如何使用硬件防火墙 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/267/2021_2022__E5_A6_82_E4_BD_95_E4_BD_BF_E7_c101_267781.htm 硬件防火墙是指把防火墙程序做到芯片里面，由硬件执行这些功能，能减少CPU的负担，使路由更稳定。 硬件防火墙是保障内部网络安全的一道重要屏障。它的安全和稳定，直接关系到整个内部网络的安全。因此，日常例行的检查对于保证硬件防火墙的安全是非常重要的。 系统中存在的很多隐患和故障在暴发前都会出现这样或那样的苗头，例行检查的任务就是要发现这些安全隐患，并尽可能将问题定位，方便问题的解决。 一般来说，硬件防火墙的例行检查主要针对以下内容： 1.硬件防火墙的配置文件 不管你在安装硬件防火墙的时候考虑得有多么的全面和严密，一旦硬件防火墙投入到实际使用环境中，情况却随时都在发生改变。硬件防火墙的规则总会不断地变化和调整着，配置参数也会时常有所改变。作为网络安全管理人员，最好能够编写一套修改防火墙配置和规则的安全策略，并严格实施。所涉及的硬件防火墙配置，最好能详细到类似哪些流量被允许，哪些服务要用到代理这样的细节。在安全策略中，要写明修改硬件防火墙配置的步骤，如哪些授权需要修改、谁能进行这样的修改、什么时候才能进行修改、如何记录这些修改等。安全策略还应该写明责任的划分，如某人具体做修改，另一人负责记录，第三个人来检查和测试修改后的设置是否正确。详尽的安全策略应该保证硬件防火墙配置的修改工作程序化，并能尽量避免因修改配置所造成的错误和安全漏洞。 2.硬件防火墙的磁盘使用情况 如果

在硬件防火墙上保留日志记录，那么检查硬件防火墙的磁盘使用情况是一件很重要的事情。如果不保留日志记录，那么检查硬件防火墙的磁盘使用情况就变得更加重要了。保留日志记录的情况下，磁盘占用量的异常增长很可能表明日志清除过程存在问题，这种情况相对来说还好处理一些。在不保留日志的情况下，如果磁盘占用量异常增长，则说明硬件防火墙有可能是被人安装了Rootkit工具，已经被人攻破。 因此，网络安全管理人员首先需要了解在正常情况下，防火墙的磁盘占用情况，并以此为依据，设定一个检查基线。硬件防火墙的磁盘占用量一旦超过这个基线，就意味着系统遇到了安全或其他方面的问题，需要进一步的检查。 3.硬件防火墙的CPU负载 和磁盘使用情况类似，CPU负载也是判断硬件防火墙系统运行是否正常的一个重要指标。作为安全管理人员，必须了解硬件防火墙系统CPU负载的正常值是多少，过低的负载值不一定表示一切正常，但出现过高的负载值则说明防火墙系统肯定出现问题了。过高的CPU负载很可能是硬件防火墙遭到DoS攻击或外部网络连接断开等问题造成的。 4.硬件防火墙系统的精灵程序 每台防火墙在正常运行的情况下，都有一组精灵程序（Daemon），比如名字服务程序、系统日志程序、网络分发程序或认证程序等。在例行检查中必须检查这些程序是不是都在运行，如果发现某些精灵程序没有运行，则需要进一步检查是什么原因导致这些精灵程序不运行，还有哪些精灵程序还在运行中。 5.系统文件 关键的系统文件的改变不外乎三种情况：管理人员有目的、有计划地进行的修改，比如计划中的系统升级所造成的修改；管理人员偶尔对系统文件进行的修改；攻击者对文件的修改。 经常性地

检查系统文件，并查对系统文件修改记录，可及时发现防火墙所遭到的攻击。此外，还应该强调一下，最好在硬件防火墙配置策略的修改中，包含对系统文件修改的记录。 6.异常日志 硬件防火墙日志记录了所有允许或拒绝的通信的信息，是主要的硬件防火墙运行状况的信息来源。由于该日志的数据量庞大，所以，检查异常日志通常应该是一个自动进行的过程。当然，什么样的事件是异常事件，得由管理员来确定，只有管理员定义了异常事件并进行记录，硬件防火墙才会保留相应的日志备查。 上述6个方面的例行检查也许并不能立刻检查到硬件防火墙可能遇到的所有问题和隐患，但持之以恒地检查对硬件防火墙稳定可靠地运行是非常重要的。如果有必要，管理员还可以用数据包扫描程序来确认硬件防火墙配置的正确与否，甚至可以更进一步地采用漏洞扫描程序来进行模拟攻击，以考核硬件防火墙的能力。 硬件防火墙是整合在主板里的，只能通过升级相应主板BIOS来进行升级