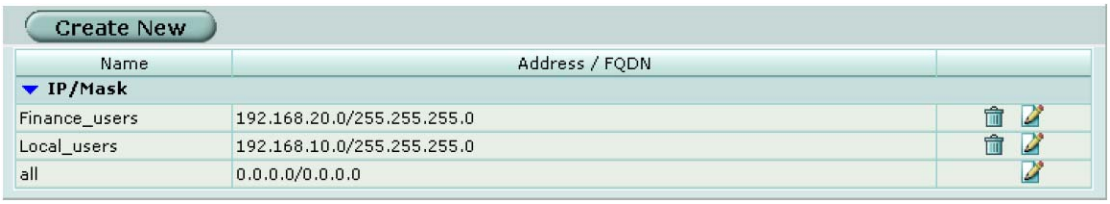
类型	子网/IP 地址范围
IP 地址范围/子网	192.168.10.0/255.255.255.0

4. 点击“新建”。

5. 输入以下信息并点击 OK 确认：

地址名称	Finance_users
类型	子网/IP 地址范围
IP 地址范围/子网	192.168.20.0/255.255.255.0

图 11：防火墙地址



使用 CLI 添加防火墙地址

config firewall address

edit Local_users

set type ipmask

set subnet 192.168.10.0 255.255.255.0

next

edit Finance_users

set type ipmask

set subnet 192.168.20.0 255.255.255.0

end

添加防火墙策略

防火墙策略的添加可以使用 VLAN 流量在 VLAN 之间以及传输到互联网。使用基于 web 的管理器或 CLI 均可以配置防火墙策略。

使用基于 web 的管理器添加防火墙策略

1. 进入“防火墙>策略”。

2. 点击“新建”。

3. 输入以下信息并点击 OK 确认：

源地址		
	接口/区域	Finance
	地址名称	Finance_users
目标地址		
	接口/区域	ATT-ISP
	地址名称	All（全部）
时间表		总是（Always）
服务		ANY
动作		ACCEPT
NAT		点击选择 NAT 模式
根据需要配置其它字段。		

4. 进入“防火墙 >策略”。

5. 点击“新建”。

6. 输入以下信息并点击 OK 确认：

源地址		
	接口/区域	Finance
	地址名称	Finance_users
目标地址		
	接口/区域	OX-ISP
	地址名称	All（全部）
时间表		总是（Always）

服务	ANY
动作	ACCEPT
NAT	点击选择 NAT 模式
根据需要配置其它字段。	

7. 进入“防火墙 >策略”。
8. 点击“新建”。
9. 输入以下信息并点击 OK 确认：

源地址		
	接口/区域	Finance
	地址名称	Finance_users
目标地址		
	接口/区域	Local-LAN
	地址名称	Local-users
时间表		总是（Always）
服务		ANY
动作		ACCEPT
NAT		点击选择 NAT 模式
根据需要配置其它字段。		

10. 进入“防火墙 >策略”。
11. 点击“新建”。
12. 输入以下信息并点击 OK 确认：

源地址		
	接口/区域	Local-LAN

	地址名称	Local-users
目标地址		
	接口/区域	ATT-ISP
	地址名称	All（全部）
时间表		总是（Always）
服务		ANY
动作		ACCEPT
NAT		点击选择 NAT 模式
根据需要配置其它字段。		

13. 进入“防火墙 >策略”。

14. 点击“新建”。

15. 输入以下信息并点击 OK 确认：

源地址		
	接口/区域	Local-LAN
	地址名称	Local-users
目标地址		
	接口/区域	OX-ISP
	地址名称	All（全部）
时间表		总是（Always）
服务		ANY
动作		ACCEPT
NAT		点击选择 NAT 模式

根据需要配置其它字段。

防火墙策略列表：



使用 CLI 添加防火墙策略

config firewall policy

edit 1

set srcintf Finance

set dstintf ATT-ISP

set srcaddr Finance_users

set dstaddr all

set schedule always

set service ANY

set action accept

set nat enable

set status enable

next

edit 2

set srcintf Finance

set dstintf XO-ISP

set srcaddr Finance_users

set dstaddr all

set schedule always

set service ANY

set action accept

```
set nat enable
set status enable
next
edit 3
set srcintf Finance
set dstintf Local-LAN
set srcaddr Finance_users
set dstaddr Local_users
set schedule always
set service ANY
set action accept
set nat enable
set status enable
next
edit 4
set srcintf Local-LAN
set dstintf ATT-ISP
set srcaddr Local_users
set dstaddr all
set schedule always
set service ANY
set action accept
set nat enable
set status enable
end
edit 5
set srcintf Local-LAN
set dstintf XO-ISP
set srcaddr Local_users
set dstaddr all
```

set schedule always

set service ANY

set action accept

set nat enable

set status enable

end

配置 FortiGate-800 设备的 IPSec 通道与加密策略

配置举例中，一个用户将被允许通过 VPN 通道从外部拨号方式连接到本地用户网络。实现以上操作，您需要进行以下的配置：

- 配置 VPN 网关
- 配置 VPN 通道
- 对本地用户网络的 VPN 用户定义 IP 地址
- 添加加密防火墙策略启动连接

配置 VPN 网关

配置 VPN IPSec 通道是典型的两个配置阶段的操作。VPN 网关配置是第一阶段。

使用基于 web 的管理器或 CLI 均可以配置 VPN 网关。

使用基于 web 的管理器配置 VPN 网关

1. 进入“VPN>IPSEC 通道>自动密钥”。
2. 点击创建阶段 1 并点击“高级选项”。
3. 输入以下信息并点击 OK 确认：

名称	Dialup_tunnel（拨号通道）
远程网关	拨号用户
本地接口	ATT-ISP
模式	主动模式（Aggressive）
验证方式	预共享密钥

预共享密钥	设置为预共享密钥，输入在阶段 1 协商期间 FortiGate 设备用来接受远程对等或拨号客户端认证时使用的预共享密钥。您必须在远程对等或客户端定义相同的密钥值。处于网络安全考虑，密钥应该是至少 16 位的包含数字字母混合的字符串。 用户必须使用相同的预共享密钥。
高级选项	点击“高级选项”配置以下的选项。以下所列的数值是默认的，无需进行更改。
阶段 1 方案	1-3DES 加密，SHA1 验证 2-3DES 加密，MD5 验证
DH 组	5
密钥寿命	28800（秒）
根据需要配置其它字段。	

使用 CLI 配置 VPN 网关

config vpn ipsec phase1

edit Dialup_tunnel

set type dynamic

set mode aggressive

set authmethod psk

set psksecret <pre-shared key>

set proposal 3des-sha1 3des-md5

set dhgrp 5

set keylife 28800

end

配置 VPN 通道

配置 VPN 网关后，便可以配置 VPN 通道了。

使用基于 web 的管理器与 CLI 均可以配置 VPN 通道。

使用基于 web 的管理器配置 VPN 通道

1. 进入“VPN>IPSEC>阶段 2”。

2. 点击“新建”并选择“高级选项”。

名称		拨号用户
阶段 1		拨号通道（Dial_tunnel）
高级选项		点击“高级选项”配置以下选项。
阶段 2 方案		1-3DES 加密，SHA1 验证 2-3DES 加密，MD5 验证
	启动数据重演检测	启动
	启用完全转发安全性（PFS	启动
	DH组	5
密钥寿命		1800（秒）
保持存活		启动
DHCP-IPsec		不启动
快速模式鉴别		
	源地址	
	源端口	
	目标地址	
	目标端口	
	协议	
根据需要配置其它字段。		

使用 CLI 配置 VPN 通道

config vpn ipsec phase2

edit Dialup-client

set phase1name Dialup_tunnel

set proposal 3des-sha1 3des-md5

set replay enable

set pfs enable

set dhgrp 5

set keylife_type seconds

set keylifeseconds 1800

set keepalive enable

end

定义 VPN 用户 IP 地址

防火墙使用目标地址判断可接受的远程 VPN 用户访问的源地址范围。设置用户从任何主机使用 VPN，防火墙策略需要设定为“全部”的防火墙地址。以下配置举例需要远程用户只能够使用 ATT-ISP 网络。

使用基于 web 的管理器定义 VPN 用户的 IP 地址

1. 进入“防火墙>地址>地址”。
2. 点击“新建”。
3. 输入以下信息并点击 OK 确认：

地址名称	ATT-net
类型	子网/IP 地址范围
IP 地址范围/子网	30.1.1.0/255.255.255.0

使用 CLI 定义 VPN 用户 IP 地址

config firewall address

edit VIP_IP

set type ipmask

set start_ip 30.1.1.0 255.255.255.0

end

添加加密策略

使用基于 web 的管理器与 CLI 均可以添加加密策略。

使用基于 web 的管理器添加加密策略

1. 进入“防火墙>策略”。
2. 点击“新建”。
3. 输入以下信息并点击 OK 确认：

源地址		
	接口/区域	Local_LAN
	地址名称	Local_users（本地用户）
目标地址		
	接口/区域	ATT-ISP
	地址名称	ATT-net
时间表		Always（总是）
服务		ANY
动作		IPSEC
VPN 通道		
	允许向内的流量	启动
	允许向外的流量	不启动
	向内的 NAT	启动
	向外的 NAT	不启动
根据需要配置其它字段。		

4. 将加密策略添加到策略列表中非加密策略之上，如果列表有多项加密策略，将具有更具体规定源与目标地址中的的加密策略放在相对设定宽泛的策略之上。

使用 CLI 添加加密策略

config firewall policy

edit 6

set srcintf Local-LAN

set dstintf ATT-ISP

set srcaddr Local_users

set dstaddr ATT-net

set schedule always

set service ANY set action ipsec

set vpntunnel Dialup-clientset inbound enable

set outbound disable set natinbound enable set natoutbound disable

set vpntunnel Dialup_tunnel

set status enable

end

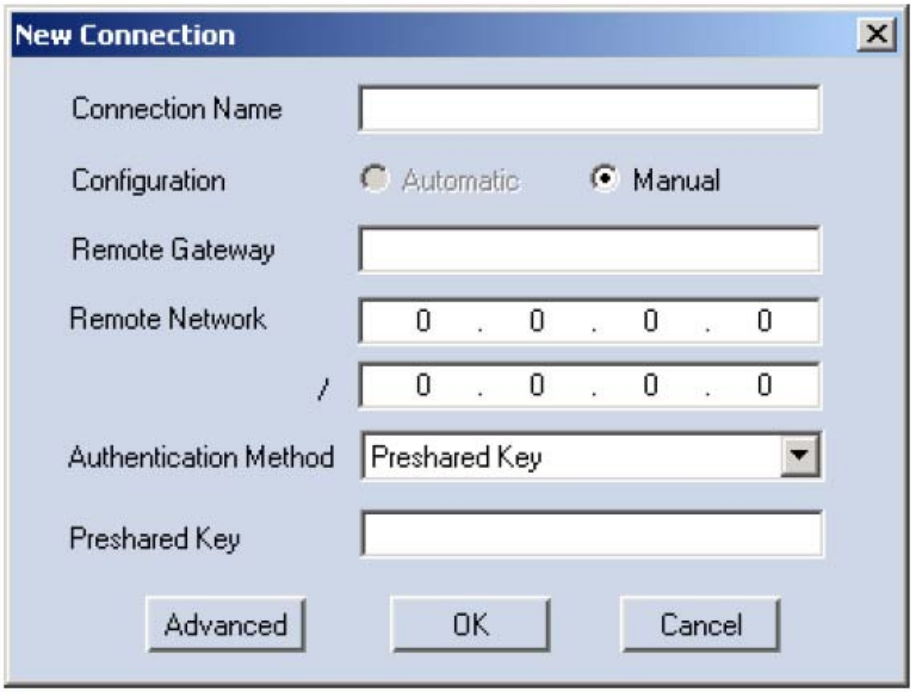
配置 VPN 用户端

以下举例说明如何配置本地用户网络允许从 ATT ISP 网络的一个 VPN 用户端的向内连接。

创建新的 VPN 连接

1. 启动 FortiClient。
2. 进入“VPN>连接”后点击“添加”。

图 12：新建 VPN 连接

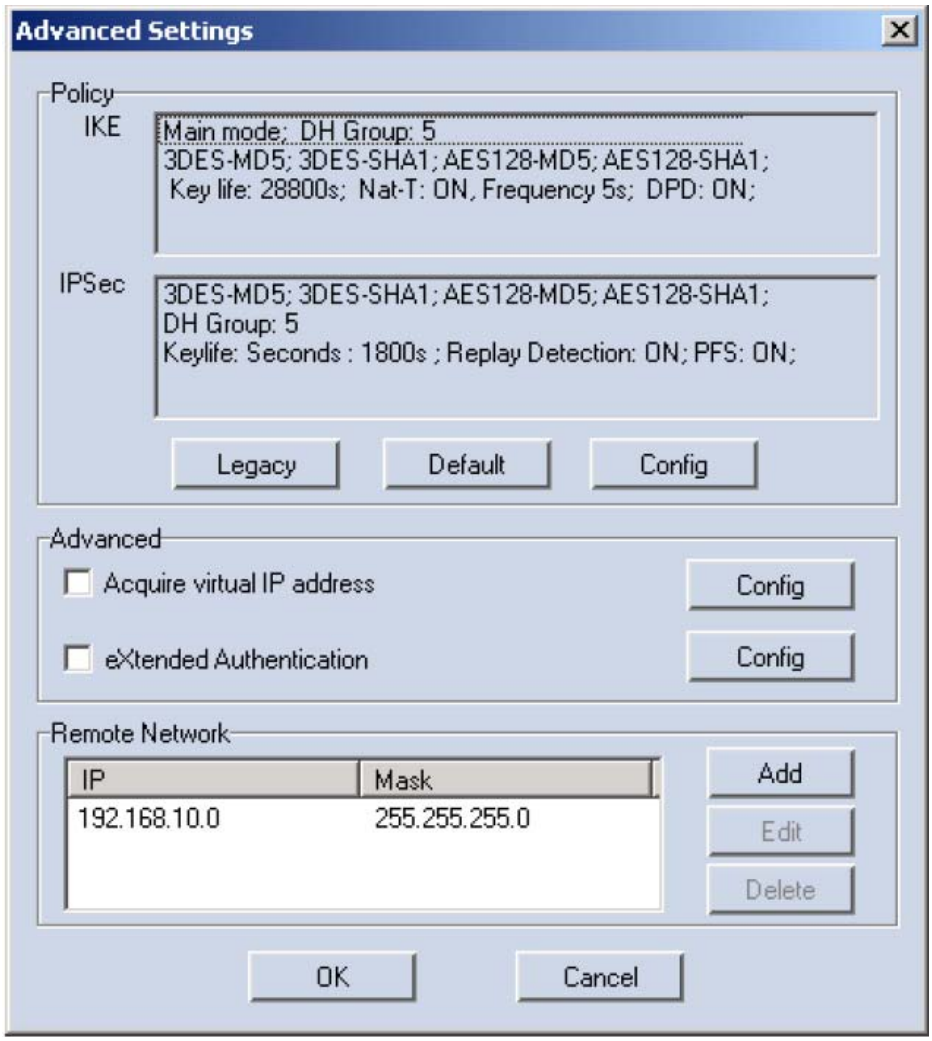


3. 在连接名称字段输入连接的名称。
4. 在远程网关 IP 地址栏输入 30.1.1.1。
5. 在远程网络地址栏输入 192.168.10.0/255.255.255.0。
6. 在验证方式中选择“预共享密钥”。
7. 在预共享密钥中设置预共享密钥。

注意：预共享密钥必须与 FortiGate 的验证密钥相匹配。

8. 点击“高级选项”。

图 13：高级选项设置



9. 选中“获取虚拟 IP 地址”功能框，并点击“配置”。

打开虚拟 IP 地址获取对话框。

10. 点击“手工设置”。

11. 输入以下信息并点击 OK 确认。

IP 地址	30.1.1.1.0
子网掩码	255.255.255.0

12. 点击 OK 完成配置 VPN 连接。

配置内部Cisco交换机

Cisco Catalyst 2950 以太网交换机连接着内部接口，您需要在交换机中的 VLAN 数据库中定义 VLAN10 与 VLAN20，并添加配置文件定义 VLAN 子接口与 802.1Q trunk 接口。

该配置需要使用 Cisco IOS 命令。

配置 VLAN 子接口与 trunk 接口

需要对与内部接口连接的交换机输入以下命令：

```
!
interface FastEthernet0/3
switchport access vlan 10
!
interface FastEthernet0/9
switchport access vlan 20
!
interface FastEthernet0/24
switchport trunk encapsulation dot1q
switchport mode trunk
!
```

交换机具有以下配置：

端口 0/3	VLAN ID 10
端口 0/9	VLAN ID 20
端口 0/24	802.1Q trunk

**注意：**在应用 VLAN 之前还有配置 VLAN 的默认网关。VALN10 的默认网关是 FortiGate VLAN10 子接口。VALN20 的默认网关是 FortiGate VLAN20 子接口。

配置外部交换机

Cisco Catalyst 2900 以太网交换机连接着外部接口，您需要在交换机中的 VLAN 数据库中定义 VLAN30 与 VLAN40，并添加配置文件定义 VLAN 子接口与 802.1Q trunk 接口。

该配置需要使用 Cisco IOS 命令。

配置 VLAN 子接口与 trunk 接口

需要对与外部接口连接的交换机输入以下命令：

!

interface FastEthernet0/3

switchport access vlan 30

!

interface FastEthernet0/9

switchport access vlan 40

!

interface FastEthernet0/24

switchport trunk encapsulation dot1q

switchport mode trunk

!

交换机具有以下配置：

端口 0/3	VLAN ID 30
端口 0/9	VLAN ID 40
端口 0/24	802.1Q trunk

**注意：**在应用 VLAN 之前还有配置 VLAN 的默认网关。VALN30 的默认网关是 FortiGate VLAN40 子接口。VALN40 的默认网关是 FortiGate VLAN40 子接

口。

测试配置

使用诊断命令（tracert,ping）测试 FortiGate 设备与 Cisco 交换机之间的路由流量。测试操作包括：

- 测试 VLAN20 到 VLAN10 之间的流量
- 测试从 VLAN20 到外部网络的流量

测试 VLAN20 到 VLAN10 之间的流量

以下测试举例中，是对两个内部网络之间的路由设置跟踪的。路由目标是本地用户网络（VLAN10）上一个主机。

从财务网络，在命令提示符下输入：

C:\>tracert 192.168.10.2

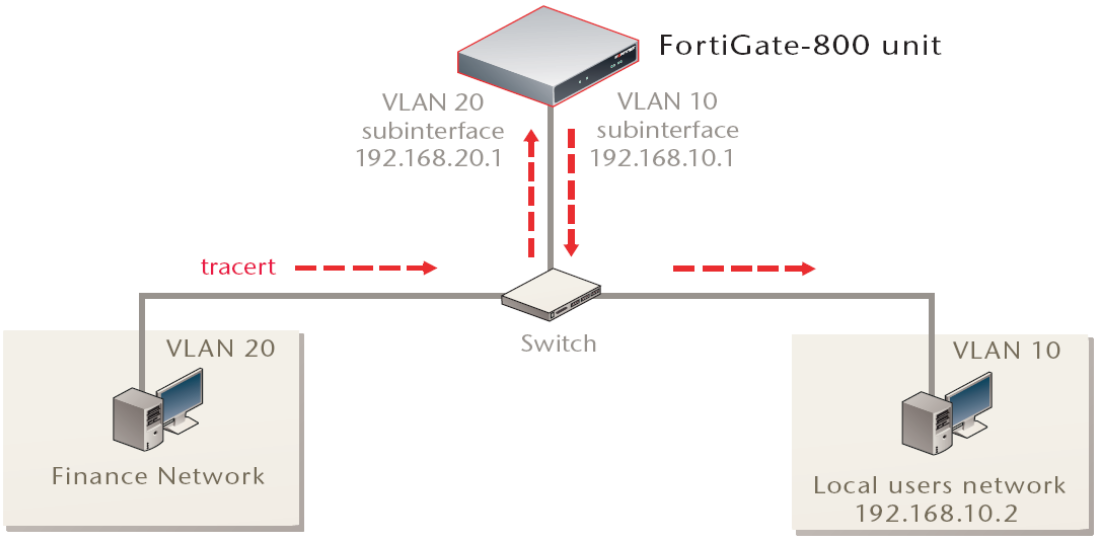
Tracing route to 192.168.10.2 over a maximum of 30 hops:

1 <10 ms <10 ms <10 ms 192.168.10.1

2 <10 ms <10 ms <10 ms 192.168.10.2

Trace complete.

图 14：从 VLAN20 到 VLAN10 的路由跟踪



测试从 VLAN10 到外部网络的流量

以下测试举例中，是对内部网络 VLAN10 到外部网络的路由设置跟踪的。路由目标是 FortiGate-800 设备的外部网络接口。

从 VLAN10，在命令提示符下输入：

C:\>tracert 172.16.21.2

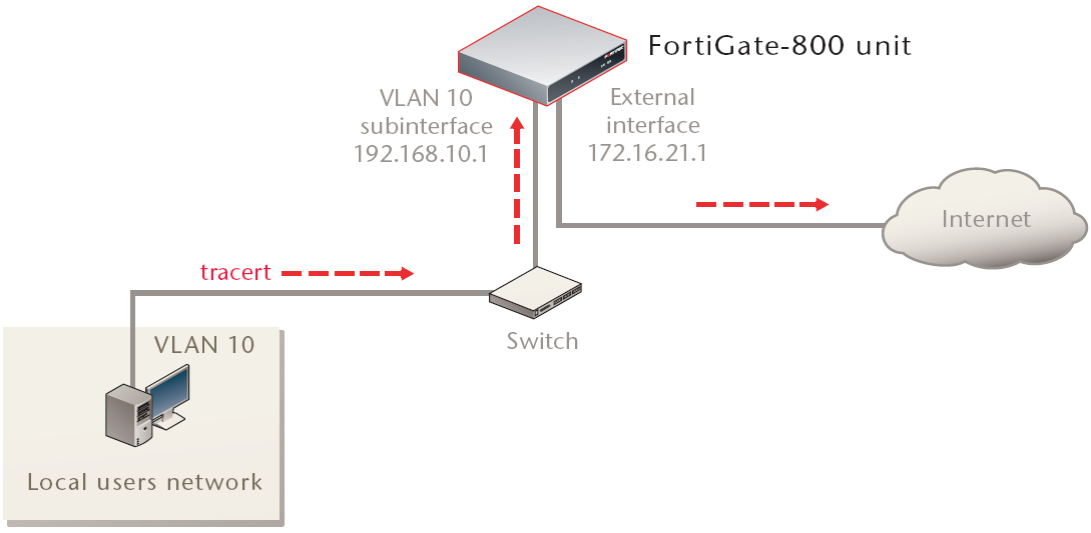
Tracing route to 172.16.83.1 over a maximum of 30 hops:

1 <10 ms <10 ms <10 ms 193.168.10.1

2 <10 ms <10 ms <10 ms 172.16.21.2

Trace complete.

图 15：从 VLAN10 到外部网络的路由跟踪



NAT/路由模式下使用 VDOM

概述

一台 FortiGate 设备中配置使用虚拟域可以对多个对象客体提供逻辑防火墙或路由器功能。每个 VDOM 都具有独立的路由与防火墙策略，以及设置属于该虚拟域的物理或虚拟接口。通过对每个 VDOM 配置独立的接口、路由表与防火墙策略简化了配置管理。

本章包括以下内容：

- 启动虚拟域
- 配置虚拟域
- NAT/路由模式下的虚拟域配置举例（简单）
- NAT/路由模式下的虚拟域配置举例（复杂）

启动虚拟域

为了配置 FortiGate 设备应用多个虚拟域，您需要：

- 启动虚拟域配置
- 创建虚拟域
- 创建虚拟域的管理员
- 访问并配置虚拟域

启动虚拟域配置

使用默认的 admin 帐户可以启动多个 VDOM 操作。

1. 使用 admin 用户名登录基于 web 的管理器。
2. 进入“系统>状态”。
3. 在系统信息项下，找到虚拟域并点击启动。
4. 确认选择。

FortiGate 设备将结束您的登录会话。您可以使用 admin 再次登录。

启动虚拟域配置后，基于 web 的管理器与 CLI 管理工具发生了如下变化：

- 全局与每个虚拟域的配置是分开的。
- 只有 admin 帐户可以查看或配置全局配置选项。

- Admin 帐户可以配置全部的虚拟域配置。
- 常规的管理员只能够配置属于其的虚拟域。

默认情况下，admin 帐户没有设置密码。为了增加安全性，您应该对该帐户设置密码。或者，您可以重命名 admin 帐户。有关管理员帐户信息，参见“FortiGate 设备管理员使用手册”。

创建虚拟域

只有 admin 管理员帐户才可以创建虚拟域。默认情况下，FortiGate 设备中具有一个固定的虚拟域，名为“根虚拟域”，您不能对该虚拟域执行删除或重命名操作。除了固有的根虚拟域外，您可以在设备中创建使用其它的虚拟域。

创建虚拟域

1. 以 admin 登录。
2. 进入“系统>VDOM”。
3. 点击“新建”。
4. 输入虚拟域的名称，并点击 OK 确认。虚拟域的名称不能超过 11 个字符，且不能包含空格。

创建新的虚拟域后，您可以通过刷新 VDOM 页面查看创建的 VDOM 是否在 VDOM 列表中存在。重复以上步骤 3 与 4 创建多个虚拟域。

默认情况下，不管是运行于 NAT/路由还是透明模式的 FortiGate 设备支持最大设置 10 个虚拟域。对于 FortiGate-3000 或更高型号的 FortiGate 设备，您可以购买许可证密钥将 VDOM 的设置数量增加到 25，50，100 或 250 个。

获得 VDOM 许可证密钥

1. 记录 FortiGate 设备序列号。使用基于 web 的管理器，进入“系统>状态”页面，系统信息项下查看。
2. 将设备的序列号发送到 Fortinet 用户服务中心要求获得创建 25、50、100 或 250 个 VDOM 的许可证。
3. 接收到许可证密钥后，进入“系统>状态”，在密钥许可证项下，点击“VDOM 允许”的旁边点击“许可证”。
4. 在“许可证密钥”字段，输入您从 Fortinet 用户支持获得的 32 位的许可证密钥。
5. 点击“应用”。

进入系统状态页面，在全局配置项下可以校验新的 VDOM 许可证。在许可证信息中将重新显示获得密钥后允许创建的最大 VDOM 数量。

创建虚拟域的管理员

只有 admin 管理帐户可以创建管理每个 VDOM 的常规管理员。

对虚拟域创建管理员

1. 以 admin 管理员登录。
2. 进入“系统>系统管理员>管理员”。
3. 点击“新建”。

弹出新建管理员的操作对话框。

4. 在虚拟域列表，对创建的管理员选择分配所要管理的虚拟域。
5. 配置管理帐户其它的选项。
6. 点击 OK 确认。

新建的管理帐户只有通过分配到被虚拟域的接口或通过 console 接口访问 FortiGate 设备。网络接口必须配置允许管理访问，如 HTTPS 与 SSH。

访问并配置虚拟域

只有 admin 帐户可以访问 FortiGate 设备中配置的全部虚拟域。常规管理员只能访问被分配管理的虚拟域，并只能通过属于该虚拟域的接口连接。

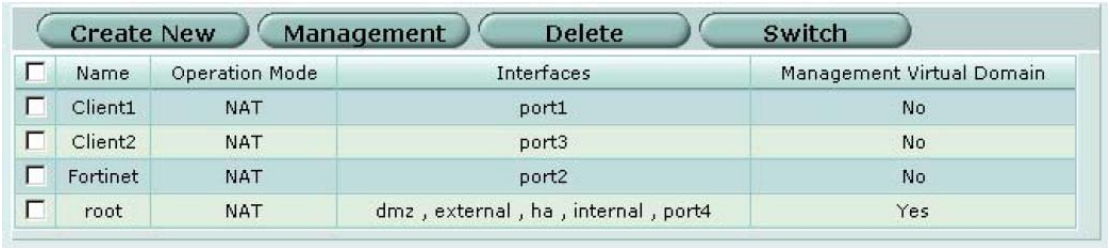
对系统进行管理的操作，如 SNMP、日志记录、报警邮件设置、使用 FDN 更新系统或使用 NTP 设置系统时间均是通过根虚拟域完成的。

通过 admin 帐户访问虚拟域

1. 使用 admin 帐户登录。
2. 进入“系统>VDOM”。

选择配置的虚拟域。

图 16：虚拟域列表



3. 选择需要配置的虚拟域名称，并点击“切换”。

打开虚拟域的配置页面。

打开页面的左下角将显示当前正在配置的虚拟域名称。

4. 虚拟域配置完成后，您可以：

- 点击“全局”退回到虚拟域配置页面。
- 退出配置页面。

作为常规管理员访问一个虚拟域

1. 连接到配置属于您要访问的 VDOM 的接口。

您也可以连接到 console 连接器，使用 CLI 配置根虚拟域。

2. 使用属于 VDOM 的管理员帐户登录。

进入基于 web 的管理器主页面。从主页面中您可以访问具体的 VDOM 配置项。

配置虚拟域

在 FortiGate 设备上配置 VDOM，您需要：

- 更改管理 VDOM
- 对虚拟域添加接口与 VLAN 子接口
- 对虚拟域配置路由
- 对虚拟域配置防火墙策略
- 对虚拟域配置 VPN

更改管理虚拟域

默认情况下，管理虚拟域是根虚拟域。当您配置了其它虚拟域后，管理虚拟域的流量设置可以转移到新配置的虚拟域。管理流量通常指从 FortiGate 设备发出的任何流量。包括：

- DNS 查询
- 将日志记录到 FortiAnalyzer 设备、syslog 或 webtrend 设备
- FortiGuard 服务
- 发送报警邮件
- 网络时间协议流量（ntpd）
- 发送 SNMP 陷阱
- 隔离可疑文件与电子邮件

在您更改管理 VDOM 之前，确定选择了虚拟域配置项。为了能够连接到 NTP 与 FortiGuard 中心这样的远程服务，管理域需要配置一个能够连接到互联网的接口。

**注意**：如果存在任何管理员使用 RADIUS 验证，您便不能更改管理虚拟域。

使用基于 web 的管理器更改管理虚拟域

以下操作将管理虚拟域从根虚拟域更改为名为 mgmt_vdom 的虚拟域。

1. 进入“系统>VDOM”。
2. 选择 mgmt_vdom 作为新的管理域。
3. 点击“应用”确认更改管理虚拟域的操作。

使用 CLI 更改管理虚拟域

configuration global

configuration system global

set management-vdom mgmt_vdom

end

mgmt_vdom 将作为新的管理域。

对虚拟域添加接口与VLAN子接口

一个虚拟域必须包括至少两个接口，可以是物理接口或 VLAN 接口。默认情况下，所有的物理接口都属于根虚拟域，并且在您创建新的 VLAN 时，默认的虚拟域是根虚拟域。

对虚拟域添加接口与 VLAN 子接口

1. 如果您不在根虚拟域中，回退到“全局”配置页面。
2. 进入 “系统>网络>接口”。
3. 点击“新建”添加 VLAN 接口。
4. 输入能够识别 VLAN 接口的名称。
5. 选择通过该 VLAN 子接口接收 VLAN 数据包的物理接口。该接口可以是 VLAN 中不同的虚拟域接口。
6. 输入与该 VLAN 子接口接收到的数据包的 VLAN ID 相匹配的 VLAN ID。
7. 选择该 VLAN 子接口属于的虚拟域。
8. 配置 VLAN 子接口的方法类似 FortiGate 接口的配置。
9. 点击 OK 保存配置更改。

在您执行步骤 5 时，将看到新的 VLAN 子接口添加到接口中。而后，点击显示该接口的全部子接口时，接口旁将出现“+”图标。

将现有的接口转移到其它虚拟域

1. 如果您不在根虚拟域中，回退到“全局”配置页面。
2. 进入“系统>网络>接口”。
3. 点击您所要移动的物理接口旁边的“编辑”图标。
4. 从虚拟域列表中选择该接口属于的新的虚拟域。
5. 点击 OK 确认。

接口转移到所选的虚拟域中。对该接口配置的防火墙 IP 池与虚拟 IP 都将被删除。您应该手工删除对该接口配置的路由。

对虚拟域添加区域

1. 进入“系统>VDOM”。
2. 点击所要编辑的虚拟域，并点击“切换”。
3. 进入“系统>网络>区域”。
4. 选择所要添加区域的虚拟域。
5. 点击“新建”。

对虚拟域配置路由

虚拟域的路由设置是每个虚拟域唯一性的，需要单独设置。每个虚拟域应该配置至少一条默认的静态路由。您可以对每个虚拟域配置动态路由，其它 VDOM 可以作为邻居。

对虚拟域配置路由

1. 作为 admin 登录，进入“系统>VDOM”。
2. 选择所要编辑的 VDOM，并点击“切换”。
3. 进入“系统>路由”。
4. 根据需要对当前虚拟域配置路由。

您所定义的路由只应用于属于该虚拟域的接口通过的流量。

对虚拟域配置防火墙策略

每个虚拟域必须具有其自己的防火墙策略。包括对虚拟域添加防火墙地址并配置防火墙策略。

设置虚拟域的防火墙策略

1. 以 admin 管理员登录，进入“系统>虚拟域”。
2. 选择所要配置的 VDOM，并点击“切换”。

3. 进入“防火墙>地址”。

4. 对当前的虚拟域添加新的防火墙地址、地址范围与地址组。

对虚拟域配置防火墙策略

1. 以 admin 管理员登录，进入“系统>虚拟域”。

2. 选择所要配置的 VDOM，并点击“切换”。

3. 进入“防火墙>策略”。

4. 点击“新建”给当前的虚拟域添加防火墙策略。

您只能对物理接口、VLAN 子接口以及区域添加防火墙策略。所添加的防火墙策略只有在您查看当前虚拟域的时才可以显示。接口与 VLAN 子接口所接收的网络流量将被添加到该虚拟域中，并且受到该虚拟域中添加的防火墙策略的控制。

对虚拟域配置VPN

每个 VDOM 的 IPSec 通道、IPSec 接口、PPTP 与 SSL 配置也是唯一性的，需要单独设置。但是，证书却是可以被所有虚拟域共享的。

对虚拟域配置 VPN

1. 以 admin 帐户登录，进入“系统>VDOM”。

2. 选择所有配置的 VDOM，并点击“切换”。

3. 进入 VPN。

4. 根据需要配置 IPSec 通道、IPSec 接口、PPTP 与 SSL。

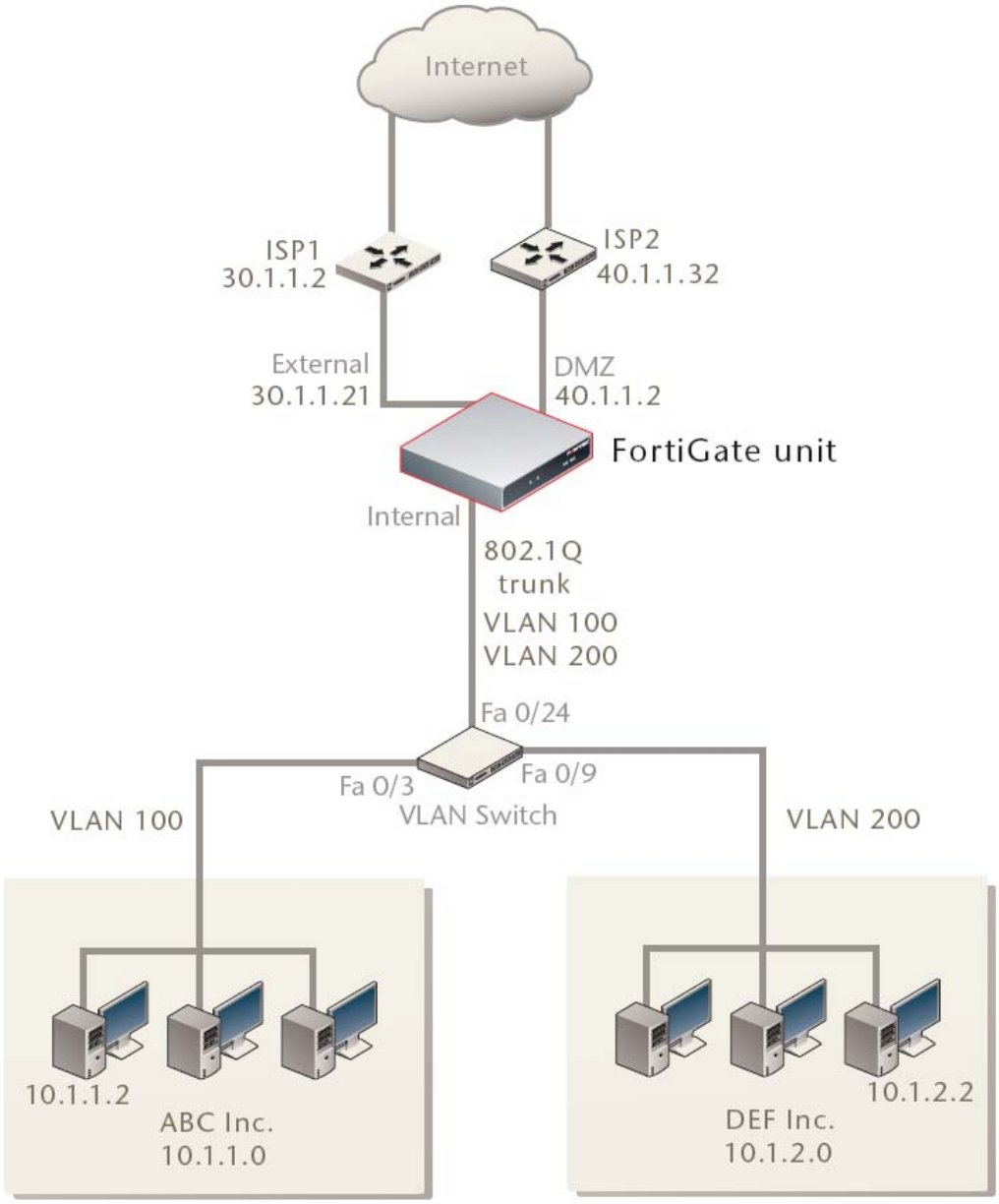
NAT/路由模式下配置虚拟域举例（简单）

图 17 所示是 NAT/路由模式下简化的 VLAN 配置，举例中 FortiGate 设备对两个保护对象的网络提供实时的防护功能。FortiGate 设备中对两个保护对象均设置了各自的虚拟域，对其进行单独的网络防护配置。

Cisco 2950 交换机将两个被保护对象所属的 LAN 通过 802.1Q trunk 连接到 FortiGate-800 的内部接口。内部接口有两个 VLAN 子接口，分别为 VLAN100 与 VLAN200。

FortiGate-800 的外部与 DMZ 接口通过不同的 ISP 连接到互联网。这些接口没有配置 VLAN 子接口。

图 17：运行于 NAT/路由模式下的 FortiGate 设备



当交换机从 VLAN100 与 VLAN200 接收数据包后，这些数据包都应用了正确的 VLAN ID 标签，交换机将这些数据包通过 trunk 转发到 FortiGate 设备。FortiGate 作为第三层网络设备，具有允许将 VLAN100 发出的流量发送到外部网络的功能，并配置了允许 VLAN200 的流量发送到 DMZ 网络的策略。

以下将对如何配置 FortiGate-800 设备与 Cisco 交换机运行于以上的拓扑结构进行说明。

常规配置步骤

该举例注明为简单配置，所以只进行大致的步骤说明。

FortiGate-800 与 Cisco 交换机的基本配置

1. 创建虚拟域。

2. 配置 FortiGate-800 外部接口与 DMZ 接口。
3. 配置 FortiGate 设备中的每个虚拟域：
   - 在外部网络接口添加一个 VLAN 子接口。
   - 对内部与外部网络添加防火墙地址与地址范围。
   - 添加防火墙策略允许 VLAN 访问外部网络。
   - 配置默认的路由访问 ISP。
4. 配置 Cisco 交换机支持 VLAN 标签。
5. 测试配置。

创建虚拟域

本示例中创建了两个新的虚拟域：ABC 域属于 ABC 公司，DEF 域属于 DEF。您可以使用基于 web 的管理器与 CLI 工具创建虚拟域。

使用基于 web 的管理器创建虚拟域

1. 以 admin 帐户登录。
2. 进入“系统>VDOM”，点击“新建”。
3. 输入“ABC 域”，并点击 OK 确认。
4. 点击“新建”。
5. 输入“DEF 域”，并点击 OK 确认。

使用 CLI 创建虚拟域

```
config vdom
edit ABCdomain
next
edit DEFdomain
end
```

配置FortiGate-800设备的外部与DMZ接口

使用基于 web 的管理器配置 FortiGate-800 设备。点击“全局配置”。对每个公司配置接口连接到互联网的连接。

注意：如果您不能更改网络接口的 VDOM，那是因为这个接口中含有一些配置条目还没有被删除。删除这些配置后，接口便重新可用并可以切换到不同的

虚拟域。例如，外部接口的一般配置条目是默认的静态路由。

配置外部接口

使用基于 web 的管理器与 CLI 均可以配置外部接口。

使用基于 web 的管理器配置外部接口

1. 以 admin 帐户登录。
2. 进入“系统>网络>接口”。
3. 点击外部接口的编辑图标。
4. 输入以下信息并点击 OK 确认。

虚拟域	ABC 域
寻址模式	手工
IP/掩码	30.1.1.21/255.255.255.0
根据需要配置其它字段。	

使用 CLI 配置外部接口

config global

config system interface

edit external

set vdom ABCdomain

set mode static

set ip 30.1.1.21 255.255.255.0

end

end

配置 DMZ 接口

使用基于 web 的管理器与 CLI 均可以配置 DMZ 接口。

使用基于 web 的管理器配置 DMZ 接口

1. 以 admin 帐户登录。
2. 进入“系统>网络>接口”。

3. 点击外部接口的编辑图标。

4. 输入以下信息并点击 OK 确认。

虚拟域	DEF 域
寻址模式	手工
IP/掩码	40.1.1.32/255.255.255.0
根据需要配置其它字段。	

使用 CLI 配置 DMZ 接口

config global

config system interface

edit dmz/ha

set vdom DEFdomain

set mode static

set ip 40.1.1.32 255.255.255.0

end

end

配置ABC虚拟域

在该示例中，ABC 虚拟域是设置应用于 ABC 公司。您可以对其配置 VLAN 子接口 VLAN_100 以及防火墙策略允许到外部接口的连接。

- 添加 VLAN 接口，提供了到 VDOM 的接收与发送数据包途径。接口是全局配置的一部分。
- 添加防火墙策略允许到外部接口的连接以及限制不需要的流量。一项防火墙策略只能应用于一个 VDOM。

添加 VLAN 子接口

VLAN100 表示 ABC 公司怎样与外界通信。确定添加了 HTTPS 这样的访问协议。否则，ABC 公司将不能管理自己的虚拟域。

添加 VLAN100 子接口

1. 以 admin 帐户登录。

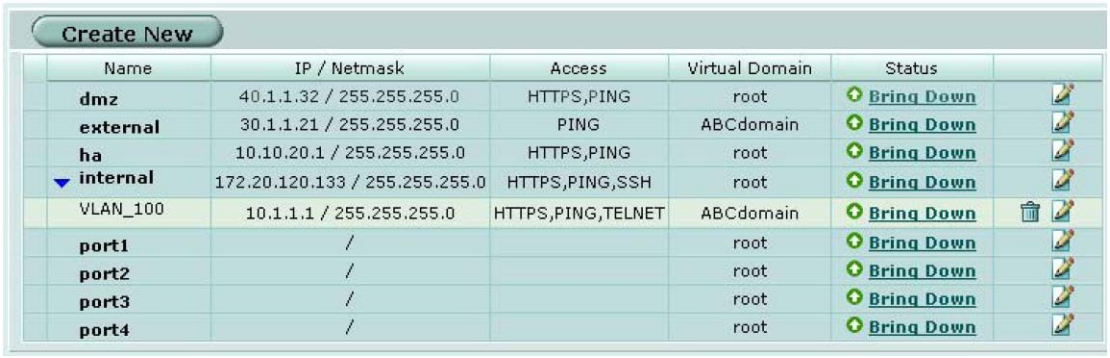
2. 进入“系统>网络>接口”。

3. 点击“新建”。

4. 对 VLAN_100 输入以下信息并点击 OK 确认。

名称	VLAN_100
接口	内部接口
VLAN ID	100
虚拟域	ABC 虚拟域
寻址模式	手工寻址
IP/掩码	10.1.1.1/255.255.255.0
根据需要配置其它字段。	

图 18：ABC 虚拟域接口与子接口



使用 CLI 添加 VLAN100 子接口

config global

config system interface

edit VLAN_100

set interface internal

set vlanid 100

set vdom ABCdomain

set mode static

set ip 10.1.1.1 255.255.255.0

set allowaccess https ping telnet

end

end

添加 ABC 虚拟域防火墙地址

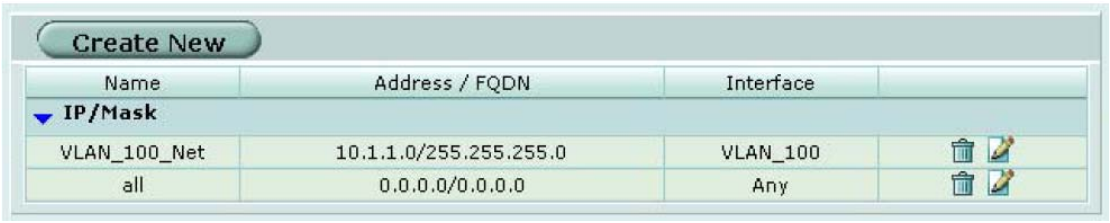
您需要定义 VLAN 子网的地址以便应用防火墙策略。FortiGate 设备提供一项默认的地址“全部”，可以当一项防火墙策略应用于数据包全部的源与目标地址时使用。

使用基于 web 的管理器添加 ABC 虚拟域防火墙地址

1. 以 admin 帐户登录。
2. 进入“系统>VDOM”。
3. 选择 ABC 虚拟域，并点击“切换”。
4. 进入“防火墙>地址”。
5. 点击“新建”。
6. 输入以下信息并点击 OK 确认。

地址名称	VLAN_100_Net
类型	子网/IP 范围
IP 范围/子网	10.1.1.0/255.255.255.0
接口	VLAN_100

图 19：ABC 虚拟域防火墙地址



使用 CLI 添加 ABC 虚拟域防火墙地址

config vdom

edit ABCdomain

config firewall address

edit VLAN_100_Net

set type ipmask

set subnet 10.1.1.0 255.255.255.0

end

添加 ABC 虚拟域的防火墙策略

使用基于 web 的管理器与 CLI 均可以配置 ABC 虚拟域的防火墙策略。

使用基于 web 的管理器配置 ABC 虚拟域的防火墙策略

1. 进入“防火墙>策略”。
2. 点击“新建”。
3. 输入以下信息，并点击“OK”：

源地址		
	接口/区域	VLAN_100
	地址名称	VLAN_100_Net
目标地址		
	接口/区域	外部接口
	地址名称	全部
时间表		总是 （Always）
服务		ANY
动作		ACCEPT
NAT		点击选择
根据需要配置其它字段。		

图 20：ABC 虚拟域的防火墙策略



使用 CLI 配置 ABC 虚拟域的防火墙策略

config firewall policy

edit 1

set srcintf VLAN_100

set dstintf external

set srcaddr VLAN_100_Net

set dstaddr all

set schedule always

set service ANY

set action accept

set nat enable

set status enable

end

添加默认路由

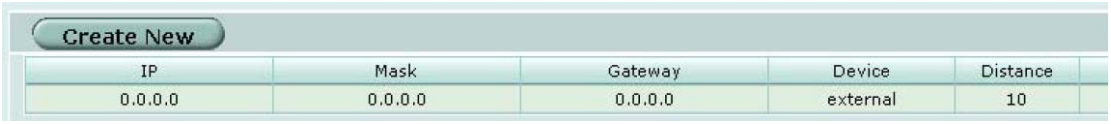
如果数据包的目标地址时 VLAN100 子网以外的网络，您需要定义默认的路由将数据包发送到外部 ISP。

使用基于 web 的管理器添加路由

1. 进入“路由>静态”。
2. 点击“新建”添加新的路由。
3. 输入以下经外部接口到 ISP1 的路由信息并点击 OK：

目标 IP/掩码	0.0.0.0/0.0.0.0
接口	外部接口
网关	30.1.1.2
管理距离	10

图 21：ABC 虚拟域的路由表



使用 CLI 添加路由

config router static

edit 1

set device external

set gateway 30.1.1.2

end

配置DEF虚拟域

在该示例中，DEF 虚拟域是设置应用于 DEF 公司。您可以对其配置 VLAN 子接口 VLAN_200 以及防火墙策略允许到外部接口的连接。

添加 VLAN 子接口

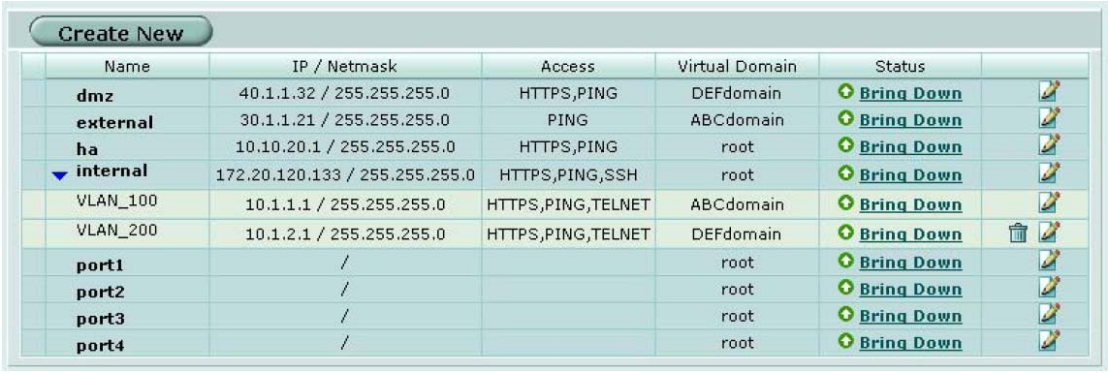
VLAN200 表示 ABC 公司怎样与外界通信。确定添加了 HTTPS 这样的访问协议。否则，ABC 公司不能管理自己的虚拟域。

使用基于 web 的管理器添加 VLAN200 子接口

1. 以 admin 帐户登录。
2. 进入“系统>网络>接口”。
3. 点击“新建”。
4. 对 VLAN_200 输入以下信息并点击 OK 确认。

名称	VLAN_200
接口	内部接口
VLAN ID	200
虚拟域	DEF 虚拟域
寻址模式	手工寻址
IP/掩码	10.1.2.1/255.255.255.0
管理访问	HTTPS，PING，TELNET
根据需要配置其它字段。	

图 22：DEF 虚拟域接口与子接口



注意上图中没有可以执行删除 VLAN_100 功能的删除图标，这是因为 VLAN_100 添加了防火墙策略。在删除 VLAN_100 之前先要删除对其配置的防火墙配置策略。

使用 CLI 添加 VLAN200 子接口

config global

config system interface

edit VLAN_200

set interface internal

set vlanid 200

set vdom DEFdomain

set mode static

set ip 10.1.2.1 255.255.255.0

set allowaccess https ping telnet

end

end

添加 DEF 虚拟域防火墙地址

您需要定义 VLAN 子网的地址以便应用防火墙策略。FortiGate 设备提供一项默认的地址“全部”，可以当一项防火墙策略应用于数据包全部的源与目标地址时使用。

使用基于 web 的管理器添加 DEF 虚拟域防火墙地址

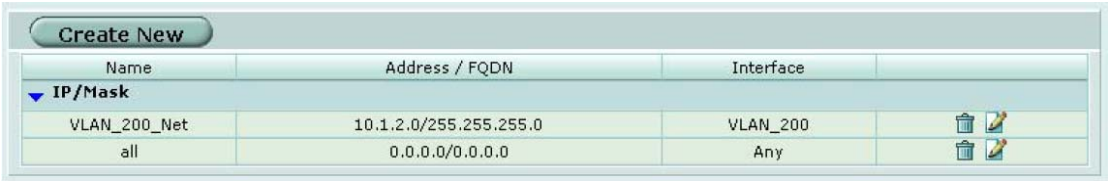
1. 以 admin 帐户登录。
2. 进入“系统>VDOM”。
3. 选择 ABC 虚拟域，并点击“切换”。
4. 进入“防火墙>地址”。

5. 点击“新建”。

6. 输入以下信息并点击 OK 确认。

地址名称	VLAN_200_Net
类型	子网/IP 范围
IP 范围/子网	10.1.2.0/255.255.255.0
接口	VLAN_200

图 23：DEF 虚拟域防火墙地址



使用 CLI 添加 DEF 虚拟域防火墙地址

config vdom

edit DEFdomain

config firewall address

edit VLAN_200_Net

set type ipmask

set subnet 10.1.2.0 255.255.255.0

end

添加 DEF 虚拟域的防火墙策略

使用基于 web 的管理器与 CLI 均可以配置 DEF 虚拟域的防火墙策略。

使用基于 web 的管理器配置 DEF 虚拟域的防火墙策略

1. 以 admin 帐户登录。

2. 进入“系统>VDOM”。

3. 选择 DEF 虚拟域，并点击“切换”。

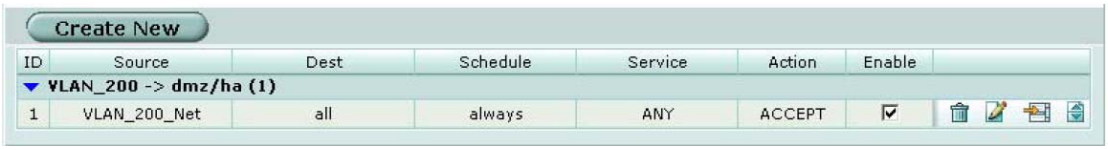
4. 进入“防火墙>策略”。

5. 点击“新建”。

6. 输入以下信息，并点击“OK”：

源地址		
	接口/区域	VLAN_200
	地址名称	VLAN_200_Net
目标地址		
	接口/区域	dmz/ha
	地址名称	全部
时间表		总是 （Always）
服务		ANY
动作		ACCEPT
NAT		点击选择
根据需要配置其它字段。		

图 24：DEF 虚拟域的防火墙策略



使用 CLI 配置 DEF 虚拟域的防火墙策略

config firewall policy

edit 1

set srcintf VLAN_200

set dstintf dmz/ha

set srcaddr VLAN_200_Net

set dstaddr all

set schedule always

set service ANY

set action accept

set nat enable

set status enable

end

添加默认路由

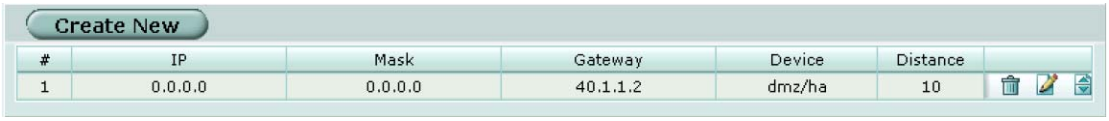
如果数据包的目标地址是 VLAN200 子网以外的网络，您需要定义默认的路由将数据包发送到外部 ISP2。

使用基于 web 的管理器添加路由

1. 以 admin 帐户登录。
2. 进入“系统>VDOM”。
3. 选择 DEF 虚拟域，并点击“切换”。
4. 进入“路由>静态”。
5. 点击“新建”添加新的路由。
6. 输入以下经外部接口到 ISP 的路由信息并点击 OK：

目标 IP/掩码	0.0.0.0/0.0.0.0
接口	40.1.1.2
网关	dmz/ha
管理距离	10

图 25：DEF 虚拟域的路由表



使用 CLI 添加路由

config router static

edit 1

set device external

set gateway 40.1.1.2

end

配置Cisco交换机

在 Cisco Catalyst 2950 以太网交换机中，您需要在 VLAN 数据库中定义 VLAN 100 与 VLAN200，然后添加配置文件以定义 VLAN 子接口与 802.1Q trunk 接口。

配置 VLAN 子接口与 trunk 接口

在 Cisco 交换机中添加以下命令：

```
!
interface FastEthernet0/3
switchport access vlan 100
!
interface FastEthernet0/9
switchport access vlan 200
!
interface FastEthernet0/24
switchport trunk encapsulation dot1q
switchport mode trunk
!
```

交换机具有以下配置：

端口 0/3	VLAN ID 100
端口 0/9	VLAN ID 200
端口 0/24	802.1Q trunk

注意：在应用 VLAN 之前还需要配置 VLAN 的默认网关。VALN100 的默认网关是 FortiGate VLAN100 子接口。VLAN200 的默认网关是 FortiGate VLAN200 子接口。

测试配置

使用诊断命令（tracert,ping）测试 FortiGate 设备与 Cisco 交换机之间的路由流量。

测试 VLAN100 到外部网络的流量

以下测试举例中，是对内部网络到外部网络的路由设置跟踪的。路由目标是 FortiGate-800 设备的外部网络接口。

从 VLAN100，在命令提示符下输入：

C:\>tracert 30.1.1.21

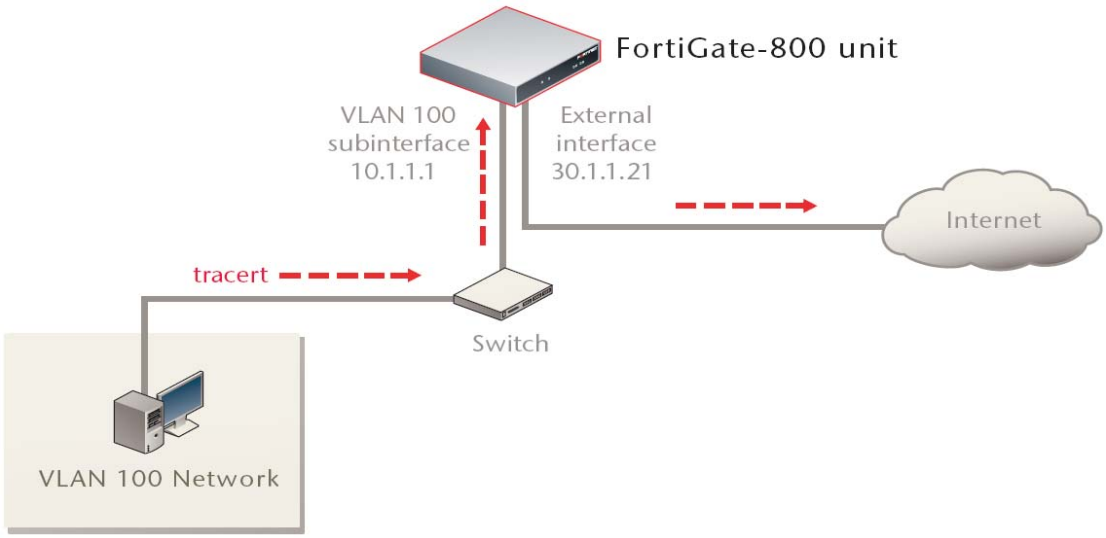
Tracing route to 30.1.1.21 over a maximum of 30 hops:

1 <10 ms <10 ms <10 ms 10.1.1.1

2 <10 ms <10 ms <10 ms 30.1.1.21

Trace complete.

图 26：从 VLAN100 到外部网络的路由跟踪



测试从 VLAN200 到 DMZ 网络的流量

以下测试举例中，是对内部网络到外部网络的路由设置跟踪的。路由目标是 FortiGate-800 设备的 DMZ 网络接口。

从 VLAN200，在命令提示符下输入：

C:\>tracert 40.1.1.32

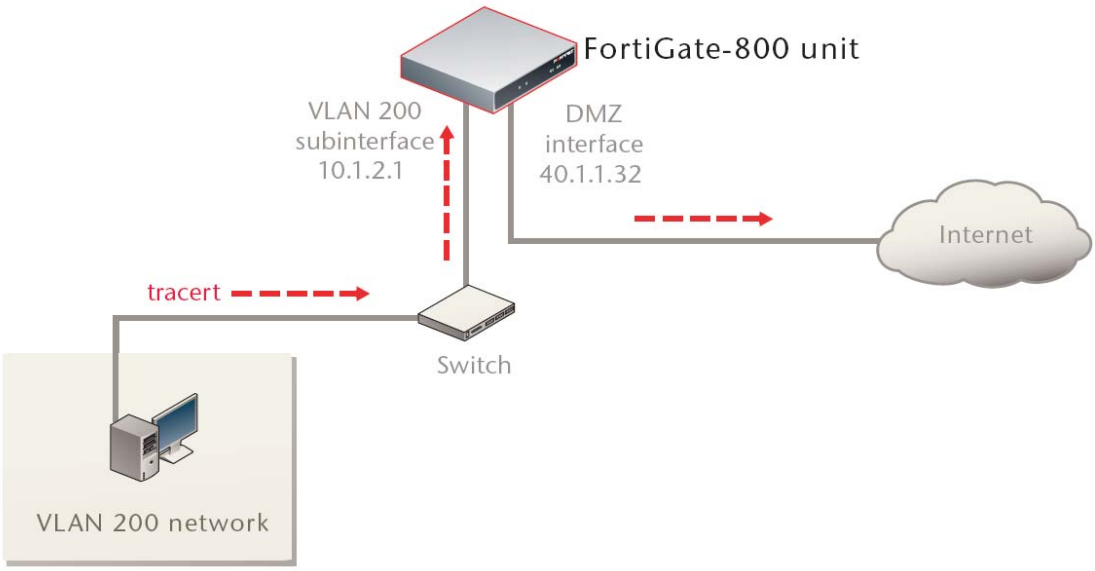
Tracing route to 40.1.1.32 over a maximum of 30 hops:

1 <10 ms <10 ms <10 ms 10.1.2.1

2 <10 ms <10 ms <10 ms 40.1.1.32

Trace complete.

图 27：从 VLAN200 到 DMZ 网络的路由跟踪



运行于 NAT/路由模式下的虚拟域配置（复杂）

在该示例中，一台 FortiGate-800 设备运行于 NAT/路由模式，对两个对象提供网络防护服务器。举例中，应用了两个虚拟域。ABC 虚拟域服务于由学生与教师组成的网络。第二个域，commercial 性质的，是由产品开发与销售构成的网络。FortiGate-800 的内部与外部接口通过传送虚拟域之间流量的 trunk 网络连接到 Cisco 交换机。

图 28 所示是示例网络的拓扑结构，红色标注区域表示 commercial 虚拟域。

需要对 ABC 虚拟域进行如下配置：

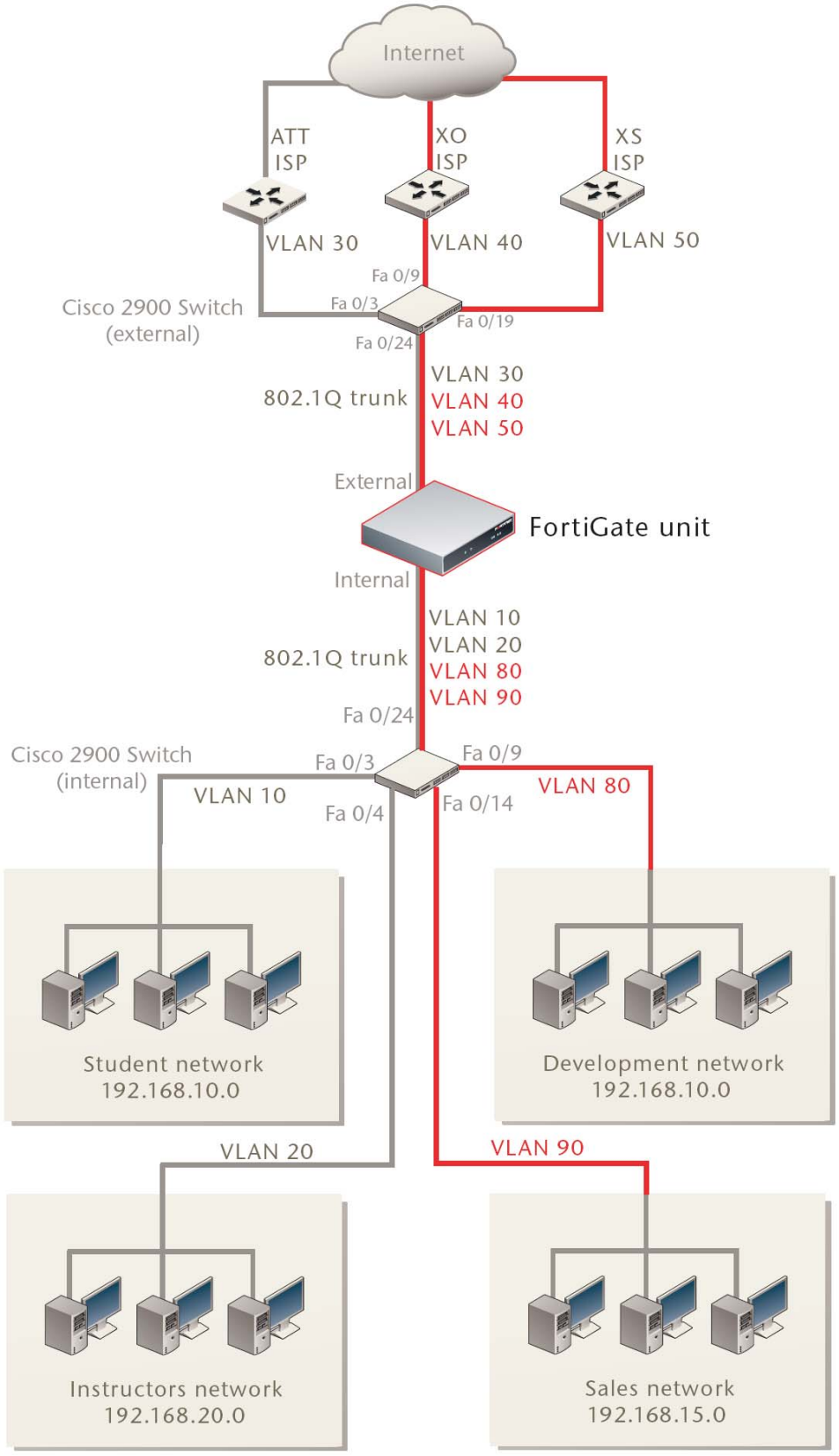
- 对内部接口配置两个 VLAN 子接口，分别为：VLAN10，应用于学生网络；VLAN20，应用于教师网络。
- 对外部接口配置一个 VLAN 子接口 VLAN30 用于 ATT-ISP 网络。
- 配置防火墙策略允许学生与教师网络通过 ATT-ISP 网络访问互联网。对于学生网络可以配置比较严格的策略控制在线的活动。
- 配置防火墙策略允许教师访问学生网络。

需要对 Commercial 虚拟域进行以下配置：

- 对内部接口配置两个 VLAN 子接口，分别为：VLAN80，应用于销售网络；VLAN90，应用于产品开发网络。
- 对外部接口配置两个 VLAN 子接口，分别为 VLAN40 与 VLAN50，用于通过冗余 XO-ISP 与 XS-ISP 网络访问互联网。
- 配置防火墙策略允许通过销售与产品开发网络访问互联网。

您应该注意到了，学生网络与产品开发网络具有相同的网络地址范围。两个地址范围是不同的虚拟域中，所以不会造成任何问题。

图 28：VLAN/VDOM 拓扑结构示例（FortiGate 设备运行于 NAT/路由模式）



常规配置步骤

根据以上拓扑结构需要配置很多个区域。以下将说明大致的配置步骤。配置中不重复登录与进入菜单项步骤。

1. 创建 commercial 域。
2. 配置 ABC 虚拟域：
   - 添加 VLAN 子接口。
   - 配置默认路由。
   - 对于 VLAN 连接的网络添加防火墙地址。
   - 添加防火墙策略以允许：
     1) 教师网络访问学生网络
     2) 教师网络访问外部网络
     3) 在配置了较严格的内容保护后，允许学生网络访问外部网络
3. 配置 commercial 域：
   - 添加 VLAN 子接口。
   - 配置默认路由与二级默认路由。
   - 对 VLAN 添加防火墙地址。
   - 添加防火墙策略以允许：
     1) 产品开发网络访问销售网络
     2) 销售网络访问产品开发网络
     3) 销售网络访问外部网络
     4) 产品开放网络访问外部网络
4. 配置 Cisco 交换机。
5. 测试配置

创建虚拟域

该示例中创建了两个虚拟域，对学校的 ABC 虚拟域，以及对公司的 commercial 虚拟域。

使用基于 web 的管理器创建虚拟域

1. 以 admin 帐户登录。
2. 进入“系统>VDOM”，点击“新建”。

3. 输入“ABC 域”，并点击 OK 确认。

4. 点击“新建”。

5. 输入“commercial 域”，并点击 OK 确认。

使用 CLI 创建虚拟域

config vdom

edit ABCdomain

next

edit Commercial

end

配置ABC虚拟域

在示例中，ABC 虚拟域配置服务于学校。您可以在内部接口与外部接口分别配置两个 VLAN 子接口，以及防火墙策略允许从内部 VLAN 到外部接口 VLAN 的连接。

选择 ABC 虚拟域

在配置 ABC 虚拟域之前，先要确定已经登录进入该虚拟域。

1. 进入“系统>VDOM”。

2. 选择 ABC 虚拟域，点击“切换”进入该虚拟域。

使用 CLI 切换到所要配置的虚拟域

config vdom

edit ABCdomain

添加 VLAN 子接口

ABC 虚拟域中，您需要在内部外部接口上配置两个 VLAN 子接口，从学生与教师网络接收 VLAN10 与 VLAN20 的数据包。在外部接口配置一个 VLAN 子接口将数据包发送到 ATT-ISP 网络中的 VLAN30。

使用基于 web 的管理器添加 VLAN 子接口

1. 如果启动 VDOM，且您不在根 VDOM 中，点击“全局”。

2. 进入“系统>网络>接口”。

3. 点击“新建”。

4. 设置 VLAN_100 的以下信息，并点击 OK。

名称	students
类型	VLAN
接口	内部接口
VLAN ID	10
虚拟域	ABC 虚拟域
寻址模式	手工
IP/掩码	192.168.10.1/255.255.255.0
根据需要配置其它字段。	

5. 点击“新建”。

6. 设置教师网络的以下信息，并点击 OK。

名称	instructors
类型	VLAN
接口	内部接口
VLAN ID	20
虚拟域	ABC 虚拟域
寻址模式	手工
IP/掩码	192.168.20.1/255.255.255.0
根据需要配置其它字段。	

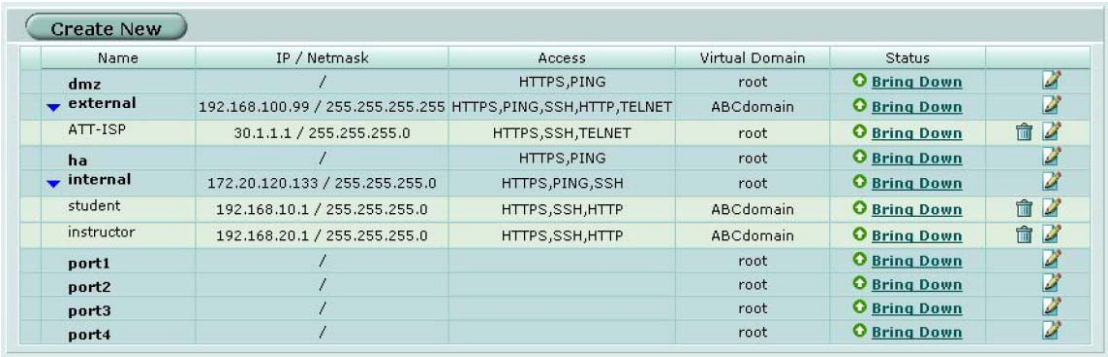
7. 点击“新建”。

8. 对 ATT-ISP 网络设置以下信息，并点击 OK 确认。

名称	ATT-ISP

类型	VLAN
接口	外部接口
VLAN ID	30
虚拟域	ABC 虚拟域
寻址模式	手工
IP/掩码	30.1.1.1/255.255.255.0
根据需要配置其它字段。	

图 29：对 ABC 虚拟域设置 VLAN 子接口



使用 CLI 添加 VLAN 子接口

config system interface

edit students

set interface internal

set vlanid 10

set vdom ABCdomain

set mode static

set ip 192.168.10.1 255.255.255.0

next

edit instructors

set interface internal

set vlanid 20

set vdom ABCdomain

set mode static

set ip 192.168.20.1 255.255.255.0

edit ATT-ISP

set interface external

set vlanid 30

set vdom ABCdomain

set mode static

set ip 30.1.1.1 255.255.255.0

end

添加默认路由

您需要对目标地址不在与 FortiGate 设备连接的 ABC 虚拟域的数据包设置默认的路由。这种情况下，设置路由最简单的方法便是设置 ISP 网关地址作为所有离开 VLAN 子接口连接 ISP 网络的地址。

使用基于 web 的管理器添加默认路由

1. 进入“系统>VDOM”。
2. 选择 ABC 虚拟域，并点击“切换”。
3. 进入“路由>静态”。
4. 点击“新建”添加新的路由。
5. 输入从 ABC 虚拟域发出离开外部接口到达 ATT-ISP 网络数据包的路由信息并点击 OK：

目标 IP/掩码	0.0.0.0/0.0.0.0
接口	ATT-ISP
网关	30.1.1.2
管理距离	10

使用 CLI 添加默认路由

config router static

edit 1

set device ATT-ISP

set gateway 30.1.1.2

next

end

添加防火墙地址

您需要在防火墙策略选项中定义 ABC 虚拟域子网的地址。FortiGate 设备中默认的地址是“全部（all）”，也就是说，对通过防火墙的所有地址，源或目标地址的数据包应用同一项防火墙策略。其它虚拟域中，您也需要创建防火墙地址。

使用基于 web 的管理器添加防火墙地址

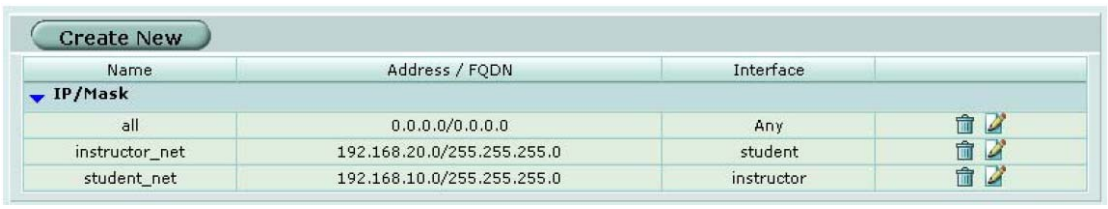
1. 进入“防火墙>地址”。
2. 点击“新建”。
3. 输入以下信息并点击 OK：

地址名称	students_net
类型	子网/IP 地址范围
子网/IP 范围	192.168.10.0/255.255.255.0
接口	任何

4. 点击“新建”。
5. 输入以下信息并点击 OK：

地址名称	instructor_net
类型	子网/IP 地址范围
子网/IP 范围	192.168.20.0/255.255.255.0
接口	任何

图 30：ABC 虚拟域的防火墙地址



使用 CLI 添加防火墙地址

config firewall address

edit all

set subnet 0.0.0.0 0.0.0.0

next

edit student_net

set subnet 192.168.10.0 255.255.255.0

next

edit instructor_net

set subnet 192.168.20.0 255.255.255.0

end

添加防火墙策略

对于每个内部网络，需要设置策略允许访问 ATT-ISP 网络以便连接到互联网。通过对每项策略选择不同的保护设置，两组用户可以应用不同级别的 web 过滤、web 过滤与内容日志。为了简化示例，以下举例中使用预先配置的内容保护设置级别“严格”与“扫描”。您可以根据需要修改保护内容设置或创建用户定义的保护设置。

使用基于 web 的管理器添加防火墙策略

1. 进入“防火墙>策略”。
2. 点击“新建”。
3. 输入以下信息，并点击“OK”：

源地址		
	接口/区域	students
	地址名称	student_net
目标地址		
	接口/区域	ATT-ISP
	地址名称	全部

时间表	总是 （Always）
服务	ANY
动作	ACCEPT
NAT	点击选择
保护设置	严格（strict）
根据需要配置其它字段。	

4. 点击“新建”。
5. 输入以下信息并点击 OK 确认：

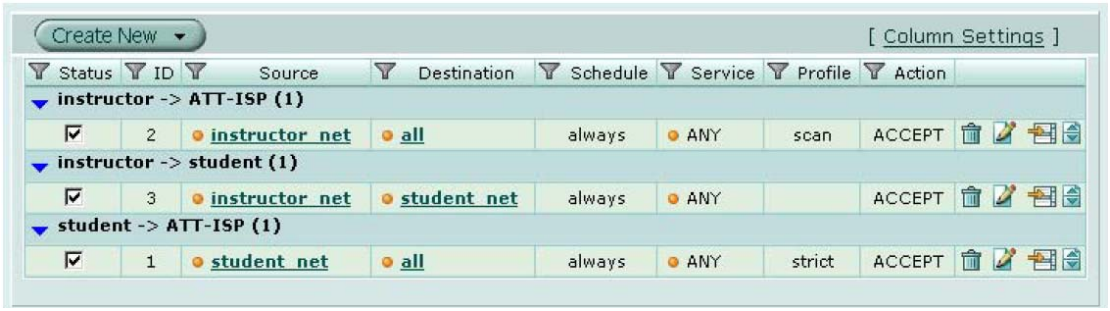
源地址		
	接口/区域	instructors
	地址名称	instructor_net
目标地址		
	接口/区域	ATT-ISP
	地址名称	全部
时间表		总是 （Always）
服务		ANY
动作		ACCEPT
NAT		点击选择
保护设置		扫描（scan）
根据需要配置其它字段。		

6. 点击“新建”。
7. 输入以下信息并点击 OK 确认：

源地址		
	接口/区域	students
	地址名称	student_net
目标地址		
	接口/区域	instructors
	地址名称	instructor_net
时间表		总是 （Always）
服务		ANY
动作		ACCEPT
NAT		点击选择
根据需要配置其它字段。		

防火墙策略如下图所示：

图 31：ABC 虚拟域的防火墙策略设置



使用 CLI 添加防火墙策略

config firewall policy

edit 1

set srcintf students

set dstintf ATT-ISP

set srcaddr student_net

set dstaddr all

```
set action accept
set schedule always
set service ANY
set profile_status enable
set profile strict
set nat enable
next
edit 2
set srcintf instructors
set dstintf ATT-ISP
set srcaddr instructor_net
set dstaddr all
set action accept
set schedule always
set service ANY
set nat enable
next
edit 3
set srcintf instructors
set dstintf students
set srcaddr student_net
set dstaddr student_net
set action accept
set schedule always
set service ANY
set nat enable
next
end
```

配置Commercial虚拟域

在示例中，Commerical 虚拟域配置服务于具有产品开发与销售网络的一个公司。Commercial 虚拟域中 VLAN 控制各部门之间的流量，并保证只有在 VLAN 中的计算机设备才可以接收流量。VLAN 的配置也可以用于多个 ISP 连接之间路由的负载平衡。

选择 Commercial 虚拟域

在配置 Commercial 虚拟域之前，先要确定已经登录进入该虚拟域。

1. 进入“系统>VDOM”。
2. 选择 ABC 虚拟域，点击“切换”进入该虚拟域。

使用 CLI 切换到所要配置的虚拟域

config vdom

edit Commercial

添加 VLAN 子接口

Commercial 虚拟域中，您需要在内部外部接口上配置两个 VLAN 子接口，从销售与产品开发网络接收 VLAN80 与 VLAN90 的数据包。在外部接口配置两个 VLAN 子接口，将数据包发送到 VLAN40 中的 XO-ISP 网络，以及 VLAN50 中的 XS-ISP 网络。

使用基于 web 的管理器添加 VLAN 子接口

1. 进入“系统>网络>接口”。
2. 点击“新建”。
3. 设置销售网络的以下信息，并点击 OK。

名称	Sales
类型	VLAN
接口	内部接口
VLAN ID	80
虚拟域	Commercial 虚拟域
寻址模式	手工

IP/掩码	192.168.15.1/255.255.255.0
根据需要配置其它字段。	

4. 点击“新建”。

5. 设置产品研发网络的以下信息，并点击 OK。

名称	Development
类型	VLAN
接口	内部接口
VLAN ID	90
虚拟域	Commercial 虚拟域
寻址模式	手工
IP/掩码	192.168.10.1/255.255.255.0
根据需要配置其它字段。	

6. 点击“新建”。

7. 对 XO-ISP 网络设置以下信息，并点击 OK 确认。

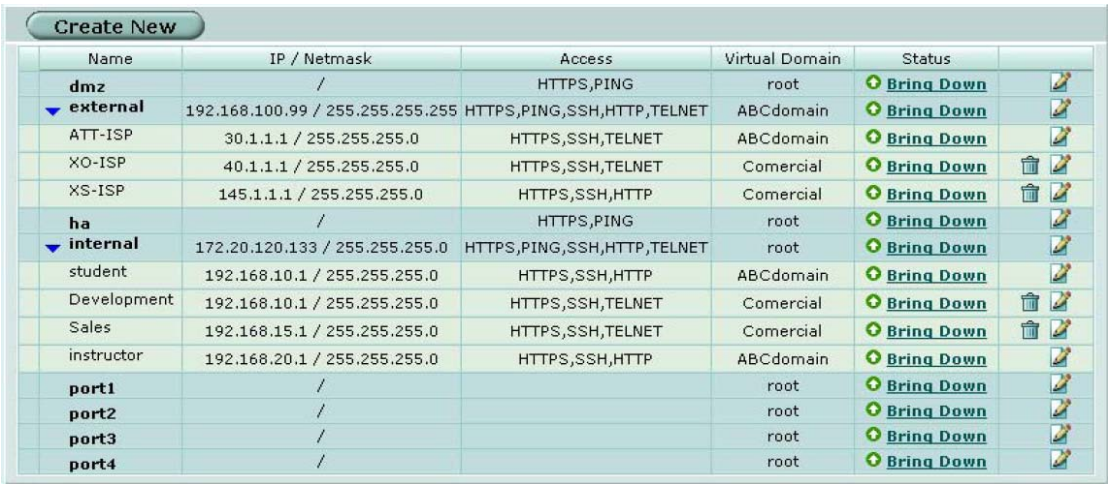
名称	XO-ISP
类型	VLAN
接口	外部接口
VLAN ID	40
虚拟域	Commercial 虚拟域
寻址模式	手工
IP/掩码	40.1.1.1/255.255.255.0
根据需要配置其它字段。	

8. 点击“新建”。

9. 对 XS-ISP 网络设置以下信息，并点击 OK 确认。

名称	XS-ISP
接口	外部接口
VLAN ID	50
虚拟域	Commercial 虚拟域
寻址模式	手工
IP/掩码	145.1.1.1/255.255.255.0
根据需要配置其它字段。	

图 32：对 Commercial 虚拟域设置 VLAN 子接口



使用 CLI 添加 VLAN 子接口

config system interface

edit Sales

set interface internal

set vlanid 80

set vdom Commercial

set mode static

set ip 192.168.15.1 255.255.255.0

next

edit Development

set interface internal

set vlanid 90

set vdom Commercial

set mode static

set ip 192.168.10.1 255.255.255.0

next

edit XO-ISP

set interface external

set vlanid 40

set vdom Commercial

set mode static

set ip 40.1.1.1 255.255.255.0

next

edit XS-ISP

set interface external

set vlanid 50

set vdom Commercial

set mode static

set ip 145.1.1.1 255.255.255.0

end

添加默认路由

您需要对目标地址不在与 FortiGate 设备连接的 ABC 虚拟域的数据包设置默认的路由。这种情况下，设置路由最简单的方法便是设置 ISP 网关地址作为所有离开 VLAN 子接口连接 ISP 网络的地址。因为本示例中还包括冗余 ISP，您也需要定义到第二 ISP 路由具有较大的距离向量。只有在默认路由不可用的情况下，FortiGate 设备才使用冗余路由。冗余 ISP 的设置是到互联网连接的备份设置。

您也可以设置使用动态路由，但是本示例中将不做说明。

使用基于 web 的管理器添加默认路由

1. 进入“系统>VDOM”。

2. 选择 Commercial 虚拟域，并点击“切换”。
3. 进入“路由>静态”。
4. 点击“新建”添加新的路由。
5. 输入从 Commercial 虚拟域发出离开外部接口到达 XO-ISP 网络数据包的路由信息并点击 OK：

目标 IP/掩码	0.0.0.0/0.0.0.0
接口	XO-ISP
网关	40.1.1.2
管理距离	10

6. 点击“新建”添加新的路由。
7. 对备份 XS-ISP 到互联网的路由连接设置以下选项并点击 OK 确认。

目标 IP/掩码	0.0.0.0/0.0.0.0
接口	XS-ISP
网关	145.1.1.2
管理距离	20

使用 CLI 添加默认路由

config router static

edit 1

set device XO-ISP

set gateway 40.1.1.2

set distance 10

next

edit 2

set device XS-ISP

set gateway 145.1.1.2

set distance 20

end

添加防火墙地址

您需要在防火墙策略选项中定义 Commercial 虚拟域子网的地址。FortiGate 设备中默认的地址是“全部（all）”，也就是说，对通过防火墙的所有地址，源或目标地址的数据包应用同一项防火墙策略。其它虚拟域中，您也需要创建防火墙地址。

使用基于 web 的管理器添加防火墙地址

1. 进入“防火墙>地址”。
2. 点击“新建”。
3. 输入以下信息并点击 OK：

地址名称	全部
类型	子网/IP 地址范围
子网/IP 范围	0.0.0.0/0.0.0.0

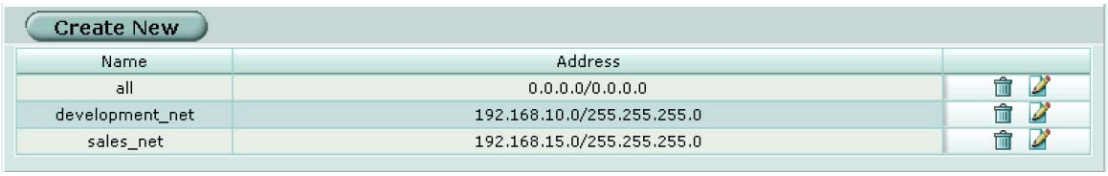
4. 点击“新建”。
5. 输入以下信息并点击 OK：

地址名称	development_net
类型	子网/IP 地址范围
子网/IP 范围	192.168.10.0/255.255.255.0

6. 点击“新建”。
7. 输入以下信息并点击 OK：

地址名称	sales_net
类型	子网/IP 地址范围
子网/IP 范围	192.168.15.0/255.255.255.0

图 33：Commercial 虚拟域的防火墙地址



使用 CLI 添加防火墙地址

config firewall address

edit all

set subnet 0.0.0.0 0.0.0.0

next

edit development_net

set subnet 192.168.10.0 255.255.255.0

next

edit sales_net

set subnet 192.168.15.0 255.255.255.0

next

end

添加防火墙策略

配置防火墙策略可以控制单向或两个具体网络之间的流量。例如，您可以设置在公司内部使用即时消息加强联络，却不希望应用连接到外部网络潜在的浪费时间与资源。或者，您想设置允许流量在所有网络中双向的传输等。凡此种种这样的情况，您均可以配置一项或多项防火墙策略实现。

通常情况下，ISP 的全部数据都可以到达 FortiGate 设备。您可以在 FortiGate 设备中配置防火墙策略阻止不良的网络流量进入您的内部网络。任何从内部网络发出到外部网络之前都需要通过防火墙策略，所以也就不需要设置额外的设备配置。

对每个内部网络，需要设置策略允许访问 XO-ISP 网络与 XS-ISP 以便连接到互联网。同样，每个内部网络需要配置防火墙策略允许其连接到其它内部网络。

使用基于 web 的管理器添加防火墙策略

1. 进入“防火墙>策略”。
2. 点击“新建”。
3. 输入以下信息，并点击“OK”：

源地址		
	接口/区域	sales
	地址名称	sales_net
目标地址		
	接口/区域	XO-ISP
	地址名称	全部
时间表		总是 （Always）
服务		ANY
动作		ACCEPT
NAT		点击选择
保护设置		扫描（scan）
根据需要配置其它字段。		

4. 点击“新建”。

5. 输入以下信息并点击 OK 确认：

源地址		
	接口/区域	sales
	地址名称	sales_net
目标地址		
	接口/区域	XS-ISP
	地址名称	全部
时间表		总是 （Always）
服务		ANY

动作	ACCEPT
NAT	点击选择
保护设置	扫描（scan）
根据需要配置其它字段。	

6. 点击“新建”。

7. 输入以下信息并点击 OK 确认：

源地址		
	接口/区域	Development
	地址名称	development_net
目标地址		
	接口/区域	XO-ISP
	地址名称	全部
时间表		总是 （Always）
服务		ANY
动作		ACCEPT
NAT		点击选择
保护设置		扫描（scan）
根据需要配置其它字段。		

8. 点击“新建”。

9. 输入以下信息并点击 OK 确认：

源地址		
	接口/区域	Development

	地址名称	development_net
目标地址		
	接口/区域	XS-ISP
	地址名称	全部
时间表		总是 （Always）
服务		ANY
动作		ACCEPT
NAT		点击选择
保护设置		扫描（scan）
根据需要配置其它字段。		

10. 点击“新建”。

11. 输入以下信息并点击 OK 确认：

源地址		
	接口/区域	sales
	地址名称	sales_net
目标地址		
	接口/区域	Development
	地址名称	development_net
时间表		总是 （Always）
服务		ANY
动作		ACCEPT
NAT		点击选择

根据需要配置其它字段。

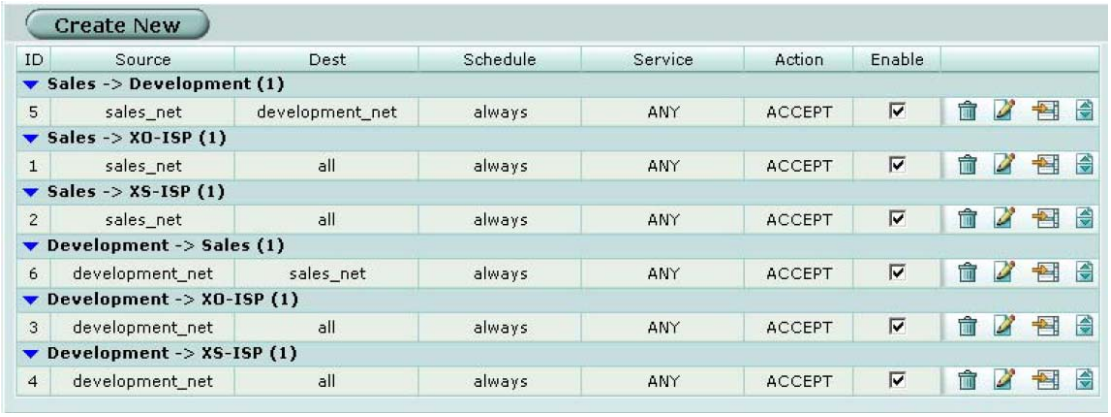
12. 点击“新建”。

13. 输入以下信息并点击 OK 确认：

源地址		
	接口/区域	Development
	地址名称	development_net
目标地址		
	接口/区域	sales
	地址名称	sales_net
时间表		总是 （Always）
服务		ANY
动作		ACCEPT
NAT		点击选择
根据需要配置其它字段。		

防火墙策略如下图所示：

图 34：Commercial 虚拟域的防火墙策略设置



使用 CLI 添加防火墙策略

config firewall policy

```
edit 1
set srcintf Sales
set dstintf XO-ISP
set srcaddr sales_net
set dstaddr all
set action accept
set schedule always
set service ANY
set profile_status enable
set profile strict
set nat enable
next
edit 2
set srcintf Sales
set dstintf XS-ISP
set srcaddr sales_net
set dstaddr all
set action accept
set schedule always
set service ANY
set profile_status enable
set profile strict
set nat enable
next
edit 3
set srcintf Development
set dstintf XO-ISP
set srcaddr development_net
set dstaddr all
set action accept
```

```
set schedule always
set service ANY
set profile_status enable
set profile strict
set nat enable
next
edit 4
set srcintf Development
set dstintf XS-ISP
set srcaddr development_net
set dstaddr all
set action accept
set schedule always
set service ANY
set profile_status enable
set profile strict
set nat enable
next
edit 5
set srcintf Sales
set dstintf Development
set srcaddr sales_net
set dstaddr development_net
set action accept
set schedule always
set service ANY
set nat enable
next
edit 6
set srcintf Development
```

set dstintf Sales

set srcaddr development_net

set dstaddr sales_net

set action accept

set schedule always

set service ANY

set nat enable

end

注意：在应用 VLAN 之前还有配置 VLAN 的默认网关。VALN10 的默认网关是 FortiGate VLAN10 子接口。VALN20 的默认网关是 FortiGate VLAN20 子接口。

配置 Cisco 交换机

在每台 Cisco Catalyst 2950 以太网交换机中，您需要在 VLAN 数据库中定义 VLAN 子接口，然后添加配置文件以定义 VLAN 子接口与 802.1Q trunk 接口。如果交换机配置不正确，网络链接不稳定且 VLAN 不能通过任何流量。

有关配置 Cisco 交换机的详细信息，参见 Cisco 交换机配置手册。

配置 VLAN 子接口与 trunk 接口

您需要在交换机配置不同的接口通过 VLAN 流量。如果交换机配置不正确，网络中没有流量通过。

配置交换机与 FortiGate-800 设备内部接口连接的接口：

!

interface FastEthernet0/3

switchport access vlan 10

!

interface FastEthernet0/4

switchport access vlan 20

!

interface FastEthernet0/14

switchport access vlan 80

!

interface FastEthernet0/16

switchport access vlan 90

!

interface FastEthernet0/24

switchport trunk encapsulation dot1q

switchport mode trunk

!

交换机具有以下配置：

端口 0/3	VLAN ID 10
端口 0/4	VLAN ID 20
端口 0/14	VLAN ID 80
端口 0/16	VLAN ID 90
端口 0/24	802.1Q trunk

配置交换机与 FortiGate-800 设备外部接口连接的接口：

!

interface FastEthernet0/3

switchport access vlan 30

!

interface FastEthernet0/9

switchport access vlan 40

!

interface FastEthernet0/19

switchport access vlan 50

!

interface FastEthernet0/24

switchport trunk encapsulation dot1q

switchport mode trunk

!

交换机具有以下配置：

端口 0/3	VLAN ID 30
端口 0/9	VLAN ID 40
端口 0/19	VLAN ID 50
端口 0/24	802.1Q trunk

测试配置

使用诊断命令（tracert,ping）测试 FortiGate 设备与 Cisco 交换机之间的路由流量。

测试教师网络到学生网络的流量

以下测试举例中，是对教师网络到学生网络的路由设置跟踪的。路由目标是学生网络中的一台主机。

从教师网络，在命令提示符下输入：

C:\>tracert 192.168.10.2

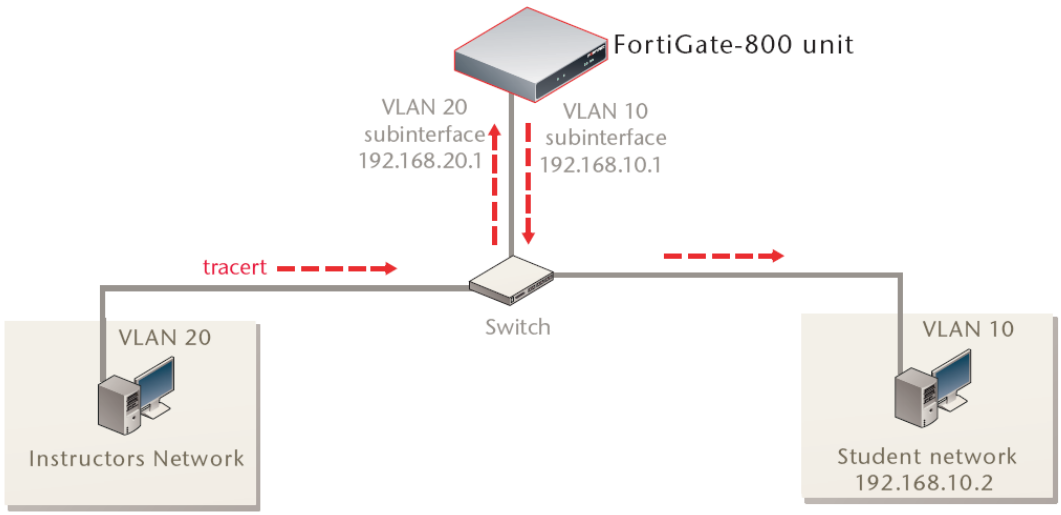
Tracing route to 192.168.10.2 over a maximum of 30 hops:

1 <10 ms <10 ms <10 ms 192.168.20.1

2 <10 ms <10 ms <10 ms 192.168.10.2

Trace complete.

图 35：从 VLAN20 到 VLAN10 的路由跟踪



其它测试

使用以上方法，您可以测试从产品研发网络到销售网络之间双向的连接情况以及每个内部网络到互联网的连接。

透明模式下应用 VLAN 与 VDOM

概述

透明模式下，FortiGate 可以在 IEEE 802.1VLAN trunk 上应用防火墙的策略和服务，例如反病毒扫描、web 过滤、垃圾邮件过滤以及入侵防护。 您可以将运行于透明模式的FortiGate设备安插到trunk链路中，不做任何的网络设置修改。典型的应用配置是，FortiGate 的内部接口接收来自与内部 VLAN 接口连接的 VLAN 交换机或路由器中一个 VLAN trunk 传输的 VLAN 数据包。FortiGate 的外部接口将没有 VLAN 标签的数据包转发到与互联网连接的外部 VLAN 交换机或路由器。您可以配置 FortiGate 设备对 trunk 中传输的 VLAN 流量应用不同的策略。

对于通过 FortiGate 设备的 VLAN 流量，您可以在设备内部接口与外部接口上分别添加具有相同 VLAN ID 的两个 VLAN 子接口；那么您可以配置防火墙策略控制内部 VLAN 接口到外部 VLAN 接口的流量。如需要，您也可以建立另一项策略允许数据包从外部 VLAN 接口到内部 VLAN 接口的连接。网络防护，如垃圾邮件过滤、web 过滤以及反病毒扫描可以在配置各项防火墙策略时指定。

对于您使用 FortiGate 设备保护的每个 VLAN，您需要定义一对 VLAN 子接口以及必要的防火墙策略。在透明模式下，通常不需要允许数据包在不同的 VLAN 之间传输。

当 FortiGate 设备在一个物理接口接收到 VLAN 标签的数据包时，该数据包将被发送到与所标记 VLAN ID 相匹配的 VLAN 子接口。与此同时，VLAN 标签将从数据包移除，并被应用防火墙策略，如同其它非 VLAN 标签数据包一样。如果数据包还需要通过 FortiGate 设备的 VLAN 子接口，那么数据包将被添加上该子接口的 VLAN ID 后转发到对应的物理接口。

VLAN与虚拟域

在添加每个 VLAN 子接口时，您需要将其与一个虚拟域建立联系。FortiGate 设备中含有一个默认的 root（根）虚拟域，在该虚拟域下，您可以添加任意多的 VLAN 子接口。

NAT 或透明模式下，一个虚拟域中最多可以添加 255 个子接口，包括 VLAN、其它虚拟接口与物理接口。配置超出 255 个接口时，您需要配套添加多个 VDOM。

如果您想配置 VLAN 子接口分为独立的组，您可以添加多个虚拟域。在一台 FortiGate 设备服务于多个对象时，这样的独立划分可以简化配置。

虚拟域的应用必要性之一在于避免当一台 FortiGate 设备连接到具有全局 MAC 列表的二层交换机时可能发生的问题。通常情况下 FortiGate 设备将 ARP 请求转发到所有的接口，包括 VLAN 子接口。那么，交换机就有可能在不同的

VLAN 中接收到重复的 ARP 数据包。一些交换机在遇到这样的情况时会重新启动。ARP 请求只需要被转发到相同虚拟域的接口，您可以通过对每个 VLAN 创建一个虚拟域来解决该问题。

配置运行于透明模式下的 FortiGate 设备

有两个必要的步骤配置运行于透明模式的 FortiGate 设备应用 VLAN：

- 添加 VLAN 子接口
- 创建防火墙策略

  您也可以配置保护内容列表如反病毒扫描、web 过滤以及垃圾邮件过滤。

透明模式下，您可以通过配置了管理访问接口并使用 HTTPS 访问管理 IP 地址连接到基于 web 的管理器。本手册示例中使用的 FortiGate-800 设备，内部接口的管理访问在默认情况下是启动的，并且默认的管理 IP 地址是 10.10.10.1。

以下示例描述中，从还没有启动虚拟域配置的操作说起。如果启动了虚拟域配置，在参见以下的操作步骤说明之前，您需要进入全局或 VDOM 配置页面。

添加VLAN子接口

每个 VLAN 子接口的 VLAN ID 必须与 IEEE802.1Q 兼容的路由或交换机添加的 VLAN ID 相匹配。VLAN ID 可以设置为 1 到 4096 之间任何的数值。您可以对接收 VLAN 标记数据包的物理接口添加 VLAN 子接口。

在透明模式下添加 VLAN 子接口

1. 进入“系统>网络>接口”。
2. 点击“新建”添加 VLAN 接口。
3. 输入能够识别 VLAN 子接口的名称。
4. 选择通过该 VLAN 子接口接收 VLAN 数据包的物理接口。
5. 输入与该 VLAN 子接口接收到的数据包的 VLAN ID 相匹配的 VLAN ID。
6. 选择该 VLAN 子接口所属的虚拟域。
7. 根据需要配置其它设置。
8. 点击 OK 保存配置更改。

FortiGate 设备将新的子接口添加到您所选择的接口中。

9. 重复步骤 2 到 8 添加其它子接口，但是得选择 VLAN 数据包通过 FortiGate 设备的物理接口。使用与以上步骤中设置的相同的 VLAN ID 与虚拟域。
10. 对于您设置添加的每个 VLAN 子接口，点击“启动（bring up）”图标启用接口。

创建防火墙策略

防火墙策略是根据通过 FortiGate 设备网络接口数据包的源与目标地址控制其流量。或者，通过防火墙策略，您可以对流量限制时间或控制一些服务。

透明模式下，FortiGate 设备对每个 VLAN 中的数据包在通过设备时应用反病毒与反垃圾邮件扫描这样的服务。您需要对数据包进入与出去的 FortiGate 设备的 VLAN 接口添加防火墙策略允许流量穿行。如果不配置防火墙策略，没有数据包能够从一个接口传输到其它的接口。

对 VLAN 子接口添加防火墙策略

1. 进入“防火墙>地址”。
2. 点击“新建”添加与 VLAN 数据包的源以及目标 IP 地址相匹配的防火墙地址。
3. 进入“防火墙>策略”。
4. 点击“新建”。
5. 从源接口/区域列表中选择数据包进入 FortiGate 设备的 VLAN 接口。
6. 从目标接口/区域列表中选择数据包通过 FortiGate 设备出去的 VLAN 接口。
7. 输入源与目标地址名称。
8. 从保护内容列表中选择保护项目。
9. 根据需要配置其它选项。
10. 点击 OK 确认。

透明模式下配置举例（简单）

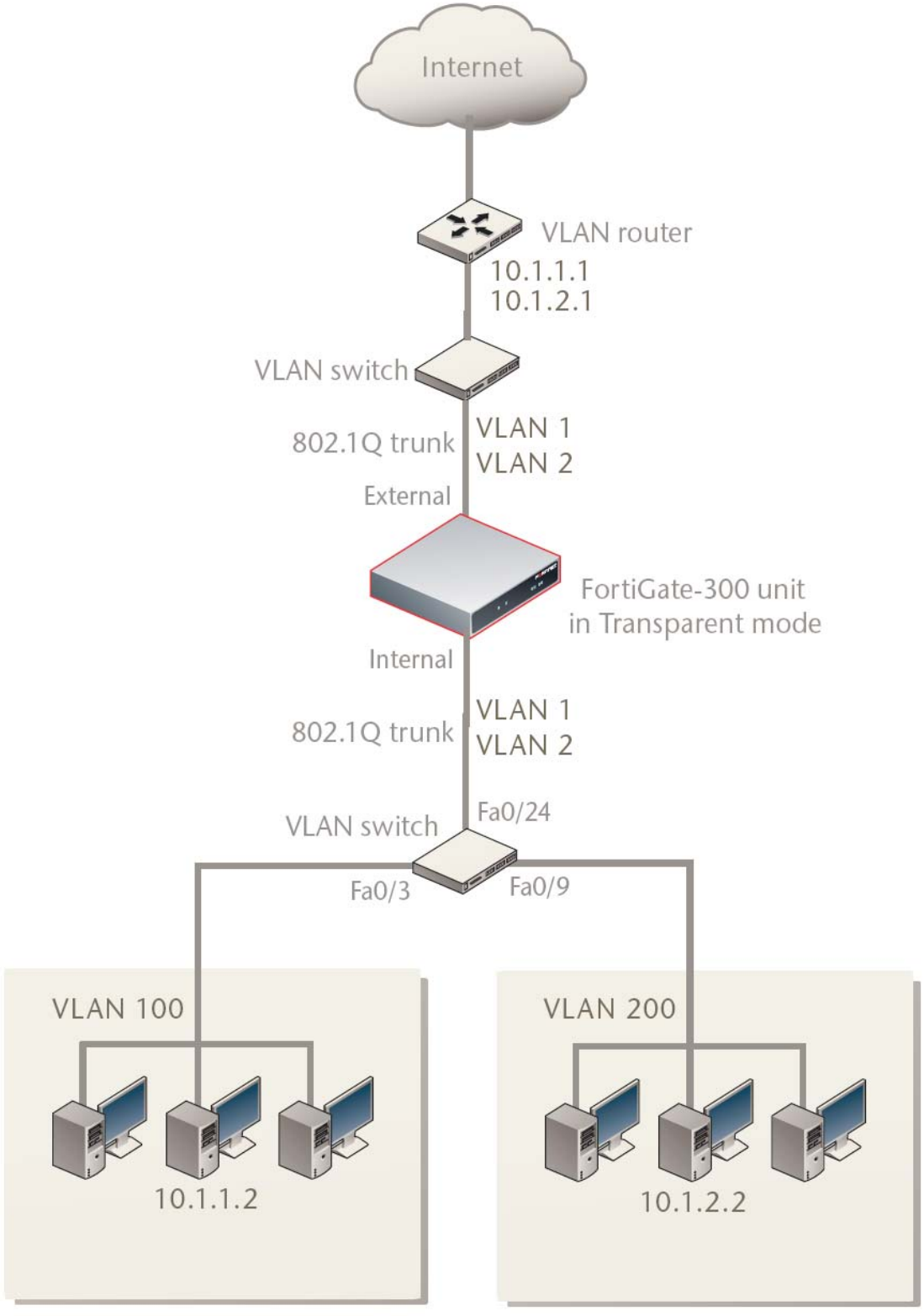
以下的配置举例中，FortiGate-800 运行于透明模式。设备配置了两个 VLAN，分别为 VLAN 100 与 VLAN 200。内部与外部物理接口上设置两个 VLAN 子接口，分别用于 VLAN 100 与 VLAN 200。

FortiGate 设备的内部网络接口与 Cisco 2900 交换机连接，外部接口与 Cisco 2620 路由器连接。交换机与路由器在数据包上添加 VLAN ID 并将数据包转发到 FortiGate 设备。当 FortiGate 设备接收到 VLAN 标签的数据包后，将其从一个 VLAN 子接口传输到另一个子接口。

例如，当交换机从 VLAN100 接收到一个数据包时，添加 VLAN ID100 标签后将数据包转发到 FortiGate 设备内部接口的 VLAN 子接口上。FortiGate 设备将数据包传输到外部接口的 VLAN 子接口 100 上。也就是从该接口数据包转发到路由器。

示例的说明将围绕下图拓扑结构网络图展开。

图 36：运行于透明模式的 FortiGate 设备应用 VLAN 的示例图



常规配置步骤

1. 配置 FortiGate-800 设备
   - 添加四个 VLAN 子接口：

i. VLAN ID 100 添加到内部与外部网络接口

ii. VLAN ID 200 添加到内部与外部网络接口

- 添加防火墙策略以允许：

i. VLAN 网络访问外部网络

ii. 外部网络访问 VLAN 网络

2. 配置 Cisco 交换机支持 VLAN 标签
3. 配置 Cisco 路由器支持 VLAN 标签
4. 测试配置

配置FortiGate-800设备

启动基于 web 的管理器配置 FortiGate 设备。

添加 VLAN 子接口

对于每个 VLAN，您需要在内部与外部网络分别创建一个具有相同 VLAN ID 的子接口。

使用基于 web 的管理器添加 VLAN 子接口

1. 进入“系统>网络>接口”。
2. 点击“新建”。
3. 设置以下信息，并点击 OK。

名称	VLAN_100_int
接口	内部接口
VLAN ID	100
根据需要配置其它字段。	

4. 点击“新建”。
5. 设置以下信息，并点击 OK。

名称	VLAN_100_ext
接口	内部接口

VLAN ID	100
根据需要配置其它字段。	

6. 点击“新建”。

7. 设置以下信息，并点击 OK。

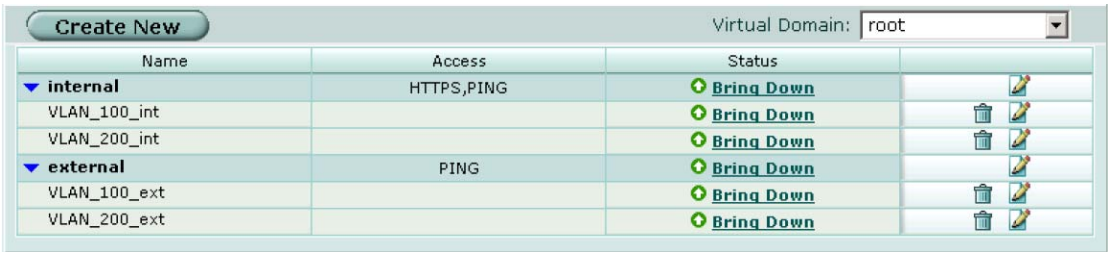
名称	VLAN_200_int
接口	内部接口
VLAN ID	200
根据需要配置其它字段。	

8. 点击“新建”。

9. 设置以下信息，并点击 OK。

名称	VLAN_200_ext
接口	外部接口
VLAN ID	200
根据需要配置其它字段。	

图 37：VLAN 子接口



使用 CLI 添加 VLAN 子接口

config system interface

edit

VLAN_100_int

set status down

set interface internal

set vlanid 100

next

edit VLAN_100_ext

set status down

set interface external

set vlanid 100

next

edit VLAN_200_int

set status down

set interface internal

set vlanid 200

next

edit VLAN_200_ext

set status down

set interface external

set vlanid 200

end

添加防火墙策略

配置防火墙策略允许数据包从 VLAN_100_int 到 VLAN_100_ext 接口的穿越，以及从 VLAN_200_int 到 VLAN_200_ext 接口的穿越。

使用基于 web 的管理器添加防火墙策略

1. 进入“防火墙>策略”。
2. 点击“新建”。
3. 输入以下信息，并点击“OK”：

源地址		
	接口/区域	VLAN_100_int
	地址名称	全部

目标地址		
	接口/区域	VLAN_100_ext
	地址名称	全部
时间表		总是 （Always）
服务		ANY
动作		ACCEPT
根据需要配置其它字段。		

4. 点击“新建”。

5. 输入以下信息并点击 OK 确认。

源地址		
	接口/区域	VLAN_100_ext
	地址名称	全部
目标地址		
	接口/区域	VLAN_100_int
	地址名称	全部
时间表		总是 （Always）
服务		ANY
动作		ACCEPT
根据需要配置其它字段。		

6. 点击“新建”。

7. 输入以下信息并点击 OK 确认。

源地址	

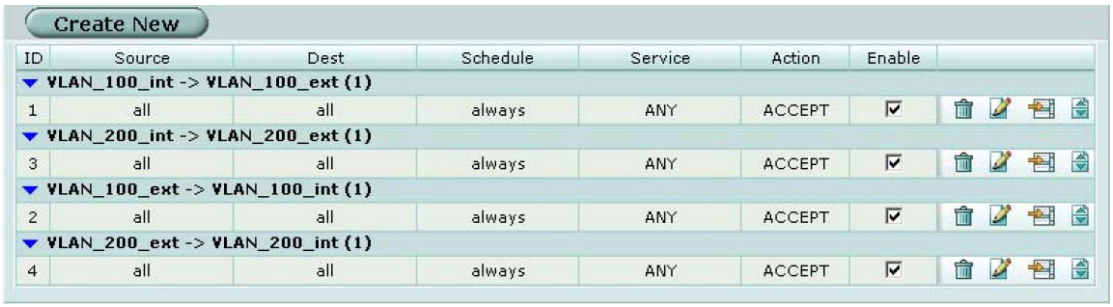
	接口/区域	VLAN_200_int
	地址名称	全部
目标地址		
	接口/区域	VLAN_200_ext
	地址名称	全部
时间表		总是 （Always）
服务		ANY
动作		ACCEPT
根据需要配置其它字段。		

8. 点击“新建”。

9. 输入以下信息并点击 OK 确认：

源地址		
	接口/区域	VLAN_200_ext
	地址名称	全部
目标地址		
	接口/区域	VLAN_200_int
	地址名称	全部
时间表		总是 （Always）
服务		ANY
动作		ACCEPT
根据需要配置其它字段。		

图 38：VLAN 的防火墙策略配置



使用 CLI 添加防火墙策略

config firewall policy

edit 1

set srcintf VLAN_100_int

set dstintf VLAN_100_ext

set srcaddr all

set dstaddr all

set action accept

set schedule always

set service ANY

next

edit 2

set srcintf VLAN_100_ext

set dstintf VLAN_100_int

set srcaddr all

set dstaddr all

set action accept

set schedule always

set service ANY

next

edit 3

set srcintf VLAN_200_int

set dstintf VLAN_200_ext

set srcaddr all

set dstaddr all

set action accept

set schedule always

set service ANY

next

edit 4

set srcintf VLAN_200_ext

set dstintf VLAN_200_int

set srcaddr all

set dstaddr all

set action accept

set schedule always

set service ANY

end

配置Cisco交换机

在 Cisco Catalyst 2900 以太网交换机中，您需要在 VLAN 数据库中定义 VLAN 100 与 VLAN200，然后添加配置文件以定义 VLAN 子接口与 802.1Q trunk 接口。

配置 VLAN 子接口与 trunk 接口

在 Cisco 交换机中添加以下命令：

!

interface FastEthernet0/3

switchport access vlan 100

!

interface FastEthernet0/9

switchport access vlan 200

!

interface FastEthernet0/24

switchport trunk encapsulation dot1q

switchport mode trunk

!

交换机具有以下配置：

端口 0/3	VLAN ID 100
端口 0/9	VLAN ID 200
端口 0/24	802.1Q trunk

配置Cisco路由器

对 Cisco Multiservice 2620 以太网路由器添加配置文件。配置文件定义了 VLAN 子接口与 802.1Q trunk 接口（802.1Q trunk 接口是路由器的物理接口）。

配置 VLAN 子接口与 trunk 接口

!

interface FastEthernet0/0

!

interface FastEthernet0/0.1

encapsulation dot1Q 100

ip address 10.1.1.1 255.255.255.0

!

interface FastEthernet0/0.2

encapsulation dot1Q 200

ip address 10.1.2.1 255.255.255.0

!

路由器具有以下配置：

端口 0/0.1	VLAN ID 100
端口 0/0.2	VLAN ID 200
端口 0/0	802.1Q trunk

注意：在应用 VLAN 之前还有配置 VLAN 的默认网关。VALN100 的默认网关是 Cisco 路由器 VLAN100 子接口。VALN200 的默认网关是 Cisco 路由器 VLAN200 子接口。

测试配置

使用诊断命令（tracert,ping）测试 FortiGate 设备与 Cisco 交换机之间的路由流量。

测试 VLAN100 到 VLAN200 的流量

以下测试举例中，是对两个内部网络的路由设置跟踪的。路由目标是 VLAN200 中的一台主机。

从 VLAN100，在命令提示符下输入：

C:\>tracert 10.1.2.2

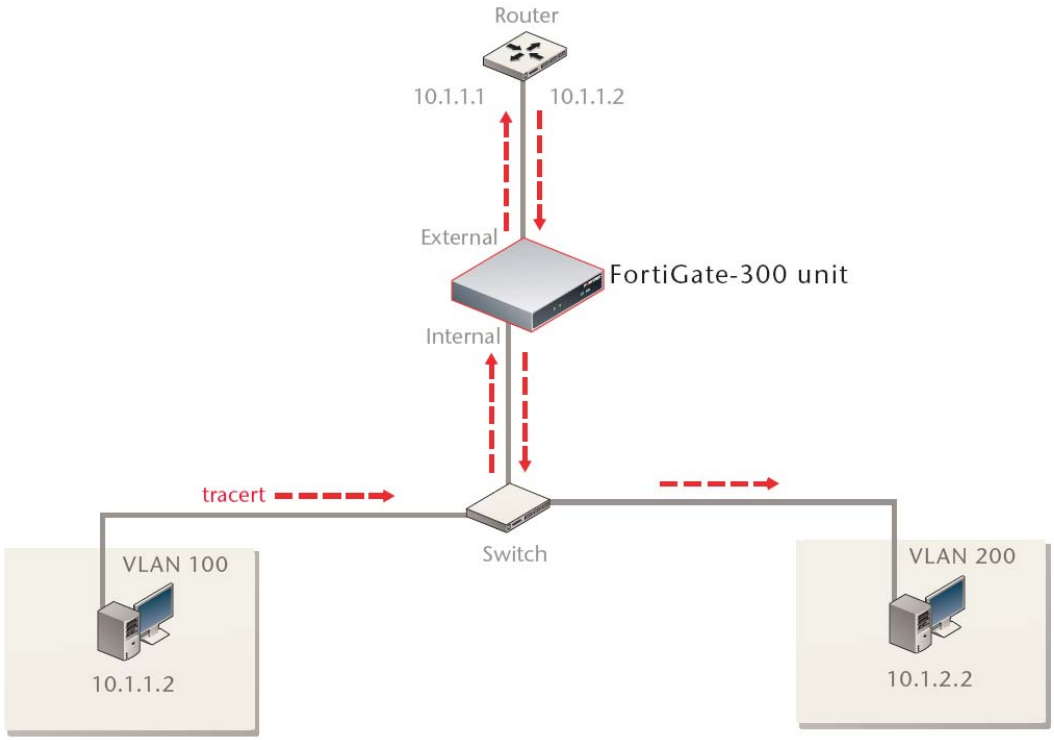
Tracing route to 10.1.2.2 over a maximum of 30 hops:

1 <10 ms <10 ms <10 ms 10.1.1.1

2 <10 ms <10 ms <10 ms 10.1.2.2

Trace complete.

图 39：从 VLAN100 到 VLAN200 之间的路由跟踪

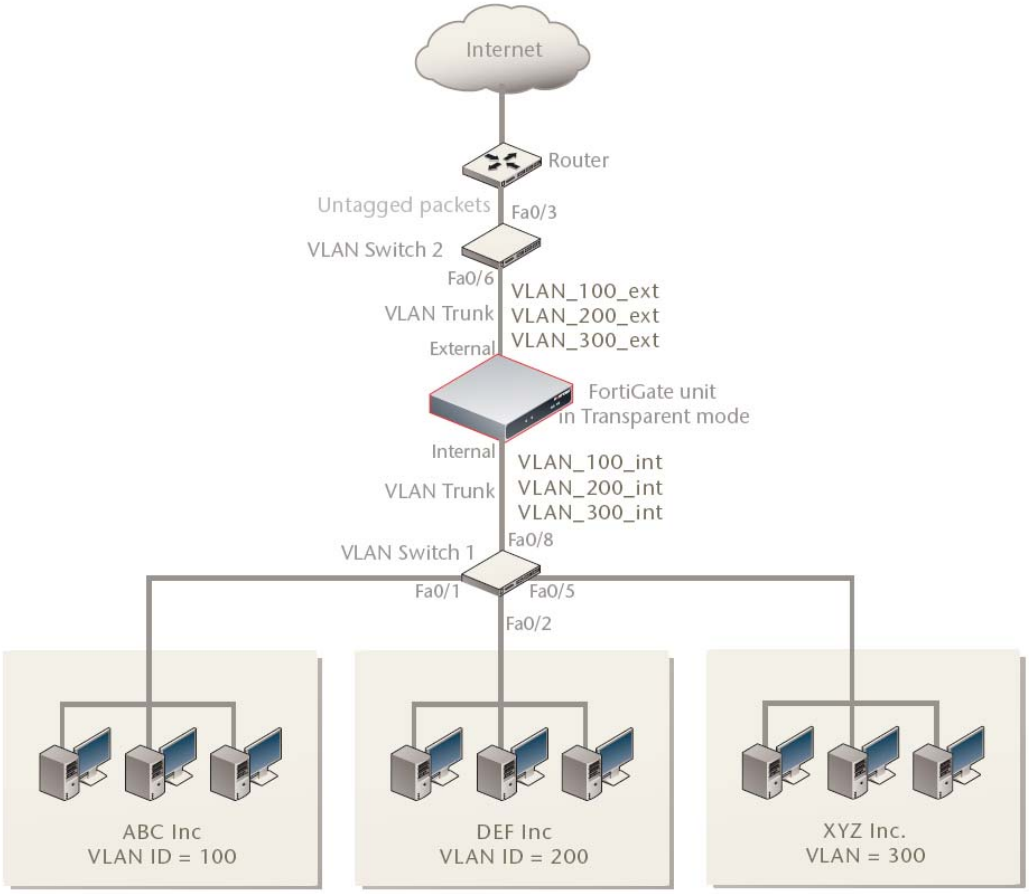


透明模式下配置多个虚拟域举例

在以下配置举例说明中，FortiGate-800 对三个对出入流量有不同要求的对象提供网络的防护功能。也就是说，需要针对保护对象的不同要求配置不同的的防火墙策略。虽然这样的网络配置在不使用虚拟域的情况下，也可能实现。但虚拟域的使用简化了配置，提供了针对每个保护对象的有效独立的管理。

示例说明从设置启动虚拟域开始。

图 40：配置运行于透明模式的 FortiGate 设备应用多个虚拟域



配置全局设置项

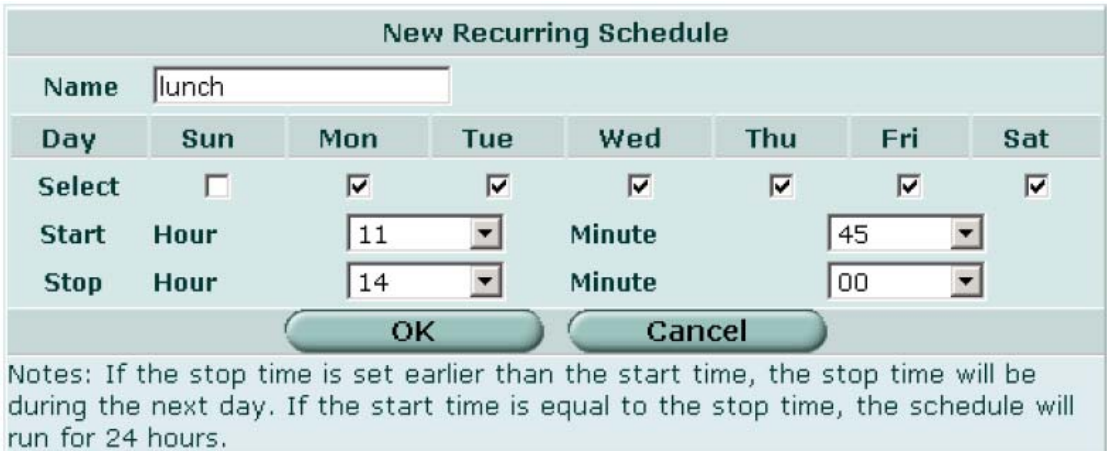
一些使用于所有虚拟域的内容保护列表可以在全局配置中进行设置。

创建时间表

举例中的 FortiGate-800 设备同时对三个均从事商业行为但每个时间段应用防火墙策略不同的对象提供服务。为了简化说明，我们假设这三个公司的午餐时间都一样。根据用户不同的时间段、不同的要求应用多个时间表配置也是可以的。

使用基于 web 的管理器对午餐时段创建循环的时间表策略

1. 进入“防火墙>时间表>循环”。
2. 点击“新建”。
3. 输入“午餐”作为时间表的名称。
4. 选择周一到周五。
5. 设置开始时间为 11：45，结束时间为 14：00。



6. 点击 OK 确认。

使用 CLI 对午餐时段创建循环的时间表策略

config firewall schedule recurring

edit Lunch

set day monday tuesday wednesday thursday friday

set start 11:45

set end 14:00

end

创建内容保护内容列表

FortiGate-800 设备提供预先配置的内容保护列表：strict（严格），scan（扫描），web filtering（web 过滤），unfiltered（未过滤）。该示例中也利用 FortiGate 设备内容屏蔽功能设置了用户自定义保护内容列表。内容保护列表是全局设置，但是您可以根据不同的保护对象的需要设置任意多的保护内容项。

本示例中所创建的内容保护列表：

内容保护列表名称	描述	应用对象
只用于商业行为	反病毒扫描、垃圾邮件过滤、禁忌词汇列	ABC 公司，DEF

（BusinessOnly）	表、防止非商业活动的 web 类别过滤。	公司
午餐（Lunch）	反病毒扫描、垃圾邮件过滤、禁忌词汇列表与 IPS。Web 类别过滤中设置在午餐时间内允许到大众兴趣类网站的浏览。	ABC 公司， DEF 公司

使用基于 web 的管理器创建“只用于商业行为”的内容保护列表

1. 进入“防火墙>内容保护列表”。
2. 点击“新建”。
3. 输入“只用于商业行为”作为一项内容保护列表的名称。
4. 选择反病毒扫描，启动对 HTTP，FTP，IMAP，POP3 与 SMTP 流量的扫描。
5. 选择 web 类别过滤并启动类别屏蔽功能。

配置类别如下：

潜在有法律责任的（类别）	屏蔽
有伤风化或存在争论的（类别）	屏蔽
潜在的非生产性的（类别）	屏蔽
潜在的带宽占用的（类别）	屏蔽
可能存在网络安全隐患的（类别）	屏蔽
大众兴趣的（类别）	屏蔽
商业（类别）	允许
其他（类别）	屏蔽

6. 选择垃圾邮件过滤，对 IMAP, POP3, SMTP 启动 RBL&ORDBL 查看。
7. 对 IMAP, POP3, SMTP 流量启动禁忌词汇查看。
8. 对于识别为垃圾邮件的流量所采取的动作，对 IMAP 与 POP3 协议传输的邮件采取标记垃圾邮件的动作，对于以 SMTP 协议传输的邮件采取丢弃的动作。
9. 选择 IPS 服务并启动 IPS 特征与 IPS 异常检测。
10. 点击 OK 确认。

使用 CLI 创建“只用于商业行为”的内容保护列表

config firewall profile

edit BusinessOnly

set ftp scan

set http scan catblock

set imap scan fragmail spamrbl bannedword

set pop3 scan fragmail spamrbl bannedword

set smtp scan fragmail spamrbl bannedword

set ips signature anomaly

set cat_allow 49-50-51-52-53 set cat_deny g01-g02-g03-g04-g05-g06-g08

end

使用基于 web 的管理器创建“娱乐性目的”的内容保护列表

1. 进入“防火墙>内容保护列表”。
2. 点击“新建”。
3. 输入“娱乐性目的”作为一项内容保护列表的名称。
4. 选择反病毒扫描，启动对 HTTP，FTP，IMAP，POP3 与 SMTP 流量的扫描。
5. 选择 web 类别过滤并启动类别屏蔽功能。

配置类别如下：

潜在有法律责任的（类别）	屏蔽
有伤风化或存在争论的（类别）	屏蔽
潜在的非生产性的（类别）	监控
潜在的带宽占用的（类别）	监控
可能存在网络安全隐患的（类别）	屏蔽
大众兴趣的（类别）	允许
商业（类别）	允许
其他（类别）	允许

6. 选择垃圾邮件过滤，对 IMAP, POP3, SMTP 启动 RBL&ORDBL 查看。
7. 对 IMAP, POP3, SMTP 流量启动禁忌词汇查看。

8. 对于识别为垃圾邮件的流量所采取的动作，对 IMAP 与 POP3 协议传输的邮件采取标记垃圾邮件的动作，对于以 SMTP 协议传输的邮件采取丢弃的动作。
9. 选择 IPS 服务并启动 IPS 特征与 IPS 异常检测。
10. 点击 OK 确认。

使用 CLI 创建“娱乐性目的”的内容保护列表

config firewall profile

edit Relaxed

set ftp scan

set http scan catblock

set imap scan

set pop3 scan

set smtp scan spamrbl

set ips anomaly

set ips signature

set cat_allow g06-g07-g08 set cat_deny g01-g02-g05 set cat_monitor g03-g04

end

创建虚拟域

FortiGate-800 设备支持配置 10 个虚拟域。根（root）虚拟域是默认的虚拟域，不能删除也不可以重命名。在本示例中没有使用根虚拟域，分别对公司 ABC，DEF 与 XYZ 创建了新的虚拟域。

使用基于 web 的管理器创建虚拟域

1. 以 admin 登录。
2. 点击“新建”。
3. 输入“ABC 公司”并点击 OK 确认。
4. 点击“新建”。
5. 输入“DEF 公司”并点击 OK 确认。
6. 点击“新建”。
7. 输入“XYZ 公司”并点击 OK 确认。

使用 CLI 创建虚拟域

config system vdom

edit ABCdomain

next

edit DEFdomain

next

edit XYZdomain

end

配置ABC虚拟域

以下是如何对 ABC 虚拟域添加 VLAN 子接口与配置防火墙策略的操作。

添加 VLAN 子接口

您需要在内部与外部接口分别创建一个具有相同 ID 的 VLAN 子接口。

使用基于 web 的管理器添加 VLAN 子接口

1. 进入“系统>网络>接口”。
2. 点击“新建”。
3. 设置以下信息，并点击 OK。

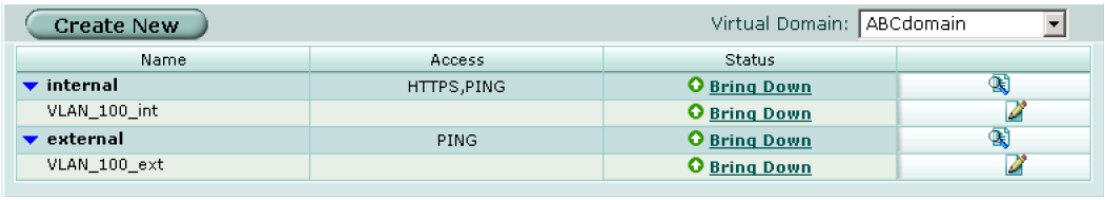
名称	VLAN_100_int
接口	内部接口
VLAN ID	100
虚拟域名称	ABC 虚拟域
根据需要配置其它字段。	

4. 点击“新建”。
5. 设置以下信息，并点击 OK。

名称	VLAN_100_ext
接口	外部接口
VLAN ID	100

虚拟域名称	ABC 虚拟域
根据需要配置其它字段。	

图 41：ABC 虚拟域的接口



使用 CLI 添加 VLAN 子接口

config system interface

edit VLAN_100_int

set interface internal

set vlanid 100

set vdom ABCdomain

next

edit VLAN_100_ext

set interface external

set vlanid 100

set vdom ABCdomain

end

进入 ABC 虚拟域配置页面

在进行以下配置 VLAN100 的操作步骤之前，先要确认当前的虚拟域是 ABC 虚拟域。

使用基于 web 的管理器进入 ABC 虚拟域

1. 进入“系统>虚拟域>虚拟域”。
2. 选择“更改当前虚拟域为以下虚拟域”。
3. 选择 ABC 虚拟域。

使用 CLI 进入 ABC 虚拟域

config vdom

edit ABCdomain

创建服务组

ABC 公司限制员工使用在线聊天与游戏软件。针对该限制与要求，您可以通过创建服务组简化防火墙策略的配置，也就是说，您可以创建一个服务组包括所有您要限制的服务。一项防火墙策略只能够管理一项服务或一个服务组。

使用基于 web 的管理器创建一个游戏与聊天服务组

1. 进入“防火墙>服务>组”。
2. 点击“新建”。
3. 在组名称字段输入“游戏-聊天”。
4. 从可用服务列表中选择 AOL，IRC，NetMeeting，Quake，SIP-MSNmessenger 这样的服务加入到成员列表中。
5. 点击 OK 确认。

使用 CLI 创建一个游戏与聊天服务组

config firewall service group

edit games-chat

set member IRC NetMeeting QUAKE SIP-MSNmessenger AOL TALK

end

配置 ABC 虚拟域的防火墙地址

根虚拟域下，地址默认为“全部”。其他虚拟域中，您必须进行设置。

使用基于 web 的管理器配置 ABC 虚拟域的防火墙地址

1. 进入“防火墙>地址>地址”。
2. 点击“新建”。
3. 在“地址名称”字段输入“新建”。
4. 在 IP 范围/子网字段输入 0.0.0.0/0.0.0.0。
5. 点击 OK。

使用 CLI 配置 ABC 虚拟域的防火墙地址

config firewall address

edit all

set type ipmask

set subnet 0.0.0.0 0.0.0.0

end

配置 ABC 虚拟域的防火墙策略

配置防火墙策略根据内容保护列表中的设置允许数据包从 VLAN100 接口穿越到外部接口。

使用基于 web 的管理器配置 ABC 虚拟域的防火墙策略

1. 进入“防火墙>策略>策略”。
2. 点击“新建”。
3. 输入以下信息，并点击“OK”：

接口/区域 源地址	VLAN_100_int
接口/区域 目标地址	VLAN_100_ext
源地址名称	全部
目标地址名称	全部
时间表	工作日
服务	游戏-聊天
动作	DENY
根据需要配置其它字段。	

该策略禁止在工作时间使用网络游戏以及聊天程序。

4. 输入以下信息并点击 OK 确认：

接口/区域 源地址	VLAN_100_int
接口/区域 目标地址	VLAN_100_ext
源地址名称	全部
目标地址名称	全部
时间表	午餐时间

服务	HTTP
动作	ACCEPT
保护内容列表名称	娱乐
根据需要配置其它字段。	

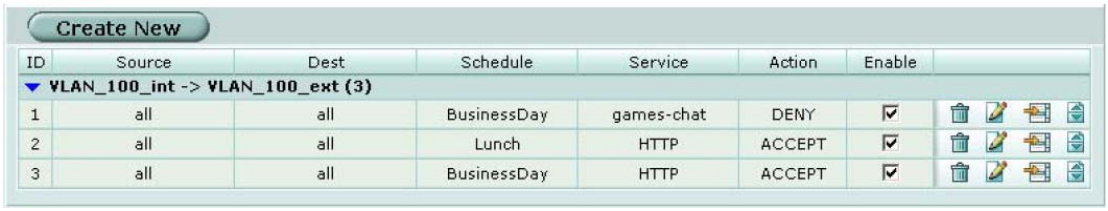
该策略配置在午餐时间放松执行 web 类别过滤。

5. 输入以下信息并点击 OK。

接口/区域 源地址	VLAN_100_int
接口/区域 目标地址	VLAN_100_ext
源地址名称	全部
目标地址名称	全部
时间表	工作日
服务	HTTP
动作	ACCEPT
保护内容列表名称	只涉及商业行为
根据需要配置其它字段。	

该策略设置在工作时间执行“严格”的 web 类别过滤。

图 42：ABC 虚拟域防火墙策略设置



使用基于 CLI 配置 ABC 虚拟域的防火墙策略

config firewall policy

edit 1

set srcintf VLAN_100_int

```
set dstintf VLAN_100_ext
set srcaddr all
set dstaddr all
set schedule BusinessDay
set service games-chat
next
edit 2
set srcintf VLAN_100_int
set dstintf VLAN_100_ext
set srcaddr all
set dstaddr all
set action accept
set schedule Lunch
set service HTTP
set profile_status enable
set profile Relaxed
next
edit 3
set srcintf VLAN_100_int
set dstintf VLAN_100_ext
set srcaddr all
set dstaddr all
set action accept
set schedule BusinessDay
set service HTTP
set profile_status enable
set profile BusinessOnly
end
```

配置DEF虚拟域

您需要在内部接口与外部接口分别配置一个 VLAN 子接口，且具有相同的 VLAN ID。

添加 VLAN 子接口

使用基于 web 的管理器添加 VLAN 子接口

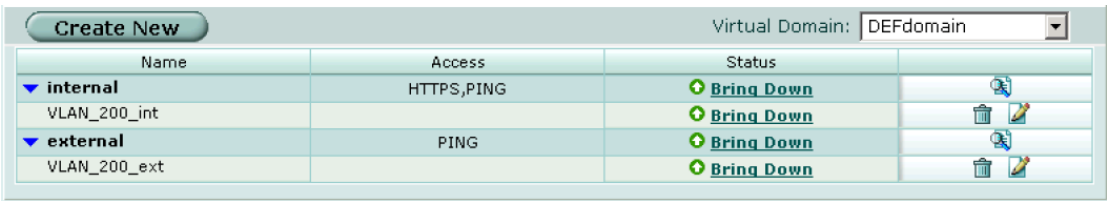
1. 进入“系统>网络>接口”。
2. 点击“新建”。
3. 输入以下信息并点击 OK 确认。

名称	VLAN_200_int
接口	内部接口
VLAN ID	200
虚拟域	DEF 虚拟域
根据需要配置其它字段。	

4. 点击“新建”。
5. 输入以下信息并点击 OK 确认。

名称	VLAN_200_ext
接口	外部接口
VLAN ID	200
虚拟域	DEF 虚拟域
根据需要配置其它字段。	

图 43：DEF 虚拟域的子接口设置



使用 CLI 添加 VLAN 子接口

config system interface

edit VLAN_200_int

set interface internal

set vlanid 200

set vdom DEFdomain

next

edit VLAN_200_ext

set interface external

set vlanid 200

set vdom DEFdomain

end

进入 DEF 虚拟域配置页面

在进行以下配置 VLAN200 的操作步骤之前，先要确认当前的虚拟域是 DEF 虚拟域。

使用基于 web 的管理器进入 DEF 虚拟域

1. 进入“系统>虚拟域>虚拟域”。
2. 选择“更改当前虚拟域为以下虚拟域”。
3. 选择 DEF 虚拟域。

使用 CLI 进入 ABC 虚拟域

config vdom

edit DEFdomain

创建服务组

DEF 公司限制员工使用在线游戏软件或除了 NetMeeting 以外的任何在线聊天软件。针对该限制与要求，您可以通过创建服务组简化防火墙策略的配置，也就是说，您可以创建一个服务组包括所有您要限制的服务。一项防火墙策略只能够管理一项服务或一个服务组。管理员可以将该组的名称简单的设置为“游戏”，虽然同时也要屏蔽聊天程序。

使用基于 web 的管理器创建一个游戏服务组

1. 进入“防火墙>服务>组”。
2. 点击“新建”。
3. 在组名称字段输入“游戏”。
4. 从可用服务列表中选择 AOL，IRC，Quake，SIP-MSNmessenger 这样的服务加入到成员列表中。
5. 点击 OK 确认。

使用 CLI 创建一个游戏服务组

config firewall service group

edit Games

set member IRC QUAKE SIP-MSNmessenger AOL TALK

end

配置 DEF 虚拟域的防火墙地址

根虚拟域下，地址默认为“全部”。其他虚拟域中，您必须进行设置。

使用基于 web 的管理器配置 DEF 虚拟域的防火墙地址

1. 进入“防火墙>地址>地址”。
2. 点击“新建”。
3. 在“地址名称”字段输入“新建”。
4. 在 IP 范围/子网字段输入 0.0.0.0/0.0.0.0。
5. 点击 OK。

使用 CLI 配置 DEF 虚拟域的防火墙地址

config firewall address

edit all

set type ipmask

set subnet 0.0.0.0 0.0.0.0

end

配置 DEF 虚拟域的防火墙策略

配置防火墙策略根据内容保护列表中的设置允许数据包从 VLAN200 接口穿越到外部接口。

使用基于 web 的管理器配置 DEF 虚拟域的防火墙策略

1. 进入“防火墙>策略>策略”。
2. 点击“新建”。
3. 输入以下信息，并点击“OK”：

接口/区域 源地址	VLAN_200_int
接口/区域 目标地址	VLAN_200_ext
源地址名称	全部
目标地址名称	全部
时间表	工作日
服务	游戏-聊天
动作	DENY
根据需要配置其它字段。	

该策略禁止在工作时间使用网络游戏以及聊天程序（除了 NetMeeting）。

4. 输入以下信息并点击 OK 确认：

接口/区域 源地址	VLAN_200_int
接口/区域 目标地址	VLAN_200_ext
源地址名称	全部
目标地址名称	全部
时间表	午餐时间
服务	HTTP
动作	ACCEPT
保护内容列表名称	娱乐
根据需要配置其它字段。	

该策略配置在午餐时间放松执行 web 类别过滤。

5. 输入以下信息并点击 OK。

接口/区域 源地址	VLAN_200_int
接口/区域 目标地址	VLAN_200_ext
源地址名称	全部
目标地址名称	全部
时间表	工作日
服务	HTTP
动作	ACCEPT
保护内容列表名称	只涉及商业行为
根据需要配置其它字段。	

该策略设置在工作时间执行严格的 web 类别过滤。

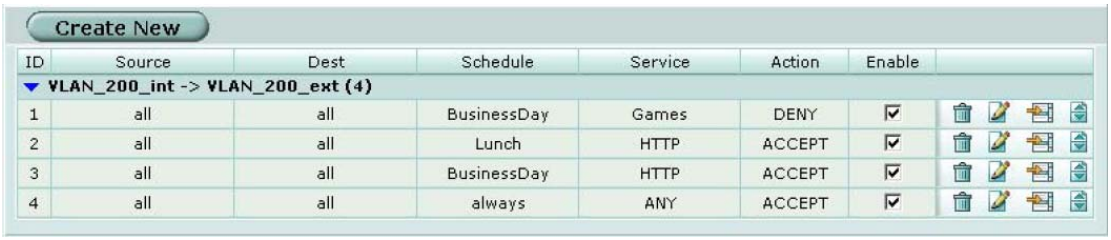
6. 输入以下信息并点击 OK：

接口/区域 源地址	VLAN_200_int
接口/区域 目标地址	VLAN_200_ext
源地址名称	全部
目标地址名称	全部
时间表	Always（总是）
服务	ANY
动作	ACCEPT
保护内容列表名称	娱乐
根据需要配置其它字段。	

该策略位于列表中最后一项，应用的时间与服务不能覆盖之前的策略范围。

也就是说，在工作时间之外，保护内容列表中“娱乐性”的设置应用于邮件查看与网页浏览以及在线聊天与游戏是被允许的。为 DEF 公司设置了该策略是处于公司的员工有时会加班这样的考虑。示例中其他公司的策略设置了固定的时间并限制工作时间外的任何互联网访问活动。

图 44：ABC 虚拟域防火墙策略设置



使用 CLI 配置 DEF 虚拟域的防火墙策略

config firewall policy

edit 1

set srcintf VLAN_200_int

set dstintf VLAN_200_ext

set srcaddr all

set dstaddr all

set schedule BusinessDay

set service Games

set action deny

next

edit 2

set srcintf VLAN_200_int

set dstintf VLAN_200_ext

set srcaddr all

set dstaddr all

set action accept

set schedule Lunch

set service HTTP

set profile_status enable

set profile Relaxed

next

edit 3

set srcintf VLAN_200_int

set dstintf VLAN_200_ext

set srcaddr all

set dstaddr all

set action accept

set schedule BusinessDay

set service HTTP

set profile_status enable

set profile BusinessOnly

next

edit 4

set srcintf VLAN_200_int

set dstintf VLAN_200_ext

set srcaddr all

set dstaddr all

set action accept

set schedule always

set service ANY

set profile_status enable

set profile Relaxed

end

配置XYZ虚拟域

添加 VLAN 子接口

使用基于 web 的管理器添加 VLAN 子接口

1. 进入“系统>网络>接口”。
2. 点击“新建”。

3. 设置以下信息，并点击 OK。

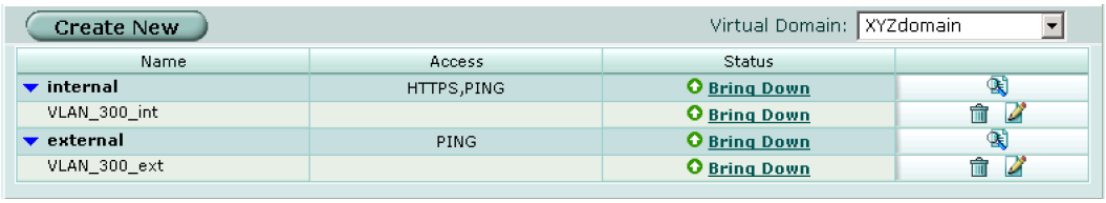
名称	VLAN_300_int
接口	内部接口
VLAN ID	300
虚拟域名称	XYZ 虚拟域
根据需要配置其它字段。	

4. 点击“新建”。

5. 设置以下信息，并点击 OK。

名称	VLAN_300_ext
接口	外部接口
VLAN ID	300
虚拟域名称	XYZ 虚拟域
根据需要配置其它字段。	

图 45：XYZ 虚拟域的子接口设置



使用 CLI 添加 VLAN 子接口

config system interface

edit VLAN_300_int

set interface internal

set vlanid 300

set vdom XYZdomain

next

edit VLAN_300_ext

set interface external

set vlanid 300

set vdom XYZdomain

end

进入 XYZ 虚拟域配置页面

在进行以下配置 VLAN300 的操作步骤之前，先要确认当前的虚拟域是 XYZ 虚拟域。

使用基于 web 的管理器进入 XYZ 虚拟域

1. 进入“系统>虚拟域>虚拟域”。
2. 选择“更改当前虚拟域为以下虚拟域”。
3. 选择 XYZ 虚拟域。

使用 CLI 进入 XYZ 虚拟域

config vdom

edit XYZdomain

创建服务组

XYZ 公司意欲对电子邮件与 web 服务设置网络保护。那么，为了简化防火墙策略的创建，您可以对以 POP3，IMAP，SMTP 协议传输的邮件创建一个邮件服务组，以及对 HTTP， HTTPS，FTP 传输的 web 服务创建一个组。

使用基于 web 的管理器创建一个邮件服务组

1. 进入“防火墙>服务>组”。
2. 点击“新建”。
3. 在组名称字段输入“邮件”。
4. 从可用服务列表中选择 POP3，IMAP，SMTP 这样的服务加入到成员列表中。
5. 点击 OK 确认。

使用 CLI 创建一个游戏服务组

config firewall service group

edit Email

set member POP3 IMAP SMTP

end

使用基于 web 的管理器创建一个 web 服务组

1. 进入“防火墙>服务>组”。
2. 点击“新建”。
3. 在组名称字段输入“web”。
4. 从可用服务列表中选择 HTTP， HTTPS，FTP 这样的服务加入到成员列表中。
5. 点击 OK 确认。

使用 CLI 创建一个 web 服务组

config firewall service group

edit web

set member HTTP HTTPS FTP

end

配置 XYZ 虚拟域的防火墙地址

根虚拟域下，地址默认为“全部”。其他虚拟域中，您必须进行设置。

使用基于 web 的管理器配置 XYZ 虚拟域的防火墙地址

1. 进入“防火墙>地址>地址”。
2. 点击“新建”。
3. 在“地址名称”字段输入“新建”。
4. 在 IP 范围/子网字段输入 0.0.0.0/0.0.0.0。
5. 点击 OK。

使用 CLI 配置 XYZ 虚拟域的防火墙地址

config firewall address

edit all

set type ipmask

set subnet 0.0.0.0 0.0.0.0

end

配置 XYZ 虚拟域的防火墙策略

配置防火墙策略根据内容保护列表中的设置允许数据包从 VLAN300 接口穿越到外部接口。

使用基于 web 的管理器配置 XYZ 虚拟域的防火墙策略

1. 进入“防火墙>策略>策略”。
2. 点击“新建”。
3. 输入以下信息，并点击“OK”：

接口/区域 源地址	VLAN_300_int
接口/区域 目标地址	VLAN_300_ext
源地址名称	全部
目标地址名称	全部
时间表	总是（always）
服务	Email
动作	ACCEPT
内容保护列表	Strict（严格）
根据需要配置其它字段。	

配置该策略将对电子邮件采取“严格（strict）”的内容保护项。管理员必须也设置反病毒、web 过滤以及垃圾邮件过滤。这些步骤在此就不加详述了。

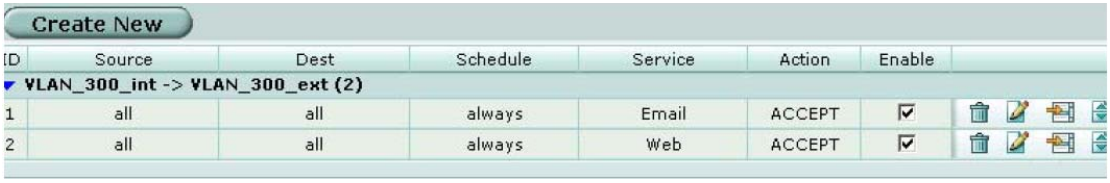
4. 输入以下信息并点击 OK 确认：

接口/区域 源地址	VLAN_300_int
接口/区域 目标地址	VLAN_300_ext
源地址名称	全部
目标地址名称	全部
时间表	总是（always）
服务	Web
动作	ACCEPT

保护内容列表名称	web
根据需要配置其它字段。	

配置该策略将对 HTTP, HTTPS, FTP 采取了默认的内容保护项。管理员必须也设置反病毒、web 过滤以及垃圾邮件过滤。这些步骤在此就不加详述了。

图 46：XYZ 虚拟域的防火墙策略设置



使用 CLI 配置 XYZ 虚拟域的防火墙策略

config firewall policy

edit 1

set srcintf VLAN_300_int

set dstintf VLAN_300_ext

set srcaddr all

set dstaddr all

set action accept

set schedule always

set service Email

set profile_status enable

set profile strict

next

edit 2

set srcintf VLAN_300_int

set dstintf VLAN_300_ext

set srcaddr all

set dstaddr all

set action accept

set schedule always

set service Web

set profile_status enable

set profile web

end

配置Cisco交换机

在 Cisco Catalyst 2900 以太网交换机中，您需要在 VLAN 数据库中定义 VLAN 100, 200 与 300，然后添加配置文件以定义 VLAN 子接口与 802.1Q trunk 接口。

配置交换机 1

在交换机 1 中添加以下命令：

!

interface FastEthernet0/1

switchport access vlan 100

!

interface FastEthernet0/2

switchport access vlan 200

!

interface FastEthernet0/5

switchport access vlan 300

!

interface FastEthernet0/6

switchport trunk encapsulation dot1q

switchport mode trunk

!

交换机具有以下配置：

端口 0/1	VLAN ID 100
端口 0/2	VLAN ID 200
端口 0/3	VLAN ID 300

端口 0/6	802.1Q trunk

配置交换机 2

在交换机 2 中添加以下命令：

interface FastEthernet0/3

switchport

!

interface FastEthernet0/6

switchport trunk encapsulation dot1q

switchport mode trunk

!

交换机 2 具有以下配置：

端口 0/1	VLAN ID 100
端口 0/2	VLAN ID 200
端口 0/3	VLAN ID 300
端口 0/6	802.1Q trunk

测试配置

使用诊断命令（tracert,ping）测试网络流量。

测试 VLAN100 到互联网的流量

以下测试举例中，是对 VLAN100 到互联网的路由设置跟踪的。路由目标是 www.fortinet.com。

1. 从 VLAN100，在命令提示符下输入：

C:\>tracert www.fortinet.com

Tracing route to www.fortinet.com [128.242.109.135] over a maximum of 30 hops:

1 <10 ms <10 ms <10 ms 172.20.120.2

...

14 172 ms 141 ms 140 ms 128.242.109.135

Trace complete.

2. 对 VLAN200 与 VLAN300 重复路由测试。

VDOM 间的路由

概述

在之前 FortiGate 设备配置使用的 VDOM 之间是相互独立操作的。VDOM 之间不进行任何内部的通信。VDOM 之间的任何通信必须通过物理接口并通过其他物理接口再进入 FortiGate 设备。

VDOM 间的路由将改变这一局面。FortiOS v3.0MR1 中对 VDOM 间路由引进后，VDOM 之间的通信可以不借助任何其它物理接口便可以实现。从 FortiManager v3.0MR1 开始，FortiManager 设备支持在所管理的 FortiGate 设备的 VDOM 之间的路由。

本站包括以下内容：

- 实现 VDOM 间路由的好处
- 配置实现 VDOM 间的路由
- 高级 VDOM 间路由的问题
- FortiManager 与 VDOM 间路由
- VDOM 间路由配置
- VDOM 间路由规划

实现 VDOM 间路由的好处

实现 VDOM 间路由相比 VDOM 独立操作有诸多的优点。包括：

- 解放了物理接口
- 传输速度比物理接口快
- 仍然能够使用安全的防护墙策略
- 更灵活的配置

解放了物理接口

与设备的物理接口绑定是个问题，鉴于物理接口的数量有限，VDOM 之间的通信配置选项也有限。

例如，一台FortiGate-800设备有8个端口，如果每个VDOM分配两个子接口（分别用于内外的流量），我们最多只可以配置4个VDOM，而不是许可证允许的10个VDOM。即使只对每个Vdom增加一个接口用于Vdom间通信，能配置的

Vdom也会减少到两个，因为需要9个接口实现3个虚拟域的配置。把一个物理接口同时用于外部和vdom间通信，还会严重降低外部流量的可用带宽。

VDOM 间的通信实现，流量可以内部穿越 VDOM，不占用物理接口对于外部流量的带宽。根据以上的举例，我们可以使用 4 个 VDOM 且所有接口均将拥有全部带宽。

传输速度比物理接口快

内部接口相比较物理接口的传输速度要快。内部接口的传输速度由 CPU 以及其负载决定，也就是说 VDOM 接口间链路接口将比向内物理接口与向外物理接口的连接要快。

通常情况下，正常流量下的一个虚拟接口要比在物理接口的传输速度要快，如果您配置的流量以及内部接口越多，那么速度就越慢，直到低于物理接口的传输速度。CPU 被其他资源占用，如 AV 或内容扫描。这将造成相同的结果，内部接口如 VDOM 间的链路将变慢。

仍然能够使用安全的防护墙策略

VDOM 的设置可以根据需要对网络流量进行分流。这样可以满足需要安全流量处理的要求。这对于那些需要每天处理敏感数据的公共卫生、法律以及财务行业尤其重要。

为了保持流量的独立性，流量必须离开 FortiGate 设备然后重新进入时再更改 VDOM。这样就迫使流量在离开以及进入时通过设置的防火墙，保持了流量的安全性。

VDOM 间路由的实现解放对物理接口的需要，但是对于全部的 FortiGate 的接口，对需要通过的接口（物理接口或虚拟接口）还是要设置防火墙策略的。这同样对内部与外部的流量提供了安全保护。事实上，您可以配置多个 VDOM 增加了设置的灵活性。

更多的配置灵活性

典型的 VDOM 设置使用至少两个物理接口，分别用于内部与外部流量。根据配置，可能会用到更多的接口。

上文已经说明，VDOM 的最大配置数量是设备可用物理接口的一半。

物理接口用于 VDOM 间的通信很严重的限制了 FortiGate 设备中的可用配置，但是 VDOM 间的路由将之前通过物理接口的连接转移到 FortiGate 设备内部进行。虚拟接口在 VDOM 间的路由应用，解放了物理接口中用于外部流量的带宽。在具有 8 个物理接口的 FortiGate 设备中使用 VDOM 间的路由，除了可以具有 4 个 VDOM 之间进行相互通信以外，还可以具有两个物理接口分别用于内部与外部流量的通信连接。以上的配置如果没有 VDOM 间路由的实现，需要用到 20 个物理接口，因为 VDOM 之间的路由需要使用 8 个物理接口，其他 12 个接

口需要作为内部虚拟接口。

VDOM 间的路由允许您能够不被 FortiGate 设备的物理接口所限制，自由的配置“单机模式 VDOM 配置”，“管理 VDOM 配置”以及“网状 VDOM 配置”。

开始配置 VDOM 间路由

配置 VDOM 后，需要配置几个步骤来实现 VDOM 间的路由。VDOM 间的配置以及撤消配置只能够使用 CLI 来完成。详细信息参见 FortiGate 设备 CLI 使用参考手册。

以下的举例中假设 FortiGate 设备已设置为多 VDOM 模式并且已配置了两个 VDOM，分别为 customer1 与 customer2。

配置 VDOM 间路由连接

1. 创建内部点到点接口，称为 vlink。

```
config global
config system vdom-link
edit vlink
next
end
```

在创建点到点接口时，您也可以创建两个额外的默认的客体，称为 vlink0 与 vlink1，接口名称以 1 与 0 结尾。

注意：步骤进行到此，您就可以访问 GUI，在“系统>网络”界面看到用于新的 VDOM 间的两个终端接口客体。通过 GUI，您只能查看 VDOM 间接口，但不可以修改。

2. 将接口客体与 VDOM 绑定。

```
config system interface
edit vlink0
set vdom customer1
next
edit vlink1
set vdom customer2
next
end
```

3. 这些设置的点到点接口现在将被当作为正常的 FortiGate 设备接口，可以如同常规接口一样进行配置，包括设置 IP 地址与掩码、以及允许的管理访问。

4. 配置适当的防火墙与策略。

删除 VDOM 间的路由连接

在您删除 VDOM 间链接时，链接客体也将一并被删除。

删除 VDOM 间链接之前，先确定所有的策略、防火墙以及包括链接的其他配置已被删除或转移或更改为不包含 VDOM 间的链接。

以下的命令可以删除称为 vlink 的 VDOM 间的路由链接，同时也将删除 vlink 的两个客体 vlink0 与 vlink1。

```
config global
config system vdom-link
delete vlink
end
```

高级 VDOM 间路由的有关问题

VDOM 间的链接基本上如同一个物理接口，但同时也存在一些情况的局限性或稍不同的操作。包括：

- VDOM 间的高级路由
- HA 虚拟群集与 VDOM 间的链接

VDOM间的高级路由

从 FortiOS v3.0 MR3 开始，VDOM 间的链接是支持 BGP 的。在这之前，一台 FortiGate 设备中的多个 VDOM 之间不能够成为邻居。除非另有注明，所有的路由均认为是在 VDOM 间的链接发生的。

HA虚拟群集与VDOM间的链接

FortiGate 设备的 HA 是通过配置两台或多台 FortiGate 设备组成一个 HA 群集来实现的。放到网络中讲，HA 群集的功能类似于 FortiGate 设备单机，处理网络流量并提供如防火墙、VPN、IPS、病毒扫描、web 过滤以及垃圾邮件过滤服务这样的网络安全服务。

虚拟群集扩展了 HA 的功能，对应用了虚拟域的 FortiGate 提供故障防护与负载平衡功能。一个虚拟群集由运行虚拟域的两台 FortiGate 设备组成。不同虚拟域的流量可以在群集设备之间实现负载平衡。

配置了虚拟群集后，VDOM 间的链接必须完全集中在一个虚拟群集中。您

不能在多个虚拟群集之间建立链接，也不能将一个 VDOM 移动到与之连接的其它虚拟群集。HA 模式下，当您在使用 CLI 命令 command config system vdom-link 在配置了多个虚拟群集的情况下创建 VDOM 链接时可以通过配置选项设置 VDOM 链接属于哪个虚拟群集。详细信息，参见 FortiGate 设备 HA 使用说明中有关 HA 配置的详细信息。

FortiManager 与 VDOM 间的路由

FortiManager 设备可以统一管理并监控多台 FortiGate 设备。从 v3.0MR1 开始，FortiManager 设备支持 VDOM 间的路由。

使用FortiManager配置VDOM间的路由

配置 VDOM 间的路由之前：

- FortiGate 设备中必须至少配置了两个虚拟域
- 虚拟域必须应用于 NAT/路由模式
- 相链接的每个虚拟域必须被分配了至少一个接口或一个子接口

FortiGate 设备配置的虚拟域信息，您可以在策略管理器中选择查看的 FortiGate 设备，进入“系统>虚拟域”进行查看。VDOM 间的链接情况，可以进入“系统>状态”进行查看。

创建 VDOM 间的链接

1. 在策略管理器中的导航条点击一个虚拟域。
2. 点击蓝色箭头扩展 VDOM 间路由配置选项。

如果没有蓝色箭头存在，表示只有一个虚拟域。在进行以下的操作之前，您必须现要创建一个或更多的虚拟域。

3. 选中一个虚拟域与当前的虚拟域（也就是在步骤 1 中选择的虚拟域）建立链接。
4. 输入所建立的虚拟域之间链接的名称，那么默认情况下虚拟接口也将延用该名称。例如 VDOM 间链接的名称为“my_link”，那么虚拟接口的名称将为“my_vlink0”与“my_vlink1”。
5. 输入用于当前 VDOM 与对等 VDOM 路由使用的虚拟接口的 IP 地址与掩码。例如，如果当前虚拟域是 vdom1。那么根虚拟域就是对等 VDOM。

   一旦建立了 VDOM 间的链接，那么这些 IP 地址可以在不删除链接的情况下更改。
6. 启动 VDOM 间的链接的流量日志。
7. 点击“应用”保存设置。

如果设置了多个 VDOM，可以重复以上的步骤建立其他 VDOM 间的链接。

只要将与当前虚拟域建立链接的虚拟域的功能框并点击“应用”，便删除了 VDOM 间的链接。

有关使用 FortiManager 的详细信息，参见 FortiManager 设备管理员使用手册。

VDOM 间的路由配置

只要将几个物理接口应用于 VDOM 之间的连接，VDOM 间的链接便可以提供您更多的配置选项。

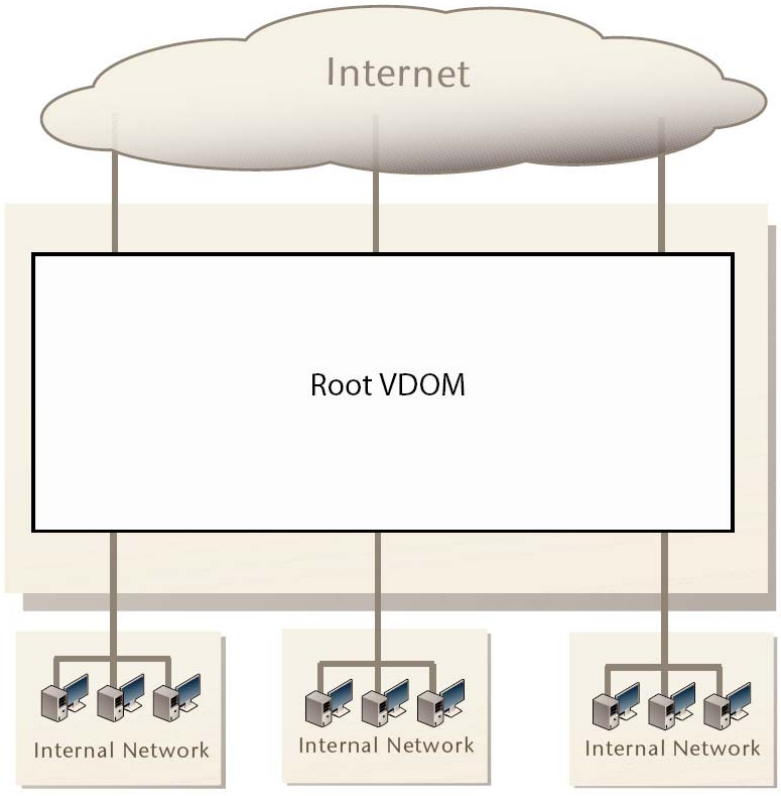
VDOM 间的配置如下：

- 单个 VDOM 配置
- 独立的 VDOM 配置
- 管理 VDOM 的配置
- 网状 VDOM 配置

单个VDOM配置

单个 VDOM 配置是指使用一个 VDOM，也就是所有 FortiGate 设备都具有的默认的 VDOM。

图 47：单个 VDOM 模式



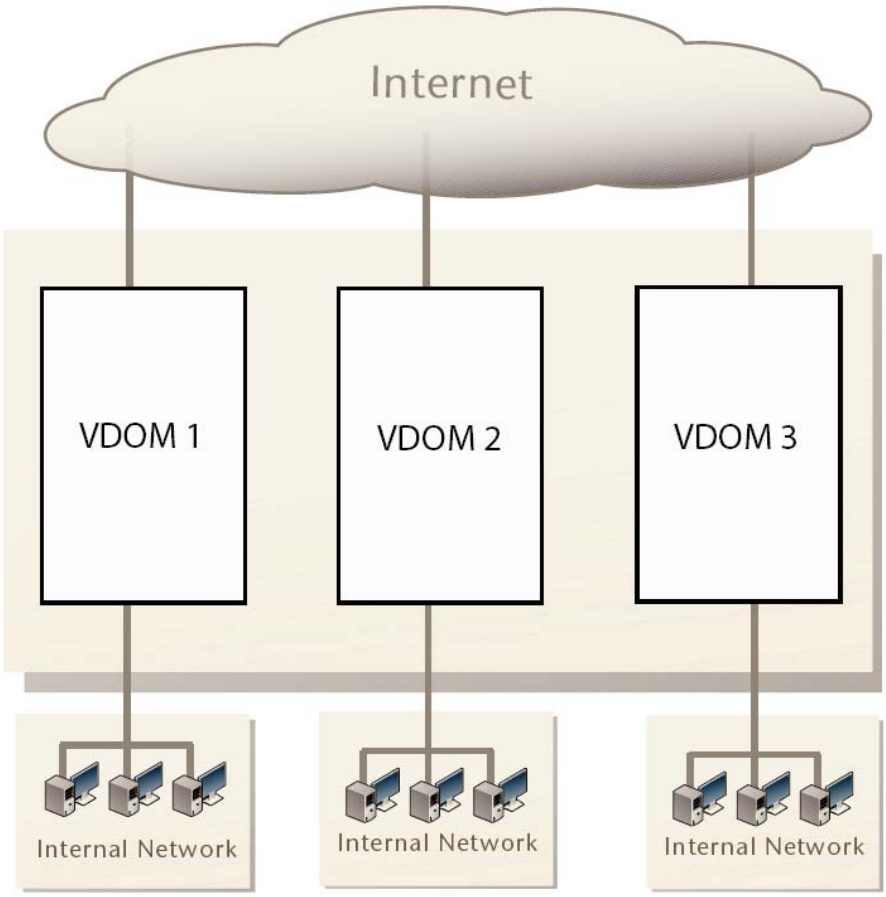
该配置下不存在 VDOM 之间的链接，不需要特殊的配置。

单个 VDOM 配置可以用于那些一个部门或一个公司管理的连接、防火墙以及其他 VDOM 的独立设置这样简单的网络配置。

独立的VDOM配置

独立的 VDOM 配置使用多个完全独立的 VDOM。

图 48：独立的 VDOM 配置



该配置下不存在VDOM之间的链接，不需要特殊的配置与设置。任何 VDOM 之间的通信可以当作是独立的物理设备之间的通信行为。

独立的 VDOM 配置可以用于不止一个部分或公司共用 FortiGate 设备的情况。这个对象在各自的 VDOM 中管理连接以及防火墙策略设置，逻辑上看，好似每个对象都享有自己的 FortiGate 设备。

管理VDOM的配置

在管理 VDOM 配置下，根 VDOM 是管理 VDOM，其它 VDOM 通过管理虚拟域也相互存在连接。

只有管理 VDOM 连接着互联网。其他 VDOM 均与内往网络链接或是与较

小的安全外部网络如 VPN 拨号连接进行连接。外部流量到各个 VDOM 的路由都要通过管理 VDOM。这样就确保了管理虚拟域完全控制到互联网的流量，包括允许通过的流量以及流量的方向。单点的出入增强了安全性。只有管理 VDOM 需要专业的管理确保网络的安全性。

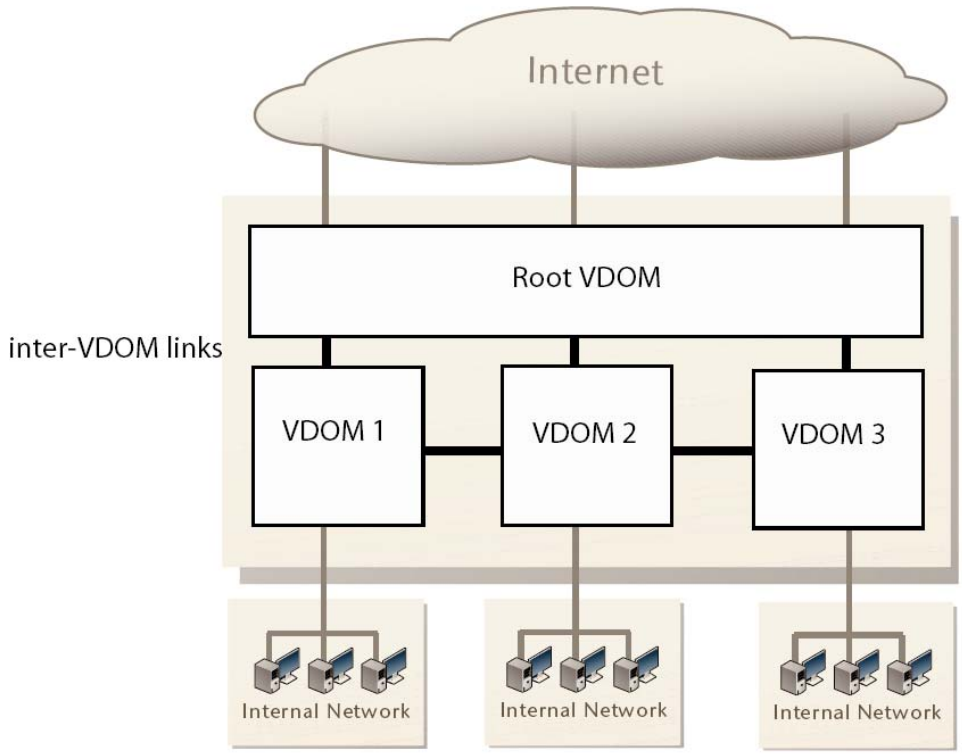
管理虚拟域的配置适用于服务提供商。服务提供商是管理 VDOM，其它用户是 VDOM 的角色。这些用户不需要分配专门的 IT 工程师管理其网络。服务提供商对流量进行控制并且可以防止用户使用被禁止的服务以及阻止其他被禁止服务发起的网络连接。例如在一个从事知识产权服务公司中禁止适用即时通讯这样的服务。防火墙策略可以控制用户的 VDOM 与管理 VDOM 之间的流量，同时也可以根据用户的需要设置策略。

网状VDOM配置

网状 VDOM 配置，包括局部与全网的 VDOM 之间的链接。没有特别的功能，只是较为复杂的 VDOM 配置。

局部网状表示整个网络中只有一些 VDOM 是相互链接的。全网配置就是全部的 VDOM 之间相互链接。这种情况可以应用于在您想提供 VDOM 之间的互访但是难于处理 VDOM 之间流量的情况下。

图 50：网状 VDOM 配置



提供对所有 VDOM 的访问，必须确保适当的安全性。建立广泛适当的防火墙以及设置管理员访问与用户访问的帐户可以保证安全性。

网状 VDOM 的配置可以变得非常复杂，全部的 VDOM 都参与进来时最为

复杂的情况。请在使用网状 VDOM 配置之前考虑必要性。

VDOM 间的路由规划

VDOM 间的路由配置启动了很多 FortiGate 设备的配置，增强了功能的灵活性的同时也存在可能的困难与问题。

复杂性

VDOM 间更多的连接会导致配置的复杂性。VDOM 的概念本身也不容易理解，加上额外的设置与配置很容易没法很好的控制。

为了避免这样的问题发生，在配置使用 VDOM 间的路由之前详细规划网络的配置确保您能够足够明了配置之前与之后的搭建情况。

配置之后，您不能随便对系统进行更改，任何更改可能会产生一些问题。另外确保更改不会对现有的 FortiGate 设备配置产生负面的影响。

例如，使用以前的方法更改 VDOM 之间的通信，通信线缆需要重新布置与安插。与 VDOM 间的路由配置，所有的更改都发生在内部比较，物理配置的更改比简单的输入 CLI 命令需要更多的查看。不严密细致专业的查看可能会导致在 VDOM 之间的交互一些意料之外的配置更改。

避免使用 VLAN 带来的问题

VLAN 的应用会带来以下问题：

- 不均衡的路由
- 第二层流量
- NetBIOS
- STP 转发
- VLAN 接口太多

不均衡的路由

您可能发现一些网络中的主机很意外的不能连接到某些其他网络。发生这样情况的原因是请求与回应的数据包走了不同的路径。如果 FortiGate 设备只发现回应数据包而没有对应的请求数据包，设备将把这些数据包作为非法数据包屏蔽。而且，如果 FortiGate 设备发现相同的数据包在多个接口出现，将把这种状况作为潜在的攻击而屏蔽会话。

这些情况就是不均衡的路由。默认情况下，FortiGate 设备在发生这样的情况时会屏蔽数据包或丢弃会话。您可以使用以下 CLI 命令允许不均衡路由：

config system settings

set asymroute enable

end

这样便解决了被屏蔽流量的问题，您也知道这是不均衡路由造成的。但是，设置允许不均衡路由不是最好的解决方案，因为这样降低了系统的安全性。最好是更改路由或更改 FortiGate 设备连接网络的方式。详细信息参见“不均衡路由与其他 Layer-2 FortiGate 设备安装技术说明”中有关不均衡路由的情况以及可能的解决方案。

⚠**警告：**如果您设置启动了不均衡路由，反病毒与入侵防护系统便不起作用了。FortiGate 设备对任何连接都不加分辨并对每个数据包单独对待，这样就造成了一个“无国家”分辨能力的防火墙。

Layer-2 流量

默认情况下，FortiGate 设备不通过 Layer-2 流量的。如果是 Layer-2 流量的传输协议例如 IPX，PPTP 或 L2TP 在您的网络中被使用，您需要配置 FortiGate 设备通过这些流量，使用 CLI 命令：

config system interface

edit <name_str>

set l2forward enable

end

这里的<name_str>中输入接口的名称。

配置允许 Layer2 流量可能导致数据包通过网络重复路由。这种情况发生在源与目标地址之间存在不止一条 Layer2 路径的情况下。这样路由就会被阻碍。路由寻址的方法之一就是在网络中的网关与路由配置生成树协议（STP）。

ARP流量

以地址解析协议（ARP）传输的流量是网络主要的流量，FortiGate 设备的接口在默认情况下便启动了对 ARP 流量的传输。通常情况下，您是希望 ARP 数据包能够通过 FortiGate 设备，特别是对用户与服务器或用户与路由之间启动该协议的传输。

ARP 流量会产生一些问题，特别是在透明模式下，在将 ARP 数据包从到达的接口发送到所有其它接口包括 VLAN 接口的情况。Layer2 的交换机在检测从不止一个交换机接口或多个 VLAN 发起的相同 MAC 地址时变得很不稳定。如果 Layer2 的交换机对每个 VLAN 没有保持独立的 MAC 地址列表时，便发生不稳定的状态。交换机不稳定可能会导致网络流量传输变慢。

多个VDOM的解决方案

一个解决方案便是在 FortiGate 设备中配置多个 VDOM，每个都对应一个 VLAN。也就是说每个虚拟域中都分别有一个向内与向外的 VLAN 接口。VDOM 之间不转发 ARP 数据包。

默认情况下，物理接口在根虚拟域中。不要在根虚拟域中配置任何 VLAN。

配置应用 VDOM 后，交换机将不会接收到具有相同源 MAC 地址不同 VLAN ID 的多个 ARP 数据包了，也不在发生不稳定的情况了。

转发域的解决方案

配置应用 VDOM 后，交换机接收到具有相同源 MAC 地址不同 VLAN ID 的多个 ARP 数据包的情况得到改善。但是上述解决方案可能在应用中存在问题。可能您需要设置了多于许可证允许的 VDOM 的 VLAN，没有足够的物理接口可以配置。这种状况下，独立的 VDOM 设置可能不能很好的工作。

这种情况下的解决方案是使用 CLI 命令 forward-domain <collision_group>。该命令可以标记属于一个特殊转发域冲突组的 VLAN 流量，并且只有属于这样冲突组的 VLAN 才接收被标记的流量。默认情况下的接口与 VLAN 均是转发域冲突组的一部分。

该解决方案的优点在于减小了管理复杂性，使用较少的物理接口并增强了网络管理的灵活性。

在以下举例中，转发域冲突组 340 包括 Port1 中的 VLAN340 流量以及 Port2 中未标记的流量。转发域冲突组 341 包括 Port1 中 VLAN341 的流量以及 Port3 中未标记的流量。默认情况下所有其它接口均是转发域冲突组 0 的一部份。

以下是完成该配置的 CLI 命令：

```
config system interface

edit “port1”

next

edit "port2"

set forward_domain 340

next

edit “port3”

set forward_domain 341

next edit "port1-340"

set forward_domain 340
```

set interface "port1"

set vlanid 340

next

edit "port1-341"

set forward_domain 341

set interface "port1"

set vlanid 341

next

end

NetBIOS

网络中运行微软 windows 操作系统的主机依赖 WINS 服务器将主机名称更改为 IP 地址。主机与 WINS 服务器之间的通信使用 NetBIOS 协议。为了支持该类型的网络活动，您需要启动将 NetBIOS 请求转发到 WINS 服务器。输入以下命令：

config system interface

edit <interface>

set netbios_forward enable

set wins-ip <wins_server_ip>

end

在<interface>出输入接口的名称，wins_server_ip 是 WINS 服务器的 IP 地址。这些命令只适用于 NAT/路由模式。

STP转发

FortiGate 设备不参与生成树协议（STP）。STP 是 IEEE802.1 协议以确定网络中没有 Layer-2 环路。网络中当流量的路由路线多余一条时便发生环路现象，这时流量将被广播流回到发出时的交换机，回路可以导致无休止的流量淤积而造成网络增溢现象的发生。

如果您在网络的拓扑结构中使用了 FortiGate 设备，需要配置设置应用 STP 对网络进行环路保护。否则，STP 将 FortiGate 视作空白链接，便将数据转发到其它路径。默认情况下，FortiGate 设备屏蔽 STP 以及其他非 IP 协议流量。

使用 CLI，您可以设置接口启动 STP 转发与其他 Layer-2 协议流量：

config system interface

edit <name_str>

set l2forward enable

set stpforward enable

end

<name_str>处输入接口的名称。该配置也允许网络中使用其他 Layer-2 协议如 IPX，PPTP 或 L2TP 协议。

太多的VLAN接口

NAT 或透明模式下，任何虚拟域最多可以设置 255 个接口，包括 VLAN、其他虚拟接口或物理接口。

FortiGate 设备可能在某些情况下允许您配置比 255 个更多的接口，但是如果您配置的接口多余 255 个，系统会不稳定并且不能正常的工作。发生这些问题是由于路由的限制。当您试图配置更多的接口时，系统将弹出错误信息提示您接口配置已达到最大数量。

如果弹出设置接口已经到达最大极限的错误信息，说明您的系统设置了太多的 VLAN 并且路由变得不稳定。为了验证该结果，您可以删除一个 VLAN 然后恢复添加。如果 VLAN 设置太多的话，那么删除的 VLAN 就不能恢复添加。这种情况下，您应该删除一些接口（包括 VLAN），使接口的数量控制在 255 个或少于 255 个。执行该操作后，重新启动 FortiGate 设备清楚这部分内存与缓存。

为了在 FortiGate 设备上配置多于 255 个接口，您不得不配置多个 VDOM 以及在每个 VDOM 中设置很多接口。这些配置需要您设置多个 VDOM 来实现，在 FortiGate 设备型号支持的基础上您可以购买额外的 VDOM 许可证。有了这些配置许可证，您可以最大配置 250 个 VDOM，每个 VDOM 可以设置 255 个 VLAN，那么理论上最多可以配置超过 63000 个接口。当然，系统没有资源可以支持这么庞大的设置。