QQ for check Point

Continuous Vulnerability Assessment and Monitoring for Check Point Firewalls

Protect Your Corporate Data Through Proactive Firewall Monitoring

As the gatekeeper between corporate data assets and the external world, firewalls are the critical line of defense against network intruders, whose increasingly sophisticated and indiscriminate break-ins render every Internet-connected network a target. And vulnerabilities can be inadvertently introduced by administrators when they execute firewall policy changes, causing the network to become vulnerable to intrusions from hackers, worms or trojans. The only solution is to proactively conduct network vulnerability surveillance as part of the
firewall policy update process.

Eliminate Vulnerabilities With the First OPSEC-Certified Security

Assessment Service for VPN-1/FireWall-1

QQ for Check Point is the first Web-based Managed Vulnerability Assessment service integrated with the OPSEC Framework that continuously audits Check Point VPN-1/FireWall-1 in real time.

The service monitors the Check Point Enterprise Management Console or Provider-1 to determine when policy
changes occur to enforcement points. When a firewall policy change is detected, the service identifies
which hosts/IP ranges the firewall protects, analyzes them, and produces near-instant feedback on how the
newly-deployed policy looks to the outside world. Email notification is sent to the firewall

Check Point 专用 QQ

针对 Check Point 防火墙实施连续的漏洞评估和监视

通过积极防火墙监测方法保护您公司的数据

作为公司数据资源与外界的一道关卡，防火墙是防御网络攻击者的关键部位。网络攻击者越来越高级，并且不加选择的攻击使得每一个与互联网连接的网络成为其攻击对象。当网络管理员执行防火墙策略变动时网络漏洞会在毫不注意的情况下引入，于是，整个网络在黑客、蠕虫和木马的攻击下就表现得分外脆弱。解决这种问题的唯一方案是把网络漏洞监视作为防火墙升级的步骤之一。

使用首家通过 OPSEC（安全性开放式平台）认可的针对 VPN（虚拟专用网）－1 和 FireWall-1 （防火墙）－1 的网络安全评估服务来消除网络中的安全隐患

Check Point 专用 QQ 系统是第一个基于 Web 的漏洞管理评估服务，它已经被集成于 OPSEC（安全性开放式平台）框架中。该框架可以实时对 Check Point VPN-1/FireWall-1 进行检查。该项服务通过监视 Check Point 企业控制管理平台或 Provider－1 来判定策略变动何时出现在实施点。当防火墙策略变动被监测到时，该项服务会查找被动放火前所保护的所有主机和 IP 地址范围，对其进行分析，从而以接近即时的速度给出反馈，描述新近部署的策略从外部的角度观察是怎样一种状态。邮件通知信息被发送到防火墙管理员处，在邮件里还附有指向完整图文形式 HTML 报告链接。同时，通过 Check Point 日志查看器，用户还可以查看带有评估总结的日志条目
。

administrator with a
link to a complete HTML graphical report, and log entries with an assessment summary can be viewed via the
Check Point Log Viewer.

Track Changes Across Your Entire Network and Perform Trend Analysis

The easiest to administer Managed Vulnerability Assessment platform, QQ for Check Point delivers a
new level of control over the impact of firewall modifications:

■ Monitors policy changes automatically via OPSEC interfaces and initiates vulnerability assessments of the
affected enforcement points.

■ Validates adherence of new policies to baseline security procedures and pinpoints network vulnerabilities,
delivering a clear understanding of risk exposure after each firewall policy change.

■ Presents summary results in an easy-to-read HTML format with email notification to one or more firewall
administrators. Via the Check Point Log Viewer, summary entries can be reviewed for each assessment as well,
so there are no new administrative interfaces to learn.

■ Compiles an ongoing record of network security history to produce trend analysis.

■ References the most comprehensive, constantly updated KnowledgeBase containing thousands of vulnerability
signatures covering over 300 applications on more than 20 different platforms.

1. Monitor

The QQ Firewall Plug-In is a Managed Vulnerability Assessment agent that operates alongside the Check Point
Enterprise Management Console or Provider-1 in a customer‘s network. Any firewall policy change made in the Policy
Editor and installed upon an enforcement

在整个网络范围内跟踪变化，并展开趋势分析

作为管理漏洞评估管理平台最简便的工具，Check Point 专用 QQ 系统可以提供新层次的控制能力，用以控制对防火墙的变动对网络所成的影响：

■ 通过 OPSEC（安全性开放式平台）接口自动监视策略变动，对受影响的实施点启动漏洞评估。

■ 检查新的策略是否与安全程序的最低要求相符，查明网络漏洞，并在每次防火墙策略变动时发送一份报告，明确指明变动后的暴露风险。

■ 以易于阅读的 HTML 格式展现评估结果，并以邮件通知的形式发送到一个或多个防火墙管理员手中。通过 Check Point 日志查看器，用户也可以查看每次评估的总结条目，因此，不必学习新的管理界面。

■ 实时编辑网络安全历史纪录，从而生成趋势分析。

■ 可供参考的信息库（KnowledgeBase）内容全面，含盖了包括 200 多个程序和 20 多个不同平台在内的数以千计的漏洞特征。

Check Point 专用 QQ 服务可以提供监视、分析、报告，和修补等服务。该服务以规定的时间间隔检查 Check Point 企业管理平台或 Provider-1，以发现策略变动，并判断变动影响到的实施点，从而通知 QQ 执行网络安全评估。QQ 将当前策略中每一个 IP 地址的评估结果与先前的结果进行对比，然后产生带有漏洞解决方案信息的微分报告。

1． 监视

QQ 防火墙插件是一种漏洞评估管理代理，它可以与客户网络中的 Check Point

point automatically triggers a QQ audit. Running on Microsoft
Windows NT and 2000 systems, the QQ Firewall Plug-In is a Windows Service that starts automatically at boot
time. If the management console is installed on a Solaris or Linux system, then the agent will reside nearby on a
Windows-based system.

2. Analyze

The QQ Firewall Policy Analysis Process is initiated remotely by the QQ Firewall Plug-In to evaluate
the security implications of a firewall policy change to one or more enforcement points. When the Plug-In detects an
installed policy change, it communicates with QQ Guard and the Firewall Policy Analysis Process. QQ
launches a vulnerability assessment for the updated enforcement points and their protected hosts, and the Firewall
Policy Analysis Process evaluates the results, comparing them to previous results for trend analysis. With its recursive
information gathering and testing processes, QQ Inference-Based Engine is faster and more accurate than any other
assessment test method.

3. Report

The QQTML-based differential report provides complete scan results in an easy-to-read format. When a
QQ assessment is complete, VPN-1/FireWall-1 administrators are notified via email with summary information
and a link to the full HTML report. Reports are designed to produce trend analysis for each scanned IP address by vulnerability status, severity, and category. The series of graphics, selected indicators, and vulnerability statuses highlight the evolution of network security through time, indicating if the network is “more secure” or “less secure.”

企业管理平台或 Provider－1 并行。在策略编辑器制定或者在实施点安装的任何一项改动都会触发一次QQ审查。在Windows NT 和 2000 系统环境下，QQ 防火墙插件是以 Windows Service 的形式安装的，每次系统启动都会自动激活。如果管理平台被安装于 Solaris 或 Linux 系统，代理还是需要安装在基于 Windows 的系统中。

2． 分析

QQ 防火墙策略分析进程是以 QQ 防火墙插件远程调用的方式启动的。它可以评估一项防火墙策略变动对一个或多个实施点在安全方面可能会产成的影响。当插件监测到一项已经安装的策略变动时，它会与 QQ 和防火墙策略分析进程取得联系。QQ 会生成一份有关被升级实施点及其保护主机的漏洞评估，然后，防火墙策略分析进程会评估结果，并将其与先前的结果比较，从而形成趋势分析。利用其递归式的信息搜集和测试进程，与其它任何评估测试方法相比，QQ 基于推论的引擎都显得既快速又准确。

3． 报告

基于 HTML，QQ 的微分报告以一种易于阅读的格式向用户提供完整的扫描报告。QQ 评估完成时，汇总信息会以电子邮件的形式发送给 VPN-1/FireWall-1 的管理员，该邮件同时还包含一个指向完整 HTML 报告的链接。报告被设计成可以同时提供每一个被扫 IP 地址的趋势分析，分析内容包括漏洞状态、严重程度和类别。一系列的图表，指标，和漏洞状态突出了网络安全状况随时间的演变状况，从而显示网络是变得更安全，还是更不安全了。

4. Remedy

The QQ service recommends verified countermeasures, patches, and workarounds for each detected vulnerability. Security experts in QQ' Vulnerability Laboratory test and validate remedies and provide time-to-fix estimates for vulnerabilities that can be resolved. QQ customers can verify and document corrected vulnerabilities upon the next QQ scan. For customers that prefer to outsource vulnerability resolution or require supplemental resources, QQ has a worldwide network of partners qualified to provide professional services on-site.

4. 补救措施

QQ 服务为每一例监测到的安全漏洞建议经认可的对策、补丁，和变通方法。位于 QQ 网络安全漏洞实验室的专家会测试并认可补救措施，并为那些可以解决的网络安全漏洞问题提供即时的修复评估。QQ 的客户可以在进行下一次 QQ 扫描时检验并记录已经修复的漏洞。对那些倾向于来自外界的漏洞解决方案或要求补充资源的客户，QQ 遍布全球的合作伙伴可以提供现场的专业服务。