pfSense - Feature #1935

Allow rule with max-src-conn-* options to make conditional use of "overload <virusprot>"

10/07/2011 09:31 AM - Dim Hatz

Status:	New	**Start date:**	10/07/2011
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Rules / NAT	**Estimated time:**	0.00 hour
Target version:			

Description

Firewall: Rules: Advanced Options offers various options, to limit max number of connections per source IP and connections/sec, however it silently puts any source IP that exceeds them into the <virusprot> table, effectively blocking all traffic from it for a significant period.

For pfsense rules involving max-src-conn-xyz restrictions, consider making the (overload <virusprot>) either an optional or a configurable action.

My aim is to do flexible TCP connection throttling with pfsense. I find it useful for e.g. outbound SMTP connections, as I wrote in http://forum.pfsense.org/index.php/topic,41679.0.html

> Throttling outgoing SMTP (port 25) connections?
>
> The situation I'm trying to mitigate is when e.g. in a public hotspot, a guest's malware-infected PC starts sending out 1000s of spam mails. I wouldn't want to block outgoing port 25 completely (as many people still connect to their mailserver using SMTP AUTH over TCP/25), but as a compromise I prefer to limit port 25 outgoing connections to a low number, e.g. 3/min.
>
> With Linux iptables I might use directives like:
> -p tcp --dport 25 --limit 3/min --limit-burst x
> etc
> This way, any port 25 connections beyond the limit of 3 per minute are dropped, but the port becomes available again very soon. And no other ports are affected.
>
> pfsense offers advanced options with similar features (pf's max-src-conn-rate), but apparently adds "offending" IPs to the <virusprot> table, thus blocking those IPs entirely for all protocols, rather than effectively throttling port 25 only.