新软周报
http://www.nusoft.com.tw
Internet Security Fighter
2008/5/26-2008/6/8 第68期

多功能UTM / MS系列报导

技术浅谈与应用 - 负载均衡各项模式解说

时代的渐渐进步下，各行各业对于网络的依赖度也越来越高，而如此依赖网络的情况下，最怕遇到的不外乎就是断线的问题。新软负载均衡器系列产品支持整合多条广域网络线路，并以智能方式安排网络流量路径或避开中断的线路，善用所有可用的广域网络联机，来发挥负载均衡，维持网络平稳，达到多线路及流量整合的管理需求。

新软负载均衡器系列产品提供了一般常见的 Auto、Round-Robin、By Traffic、By Session、By Packet 负载均衡模式之外，同时也提供了 By Source IP 与 By Destination IP 两种负载均衡模式，来因应各种网络环境的需求。

Auto（自动分配模式）

使用"自动分配"负载均衡模式时，系统将会自行计算现阶段网络上传、下载带宽的使用情形，包括了流量、封包数、联机数…等，实时调整对外的网络联机使用。此方式让大多使用者可以更方便的利用新软公司产品来完成最优化的网络负载均衡。选择此模式，则可省去不少设定上的时间。

Round－Robin（循环分配模式）

此模式将会把 Session 循环分配至各 WAN 埠，来安排使用者对外联机的路径，可有效的将流量分散至各个 WAN 埠，减少流量及带宽问题。而使用者若中途断线，再次联机，系统仍然会依循环分配的方式来建立使用者的联机。

By Traffic（依照流量分配模式）

由管理人员依照已知的各线路带宽大小，来决定各 WAN 埠的流量比例。此模式系统则会依照各线路所累积的流量高低，来分配各线路至管理人员所设定的 WAN 埠。管理人员可藉此来更进一步的控管网络的资源分配。

By Session（依照联机数分配模式）

由管理人员设定各 WAN 埠所容许的联机数比例，系统将会依照所设定的内容，将所有的联机数按设定上的比例，分配给各 WAN 埠来提供联机。

By Packet（依照封包数分配模式）

流量的大小并不等于封包数量的多寡，此方式是由管理人员来设定封包数的比例，系统则会依照设定上的比例自动调整联机时所使用的 WAN 埠。

由于“单一性 IP 判断”的机制方式，目前仍然广泛的被金融企业、公司服务器所为使用，相对的对于利用“多个 WAN 埠路由设备”联机上网的使用者来说，却会因为设备上的“负载均衡功能”，让使用者有机会同时使用到两条以上的 WAN 联机到目的服务器，而导致目的服务器判断该使用者联机异常而终止联机服务提供。面对此问题，一般企业管理者可使用“策略路由”指定联机路径来解决，但面对网吧、学生宿舍这类大量且复杂的使用者，要一一的使用“策略路由”来指定联机路径，实在是难上加难。

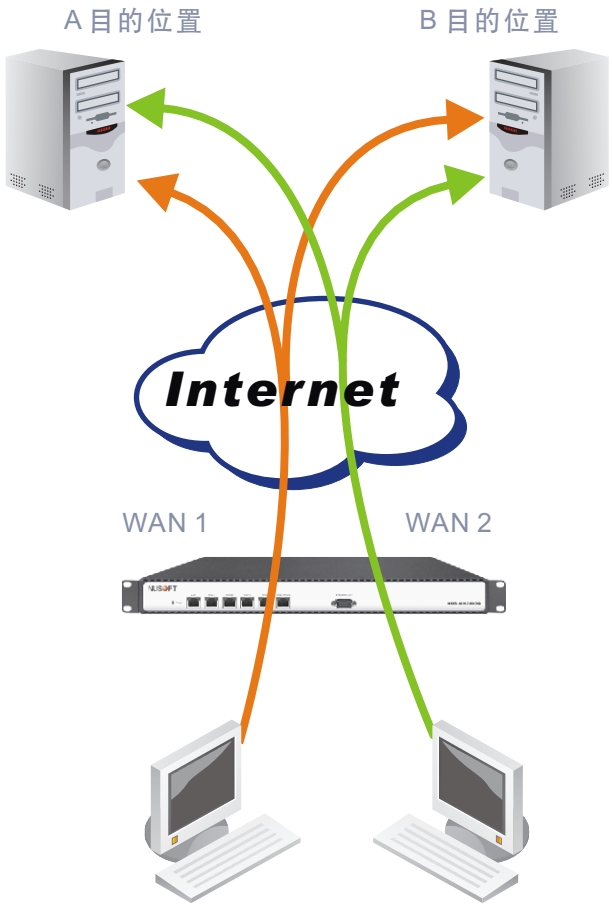
此时则可使用 By Source IP 与 By Destination IP 两种负载均衡模式，来解决这种困境。

By Source IP（在线游戏模式）

此模式是根据来源地址（使用者 IP），将使用者每次的联机由系统来决定透过哪一个 WAN 埠连接因特网。同一个使用者对外的联机不论目的地址为何，当下皆固定以同一线路发送。直到使用者对该次的所有联机结束，在下一次进行联机时，系统会对使用者重新分配新的线路。

由于 By Source IP 模式会强制将使用者所有的联机动作，全部皆由已指定的 WAN 埠做传输，在使用人数少的情况下，可能会造成别条线路的带宽浪费。

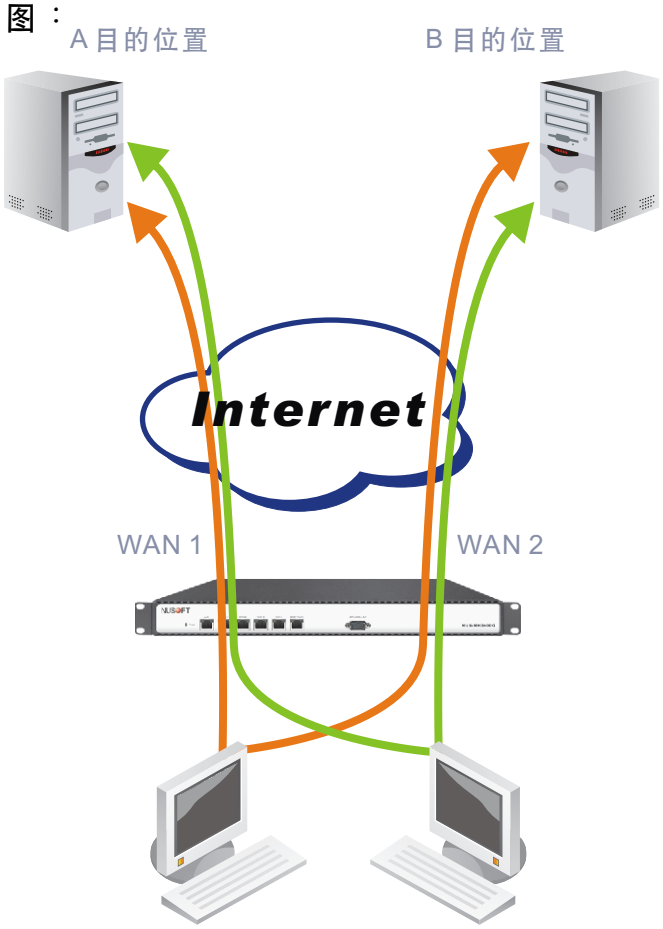
By Source IP 示意图：



By Destination IP（依照目的位置分配模式）

由于负载均衡机制的关系，每次对外联机所走的线路不尽相同，利用此模式情况下，系统会将**第一次**对外联机的**目的位置**锁定，藉由此负载均衡模式，把当下联机至同一目的地址的所有使用者，由相同 WAN 埠线路做发送、连结。直到所有使用者对该目的位置的联机结束后，系统会在下一次的联机重新锁定。

By Destination IP 示意图：



负载均衡模式	适用环境
自动分配模式	无特别情况下，一般企业环境建议使用
循环分配模式	所有外线带宽皆相同之环境较为适用
依照流量分配模式	企业需要自行规划线路分配方式
依照联机数分配模式	
依照封包数分配模式	
在线游戏模式	网吧、学生宿舍、小区网络…等，使用人数多且复杂不易一一管理之环境建议使用
依照目的位置分配模式	

各负载均衡模式适用之环境对照表

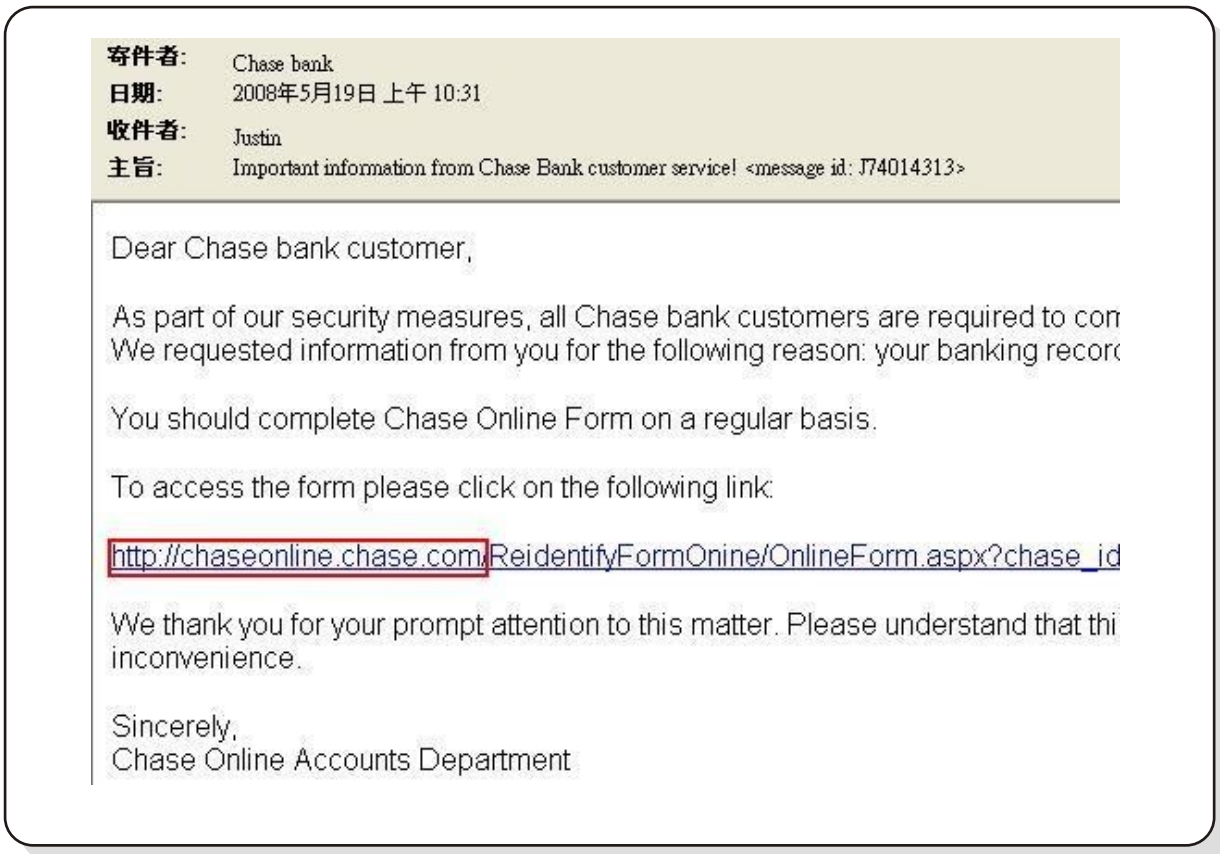
文 陈殿鸿 kim@nusoft.com.tw

市场营销报导 - 拒绝内含恶意网页及网络钓鱼的邮件

近几年最盛行的资安威胁莫过于恶意网页与网络钓鱼的陷阱，信息罪犯利用大众普及的讯息传输工具－邮件，来做为散播的途径，以诱人耸动的标题或伪造官方网站的通知信，企图让收件者开启信件掉入陷阱。

这些内含恶意网页连结的病毒邮件通常利用「iFrame」隐藏恶意程序的手法，让收件者在开启信件的同时，自动连结到恶意的网页，但从信件内文中却察觉不出有任何异常。黑客便利用这种方式以耸动的信件标题，引诱收件者开启信件，趁机植入木马程序于收信者的计算机中。根据调查发现，恶意网页仍是今年最盛行的资安威胁，当中以「iFrame」的手法最为泛滥，每天企业收到来历不明的信件数量之多，若没有做好事当的防备，一不小心便踏入黑客的陷阱。

然而网络钓鱼邮件最常出现的内容则多半为「系统变更，请比对个人数据」或「为了保障信息安全，请变更密码」诸如此类要求收件者输入账号密码等个人数据的信件，而大多数均由伪造金融单位与购物网站所发出的信件，以欺骗收件者上当连结至伪造的官方网站输入个人数据，黑客再进而从中获取金钱利益。就如以下这封伪造来自银行要求客户维护账号的信件，当开启信件内文所提供的连结时，实际上所连结的网址并非银行的官方网站，而是一个网址相似的陷阱，收信者只要一时没察觉，便会将个人的数据双手奉送给黑客。



寄件者: Chase bank
日期: 2008年5月19日 上午 10:31
收件者: Justin
主旨: Important information from Chase Bank customer service! <message id: J74014313>

Dear Chase bank customer,

As part of our security measures, all Chase bank customers are required to con
We requested information from you for the following reason: your banking recor

You should complete Chase Online Form on a regular basis.

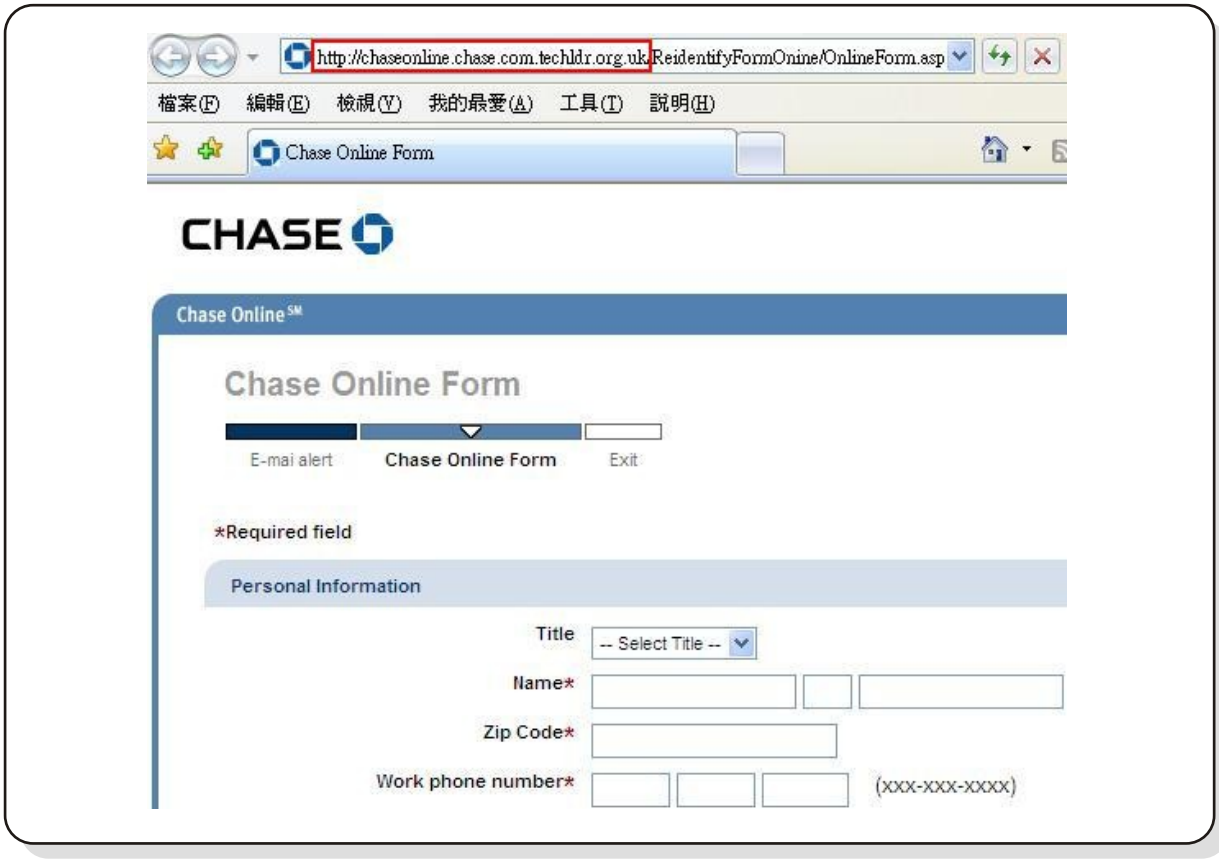
To access the form please click on the following link:

http://chaseonline.chase.com/ReidentifyFormOnine/OnlineForm.aspx?chase_id

We thank you for your prompt attention to this matter. Please understand that thi
inconvenience.

Sincerely,
Chase Online Accounts Department

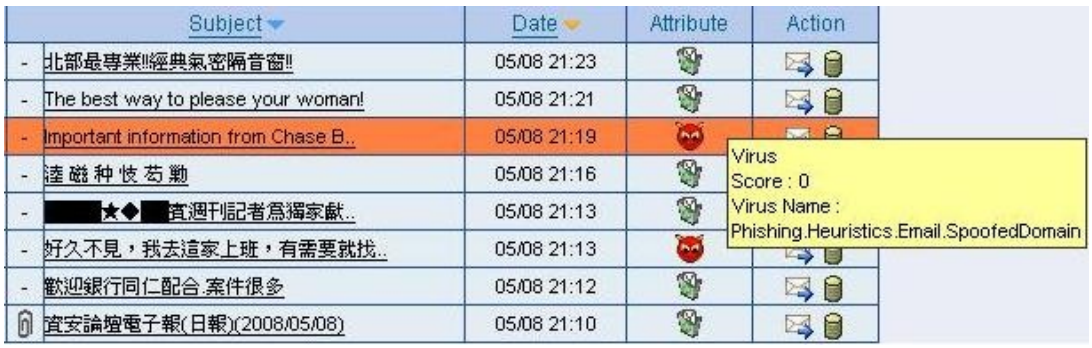
信件内容



伪造的官方网站

这些内含恶意网页连结及网络钓鱼的病毒邮件层出不穷，为了防止误开病毒信的情事发生，建议在企业对外网关处设置过滤病毒邮件的设备，新软多功能 UTM 操控接口简单，功能毫不马虎，内含 Sophos、Clam 双扫毒引擎，上述情形均能迎刃而解，为企业的信件把关。

扫描到内含有恶意网页连结的程式代码



扫描到这是一封网络钓鱼信件

文 黄智杰 alex@nusoft.com.tw