

## 用于确保无线、远程、内部局域网访问的通用方法 [概述](#) [挑战](#) [解决方案](#)

### 概述

在当今的企业环境下，访问方法日益增多，如千兆位有线连接、高速宽带访问、从不同位置的远程访问（信息亭、网吧），以及无线网络等，这些访问方式推动了对全新服务的需求。企业资源的移动及远程访问对远程工作人员的生产效率及业务效率至关重要。然而，无线通信的大规模部署同时却提出了新的安全及性能方面的需求。

在这种环境之下，管理员则面临着不断增长的用以保护关键企业资源免遭攻击的需求。根据用户标识/认证凭证、用户组及客户端设备，控制对不同资源的访问，而客户端设备在这种环境下是安全性要求最高的设备。

典型的企业环境能够包含如下组件：

#### 访问网络

- ☆ 有线网络（称为内部 LAN）
- ☆ 无线访问
- ☆ 广域网 (WAN) 或公共互联网

#### 资源网络

- ☆ 隔离区 (DMZ)，用于互联网可访问的服务
- ☆ 远程访问网关，为 DMZ 服务的一部分
- ☆ 具备服务器与大型机（用于托管业务应用）的数据中心

#### 访问与控制

- ☆ AAA 基础设施包括认证和会计服务器

企业环境的差异要求在计划访问时，需进行多方面的考虑。通常情况下，内部 LAN 被认作是安全的网络。但由于无线网络存在广播特性，因此不被认作是安全网络。这种网络容易受到窃听、非法接入点 (rogue access point) 及其它破解方法的攻击。对于远程访问，通常采取虚拟专用网 (VPN) 解决方案，如拨号、IPSec VPN、及安全套接层 (SSL) VPN。并且，对数据中心设备的所有访问都必须受到安全保护。数据中心使用访问列表阻止非法访问，同时反向代理服务器使用认证机制为应用提供更高级别的安全性。

### 挑战

在企业环境，对安全性的要求持续增长。为各种访问环境提供单独的安全方法（如单一认证或访问控制列表）无法出色地进行扩充，同时还会增加管理负担，使其极其昂贵。必须有一种更好的方法用于提供安全可靠的企业访问。这种方法应经济高效、易于管理、安全可靠，同时还能实现性能与可扩充性需求。

基本的安全性要求包括：

- ☆ 验证用户认证凭证与服务，规定用户的访问。
- ☆ 客户端完整性检查，包括端点安全验证，以及重新引导用户至预先定义子网，下载符合标准的反病毒软件、防火墙、操作系统更新和补丁。
- ☆ 防火墙规则，如基于协议、端口和目的地的精细访问控制及数据包过滤。

同一个用户常常从不同的地点访问企业资源，因而安全机制和访问策略应独立于用户访问方法（如无线、内部 LAN 及远程访问）。由此需要具备访问规则的统一安全策略，这样便能确保用户在采取任何访问方法，都能达到相同的用户服务级别。统一的方法同时也更加经济高效、易于管理和维护，并且不易出错，因为所有的访问策略仅需定义一次。

该白皮书列出了内部 LAN、无线及远程访问架构的技术要求和特性，指出了通用方法所提出的挑战。F5 使用涵盖网络层到应用层的通用访问方法，由网络层到应用层全部使用单独、统一且经济高效的管理解决方案。案例研究显示，F5 方法提供了统一的安全策略，可满足多种访问方法要求。

## 无线、远程及 LAN 访问的特性

尽管统一的方法相当吸引人，但它必须满足内部 LAN、无线及远程访问方法的不同特性。以下章节说明了每种访问方法的特性。

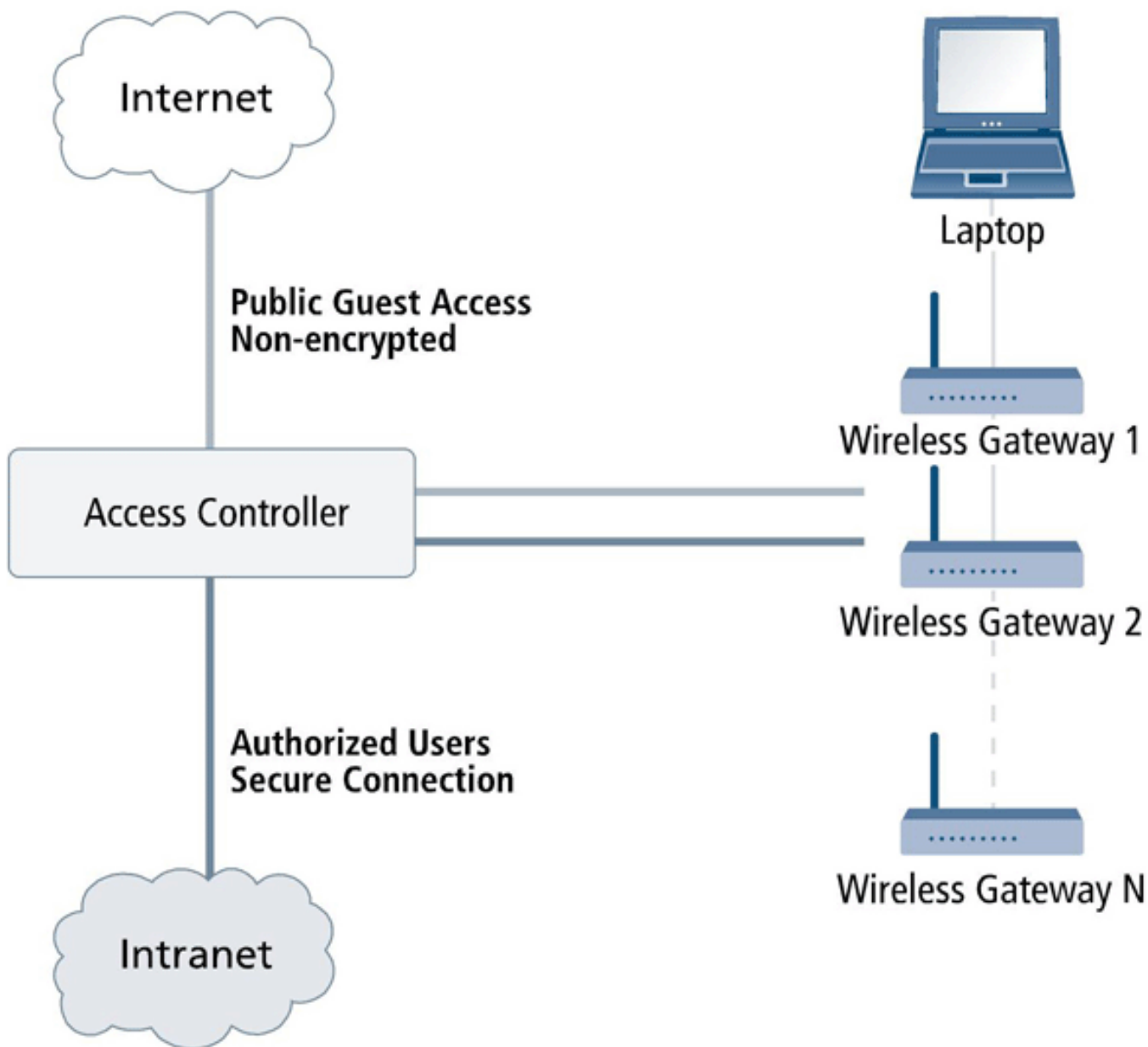
### 无线访问

无线网络设计用以实现高度移动性及灵活性。移动性是指用户在不同位置（建筑物的不同楼层、网吧与机场）之间移动时，还能保持与网络的连接。灵活性是指能够使用不同的设备（个人数字助理、智能电话、笔记本电脑）与网络连接。

在无线环境中，主要有两种连接环境：

- ☆ 公共热点访问
- ☆ 内联网安全访问

在每种情况下必须进行用户认证才可访问。热点认证将用户流量路由至公共互联网，而内联网流量则采用 VPN 加密方法进行控制。可根据用户组、服务器、资源，以及反映企业策略的安全策略进一步划分内联网访问。图 1 显示了适用于无线访问



的典型配置。

图 1：无线访问

### 远程访问

远程访问使用户可以从任意位置（网吧、机场或家庭办公）访问企业资源。其主要要求是为多个用户组（授权用户、合作伙伴、客户）提供访问，并将它们与允许访问的资源相关联。应能从任意客户端设备（公司笔记本电脑、家用计算机、信息亭、合作伙伴计算机等）对资源进行访问。

图 2 显示了适于远程访问的典型配置

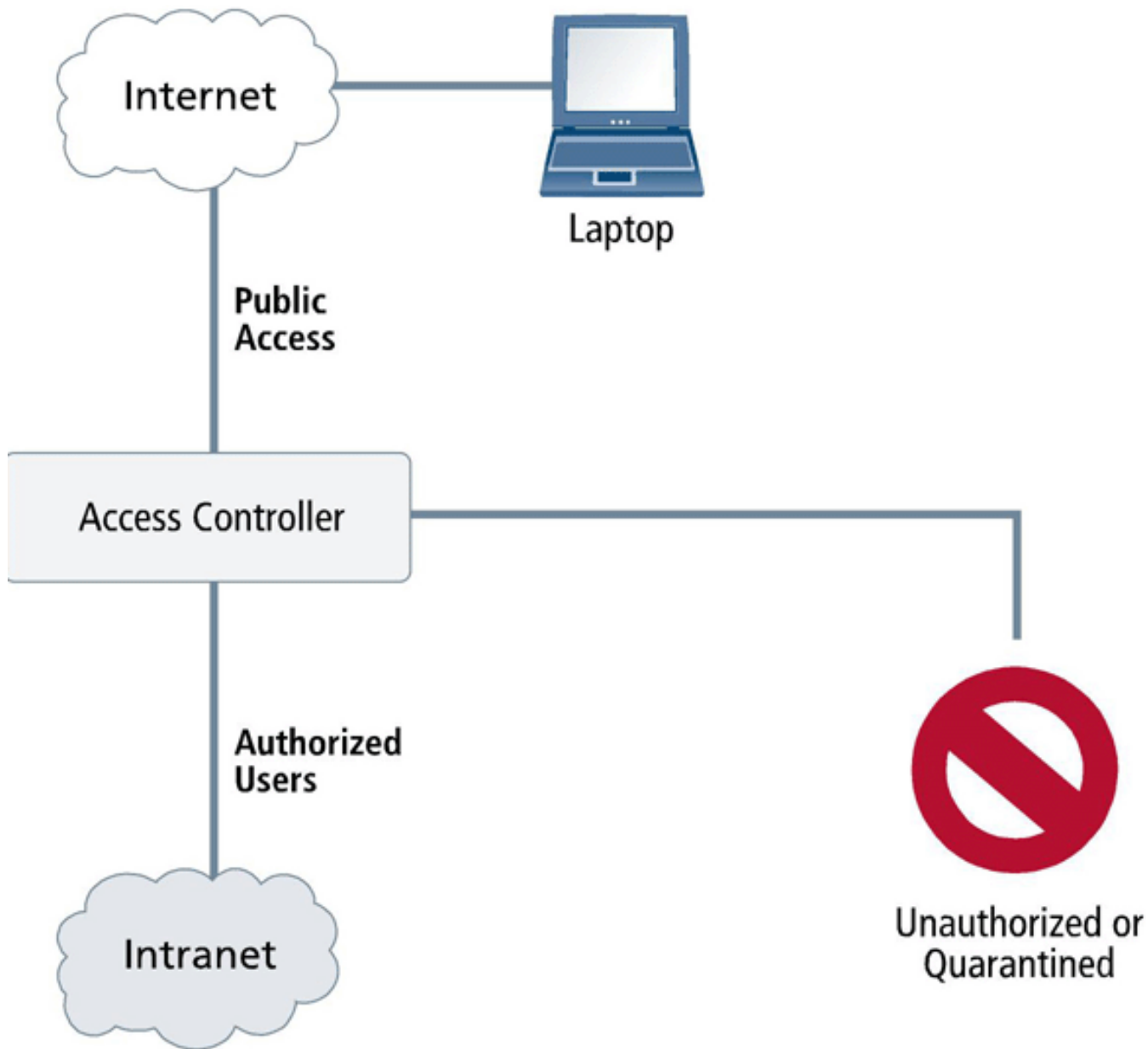


图 2：远程访问

### 内部 LAN 访问

在本文中内部 LAN 是指企业内的有线网络。通常认为，内部 LAN 比无线和远程访问网络更加安全；然而，向任意用户开发内部 LAN 仍具备安全风险。许多有线网络允许大部分通信进行无加密传输。然而，有线网络同无线网络一样容易遭受窃听，特别是当外部人员能够进行物理连接时。同样，内部用户可能会嗅探流量并访问其他用户的电子邮件（首席执行官的邮件、及其它授权用户的机密信息）。

图 3 显示了适于内部 LAN 访问的典型配置。

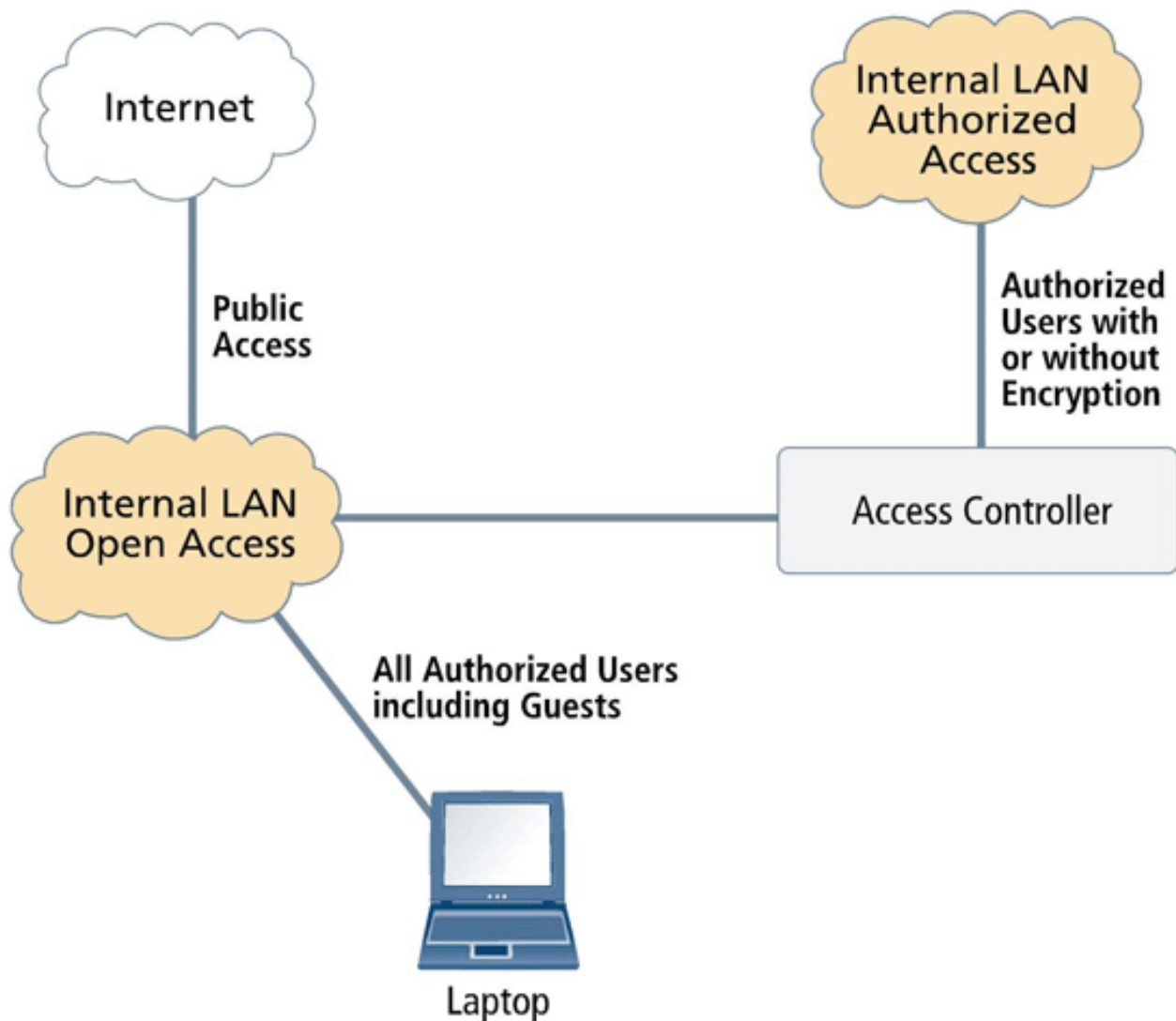


图 3：内部 LAN 访问

为确保各种访问方法的安全，您必须考虑：

☆ 是否易受窃听——通过无线网络访问的数据容易遭到嗅探或窃听。

☆ 入侵者攻击——入侵者能利用非法 (rouge) 接入点访问用户数据以及敏感的企业资源。有线对等加密 (WEP) 安全协议并不可靠，能够被破解。Wi-Fi 保护访问 (WPA)/WPA2 是新型的安全技术，要求具备特定的管理技能才能对其进行配置和管理。

☆ 客户端完整性检查——客户端完整性检查与端点安全对于远程访问至关重要，因为远程访问极易受到病毒和其它恶意代码攻击。网络管理员需要配置、监控并执行企业标准策略，来实现端点安全及用户认证凭证（包括操作系统补丁级别、防病毒版本与更新，以及防火墙版本）。

☆ 网段——利用单独的策略划分各种访问和资源网络，从而确保访问到特定的资源网络或资源网络中的服务。

☆ 终端设备支持——应允许多种客户端设备（包括台式机、PDA 和智能电话）访问内部资源，且不会因此降低安全性。

☆ 对等 (Peer-to-Peer) 流量控制——尽管客户端完整性检查能够保证客户端符合企业安全标准，但仍需要对实时流量进行监控。否则，对等流量能轻松滥用带宽，从而影响互联网访问的服务质量，并可能扩散恶意代码和蠕虫。

☆ 稳定的连接——用户连接可能会发生暂时性连接丢失，客户端 IP 地址也有可能发生改变（例如无线客户端正在漫游或采用 ADSL 连接时 IP 地址更改）。适当时，都应尽力提供机制来应对暂时性的连接丢失，并重新建立最初的对话环境来确保应用级透明。

☆ 性能——大量用户与带宽是典型的可扩展参数。无线及有线网络可能要求数百 Mbps 甚至 Gbps 的吞吐率。

☆ 多个地理位置——在延伸至多个地理位置的企业网络中，分散的方法要优于集中的策略引擎，即便所有站点的策略都相同。例如，如果需要访问本地资源，通过 WAN 链路将所有的流量路由至中央策略引擎可能不太适当。

☆ 高可用性——冗余配置可确保执行并控制这些安全要求，从而，当某个设备发生故障时，故障切换设备能够接管操作。

☆ 易于访问——用户应可在不同位置轻松、持续访问网络。为了便于管理，访问方法不应过于复杂。例如，移动用户需要从不同的位置的无线热点借助 web 浏览器轻松访问互联网。

☆ 可管理性——无线网络中，在每个无线接入点对安全策略进行管理相当复杂，容易出错，而且无法进行出色扩充。例如，用户访问内部 LAN 前应该检查端点安全性。然而，该功能仅可通过 WEP/WPA/WPA2 实施来完成。

☆ 可扩充性——在端口级别管理多个交换机和路由器上的安全策略或使用访问列表，并不是可扩充模式。

限制 VLAN 端口到 MAC 地址访问的 ACL 不能出色扩充或确保该方案还限制了用户的移动性。因此，集中的安全策略管理方法能根据用户认证凭证和分配至每个用户的角色（而非低级别的、容易出错的访问列表）来定义同类公司整体策略。这样就减少了管理和维护成本，同时降低了总体拥有成本 (TCO)。

下表总结了每种类型网络的访问特性。

访问	无线	远程	有线
是否易受窃听	高风险	低风险，因为流量加密	高风险
入侵者攻击	如果未部署扫描仪，则对入侵者开放	仅当入侵者成功验证时才能获得访问	入侵者能够访问 LAN 资源
客户端完整性检查	不具备 WEP/WPA/WPA2	能够在验证过程中执行	通常不适用该功能
网段	无线访问是不安全的网段 需要认证和实时流量监测机制	远程访问是非可信的网络 通常需要最高的安全性策略 不同的服务应采用不同策略	有线企业网络能分为可信任的、不可信任的、公共及私有区域 数据中心与特殊应用需要额外的认证

支持不同的终端设备	PDA、笔记本电脑与智能电话 可信任的用户与游客  各种操作系统	PDA、笔记本电脑、智能电话、网吧、家庭办公用户、移动用户  各种操作系统	可利用台式机、预先配置的设备、笔记本电脑访问  各种操作系统
对等流量控制	对于非 <b>adhoc</b> 网络，根据应用配置的不同，可支持对等流量控制，或所有的流量可路由至集中网关（通用访问控制器）	远程访问控制器能够检测来自或去往远程用户的对等流量	只有当对等流量首先通过交换机或路由器，才会被检测
稳定的连接	移动和漫游必须在无线网关上进行配置  通常需要移动 IP 和定制 GRE 通道	具有 SSL 重新协商的 SSL VPN，可确保可靠的连接	通过定义实现可靠的连接
可扩充性与性能	大量用户  跨多个站点进行分布，需要数百 Mbps 或 Gbps 吞吐率	一部分企业用户将同步使用远程访问  吞吐率取决于企业互联网带宽，通常为几十或数百 Mbps	大量用户  跨多个站点进行分布，需要数百 Mbps 或 Gbps 吞吐率
需要高可用性	需要	需要	需要
轻松访问	游客能够轻松访问，无需安装额外的软件	网吧或 PDA 访问，访问机制极为方便，无需任何额外的软件	
可管理性	完整的策略和用户管理	完整的策略和用户管理	完整的策略和用户管理

## 多访问概览

图 4 为三种不同的用户访问方法概览，包括：

☆ 远程访问和无线网络是隔离的，但借助适当的机制，可以控制它们对内部 LAN 的访问。远程访问控制器是远程用户能够访问内部资源之前对其访问进行控制的设备。因此，对于远程访问来说，强大的认证和加密功能是至关重要的。

☆ 无线网关解决与 RFID 及接入点相关的问题，并可能对无线流量进行加密。远程访问控制器能够在流量进入内部资源前

管理认证和 VPN 加密。

☆ 在内部 LAN，用户通常是可使用到资源。安全敏感应用和相应的安全性策略位于一个或多个受保护的区域。

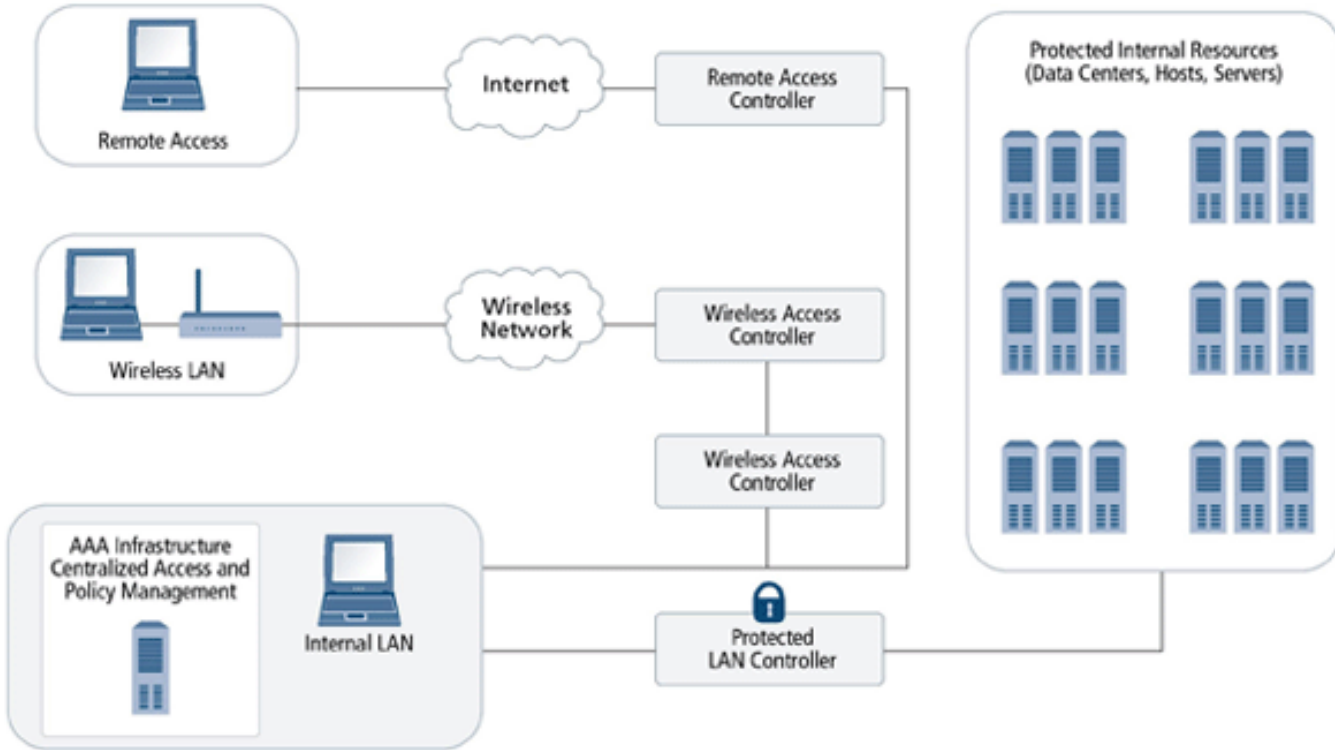


图 4：多访问概览

在办公时间对内部 LAN 进行正常访问的用户，在其离开办公室时即成为远程访问用户，而当他们离开办公桌在办公楼内走动时又成为了无线用户。因此，不考虑用户所采用的访问类型，而将一组访问策略应用于相同的用户是可行的。适于所有的访问方法的要求，包括：

- ☆ 端点安全
- ☆ 认证
- ☆ 访问策略管理
- ☆ 根据用以访问（可信任的或不可信任的）的设备，制定不同的服务级别
- ☆ 灵活性和移动性支持
- ☆ 服务质量和带宽管理
- ☆ 支持大量 SSL 对话的性能及可扩充性
- ☆ 审核能力

## 解决方案

统一访问

F5 通用访问方法基于 F5 的 FirePass 产品——安全套接层虚拟专用网 (SSL VPN)，该产品与 F5 的 BIG-IP 本地流量管理器

相集成。该集成使 F5 成为业内唯一一家能够为远程、无线 LAN (WLAN) 及本地局域网 (LAN) 用户提供统一且集中的安全性与访问控制的厂商，同时还可满足统一访问的吞吐量要求。BIG-IP 可保护网络层（例如，VLAN）的访问安全，提供了高速加密能力以及实时数据包检测与流量监测技术。借助 SSL VPN（具备增强的用户验证、访问控制、端点安全性、策略管理以及审核支持），FirePass 提供了可扩充的精密访问方案。

F5 通用访问方法既能够集中于某个位置，也可分布于多个地理位置（如以下部署环境中所示）。

F5 通用访问方法支持如下功能：

- ☆ 端点安全
- ☆ 用户认证
- ☆ 网络安全
- ☆ 统一的访问策略管理
- ☆ 高性能
- ☆ 可扩充性
- ☆ 审核与报告

以下章节对每项功能进行了描述。

## 端点安全性

端点安全性包括：在授权客户端访问资源之前进行安全检查。它是一种前瞻性的方法，用来确保只有符合所有安全策略的客户端才可以对资源进行访问。它同时还能阻止病毒或恶意软件进入企业网络。

对于不同类型的客户端设备（如笔记本电脑、PDA、网吧），安全性措施应该是不同的，并且应包括检测客户端的防病毒软件和版本，以使个人防火墙设置生效，并校验客户认证凭证。

端点安全性的优势之一是访问的范围和安全控制。从任何设备或位置访问任何应用都会潜在地导致安全隐患。借助适当的客户端安全性，端点安全性机制能够使管理员定义不同的访问级别，从而确保客户端和资源能够得到保护。例如：

☆ 具有高速缓存清除特性的信息亭用户可以访问终端服务器、文件、内联网和电子邮件。当用户退出后，高速缓存的位置和内容都会被自动清除。

☆ PDA 用户只能访问电子邮件和某些网络应用，不可以访问其它任何服务器。

☆ 如果笔记本电脑用户符合所有的端点安全性规则，则为他们提供完整的网络访问，并支持所有的客户端/服务器应用。

根据使用的设备，F5 通用访问方法可以动态地调整用户的策略。例如，您可以为移动设备、信息亭访问、笔记本电脑策略以及默认策略定义不同的策略。统一的端点安全性支持客户端完整性检查，如，检查系统注册表设置、任意特定程序的有无，以及操作系统服务包，检验客户端防病毒软件版本以及有无客户端认证的不同策略决定，等。

如果用户不符合安全性策略，您可以通过将用户重新引导至某一隔离网络来定义一个“返回”环境，在该网络中，用户可以更新其客户端。这一隔离网络可提供软件和修复操作，例如使用正确的软件版本更新杀毒程序。

## 用户认证

F5 通用访问方法支持动态认证方式。根据认证结果，您可以将用户分配到不同的组，以标明其能够额外访问某些特定的资源，如，访问特定的网段或服务器。F5 可插拔认证模块 (PAM) 扩展可以支持多种认证方案，包括：

- ☆ RADIUS
- ☆ 带 Kerberos 的活动目录
- ☆ 客户端证书 LDAP 和 OCSP
- ☆ 基本认证
- ☆ LDAP/LDAPs
- ☆ TACACS+
- ☆ RSA 安全 ID

该架构可以使您根据用户认证凭证动态定义每个用户的角色。

F5 通用访问方法也提供单点登录 (SSO) 工具，通过自动传递用户认证凭证，对用户访问 Web 服务器、网络资源及传统应用进行认证，同时不会对现有应用做任何修改。SSO 选项包括：

- ☆ 基于表格的认证
- ☆ 基本认证
- ☆ NTLM 认证
- ☆ 域认证

## 网络安全

F5 通用访问方法的一个重要要求是，能够将网络划分为多个网段，从而保护并监控从一个网段到另一个网段的访问。

在网络级别，您能够根据诸如发出或目的 VLAN、IP 地址以及协议等任意网络参数，并利用 IP 地址、VLAN、MAC 地址和数据包过滤机制，定义几乎所有的网络安全策略组合。您能够根据认证结果或应用响应，采用更严格的访问规则来确保安全性。利用 F5 的 iRules 和通用检查引擎，您可以定义定制安全策略。基于 TCL 编程语言的 iRules，是一个简单但功能强大的进行精细控制的工具；通用检查引擎能够解析用户流量的全部有效负载。定制安全策略使您能够根据 IP 地址、认证结果或有效负载，允许、拒绝、转发或丢弃流量。通过 BIG-IP 的对等流量也可用于对已知签名进行检查、完全重新引导至外部病毒扫描程序，或将其丢弃。

所有这些功能可用于实施 LAN 段和不同的区域，如可信任的、公共的、私人的以及受保护的区域，等等。是否需要认证及

功能强大的 VPN 加密功能，可通过位于每个段和区域边界的 BIG-IP 来确定。该配置成为进行划分操作的关键，可用于分类和定义网段、识别不同的流量类型，以及监控实时流量。

结合 SSL VPN 访问，您能够定义单独的路由表，以及同每个路由表相关联的 VLAN。LAN 段成为隶属于某一用户组的受保护资源。因此，能够拒绝其它组用户访问该 LAN 段，从而实现 OSI 模型第 2 层和第 3 层的网络安全。例如，属于公共组的用户，不能交换或路由到属于私人用户组的 VLAN。

F5 通用访问方法还提供了一系列的内置安全特性，用来保护网络免受 DoS、DdoS 以及协议篡改攻击，包括：

- ☆ 默认拒绝
- ☆ 自动防护
- ☆ SYN 检测
- ☆ DoS 和 Dynamic Reaping
- ☆ 虚拟服务器上的连接限制
- ☆ 协议无害处理 (Sanitization)
- ☆ 数据包过滤
- ☆ 资源隐藏
- ☆ 安全网络转换
- ☆ 无线漫游
- ☆ 审核
- ☆ 报告

欲了解 BIG-IP 安全功能的更多信息，请参阅《借助 BIG-IP，保护企业应用安全》。

FirePass 和 BIG-IP 通用访问方法实现了一个基于新的服务和策略的更为强健的安全模型，这些服务和策略易于定义，并能提高生产效率、降低总体拥有成本。

## 通用访问策略管理

F5 通用访问方法利用单独的、通用的策略，同时在网络层和应用层保护对网络资源的访问。这种单点控制降低了管理的负荷，并能够提高资源利用率，同时还能降低总体拥有成本。

根据 LAN 段（用户所处的源或目的 LAN 段）或认证结果（如用户认证凭证），F5 提供了多种不同的分配用户组和资源的方法。当进行认证时，您可以根据认证服务器的响应静态或动态地标明组和资源的分配。举例来说，如果用户利用 Active Directory（活动目录）顺利通过认证，则 Active Directory（活动目录）可返回一个属性（F5 利用该属性将用户映射至指定的组）。

另外，FirePass 提供了 Visual Policy Editor（可视化策略编辑器），它是唯一一款能够使安全管理员以图形方式定义复杂安全策略、并消除可能导致安全漏洞的策略错误配置的工具。生成的流程图同样能够使审核员以可视化的方式轻松审核安全策略，而无需通过复杂的产品配置进行分类。

您还可以将组管理策略与 F5 的带宽调整软件插件模块结合起来，通过为关键应用保留带宽并区分流量优先级，来确保服务质量。

## 可扩充性

F5 通用访问方法为企业以及互联网服务供应商和应用服务供应商提供了一种高度可扩充的模块。单个 FirePass 设备最高可托管 255 个互不相同的 URI，从而您可以为每个类型的用户组创建唯一的登录 URI。例如，授权用户可以登录 `company.example.com`，而合作伙伴则能够登录 `partners.example.com`。该虚拟化技术能够容纳不同的用户组，而 FirePass 同时负责在幕后将其映射至后端设备。

您可以在不同的配置模式下配置 F5 通用访问方法：

- ☆ 主动——被动，用于不断增加的冗余
- ☆ 集群，用于最大限度的可扩充性

集群高达 10 个 FirePass 设备，能够为最多 20,000 个并发用户提供安全的远程访问。在集群配置中，FirePass 通过自动同步 FirePass 策略简化管理。您也可以手动同步配置，包括策略和安全规则。

## 无线漫游

无线用户可通过两种方式与 F5 通用访问配置相连：

- ☆ 当用户在 AAA 服务器上成功通过认证后，就可以访问诸如互联网和公共打印机等公用资源。BIG-IP 代理认证请求并把用户认证凭证传给 AAA 服务器。成功认证后，允许用户对访问策略定义的资源网络进行访问。
- ☆ 其它所有访问都需要安全连接到通用的访问配置上。

无线用户必须在 FirePass 上进行认证，才能访问内部网络。FirePass 利用 SSL VPN 提供强大的认证和 VPN 访问功能，以符合最高安全标准。

FirePass SSL 连接借助 SSL Session Identifier（SSL 会话标识符）保留会话的上下文环境。当进行漫游，或发生临时性连接丢失而改变 IP 地址时，SSL 重新协商能够确保 SSL 连接及上下文环境重新建立。这保证了跨无线漫游区域的透明连接。

加密的 cookie 支持维持相同的用户认证上下文环境，可用于与单点登录特性配合使用。因此，当无线用户漫游时，应用会

话上下文环境和用户认证上下文环境都能保留下来。

## 审核与报告

F5 通用访问方法提供了以下审核和报告功能：

☆ 将虚拟服务器/池、接口、VLAN、带宽调整、数据包过滤、系统日志和 SNMP MIB 的统计数据记录下来。记录的信息包括用户登录、会话活动、组级别统计 (group-level statistics) 以及用户操作历史记录。鉴于 F5 的深层数据包检查能力，您也可以利用 iRules 记录其它信息。

☆ 以图形显示关于系统利用的统计数据（如 CPU 负载、接口统计数据 and 用户计算等信息）使您能够对系统状况有一个快速的概览。

## 部署情境

以下示例说明了 F5 的通用访问方法怎样为不同网络拓扑管理安全策略。在每个实例中，F5 通用访问方法都能利用高度可扩充和灵活的架构，同时在网络层和应用层保护您的企业。这种通用方法为任意规模的部署降低了总体拥有成本。

### 例 1：园区网部署

园区网配置如下：

- ☆ 内部 LAN 被分割为可信任、不可信任、受保护、公共，以及隔离的区域。
- ☆ 访问公用区域不需要访问可信任和不可信任区域所需的特殊认证或其它验证。
- ☆ 来自可信任的 LAN 的用户可以访问受保护的 LAN。
- ☆ 不可信任的、无线的和远程访问用户在其访问任何受保护资源前，都需要认证。

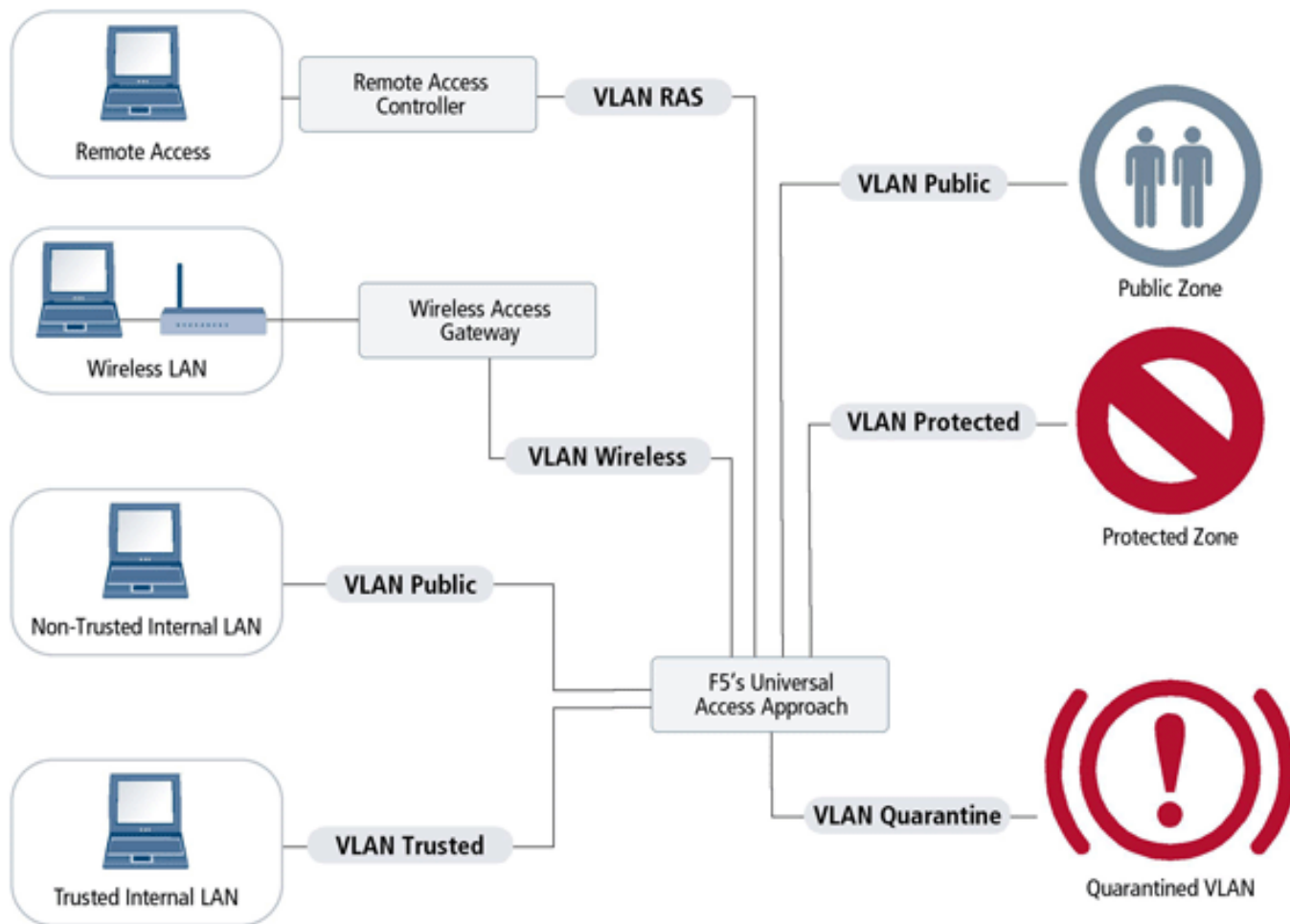


图 5：园区网中的 F5 通用访问方法

利用这种部署，F5 通用访问方法能够降低总体拥有成本：

☆ 每个区域分离处进行划分的中心点。

☆ 借助独立 VLAN，每个区域得以区分。能够为每个 VLAN 和/或每个 VLAN 内的服务单独定义高度灵活的访问规则、安全策略、认证方案，并确保 NAT 转换的安全性。

☆ 单独的认证服务器能够定义用户及其角色，以满足不同访问方法的需求。

☆ 您可以扩展 F5 通用访问方法，实时检查数千兆位吞吐流量，以支持园区网内非常流行的三重播放（数据、视频、语音）。深层数据包检查、通用检查引擎以及 iRules 提供了无人企及的控制功能，可用来管理和监控每秒数千兆位吞吐率的实时流量。

☆ 同 SSL 卸载及负载均衡结合使用，F5 解决方案支持数千兆位加密吞吐量，并能每秒处理成百上千项 SSL 交易。

## 例 2：多站点企业部署

对于其园区网络分布在多个不同地理位置的大型企业而言，每个园区都有一个小型或大型的园区网，这些网络与上述例子中描述的实例有着同样的要求。对于每种访问方法，都能采用灵活的安全及访问策略，实现无线和内部 LAN 访问。同时，它还支持内部 LAN 分段。远程访问服务通常集中于一个或两个位置（总部）。

图 6 显示了几个分布于不同地理位置的园区网配置。

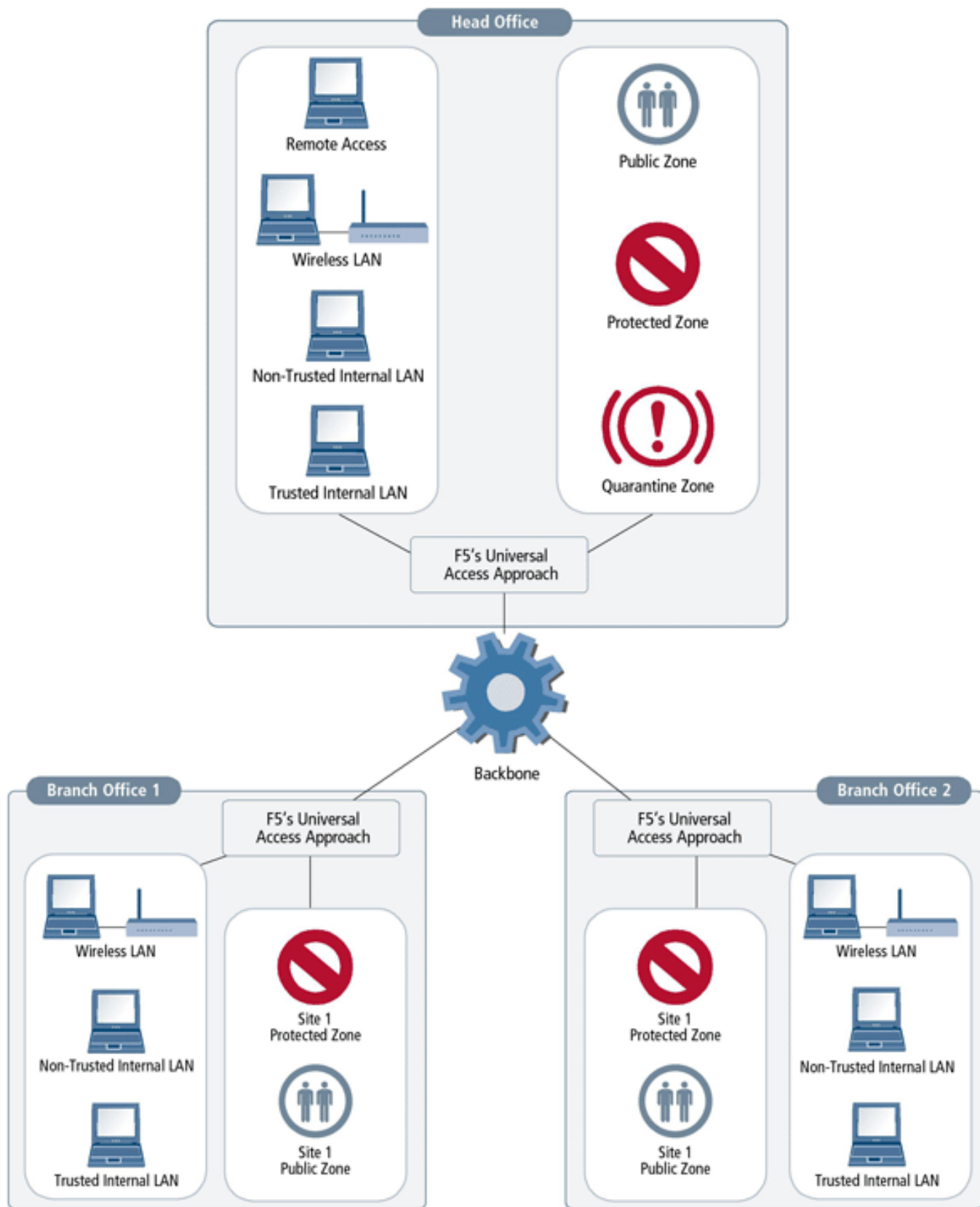


图 6：企业网络中的 F5 解决方案

在这种部署环境下，F5 通用访问方法能够降低总体拥有成本：

- ☆ F5 解决方案位于所有访问域的中心位置，包括远程访问域。
- ☆ 每个分支机构都有专用的 F5 通用访问方法，从而将园区划分为不同的区域。
- ☆ 中心位置包括用户访问权限及用户组定义，这些定义标明了安全策略和访问规则。
- ☆ 借助集群功能，F5 配置可实现自动同步。
- ☆ 在分支机构处可以设定受保护的部分，并对公共 LAN 进行划分。
- ☆ 分支机构能够访问中心位置的资源。

## 结论

F5 BIG-IP 和 FirePass 产品的集成构成了一套独一无二的解决方案，该方案能够提供一种通用的方法，可用于保护和管理基础设施，并能实现内部 LAN、无线及远程访问方法。F5 通用访问方法通过提供如下功能使企业获益：

- ☆ 针对无线、远程和内部 LAN 访问的单一安全策略。
- ☆ 针对所有企业用户和 guest 用户，提供一种与访问方法无关的通用认证方式。
- ☆ 单一的管理方法，可实现经济高效的管理。
- ☆ 可安全访问所有企业关键资源。
- ☆ 对于要求有多千兆位吞吐量，且需要具备大量用户的加密 SSL VPN (AES、3DES) 功能和透明代理功能，F5 也提供了支持。
- ☆ 用于选择性服务的所有 SSL VPN 功能，支持特定用户组、门户及 Webifyer 访问预定义的应用。
- ☆ 借助 DoS Reaping (DoS 调整)、带宽限制、数据包过滤、深层数据包检查和安全网络转换功能，可实现更强的安全性，使其免受网络、DoS、DdoS 和协议篡改攻击。
- ☆ 通用的可视化访问策略管理、审核，以及监控，能够降低总体拥有成本。
- ☆ 应用的高可用性和快速交付。
- ☆ 资本开支/运营开支方面的大量节约。
- ☆ 降低园区和分布式环境下的总体拥有成本。
- ☆ 完全虚拟化功能，为可管理服务部署降低资本开支/运营开支。