

[TOOL] FireHOL – Stateful Iptables Configuration

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-11/0018.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/03/04

To: list@securiteam.com

Date: 3 Nov 2004 18:05:17 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

FireHOL – Stateful Iptables Configuration

SUMMARY

DETAILS

FireHOL a simple yet powerful way to configure stateful iptables firewalls. It can be used for almost any purpose, including control of any number of internal/external/virtual interfaces, control of any combination of routed traffic, setting up DMZ routers and servers, and all kinds of NAT. It provides strong protection (flooding, spoofing, etc.), transparent caches, source MAC verification, blacklists, whitelists, and more. Its goal is to be completely abstracted and powerful but also easy to use, audit, and understand.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:costa@tsaousis.gr>> Costa Tsaousis.

To keep updated with the tool visit the project's homepage at:
<<http://firehol.sourceforge.net/>> <http://firehol.sourceforge.net/>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

Securiteam: [TOOL] FireHOL – Stateful Iptables Configuration

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.