

NETGEAR® ProSecure™ UTM

如何帮助商用网络达到PCI规定

介绍

支付卡行业数据安全标准 (PCI DSS) 是 2004 年由 PCI 安全标准委员会制定, 用于被委托的公司对信用卡处理, 储存和传输时保护持卡人的资料的统一的安全标准, 简称为“PCI”, 其目的是保护消费者, 防止信用卡欺诈, 窃取数据, 和其他安全威胁。

遵守支付卡行业数据安全标准(PCI DSS)是任何一个从事商家或服务提供商用于传输, 储存, 或处理任何信用卡公司的持卡人有关数据必不可少的——美国运通, Discover Financial Services 公司, JCB 国际, 世界范围内的万事达卡, 和签证等, 每月发现有不遵守 PCI 标准的企业需罚款\$5000 到\$25000 美元不等, 如果在不符合标准的公司发现有数据被破坏, 最终的罚款可高达\$500000 美元。

近年来, 黑客和网络犯罪分子已经成功渗透商业系统, 获得以百万计消费者的信用卡号码和其他敏感的财务信息。2007 年 1 月, 美国的折扣零售商链的 TJ Maxx 的计算机系统至少有 4570 万的信用卡和借记卡被盗, 这些受害的资料包括信用卡号码, 交易信息和客户数据。在 2009 年 1 月, 支付处理中心的核心支付系统公开披露说, 2008 年其处理系统遭到破坏, 破坏的程度可能超过 100 万记录。

遵守PCI的健全安全规定

攻击网络犯罪分子越来越复杂, 使它们能够很容易地绕过防火墙和其他的传统的网络安全的措施。因此, 维护该公司的网络资产对现在需要一个多层次的安全解决方案来防范这些威胁。PCI 安全标准委员会已制定出商户必须遵守的以下六个安全类别:

1. 建立和维护安全网络

规定 1: 安装和维护防火墙配置以保护持卡人的数据

规定 2: 不使用提供商提供的默认值作为系统密码和其它安全参数

2. 保护持卡人数据

规定 3: 保护存储的持卡人数据

规定 4: 对经由开放的公共网络传输的持卡人数据进行加密传输

3. 保护有漏洞的管理程序

规定 5: 使用并定期更新防病毒软件

规定 6: 开发和维护安全系统和应用

4. 采用强大的接入控制措施

规定 7: 按照业务须知限制持卡人的数据接入

规定 8: 为接入计算机的每个人分配一个独特的 ID

规定 9: 限制持卡人数据的物理接入

5. 定期监控和测试网络

规定 10: 跟踪并监控所有网络资源和持卡人数据的接入

规定 11: 定期测试安全系统和流程

6. 维护信息安全策略

规定 12: 维护应对信息安全的策略

PCI 安全标准委员会持续监控这些预防规定, 以确保最高级别的安全性。

遵守PCI的实施和维护

遵守 PCI 不仅仅是避免安全标准委员会的罚款, 这也是公司对消费都的敏感数据安全保护的承诺。坚持采用强有力的安全标准也有助于保护公司的声誉和品牌形象。因数据库的安全漏洞可能会造成无法弥补的损害客户的信任。

同一个企业级的 2 路防火墙, 业界领先的防病毒和防垃圾邮件, 和强大的数据加密技术, NETGEAR®ProSecure™ UTM 设备支持下列要求的 PCI 规定:

PCI DSS 规定	详细内容	NETGEAR 的解决方案
建立和维护安全网络		
规定 1: 安装和维护防火墙配置以保护持卡人的数据		
1.2	设置一个限制持卡人数据环境中不受信任网络 and 任何系统组件之间的防火墙配置。	NETGEAR 的 ProSeucre™ UTM 设置限制了 DMZ 和信任网络的流量,除非另有设置了防火墙配置。
1.2.1	确认进出流量受到持卡人数据环境需要的限制。	NETGEAR 的 ProSecure™ UTM 设备限制在 LAN,WAN 和 DMZ 区域之间限制输入和输出流量的规则, 除非另有规定。
1.2.3	在任何无线网络和持卡人数据环境之间安装外围防火墙, 并且将这些防火墙配置为禁止或控制 (如果业务目的需要这样的流量) 从无线环境流入持卡人数据环境的任何流量。	在 NETGEAR 的 ProSecure™ UTM 设备的 DMZ 端口上连接一个无线接入点使无线流量从信任网络中分离 (持卡人环境)。
1.3	禁止在持卡人数据环境中的 Internet 和系统组件之间的直接公共访问。	NETGEAR 的 ProSecure™ UTM 提供了经验证的防火墙, VPN, IPS 和与企业级内容安全过滤器, 以防止未经授权访问系统组件在公司内部网络。
1.3.1	实施 DMZ 以只限制那些持卡人数据环境需要的协议的进出流量。	NETGEAR 的 ProSeucre™ UTM 设置限制了 DMZ 和信任网络的流量,除非另有设置了防火墙配置。

1.3.2	限制进入 DMZ 内部 IP 地址的 Internet 流量。	NETGEAR 的 ProSecure™ UTM 能够配置限制进入 DMZ 内部 IP 地址的 Internet 流量。
1.3.3	不允许 Internet 和持卡人数据环境之间进出流量的任何直接路由。	NETGEAR 的 ProSecure™ UTM 在局域网(持卡人数据环境)和 WAN(互联网)区域中设置了限制输入和输出流量的防火墙规则。
1.3.4	不允许从 Internet 至 DMZ 的内部地址通过。	NETGEAR 的 ProSecure™ UTM 不允许从 Internet 至 DMZ 的内部地址通过。
1.3.5	限制从持卡人数据环境至 Internet (例如传出流量)的输出流量只能访问 DMZ 内部的 IP 地址。	NETGEAR 的 ProSecure™ UTM 能够设置只允许从局域网的输出流量只能访问 DMZ 内部的 IP 地址。
1.3.6	实施状态检测, 也即动态包过滤。(也就是只有“建立”的连接才允许进入网络。)	NETGEAR 的 ProSecure™ UTM 平台是状态数据包检测的。
1.3.7	在内部网络区域(从 DMZ 隔离开来的)中使用数据库。	NETGEAR 的 ProSecure™ UTM 设置限制了流量不允许从 DMZ 区域进入信任网络, 除非另外设置防火墙配置。数据库放在局域网区域, 从而与 DMZ 区域隔离。
1.3.8	实施 IP 伪装以防止内部地址被转译和发布到 Internet 上, 使用 RFC 1918 地址空间。使用网络地址转译 (NAT) 技术, 例如端口地址转译 (PAT)。	网络地址转换 (NAT)和端口地址转换 (PAT) 是 NETGEAR 的 ProSecure™ UTM 的标准特性。
规定 2: 不使用提供商提供的默认值作为系统密码和其它安全参数		
2.1	在网络上安装系统以前, 务必更改供应商提供的默认项, 例如包括密码、简单网络管理协议 (SNMP) 机构字串, 并删除不并要的账户。	NETGEAR 的 ProSecure™ UTM 包含一个简单的 10 步安装向导, 能在把 UTM 设备安装到网络之前管理员能够修改管理员的默认密码。
2.2.2	禁用所有不必要和不安全的服务和协议 (不直接需要用来执行设备特定功能的服务和协议)。	NETGEAR 的 ProSecure™ UTM 支持提供详细的颗粒控制某些协议, 端口及内容的防火墙和内容过滤策略通过 UTM 设备。此外, NETGEAR 的专利串流扫描技术, 以及企业级的防病毒, 反间谍软件和入侵检测技术, 并利用被策略允许的服务和协议保证您的网络安全。
2.2.3	配置系统安全参数以防止滥用。	NETGEAR 的 ProSecure™ UTM 支持提供详细的颗粒控制某些协议, 端口及内容的防火墙和内容过滤策略通过 UTM 设备。

2.3	对所有非控制台管理访问进行加密。对于基于 Web 的管理和其他非控制台管理访问使用诸如 SSH、VPN 或 SSL/TLS 等技术。	NETGEAR 的 ProSecure™ UTM 支持基于加密的 HTTPS 的 Web 管理。
保护持卡人数据		
规定 4: 对经由开放的公共网络传输的持卡人数据进行加密传输		
4.1	使用强效加密法和安全协议（例如 SSL/TLS 或 IPSEC）以保护在开放型公共网络中传输敏感持卡人数据的安全。 PCI DSS 范围内的开放型公共网络示例如： * Internet, * 无线技术, * 移动通信的全球系统 (GSM) 和 * 通用无线分组业务 (GPRS)。	NETGEAR 的 ProSecure™ UTM 支持在公共网络上建立数据传输安全 SSL 和 IPsec VPN 连接。
保护有漏洞的管理程序		
规定 5: 开发和维护安全系统和应用		
5.1	在所有经常受恶意软件影响的系统上部署杀毒软件（特别是个人电脑和服务器上）。	NETGEAR 的 ProSecure™ UTM 配置了同类产品最佳的反病毒/反恶意软件的扫描引擎，以补充在个人电脑上反病毒软件的不足。
5.1.1	确保所有杀毒程序都能够监测、删除并防止所有已知类型的恶意软件的攻击。	NETGEAR 的 ProSecure™ UTM 采用了全面的，最佳的安全解决方案，包括通过主动防御、“零时差”检测和专利扫描技术来主动防止超过 1300 万各种类型的病毒，蠕虫，间谍软件，特洛伊木马、rootkits、键盘记录器和其它基于互联网的威胁进入商业网络。
5.2	确保所有杀毒机制都是最新并且在运行，而且能够生成审核日志。	NETGEAR 的 ProSecure™ UTM 特征数据库是 24 小时自动更新的，从而满足这种要求，UTM 设备上的恶意软件检测将生成日志。
规定 6: 开发和维护安全系统和应用		
6.1	确保所有系统组件和软件都安装了最新的供应商提供的安全补丁。在发布的一个月以内安装关键的安全补丁。	NETGEAR 的 ProSecure™ UTM 自动检测和下载最新的固件版本到设备上，管理员能够从 Web 管理界面上直接安装它。
6.2	建立一个流程来识别新发现的安全漏洞（例如，订阅 Internet 免费的警告服务）。根据 PCI DSS 要求 2.2 更新配置标准，以解决新的漏洞问题。	NETGEAR 在线提供全面的最新的威胁和攻击信息资源，24 小时不断地更新，让您不断地了解新出现的威胁。

6.6	<p>对于面向公众的 Web 应用程序，经常解决新的威胁和漏洞，并确保保护这些应用程序不受到以下任一方法的攻击：</p> <ul style="list-style-type: none"> * 通过手动或自动应用程序漏洞安全评估工具或方法检查面向公众的 Web 应用程序，至少每年一次并在所有更改后进行检查。 * 在面向公众的 Web 应用程序前端安装 Web 应用程序防火墙 	<p>NETGEAR 的 ProSecure™ UTM 的 IPS,Web 反恶意软件扫描, URL 过滤功能可以同时使用防火墙策略, 以保障公众的 Web -应用/服务器。</p>
采用强大的接入控制措施		
规定 8: 为接入计算机的每个人分配一个独特的 ID		
8.2	<p>除分配唯一的 ID 之外, 至少采用以下一种方法验证所有用户的身份:</p> <ul style="list-style-type: none"> * 密码或口令 * 双因素验证 (例如令牌设备、智能卡、生物测定技术或公共密钥) 	<p>NETGEAR 的 ProSecure™ 的 UTM 支持双因素认证。</p>
8.3	<p>员工、管理员和第三方采用双因素验证以远程访问 (从网络外进行网络级的访问) 网络。使用远程拨入用户认证服务 (RADIUS)、带有令牌的终端访问控制器访问控制系统 (TACACS) 或带有个人证书的 VPN (基于 SSL/TLS 或 IPSEC) 等技术。</p>	<p>NETGEAR ProSecure™ 的 UTM 支持双因素认证, 包括 WIKID, RADIUS, LDAP 和私有的 VPN 证书。</p>
8.4	<p>在所有系统组件上进行传输和存储操作时, 采用强效加密术 (参照《PCI DSS 术语与缩略语》中的定义) 使所有密码不可读。</p>	<p>NETGEAR 的 ProSecure™ 的 UTM 基于 Web 的管理界面的所有的数据和密码均是采用 SSL 加密, UTM 上的所有文件系统均是加密的。</p>
定期监控和测试网络		
规定 10: 跟踪并监控所有网络资源和持卡人数据的接入		
10.1	<p>为每个人用户建立一个可连接访问所有系统组件 (尤其是具有根权限等管理权限的访问) 的流程。</p>	<p>每个用户在 UTM 的基于 Web 管理接口的操作均被记录。</p>
10.2.1	<p>对持卡人数据的所有个人访问</p>	<p>每个用户在 UTM 的基于 Web 管理接口的操作均被记录。</p>
10.2.3	<p>访问所有核查记录</p>	
10.2.4	<p>无效的逻辑访问尝试</p>	
10.2.5	<p>使用身份认证和验证机制</p>	
10.2.6	<p>初始化核查日志</p>	
10.2.7	<p>创建和删除系统级对象</p>	<p>每个用户在 UTM 的基于 Web 管理接口的操作均被记录。</p>
10.3	<p>针对每个事件的所有系统组件至少记录以下核查记录条目:</p>	
10.3.1	<p>用户身份认证</p>	
10.3.2	<p>事件类型</p>	
10.3.3	<p>日期和时间</p>	

10.3.4	成功指示或失败指示	
10.3.5	事件起源	
10.3.6	受损数据、系统组件或资源的特征或名称	
10.4	同步所有重要的系统时钟和时间。	NETGEAR 的 ProSecure™ UTM 支持 NTP 同步。
10.6	每天至少检查一次所有系统组件的日志。日志检查必须包括检查执行入侵检测系统(IDS) 和验证、授权等安全功能的服务器以及记账协议 (AAA) 服务器 (例如 RADIUS)。	NETGEAR 的 ProSecure™ UTM 保持以下记录: 流量, 恶意软件, 垃圾邮件, 内容过滤, 电子邮件过滤器, 系统, 服务, IPS, 端口扫描, 即时消息, P2P, 防火墙, IPSec VPN, SSL VPN
规定 11: 定期测试安全系统和流程		
11.4	使用入侵检测系统或入侵防御系统, 以监控持卡人数据环境中的所有流量并在发现可疑威胁时提醒员工。随时更新所有入侵检测引擎和入侵防御引擎。	NETGEAR 的 ProSecure™ UTM 的网络入侵预防和检测系统利用规则驱动的语言, 结合病毒特征库的优点, 协议和基于异常检测方法, 防止黑客穿透网络边界。

PCI规定以外的

遵守的 PCI 规定是确保公司网络的一个重要开端。但是, 必须指出的是, 除了遵守 PCI 规定外, 还有支付卡行业数据安全标准 (PCI DSS) 未覆盖的其它重要的网络情况。公司的关键业务信息和其他网络资产的风险依然存在, 包括黑客, 恶意程序, 和其他基于互联网的威胁。安全专家每年获得大约 1500 万独特的恶意软件样本, 新的威胁和攻击类型载体不断涌现。为了有效地打击这些不断新出现的威胁, IT 经理必须制定全面的保安措施, 其中包括一个强大的防火墙和全套互联网安全解决方案。

正如上表可以看出, NETGEAR 的 ProSecure™ UTM 是帮助您实现和维持 PCI 规定的一个全面的解决方案, 此外, ProSecure™ UTM 还帮助您从一系列的基于互联网威胁中保护您的网络。

NETGEAR® ProSecure™安全网关设备解决方案

ProSecure™ STM 和 UTM 平台采用了一个经验证的防火墙，支持 SSL 和 IPsec VPN, IPS 和企业级内容过滤器，以防止未经授权访问在公司内部网络的系统组件。

ProSecure™ STM 和 UTM 平台采用了专利的串流扫描技术，能够在数据流进入网络的时候马上进行扫描。NETGEAR STM 和 UTM 使用单一的平台即可实现对垃圾邮件、恶意软件、安全破坏或不必要的应用程序进行扫描，通过串流扫描技术，能够实时地扫描大量的数据。这使得局域网中的用户可以接收到安全的 Email 和 Web 内容但却没有任何延时。

ProSecure™ STM 和 UTM 平台提供了简单的安装和维护。STM 是可以在在现有网络架构无缝集成的一个透明网关，而 UTM 是一个集所有功能于一身的安全解决方案，能取代现有的防火墙或路由器，任一个解决方案都为您的企业提供所有的安全软件，而没有每用户许可的要求。