

<<微软防火墙Forefront TMG配置>>

图书基本信息

书名：<<微软防火墙Forefront TMG配置管理与企业应用>>

13位ISBN编号：9787302306870

10位ISBN编号：7302306877

出版时间：2013-1

出版时间：王春海 清华大学出版社 (2013-01出版)

作者：王春海

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<微软防火墙Forefront TMG配置>>

内容概要

《微软防火墙Forefront TMG配置管理与企业应用》系统全面地讲解了Forefront TMG的基础知识，同时介绍了Forefront TMG在政府、企业中的应用案例，以及使用Forefront TMG中可能碰到的多种问题和常见故障的解决方法，让读者能够“按图索骥”般地学习与借鉴。

<<微软防火墙Forefront TMG配置>>

作者简介

王春海，河北经贸大学信息技术学院实验中心高级实验师，MCSE、MCDBA。

主持组建过若干广域网、局域网工程，有着非常丰富的网络规划和建设经验，并且在网络维护、网络故障、网络安全、数据恢复和虚拟机应用等方面有独到的见解。

在《电脑报》、《中国计算机报》、《网管员世界》等报刊发表几十篇文章，出版《最新无盘工作站与终端配置及应用实例详解》丛书、《非常网管》丛书、《网管天下》丛书。

<<微软防火墙Forefront TMG配置>>

书籍目录

第1章Forefront TMG 2010功能概述 1.1 Forefront TMG 2010主要功能 1.2 Forefront TMG不能封杀P2P 1.3 Forefront TMG的功能 1.4 Forefront TMG版本 1.5 Forefront TMG系统需求 1.6 Forefront TMG的防火墙类别与多网络支持 1.7与VPN的集成 1.8多功能代理服务器与协议组管理 1.9恶意软件检查 1.10路由架构改进 1.11 网络入侵保护系统 1.12 Forefront TMG阵列与NLB功能 第2章Forefront TMG的安装与基本应用 2.1 Forefront TMG基础知识 2.1.1 了解Forefront TMG所处的网络位置 2.1.2 Forefront TMG基础知识 2.1.3网络基础知识 2.1.4通过电话系统理解路由、NAT、NAPT概念 2.1.5网络服务与TCP / IP端口 2.1.6代理与转换 2.1.7端口映射与端口转发 2.1.8理解Forefront TMG中的网络 2.1.9理解Forefront TMG的网络规则 2.1.10理解Forefront TMG的客户端 2.2 Forefront TMG部署与使用注意事项 2.2.1 多VLAN网络中三层交换机的配置 2.2.2在计算机上添加到其他网段的静态路由 2.3 Forefront TMG标准版的安装 2.4 Forefront TMG入门向导 2.4.1配置网络设置 2.4.2配置系统设置 2.4.3定义部署选项 2.4.4 Web访问向导 2.5 Forefront TMG控制台界面与仪表盘功能 2.6 Forefront TMG的监视功能 2.6.1 警报 2.6.2 会话 2.6.3连接性验证程序 2.6.4服务 2.6.5配置 2.7防火墙策略 2.7.1防火墙策略基础 2.7.2通过案例介绍访问规则与服务器发布规则 2.7.3系统策略 2.8 Web访问策略 2.8.1恶意软件检查 2.8.2 URL筛选 2.8.3 HTTPS检查 2.8.4 HTTP筛选 2.9入侵防御系统 2.9.1 网络检查系统概述 2.9.2部署NIS需要考虑的事情 2.9.3配置网络检查系统 2.9.4行为入侵检测 2.10远程访问策略 2.10.1在Forefront TMG中启用VPN服务器 2.10.2用户管理与设置 2.10.3 配置站点间VPN路由 2.11网络连接 2.11.1 网络 2.11.2网络规则 2.11.3网络适配器 2.11.4路由 2.11.5 ISP冗余 2.12 日志和报告 2.13疑难解答 第3章Forefront TMG应用之双线路与多台服务器发布 3.1 L市政府网络概述 3.2基于NAT的共享上网的实现 3.2.1 SecureNAT客户端概述 3.2.2准备Forefront TMG服务器 3.2.3安装Forefront TMG 3.2.4配置Forefront TMG的访问策略 3.2.5禁用Web恶意软件检测与网络检查系统 3.3发布单位内部的服务器与远程桌面 3.3.1 从SecureNAT客户端访问发布内部服务器的注意事项 3.3.2发布服务器到Internet的示意拓扑图 3.3.3发布Web服务器到Internet 3.3.4创建策略组 3.3.5发布多个终端服务器到Internet 3.4发布多个FTP服务器到Internet 3.4.1 FTP的PASV与PORT模式概述 3.4.2使用防火墙发布FTP服务器通常选择PASV模式 3.4.3发布双线FTP服务器到Internet 3.5通过域名访问单位内部网站的问题 3.6实现双线ISP功能 3.7 Panabit流量监控 3.7.1 Panabit概述 3.7.2 Panabit体系结构 3.7.3服务器与磁盘选择 3.7.4 Panabit安装 3.7.5让Panabit开始工作 3.7.6 Panabit策略设置要点 3.7.7升级Panabit系统及特征库 3.7.8重安装与升级 3.7.9当Panabit启动到“ Starting local daemons ” 时死机的解决方法 3.8对内部服务器进行旁路跳过流量监控 3.9旁路跳过Forefront TMG与流量监控 3.10使用HP iLO功能实现服务器的监控与管理 3.10.1为iLO设置管理IP地址 3.10.2设置时区与时间服务器 3.10.3添加管理用户名 3.10.4添加License 3.10.5服务器电源控制 3.10.6虚拟光驱与软驱功能 3.10.7远程KVM 3.10.8查看iLO日志 3.10.9系统信息 3.10.10 iLO升级 3.10.11 用iLO管理HP服务器的一些截图 第4章 多Forefront TMG应用之内网与防火墙客户端应用 4.1 G政府网络状况概述 4.1.1政府内网介绍 4.1.2 G市政府原有网络概述 4.1.3用户需求与网络改造总体方案 4.2交换机与路由器配置及服务器总体规划 4.2.1三层交换机的设置 4.2.2双线（电信、网通）路由器的安装与配置 4.2.3 网络中各服务器的规划 4.3基础服务器的安装与配置 4.3.1 Active Directory服务器的安装 4.3.2 DHCP服务器的安装与配置 4.3.3 WSUS服务器的安装与配置 4.3.4 NOD32服务器的安装与配置 4.3.5委派用户权限 4.3.6 Windows Update设置 第5章使用Forefront TMG保护电子政务中心案例应用 第6章组建基于SSTP的VPN网络 第7章组建使用智能卡进行身份验证的VPN网络 第8章组建Forefront TMG独立阵列 第9章使用Forefront TMG组建EMS管理的阵列 第10章ISA Server与TMG 2010经典应用与疑难故障排除 附录A VMware Workstation基础

<<微软防火墙Forefront TMG配置>>

章节摘录

版权页：插图：2.1.7端口映射与端口转发 端口映射与端口转发，用于发布防火墙内部的服务器或者防火墙内部的客户端计算机，有的路由器也有端口映射与端口转发功能。

端口映射与端口转发实现的功能类似，但又不完全一样。

端口映射是将外网的一个端口完全映射给内网一个地址的指定端口，而端口转发是将发往外网的一个2n的通讯完全转发给内网一个地址的指定端口。

端口映射可以实现外网到内网和内网到外网双向的通讯，而映射转发只能实现外网到内网的单向通讯。

例如，一台防火墙有两个端口，一个端口用于外网，设置的IP地址为202.206.197.125，另一个端口用于内网，设置的IP地址为172.30.1.254，一台Web服务器放置在内网，其IP地址为172.30.1.100。

如果想让这台服务器对外提供Web服务，则可以在防火墙上将202.206.197.125的TCP的80端口映射到172.30.1.100的80端口，这样，当外网用户访问202.206.197.125的Web服务时，实际上访问的是内网服务器上提供的服务，如图2.17所示。

如果在内网的172.30.1.100服务器上提供Web服务的端口不是80而是另外的端口如3333，则需要在防火墙上将TCP的80端口映射到内网172.22.100.100的3333端口。

2.1.8理解Forefront TMG中的网络 在安装Forefront TMG的计算机中，可以安装多个网卡，其中每个网卡，可以连接一个不同的网络。

如果用Forefront TMG做“边缘防火墙”，则至少需要安装两块网卡。

在边缘服务器中，Forefront TMG网络可分为内部、外部、本地主机、VPN客户端、被隔离的VPN客户端，如果Forefront TMG配置为“3向外围网络”，还将包括“外围”，网络，下面分别介绍。

内部：代表企业内部局域网，此网络的地址范围在Forefront TMG安装的过程中指定，并且在安装以后可以更改。

建议你总是通过添加适配器来添加内部网络地址。

Forefront TMG认为此默认的内部网络来代表受信任的受保护的内部网络。

Forefront TMG的默认防火墙策略会通过系统策略允许本地主机访问此内部网络上的资源，但是拒绝所有其他网络到内部网络的访问，您必须自行创建规则来允许到内部网络的访问，不能删除默认内部网络。

本地主机：此网络代表Forefront TMG本身计算机，与Forefront TMG之间的所有通讯都被认为是和本地主机网络之间的通讯，你不能修改或删除本地主机网络。

外部：指连接到Internet的网络，此网络包含未明确包含在其他任何网络中的所有IP地址，通常被视为不受信任的网络。

在刚结束Forefront TMG的安装时，外部网络包含所有未包含在内部网络中的地址、本地主机网络的IP地址（127.0.0.1）以及Forefront TMG上其他所有网络适配器的IP地址。

通常情况下，设置了“网关地址”的网卡被认为“默认的外部网络”。

VPN客户端：它代表通过VPN连接到TMG服务器的客户端计算机，由Forefront TMG动态生成，不能删除VPN客户端网络。

被隔离的VPN客户端：此网络包含尚未解除隔离的VPN客户端的地址，由Forefront TMG动态生成，不能删除被隔离的VPN客户端网络。

<<微软防火墙Forefront TMG配置>>

编辑推荐

《微软防火墙Forefront TMG配置管理与企业应用》内容翔实、结构清晰、以实践应用为主、理论为辅，适合Windows系统管理员和网络维护人员阅读，也可供从事网络维护与系统集成工作的用户参考，同时可以作为各大中专院校相关专业的教材。

《微软防火墙Forefront TMG配置管理与企业应用》要求读者具有一定的网络知识，有一定的学习能力

。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>