Detecting and preventing peer-to-peer connections by Linux iptables

ABSTRACT

Most of companies use Linux iptables as their edge networksô firewall. Although Linux iptables is a reputed secure stateful packet filter firewall package, it has some weaknesses. This package can not detect or control all peer-to-peer connections. One of the packages which is written for Linux iptables to manage peer-to-peer connections is layer 7-module. This module can not detect all peer-to-peer connections and drop them. Some peer-to-peer connections which use HTTP port for connecting to other peers are detected with this netfilterôs patch-o-matic but those which use static ports or dynamic ports for connecting to peers can not be detected with this module. For controlling peer-to-peer connections investigator blocked some peer-to-peer well known static ports with Linux iptables and then, for increasing the control of other peer-to-peer applications which used dynamic ports, he used QOS rules. Although this trend could drop most of peer-to-peer connections and save internet bandwidth, it was not the complete solution. He decided to control peer-to-peer connections by implementing a new module which checks peer-to-peer payloads in his next investigation.