



使用入门

本章简要介绍了 Cisco Secure Firewall 的功能以及支持的分支机构和 WAN 功能。

- [关于本出版物，第 1 页](#)
- [Cisco Secure Firewall，第 1 页](#)
- [简化的分支机构概述，第 2 页](#)
- [功能，第 3 页](#)

关于本出版物

本指南详细介绍了使用 Cisco Secure Firewall 支持的分支机构和 WAN 功能的主要使用案例。

这些方法并不能满足所有可能的网络需求；相反，它们提供了一些模型，您可以在在此基础上构建自己的网络。您可以选择不使用示例中的功能，也可以添加或替换更适合自己需要的功能。

本指南假定您熟悉 Cisco Secure Firewall。有关配置的详细信息，请参阅《[Cisco Secure Firewall Management Center 管理指南，7.3](#)》和《[Cisco Secure Firewall Management Center 设备配置指南，7.3](#)》。

Cisco Secure Firewall

Cisco Secure Firewall 是一种非常强大的防火墙解决方案，具有 Snort IPS、URL 过滤和恶意软件防御等先进功能。

这一全面的产品通过在物理、私有和公共云环境中执行一致的安全策略，大大简化了威胁防护。

此外，它还能对网络基础设施提供广泛的可见性，从而迅速识别潜在威胁的来源和活动。掌握这些知识后，您就可以及时采取行动，在攻击有机会破坏您的运营之前阻止它们。

除了传统的防火墙功能外，它还提供以下功能：

1. 应用可视性与可控性
2. 用户身份感知和控制
3. 入侵预防和入侵检测

4. SSL/TLS 解密
5. 基于信誉的阻止
6. 文件和恶意软件防护
7. 虚拟专用网络 (VPN)

为了进一步确保网络部署的安全，Cisco Secure Firewall 在后期版本中提供了更多安全功能，例如：

- **加密可视性引擎 (EVE)**，可增强加密流量检查，而无需实施完整的中间人 (MITM) 解密。
- **象流检测**，用于检测和补救象流（通常大于 1 GB/10 秒的流），避免 CPU 占用率过高和丢包。
- **思科安全动态属性连接器 (CSDAC)**，通过利用标记和标签进行策略配置，而不是传统的基于 IP/网络的策略配置，为您的安全策略管理带来灵活性和智能。

简化的分支机构概述

随着组织在多个分支机构扩展其运营，确保安全和简化的连接变得至关重要。部署安全的分支机构网络基础设施涉及复杂的配置和管理流程，如果处理不当，不仅耗时，还容易出现安全漏洞。但是，组织可以通过利用 Cisco Secure Firewall 解决方案来简化分支机构的安全部署，从而克服这些挑战。

在本指南中，我们将探讨使用强大的防火墙解决方案简化安全分支机构部署的概念。通过集成 Cisco Secure Firewall 作为分支网络架构的基础组件，企业可以建立强大的安全基线，同时简化部署流程。这种方法使企业能够执行统一的安全策略，优化流量路由，并确保弹性连接。

Cisco Secure Firewall 支持的一些简化的分支机构和 WAN 功能包括：

- **安全弹性连接：**
 - 总部（中心）和分支机构（分支）之间的基于路由 (VTI) 的 VPN 隧道
 - IPv4 和 IPv6 BGP、IPv4 和 IPv6 OSPFv2/v3 以及 IPv4 EIGRP over VTI
 - 对具有静态或动态 IP 的分支的 DVTI 支持
- **高可用性，网络停机时间接近于零：**
 - 双 ISP 配置
 - 基于应用的接口监控优化路径选择
- **增加可用带宽：**
 - ECMP 支持在多个 ISP 之间实现负载均衡
 - SVTI 的 ECMP 支持
 - 使用 PBR 的基于应用的负载均衡
- **公共云和访客用户的直接互联网接入：**

- 使用应用作为匹配条件的策略型路由
- 为 Umbrella 提供本地隧道 ID 支持
- 简化管理:
 - SASE: Umbrella 自动隧道部署
 - DVTI 中心辐射型拓扑简化

功能

此表列出了一些常用的 WAN 功能

特性	已引入...
VTI 的环回接口支持	版本 7.3
对站点间 VPN 的动态 VTI (DVTI) 支持	版本 7.3
Umbrella 自动隧道	版本 7.3
VTI 支持 IPv4 和 IPv6 BGP、IPv4 和 IPv6 OSPFv2/v3 以及 IPv4 EIGRP	版本 7.3
具有中心辐射型拓扑的基于路由的站点间 VPN	版本 7.2
具有路径监控的策略型路由	版本 7.2
站点间 VPN 监控控制面板	版本 7.1
直接互联网接入/策略型路由	版本 7.1
带 WAN 接口的等价多路径 (ECMP) 区域	版本 7.1
带 VTI 接口的等价多路径 (ECMP) 区域	版本 7.1
备份基于路由的站点间 VPN 的 VTI	版本 7.0
通过站点间 VPN 支持静态 VTI (SVTI)	版本 6.7

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。