绿盟 NF 防火墙

产品白皮书

目录

插图索引

一. 当今网络边界安全的新挑战

现阶段，随着以 Web 2.0 为代表的下一代网络技术的迅猛发展，Web 化应用呈现出爆发式增长趋势，如今网络有近三分之二的流量都是 HTTP 和 HTTPS 应用。一方面，Web 2.0 应用可以显著增强协作能力，提高生产效率，但另一方面也不可避免的带来了新的安全威胁，体现在：

1) 新一代网络中以协议和端口来辨别应用，进而进行网络访问控制的方式已失效。当今网络，大量应用可以直接复用同一标准协议的知名端口（如 80 端口已不再专属 HTTP，可被 P2P、IM 等大量应用使用），或者直接承载在标准协议中（如 Web 视频直接承载在 HTTP 协议中）。并且，即使同一种应用，其通信端口和协议也会动态变更和跳变。此种环境下，如何还能精准识别不同应用，继续有效管控网络通信、合理分配带宽资源需要我们进行重新审视和思考。
2) 移动设备接入、无线网络连接、访客临时 IP 等已使网络边界模糊不清，接入渠道多样，入网设备繁杂，地址身份变化不定等已经使传统边界安全设备捉襟见肘，如何继续有效进行身份识别、执行接入控制，是新时代网络环境下又一难题。
3) 威胁入侵多以外网攻击或内网感染为触发点，一台设备被攻陷或感染后，作为跳板或传染源对内网其他资产进行扩散和传播，引起内网泄密、资源占用等财产损失。如何在新一代网络环境下评估现网、尽早发现内网资产易受攻击的薄弱环节、填补漏洞、防患于未然，而将安全事件扼杀于事前，是较事中、事后等被动防范更加主动有效的安全防护措施。
4) 随着防火墙各种功能模块的开启，产生的日志越来越多，如何从大量的日志中发现一些异常的行为，并且能快速定位，是当前亟待解决的问题。
5) 新形势下的网络威胁日益复杂和增多，用户的安全工程师为管理众多的安全设备而疲于奔命，如果自建安全管理平台则成本又太高。同时，即便对于已经部署安全管理平台的用户，在使用过程中也并不是得心应手，体验较差。而且，有些威胁事件发生后，工程师并不在现场，要想第一时间了解威胁事件详情，处理威胁事件非常困难，尤其是连入内网的操作更加繁琐，得具备一定的工作环境才能够完成。如何在保持低成本投入的前提下，便捷、高效的管理网络安全是用户亟待解决的问题。
6) 安全是动态的，仅靠一个设备，无法达到全面防护的效果，如何将众多的安全产品联合起来起到 1+1>2 的效果，是值得我们去思考的。

二. 现有防火墙解决方案的不足

而在上述网络应用层出不穷、新型威胁不断涌现的背景下，无论是传统防火墙、统一威胁管理设备（UTM）还是“下一代防火墙”们，均已远远不能满足用户对自身网络的安全防护诉求，主要体现在：

- **传统防火墙不能对网络应用、用户进行有效识别和控制**

  - **基于端口的访问控制已失效**

传统防火墙只能对网络流量进行静态的、基于端口或协议的应用识别，而对下一代网络中大量应用的端口复用（如 80 端口已不再专属 HTTP，可被 P2P 使用），端口跳变等均已束手无策，更无法实现精确管控，比如，允许访问 80 端口的策略很可能会让不期望的非法流量（如 P2P）通过，甚至让黑客程序借此漏洞发动网络攻击，而若干脆禁止 80 端口则会殃及 Web 应用，导致正常的网页访问无法进行，等等。

同样，流量控制和管理也到了细分应用种类的地步，传统的基于端口的粗放型流量管理不仅可能会“误伤”应该保证的良性应用，更可能会“助长”不良应用。

  - **基于 IP 地址的访问控制已不可靠**

传统防火墙通过 IP 地址对各安全区域进行访问控制，同时对威胁和应用来源进行跟踪审计。然而，除了固定的 IP 接入方案，随着无线通信和移动计算设备的飞速发展，越来越多的企业给员工配置移动办公设备，甚至允许员工自带私有设备工作。在这种多网多终端接入的环境下， IP 地址分配具有极强的随机性和不唯一性，IP 地址本身对用户身份信息的传递已经越来越不具有代表性，进而，传统的通过 IP 地址来进行用户访问控制已不再完全有效。而对网络访问者真正身份的全面有效、深度广泛的鉴定识别，才是适应社会和网络发展的最有效手段。

- **UTM 架构安全处理性能不足**

UTM 设备虽比单一防火墙提供了更全面的安全防护能力，但其安全性能却始终饱受诟病。在架构上，UTM 设备只是将各个安全模块“糖葫芦”似的串在一起，各模块间实则彼此分离，并重复对数据包解码，这种低效的架构缺陷致使安全性能随着模块的逐个开启而逐级大幅递减。

- **现有“下一代防火墙”，对内网安全的把控鲜有建树**

近几年涌现的林林总总的“下一代防火墙”产品们更多强调对边界流量的深入识别以及对外部入侵行为的检测和防护，而忽略了加固内部安全，“防患于未然”，从而并未形成一

套由外到内，再由内到外的全方位 360 度安全加固的解决方案，特别是随着 0day 及 APT 攻击的快速多变化，其单方面基于事中防范的被动检测方案也必将出现瓶颈而力不从心。

- **现有方案，未能简化运维**

攻击的多元、多样、复杂化对用户来说意味着安全设备采购、人力运维成本的持续增加，即便如此，复杂精深的安全专业对用户运维人员要求极高，很难不令防护效果大打折扣，如何提供一种有效的服务模式，将运维简化、高效、可视化，让用户无论何时何地都能简便、易用的对网络安全攻防进行高效运维，而这点无论是传统还是“下一代”防火墙产品也均无有效建树。

在上述威胁新趋势和现有边界安全产品防护能力、性能、解决方案不足、服务模式局限的现状下，用户迫切需要一种能够代表新一代网络和安全发展诉求的全新一代防火墙产品来解决关键痛点。

基于此种预见，结合 Gartner 于 2009 年提出的下一代防火墙定义，作为资深的网络安全厂商，绿盟科技结合多年业界领先的网络攻防经验和安全技术沉淀，推出了完全适应下一代网络攻防发展趋势和客户需求，并极具自身优势特色的新一代防火墙产品：绿盟 NF 防火墙（NF）。

三. 绿盟 NF 防火墙产品

3.1 客户价值

3.1.1 洞察网络应用，识别安全风险

传统防火墙无法有效分辨和检测出当今网络中出现的各种复杂应用，其中包括低风险应用（如 WebEx, ERP, Oracle 等），也包括高风险应用（如 Bit，QQ、电驴下载等），因而更无法准确的识别和拦截各类应用中的安全风险。

绿盟 NF 防火墙（以下简称 NF）能精确分类与辨识出包括低风险、高风险在内的 1200+ 种应用，根据应用不同风险等级分别进行不同级别的安全扫描，从而及时准确的识别和拦截各种威胁攻击，保障用户网络应用的安全性。

同时，NF 将当前网络中发生的一切安全威胁状况都及时清晰、可视直观的展现给用户，如当前网络中的应用流量分布，用户访问分布，以及在应用的安全防护中发现或拦截了哪些安全威胁等。

这些威胁按照风险等级，以统计告警、报表、日志的形式可视化的呈现给用户，使用户可以对网络的近日、近期、长期的安全状况都能有非常直观的了解和把握，从而可以及时有效的采取防御措施。

3.1.2 融合安全功能，保障应用安全

随着下一代网络 Web2.0 应用技术的高速发展，随之而来的基于应用的威胁攻击无论从数量上、形式上还是技术手段上都呈现出井喷式的增长和变化，如借助应用漏洞的威胁入侵，机要窃取，或由员工非法网页访问引起的挂马植入，或由邮件和文件下载引起的病毒传播，或以应用为载体的不良、敏感信息的传播等均呈现出多样化、复杂化和融合化。

怎样提供一种手段能够全面准确且管理简便的将所有安全威胁一网打尽。NF 结合公司多年来业界领先的攻防优势，推出具有自主知识产权的集入侵防护、防病毒、URL 过滤、内容过滤为一体的一体化安全引擎，一体化安全引擎可对应用流量进行 2-7 层一体化、全方位、多层面的安全过滤，一次解码即可发现并拦截全部威胁攻击和安全风险，保障用户网络环境的应用安全。

3.1.3 高效安全引擎，实现部署无忧

NF 使用专用的数通引擎、一体化安全引擎双引擎模式，并将其构筑于最新一代高速多核并行硬件平台之上。数通引擎与一体化安全引擎多核、并发的进行着高吞吐交互，从技术上保障了：在高网络层转发性能的基础上，开启安全模块性能不出现明显下降，从而保证用户可以放心的使用安全功能。同时提供的接入方案从百兆到千兆，再到万兆级，充分满足用户在各种网络环境下对安全接入的高性能吞吐需求。

3.1.4 内网风险预警，安全防患未然

全面掌控当前网络资产健康及风险状况，专家级的健康改善及安全防护方案指导，专业级

资产健康评分及分析系统。让用户随时洞悉网络当前潜在威胁风险，并可根据风险建议及时执行管控策略，或对风险资产堵漏升级，或进行访问控制和风险防范，最终核查改善效果，将威胁入侵扼杀在摇篮，防患于未然，呈现 7*24 小时的健康绿色网络。

3.1.5 事件关联分析，快速定位异常问题

以用户、应用、IP 等多种维度为入口，进行流量、会话、威胁方面的统计及排名，并且将 IP、应用、安全事件等进行关联，用户可以根据需求，对事件进行挖掘，快速定位异常问题。同时，用户可以对非 TOP N 排名中的 IP 进行监控，将其产生的所有日志进行关联分析。

3.1.6 云端高效运维，安全尽在掌握

通过绿盟科技云端安全运维模式，用户可以随时随地，7*24 小时的实时在线监控安全设备负载和运行状况，在线掌控用户网络安全事件状况，通过云端专业分析，第一时间帮助用户预防和发现各类安全威胁和攻击，帮助客户在攻防难度与日俱增的当今网络时代下，实现防护效率和准确度提高，同时此种模式使用户的安全运维投入大大减少，将用户从繁重吃力的安全对垒中解放出来，从而可以全部精力投入到业务发展中去。

3.1.7 多方位组合，打造安全防护生态圈

NF 支持与绿盟科技的多种产品进行联动，形成组合方案，达到 1+1>2 的效果。比如：与绿盟堡垒机组合，将远程运维变得更安全快捷；与绿盟远程评估分析系统组合，可以将内部资产的漏洞及防护情况尽收眼底；与金山 V8+组合，可以严格控制内部资产的安全性，将风险降到最低；与 TAC（沙盒）联动，全面提高对未知威胁的防御能力；与黑洞清洗云服务联动，借助云端黑洞云服务清洗本地流量，高效提升本地防御 DDOS 攻击的能力。

3.2 产品概述

绿盟 NF 防火墙（英文简称 NF）是绿盟科技构筑在最新一代 64 位多核硬件平台基础之上，采用最新的应用层安全防护理念，同时结合先进的多核高速数据包并发处理技术，研发

而成的企业级下一代边界安全产品。其核心理念是立足于用户网络边界，建立起以应用为核心的网络安全策略和以内网资产风险识别、云端安全管理为显著特征的全方位的安全防护体系。

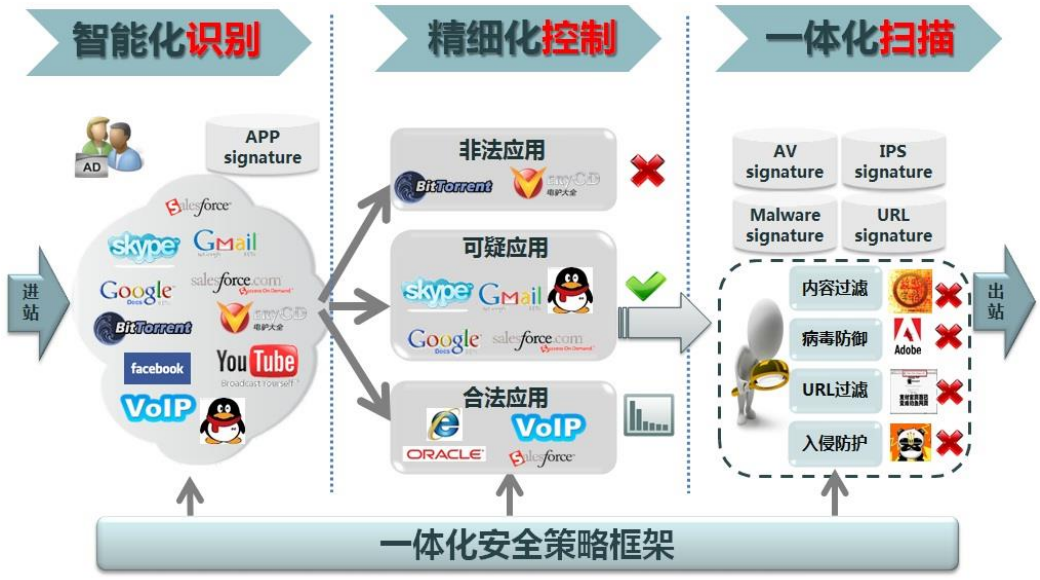

图 1 核心理念

- **智能化识别应用**

通过智能化应用、用户身份识别技术，绿盟 NF 防火墙可以将网络中单纯的 IP/端口号（IP/Ports），以及流量信息，转换为更容易理解、更加智能化的应用程序信息和用户身份信息，为后续的基于应用程序的策略控制和安全扫描，提供了识别基础。

- **精细化控制应用**

绿盟 NF 防火墙可以根据风险级别、应用类型、是否消耗带宽等多种方式对应用及应用动作进行细致分类，并且通过应用级访问控制，应用流量管理以及应用安全扫描等不同的策略对应用分别进行细粒度的控制和过滤。

- **一体化安全扫描**

在完成智能化识别和精细化控制以后，下一代防火墙对于允许使用且可能存在高安全风险的网络应用，可以进行漏洞，病毒，URL 和内容等不同层次深度扫描，如果发现该应用中存在安全风险或攻击行为可以做进一步的阻断并且记录成为详细的安全日志和风险报表。

- **资产风险识别和云端安全管理**

绿盟 NF 防火墙可以主动、先发性的对用户内网脆弱资产进行风险评估，并提出加固方案，是用户的内网安全管理专家，同时又可以通过接入云端，简化运维，对安全威胁在线分析和把控，是用户的云端安全管理专家。

3.3 产品架构

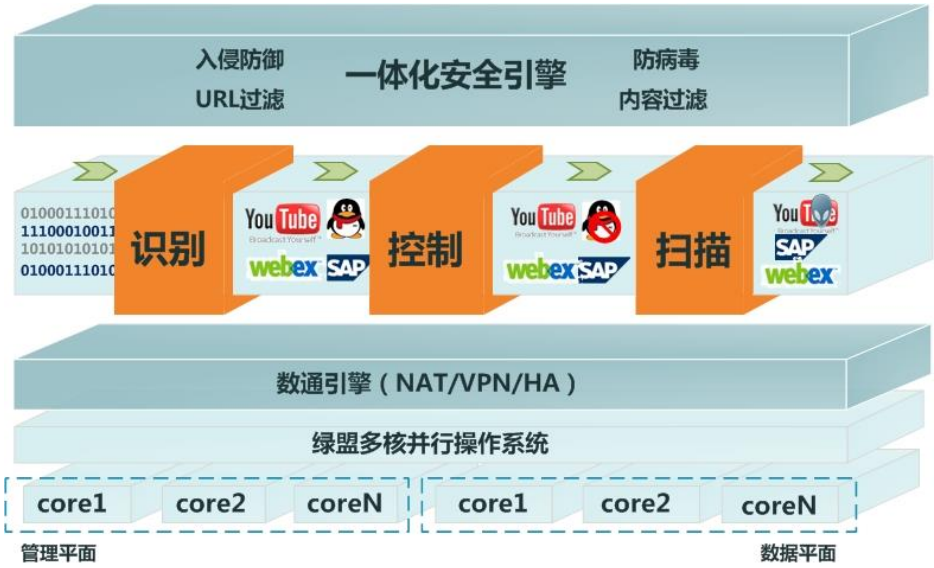

图 2 整体架构

NF 产品构筑在 64 位多核并发，高速硬件平台之上，采用自主研发的并行操作系统，将管理、数通、安全平面并行部署在多核平台上。多平面并发处理，紧密协作，极大的提升了网络数据包的安全处理性能。

NF 产品采用数通引擎和一体化安全引擎，双引擎设计。数通引擎实现基础防火墙功能，并作为整个系统运转的核心，将底层数通处理和高层应用安全处理，高度整合和驱动起来。

具有绿盟科技自主知识产权的一体化安全引擎技术，与数通引擎无缝结合。该引擎对网络数据包只需进行一次解码，即可完成 4-7 层全部安全扫描和过滤，从根本上解决了传统 UTM 设备各安全模块彼此分离、解码重复的问题，从而保证模块开启安全性能不明显下降。

在数通引擎的网络底层支持和一体化安全引擎的高层防护的双引擎模式下，NF 对用户网络流量全天 24 小时不间断、高速的进行着应用识别、控制和安全扫描。保障着用户业务安全无忧的正常运转。

3.4 主要功能

3.4.1 识别和可视性

- **应用识别与控制**

  - **应用管理**

NF 内置应用识别库，支持 1400+种应用识别。在配置界面上为用户提供应用列表，并可将应用进行 5 维度分类，包括按风险等级分类（1-5 级威胁度），按商业类别、子类别分类（如媒体类，图片视频子类），按实现技术分类（如 P2P），以及按照特征标签分类（如消耗带宽类，传输文件类应用等）。同时支持按照以上 5 维度的任意组合供用户对应用进行详细查询定位。

  - **自定义应用**

随时更新的内置应用库已经涵盖当今互联网、企业绝大多数应用，然而如遇特殊需求，NF 支持应用自定义功能。通过指定应用特征识别码、特征域名、数据包大小、识别起止范围、端口号以及服务模式，用户可定义对特殊应用的识别方法，并可将该应用进行 5 维度归类，实现对应用特征的标识。

  - **未知应用自识别**

未知应用特征自动识别模块配置简便，针对 HTTP 协议只需配置应用名称、服务 IP 和服务端口，NF 将会自动识别应用，在识别过程中无须人工干预，识别完成后可以输出规则描述 xml 文件，形成最终的应用特征库，此后网络中的同类型应用则均可识别。

  - **应用过滤器**

虽然 NF 已经对应用进行了 5 维度分类，但在实际使用环境中，用户仍可以以其他方式将应用进行归类，并在一体化应用配置策略中进行引用。应用过滤器功能就是为满足用户上述需求而产生。用户可先在应用过滤器中根据需求对应用进行多维查询，当确认过滤出的应用正是所需时，即可对此过滤器进行冠名保存。在之后的一体化应用策略配置中，用户可任意选择多个冠名过滤器，设备将会对过滤器中的归类应用，执行一致的识别和控制策略，极大的方便了用户的应用策略管理和使用。

- **用户身份识别**

作为下一代防火墙显著特征之一，NF 对在线用户身份识别功能做了全面细致的支持。与传统的将用户认证策略混入防火墙策略配置中不同，NF 将用户认证从防火墙复杂的策略配置中抽离出来，从逻辑上做出更合理清晰的呈现。

用户可对不同的安全区域指定不同的认证策略，并可根据不同场景选择不同的身份识别方案，例如，可从域控服务器直接获取身份信息，与第三方认证服务器（Radius、AD、LDAP）认证，本地帐号库认证，证书认证，以及结合以上多钟认证方式于一体的多因素认证。

同时，为方便用户理解和使用，NF 对用户账号进行了集中管理和控制。只需集中配置好账户信息（包括 Radius、AD、LDAP、本地数据库、证书账号等）即可在用户认证策略、VPN 授权、设备管理员授权等多处便捷使用。

- **日志记录和统计报表**

NF 让用户随时可以了解当前网络正在发生什么。具体体现为，可实时了解当前网络中正遭受哪些威胁攻击（包括入侵攻击、病毒、恶意站点及敏感信息），以及相应的威胁等级、攻击数目等。

同时，用户可实时了解当前网络中一段时间以来各网络接口带宽使用情况，流量排名前十的应用以及流量使用排名前十的用户，并可实时互查应用与用户流量间的使用关系。

除了实时网络状况，NF 为用户提供按日、按周、按月、按年的安全趋势分析报表以及以往所有的访问控制和安全日志。从而让用户对安全威胁、业务应用、用户流量、网络负载从时间、数量、程度上通过各种形象化图形和数据手段有了高度可视化的跟踪和了解。

- **事件关联分析（ECA）**

我们知道传统防火墙的事件主要是从流量和会话的维度来进行统计和 TOPN 的排名，但这种统计针对不同的事件之间是无法关联的，也就无法快速的发现、定位和解决问题。而 ECA 具备将各种事件进行关联分析，可以从不同维度出发，一步一步挖掘问题的根源，帮助用户快速的定位并解决问题。

3.4.2 一体化策略与控制

- **一体化配置策略**

基于安全引擎的一体化设计，NF 在配置界面上为用户提供了较传统防火墙和 UTM 完全不同的清晰和简捷的管理体验，即一体化配置策略。

一体化配置策略将传统五元组访问控制与具有下一代防火墙特征的用户识别、应用识别控制有机的结合起来，同时对其他防火墙产品一贯分离且重复的安全策略配置方式，进行了高度集中和融合。

在一条策略中即可全部或部分选择：入侵防护、防病毒、URL 过滤、内容过滤。免去用户以往在多个不同安全配置页面间频繁切换，重复配置的不便。其结果是在其它防火墙产品上需要配置 5、6 条策略才能实现的功能，现在在 NF 上，只需要一条策略即可完成，且逻辑上更加清晰简单，便于理解，极大的提高了管理易用性和可维护性，防止了繁琐配置引起的错误风险。

- **流量管理和分析**

基于强大细致的用户、应用识别能力，NF 支持用户以安全区、IP 地址（网段）、时间、用户、应用多维度的对流量进行管理和控制，包括限制应用上下行最大带宽、保证应用上下行最小带宽、保证带宽下的优先级排序以及每 IP 的进行应用流量控制，从而做到合理分配网络带宽，保证重要业务的正常优质运行，限制或防范非法滥用网络资源的应用对流量的过度占用等。

3.4.3 应用层防护

- **入侵防护**

NF 内置 4200+威胁特征库，并将威胁入侵分为 5 大类，分别是按攻击手段分类（如获取权限、信息收集类），按技术手段分类（如蠕虫、P2P），按流行程度分类（非常流行、中等流行），按危险程度分类，按服务类型分类等（如 WWW、FTP 事件等）。

NF 可防护远程扫描、暴力破解、缓存区溢出、蠕虫病毒、木马后门、SQL 注入、跨站脚本等各种网络及应用攻击。同时支持用户自定义规则，建立规则组等功能。并能够对检测到的入侵事件实时告警、阻断、记录和提供统计报表。

- **URL 过滤**

NF 具有业界领先的基于云端的 URL 分类库，内含按照不同类型（如不良言论、色情暴力、网络“钓鱼”、论坛聊天等）划分，可实现对工作无关网站、不良信息、高风险网站的准确、高效过滤；

同时 NF 内置的 Web 信誉库，通过对互联网站点资源（域名、IP 地址、URL 等）进行威胁分析和信誉评级，将含有恶意代码的网站列入 Web 信誉库，可有效阻挡用户对挂马等不良信誉网站的有意或无意访问，实现对终端用户的安全保护。

- **僵尸网络防护**

攻击者通过各种途径传播僵尸程序感染互联网上的大量主机，并且通过一个控制信道来控制而被感染的主机将，组成一个僵尸网络，是 DDOS 攻击的一种手段。

NF 从两个方面对僵尸网络进行防护。一方面，当用户访问挂马等有安全风险的网页时，给予及时报警和阻断；另一方面，即使用户通过其他途径（如：通过 U 盘、移动硬盘等拷贝文件、内部网络互传文件等）被感染，NF 也可阻止被感染的主机与攻击者建立控制信道，使攻击者无法控制被感染的主机，从而保证用户不会被攻击者所利用。

- **防病毒**

NF 采用流模式和启发式文件扫描技术，对利用 HTTP、SMTP、POP3、FTP、IM 等多种协议进行传播的病毒进行扫描，完成对木马病毒、蠕虫病毒、宏病毒、脚本病毒等的查杀，同时支持多线程并发控制、深层次压缩文件杀毒、病毒白名单等功能。

此外，NF 将专业防病毒引擎和多核并行处理技术完美融合，实现高速病毒处理性能。

- **内容过滤**

通过内容安全关键字，NF 可对任意安全区域间交互的网页内容、搜索引擎信息内容、文件传输（文件名、格式、内容）、邮件收发（包括收发人、标题、内容、文件等）、论坛发言、服务器操作、以及即时通讯内容等进行基于内容关键字的准确检测、阻断、告警、记录和信息还原，实现深度内容安全管理与跟踪，避免用户机密信息、重要文件通过网络外泄，也避免了非法言论及不良信息的传播。

3.4.4 内网资产风险识别

图 3 资产管理

- **资产风险识别**

可根据用户指定的网络范围，通过自动及手动识别等多种方式，识别出多种资产类型，如 PC、移动设备、服务器等等资源类型。并在此基础上，评估资产安全因素，分析资产受攻击可能性、危害程度、攻击范围及防护难度。针对易受攻击的系统及应用软件进行打分告警、报表分析，如操作系统版本漏洞威胁度、上网浏览器客户端漏洞威胁度等，让用户实时了解当前网络资产资源中的脆弱度，勾勒脆弱度全景图，并可针对性的实施漏洞填补，升级补丁，防火墙策略访问控制，流量监控等安全措施，从而达到防范潜在入侵攻击的可能性。

- **安全加固方案指导及实施**

针对识别出的资产风险，为用户提供一键安全策略生成的功能，从网络通信层面首先加强与脆弱资产通信数据的一体化安全扫描和防护，及时发现及时防护，弥补了漏洞填补，软件更新升级延时长，反应慢的不足。并可实时告警和记录入侵安全事件，形成安全事件报表和趋势图，指导用户及时做出加固防护。

- **资产风险持续评估**

从资产风险识别，到相关加固方案实施后，系统会继续跟进风险防范验证效果，通过二次识别打分、相关日志报表、审查记录的跟踪查询等手段验证对比防范方案的实施效果。从而从发现到解决问题到验证形成闭环，极大体现产品客户价值。

3.4.5 云端接入

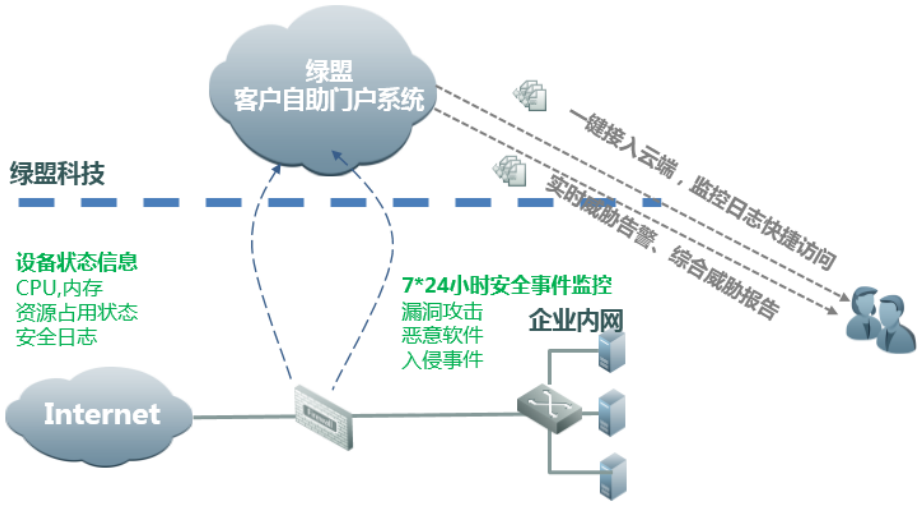

图 4 云端接入

绿盟 NF 防火墙支持一键接入云端功能，用户可以 7*24 小时在线监控安全服务，除基础的设备状态及资源使用情况监控，保障设备健康运行以外，对用户网络中发生的入侵嗅探、漏洞攻击、恶意软件侵入、远程越权操作窃取机密信息等攻击行为第一时间进行云端捕获并记录。

同时，用户亦可通过绿盟云登录云端，对防火墙设备状态、网络实时及历史安全事件、事件趋势及详细日志、报表、甚至全国其他地区的安全形势进行查询和跟踪。

3.4.6 远程运维安全解决方案

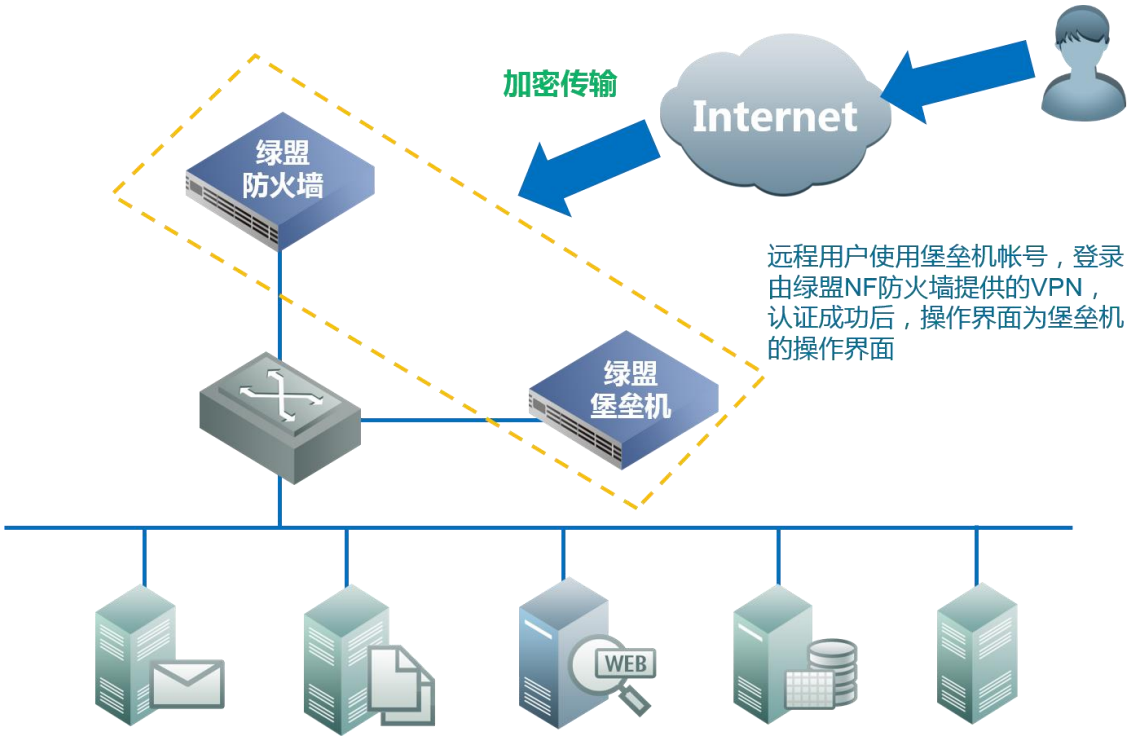

图 5 远程运维安全解决方案

堡垒机一般部署在企业网络内部，而企业内部网与互联网隔离，远程用户无法直接登陆部署在企业内部网的堡垒机设备进行管理。如果将堡垒机映射到互联网上，虽然方便了远程用户，但是将会受到被攻击或入侵的风险，如果未采用任何加密措施，还会有被监听的风险。通过该功能，远程用户使用堡垒机帐号，登录由绿盟 NF 防火墙提供的 VPN，认证成功后，可直接登录堡垒机。

3.4.7 智能补丁解决方案

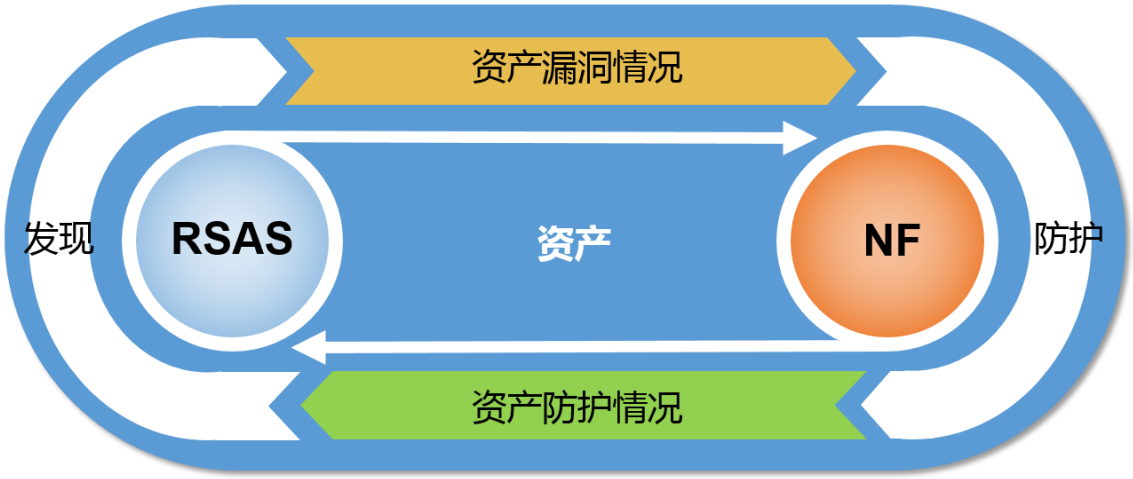

图 6 智能补丁解决方案

NF 与绿盟远程安全评估系统共享漏洞和安全防护信息，互通有无，实现对无防护的高风险漏洞和漏洞防护情况的展示，使用户对网络安全状况一目了然，从而为用户制定更高效网络维护计划，提供参考依据。

3.4.8 终端安全检查解决方案

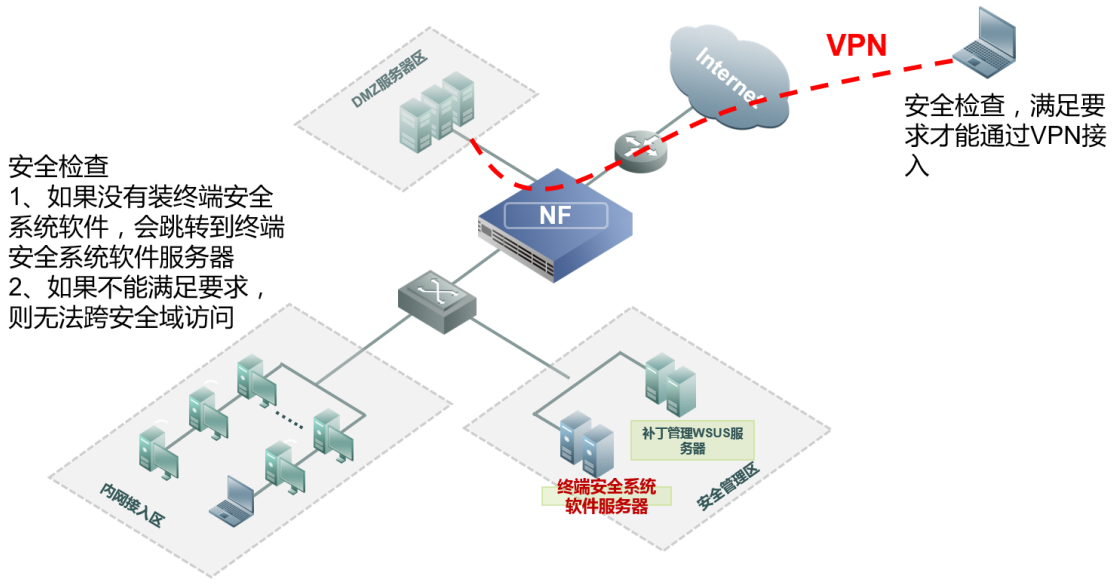

图 7 终端安全检查

通过与终端安全系统软件的配合，全面提升内部资产的安全性，以及远程接入终端的安全性，从而降低病毒带来的危害。

3.4.9 云清洗解决方案

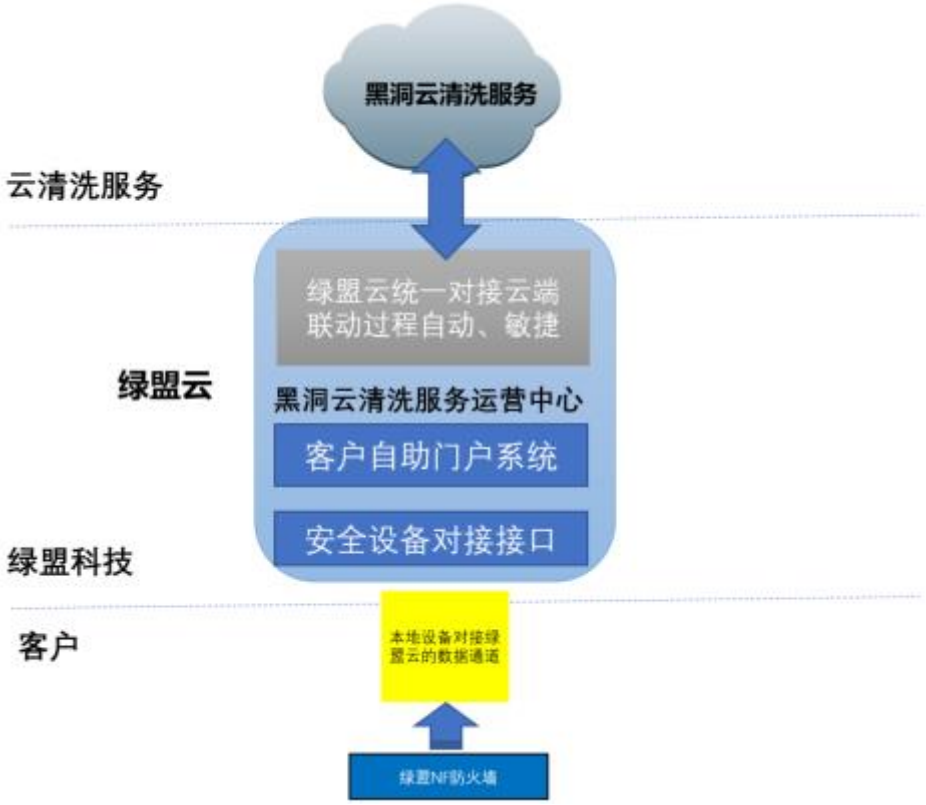

图 8 云清洗解决方案

绿盟 NF 防火墙与云端清洗服务组成本地+云端的组合清洗方案，提升本地流量清洗能力，保护网络环境免遭 DDOS 攻击。

3.4.10 基础防火墙特性

绿盟 NF 防火墙兼容传统防火墙所有功能特性，包括交换/路由、访问控制，A-A/A-S 双机热备、软硬件 Bypass、系统管理、日志报表、会话管理、抗 DDoS 攻击、应用代理、DHCP/DNS 等等。

- **PPPoE**

通过 ADSL 接入 Internet 已经成为越来越多中小企业的选择，而 ADSL 需要拨号以后才能获得 IP 地址。绿盟 NF 防火墙支持 PPPoE 协议，作为 PPPoE Client 端完成与 PPPoE Server 的建连和地址获取，通过设置用户名和口令即可支持 ADSL 接入，获得动态 IP 地址、网关及 DNS 地址，自动完成拨号过程，接入 Internet 网络。解决中小企业上网问题。

- **NAT 地址转换**

支持静态网络地址转换（Static NAT）和动态网络地址转换（Dynamic NAT），实现内网地址转换成公网地址后进行网络通信。支持目的 NAT，将对外网地址的访问映射为对内网地址访问，支持将对一个公网地址的访问映射为内网多个地址，实现内网服务器的负载均衡访问，同时支持目的端口转换。

- **IPv6/IPv4 双协议栈**

支持 IPv6 安全控制策略设置，能针对 IPV6 的目的/源地址、目的/源服务端口、服务、等条件进行安全访问规则的设置；支持 IPv6 静态路由；支持双栈、6to4 及 6in4 隧道实现 IPv6 网络与 IPv4 网络访问等。绿盟 NF 防火墙产品已获 IPv6-Ready 认证。

- **VPN**

绿盟 NF 防火墙根据企业 VPN 常见使用场景，支持多种 VPN 隧道业务，包括 IPSec、GRE、SSL、L2TP VPN 等。用户可通过 GRE、IPSec 或 SSL VPN 隧道实现分公司与总部之间的数据安全传输，通过 SSL 或 L2TP VPN 隧道实现 PC 以及移动客户端与总部之间的数据安全传输；支持多种隧道模式，即可以让用户通过七层 Web 链接进行内网资源的快速访问，又可以让用户通过三层隧道实现内网应用资源的便捷使用。

3.5 产品优势

3.5.1 全面的应用、用户识别能力

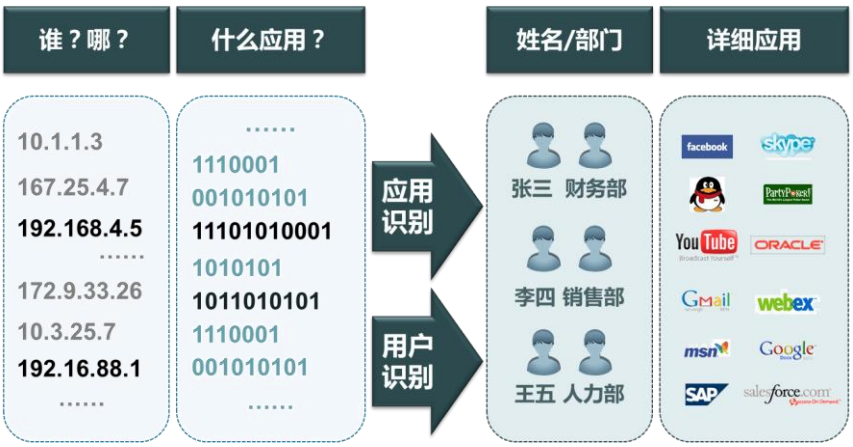

图 9 应用/用户识别

- **应用识别**

应用识别是下一代防火墙技术的关键特征之一，NF 无论在可识别应用数，还是在应用服务上，均具有显著优势。绿盟 NF 防火墙可识别 1200+种应用，并可辅助用户对这些应用进行高效管理和筛查，包括 5 维度分类组织、基于特性查询应用、自定义特殊应用等，让用户明显的感觉到 NF 在应用识别和管理方面的专业性。

同时，绿盟科技拥有一支业界知名的，由资深安全专家组成的安全研究团队，他们长期不懈的跟踪前沿安全市场，保持着对最新网络应用和企业业务需求的提炼和积累，从而保证 NF 的应用识别和安全库时时刻刻保持最高、最精确的应用和威胁识别率。

技术方面，NF 结合智能应用协议识别、高层应用特征匹配、动态流量及行为分析等多种技术，保证了对应用精准识别的技术优势，体现在：

- **智能应用协议识别**

应用协议识别是新一代网络安全产品的核心技术。传统防火墙，通过固定的协议端口映射表来判断流经的网络报文属于何种应用协议。但事实上，应用协议与端口是完全无关的两个概念。同样的端口可能会运行多种不同的应用，而应用也可能在任意一个指定的端口上运行，比如基于智能隧道的 P2P 应用（如各种 P2P 下载工具、IP 电话等），IMS（实时消息系统 如 MSN、Yahoo Pager），网络在线游戏等应用都可以运行在任意一个指定的端口，从而使传统的基于固定端口协议来区分应用的防火墙技术失效。

NF 采用特有的智能应用协议识别技术，通过动态分析网络报文中包含的协议特征，发现其所用协议，然后递交给相应的协议分析引擎进行处理，能够在完全不需要管理员参与的情况下，高速、准确地识别出通过动态端口或者智能隧道运用的真正应用。

- **应用特征匹配**

应用特征匹配主要检测各类已知应用，在全盘了解应用特征后，制作出相应的应用特征库及应用过滤器，对网络中传输的数据包进行高速匹配，确保能够准确、快速地检测到此类应用。

NF 装载权威的应用专家知识库，提供高品质的应用特征介绍和分析，能够精确识别各种复杂应用，包括 P2P 应用、即时通讯、Web2.0 应用等，并通过不断升级应用特征，保证第一时间最新应用的识别能力。

- **动态流量及行为分析**

除了对应用协议进行智能识别及对高层特征进行精确匹配，网络中的应用数据流在其他方面还具有特征、特异化的表现和踪迹，NF 针对应用的这部分特征也进行了跟踪、判断和识别，如基于应用数据包上下行流量分布差异化进行的分析识别，以及基于客户端/服务器访问模式、多协议转换尝试等动态行为进行的分析辨识。使得无论从静态到动态，从固定到智能，NF 在应用识别方面均做到了全面与精确。

- **用户识别**

传统防火墙通过安全域的划分，把物理网络分割成几个部分，每个部分具有不同的安全属性，并且基于 IP 地址范围对各部分进行访问控制。随着无线网络发展、移动设备多元化接入，IP 地址出现随机和无序化，已不能有效代表用户身份，且基于 IP 的身份管理效率低下。

NF 可以从域控服务器实时获取身份账号与 IP 地址的对应关系，从而免打扰的实现身份识别。在未部署域控服务器的环境中，NF 通过 Web 认证页面来完成身份识别，支持管理员指定认证策略，并于策略中指定认证方式（包括本地认证、Radius、AD、LDAP 等），增强了用户接入验证的灵活性、安全性和准确性。

3.5.2 细致的应用层控制手段

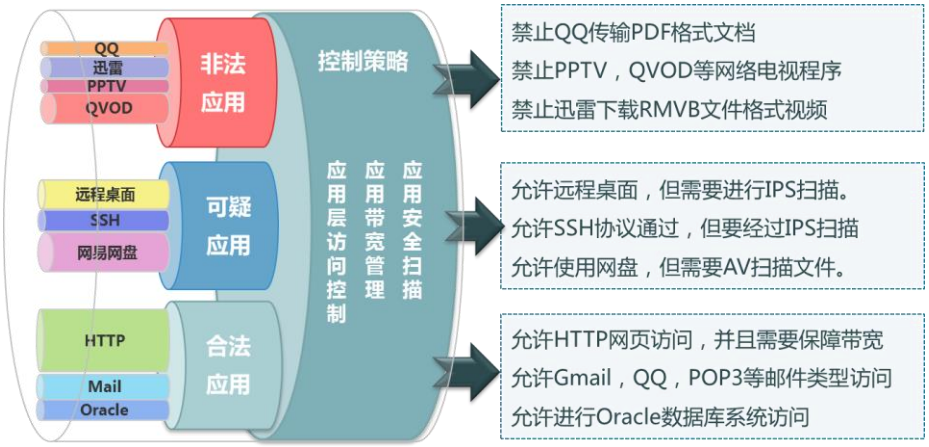

图 10 应用控制

传统防火墙的访问控制或流量管理粒度粗放，只能基于 IP/端口号对数据流量进行一刀切式的禁止或允许。NF 基于卓越的应用和用户识别能力，对数据流量和访问来源进行精细化辨识和分类，使得用户可以轻易从同一个端口协议的数据流量中辨识出任意多种不同的应用，或从无意无序的 IP 地址中辨识出有意义的用户身份信息，从而针对识别出的应用和用户施加细粒度、有区别的访问控制策略、流量管理策略和安全扫描策略，保障了用户最直接、准确、精细的管理愿望和控制诉求。

例如，允许 HTTP 网页访问顺利进行，并且保证高访问带宽，但是不允许同样基于 HTTP 协议的视频流量通过；允许通过 QQ 进行即时通信，但是不允许通过 QQ 传输文件；允许邮件传输，但需要进行防病毒扫描或敏感信息过滤，如发现有病毒入侵或泄密事件马上阻断，等等。

3.5.3 专业的安全防护能力

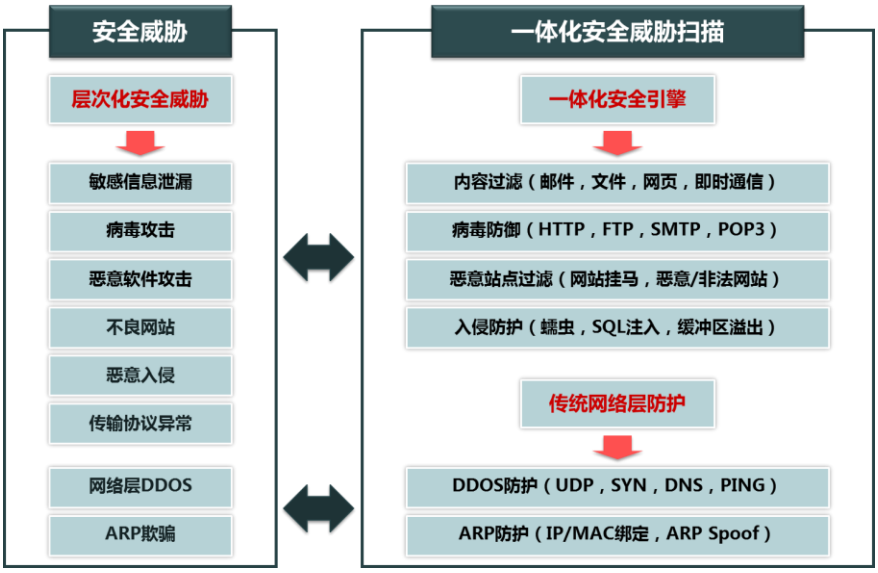

图 11 一体化安全引擎

- **全面的防攻击能力**

在充分考虑到现在及未来安全业务情景的前提下，NF 核心安全功能采用了高度一体化的架构设计方案，将所有的安全特性纳入到一体化的引擎中去。这样的一个明显优势是去除了传统 UTM 设备上各安全模块引擎间彼此独立，层层堆叠，每个引擎重复拆解数据包，彼此间没有任何传承配合，安全性能低下的冗余架构。同时，一体化安全引擎在系统中多核多进程并行执行，对网络海量数据进行实时、并发安全扫描和过滤，从而使产品安全性能有了一个质的飞跃，不仅是传统防火墙无法比拟，也从根本上解决了 UTM 设备安全模块开启，安全性能指数下降的传统顽疾。

- **强大的自身抗攻击能力**

对于安全产品好还有最重要的一点我们容易忽略掉，那就是自身的安全性，如果自身安全性达不到要求的话，反而会给攻击者创造便利的条件。绿盟 NF 防火墙针对每个版本、每个补丁都会进行脆弱性评估，根据绿盟科技《产品脆弱性测试工作规范》，从 7 个方面 44 个小项对产品进行全面评估，最大程度消除产品本身带来的隐患，从而全面提升整个网络的安全性。

除了自测，绿盟 NF 防火墙还获取了，由中国信息安全测评中心针对信息安全产品 EAL 测试的**最高级别**（防火墙类），进一步证明了绿盟 NF 防火墙自身的抗攻击能力。

- **快速响应能力**

针对危害级别高的漏洞，绿盟 NF 防火墙能够在 48 小时之内响应，加强特征库来提高检测及防护的能力，提供补丁来提高自身的抗攻击能力。

3.5.4 卓越的应用层安全处理性能

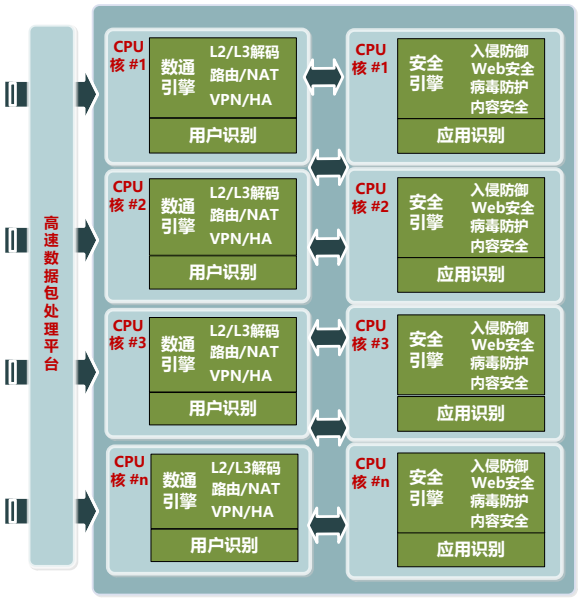

图 12 双引擎多核并发

NF 构筑在新一代 64 位多核并发，高速硬件平台之上，拥有业界独有的数通、安全双引擎设计模式。双引擎多核并发的高速运行在多个 CPU 核心之上，各司其职，不仅保证了基础网络数据包的高速转发，更加确保了应用层安全处理的高性能。

不仅于此，NF 采用的高速数据包处理技术专门针对 I/O 密集型网络设计。它为上层安全服务和底层硬件平台提供了一个高速通信隧道，极大提升了平台安全处理性能和吞吐率，使下一代防火墙设备在安全处理性能上有了一个质的飞跃。

3.5.5 首创的内网资产风险管理

绿盟 NF 防火墙，除了具备国际权威咨询机构 Gartner 所定义的下一代防火墙全部特性，不仅在新一代网络中保障用户的边界网络安全，防范“外敌”入侵，更首创性的提供内网资产风险识别功能，让用户对内网易受攻击资产进行风险提前评估和预警，双向安全，双向保障。即作为事中安全拦截设备，又作为事前风险防范设备，为用户在安全投资不变的情况下提供一举两得的加强安全效应。

3.5.6 先进的云端安全管理模式

业界首创的云端安全管理模式，对传统防火墙及业界其它下一代防火墙产品，在运维服务模式上迈出了崭新的一步。绿盟科技凭借多年对用户安全攻防服务经验的积累，分析沉淀国际及国内市场的用户需求趋势，深刻把脉真正下一代安全的未来走向，通过构造云端安全管理平台，让用户在便捷、高效安全管理上有了全新的体验，极大减免了用户的安全运维投入，从而有能力在应对不断增长变化的威胁攻击中百战不殆，游刃有余。

3.5.7 高级威胁 APT 攻击防御

能有效针对用户遭受的新型 APT 攻击、0day 漏洞攻击进行安全防御，通过接入云端信誉库，获取全球 APT、0day 攻击特征和恶意站点源，使得用户得以第一时间发现、防御 APT 攻击。经过绿盟安全专家认真分析过滤的云端信誉库，以高准确率和识别率助力用户实现未知威胁的坚固防御。另外，NF 还支持与 TAC（沙盒）联动，进一步加强 APT 攻击防护的能力。

3.5.8 完全涵盖传统防火墙功能特性

NF 兼容传统防火墙的所有功能特性，包括路由、交换、访问控制、流量管理、SNAT/DNAT、ISP 负载均衡、DDoS 防护、VPN、HA、日志报表等，使用户原有成熟的安全解决方案可以无更改，平滑的过渡到 NF 下一代防火墙安全解决方案上来。

3.6 典型部署

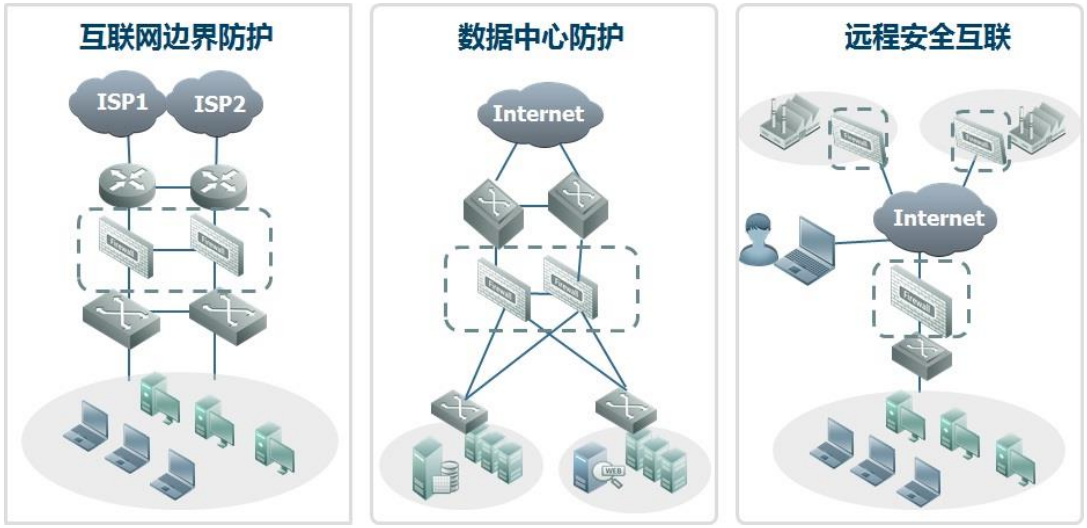

图 13 典型部署

NF 的典型部署方式如图所示，可分为互联网边界防护、数据中心防护、远程安全互联等 3 种主要部署场景。

放置在企业网络边界的 NF，按照安全程度的不同，将网络逻辑隔离成不同的安全区域，常见安全区域包括互联网区，DMZ 区、内网区等。其中，互联网区被视为最危险区，DMZ 区是企业对外提供的应用服务区，被视为次危险区，内网区被视为安全区。

NF 作为此 3 种安全区的边界安全防护设备，在内网和互联网区之间可发挥如下作用：基于应用/用户识别的访问控制、流量控制、上网行为管理、SNAT 转发、ISP 链路负载均衡、安全威胁阻断等；在互联网与 DMZ 区之间可发挥如下作用：访问控制、DNAT、服务器负载均衡、基于应用/户识别的流量控制、安全威胁阻断等。在内网区的用户与服务器群之间可发挥如下作用：访问控制、基于应用和用户识别的流量控制、访问行为记录审计等功能。部署在边界的 NF 可根据用户稳定性需求，提供网络容灾备份方案，保证用户网络安全访问无中断。

对部署有机构庞大、网络环境复杂、安全要求高的数据中心的企业用户而言，可将 NF 作为安全防护方案部署到数据中心进行安全防护。NF 可通过更精确细致的访问控制、安全扫描策略以及更精确的流量监控和管理手段，提供对数据中心服务区的贴身安全防护。

远程安全互联场景用于实现公司各分支机制之间、分支与公司总部之间的 VPN 网络互联，实现业务跨地域共享和交互。NF 支持全面多样的 VPN 接入方式，包括 SSL VPN、IPSec VPN、L2TP VPN 等。实施中可将 NF 设备部署于各分支机构网络出口处，其与总部中心部署的另一台 NF 设备建立 VPN 隧道，或者直接由个人客户通过终端设备与总部中心

NF 建立 VPN 隧道连接。NF 通过对接入客户身份和权限的严格审查、隧道安全加密等方式，提供了对远程访问的接入支持和数据安全保障。

四. 总结

绿盟科技公司深度洞悉下一代网络技术发展方向，深刻理解用户需求趋势，在此基础上隆重推出下一代防火墙产品——绿盟 NF 防火墙。

构建在新一代高速多核硬件平台之上的 NF 产品，高度融合绿盟科技公司在安全、技术方面的一贯优势，体现了专业的应用和用户识别控制能力，深度的应用管理和控制能力，高性能的一体化安全防护能力，以及多方位的联动能力。

结合诸多的产品优势和丰富的产品功能，NF 将为用户带来极大的客户利益，包括安全风险的可视可知，全面一体的安全防护以及稳定高效的无忧部署，是客户在下一代网络及需求发展中的最佳选择。