finjan
Vital Security™
securing your web

Forwarding IP Addresses

Forwarding IP addresses from a Squid Cache to a NG appliance

For additional information, please visit www.finjan.com or contact one of our regional offices:

USA: San Jose 2025 Gateway Place Suite 180 San Jose, CA 95110, USA Toll Free: 1 888 FINJAN 8 Tel: +1 408 452 9700 Fax: +1 408 452 9701 salesna@finjan.com	**Europe: UK** 4th Floor, Westmead House, Westmead, Farnborough, GU14 7LP, UK Tel: +44 (0)1252 511118 Fax: +44 (0)1252 510888 salesuk@finjan.com
USA: New York Chrysler Building 405 Lexington Avenue, 35th Floor New York, NY 10174, USA Tel: +1 212 681 4410 Fax: +1 212 681 4411 salesna@finjan.com	**Europe: Germany** Alte Landstrasse 27, 85521 Ottobrun, Germany Tel: +49 (0)89 673 5970 Fax: +49 (0)89 673 597 50 salesce@finjan.com
Israel/Asia Pacific Hamachshev St. 1, New Industrial Area Netanya, Israel 42504 Tel: +972 (0)9 864 8200 Fax: +972 (0)9 865 9441 salesint@finjan.com	**Europe: Netherlands** Printerweg 56 3821 AD Amersfoort Netherlands Tel: +31 334 543 555 Fax: +31 334 543 550 salesne@finjan.com

Catalog name:
Email: support@finjan.com
Internet: www.finjan.com

CONTENTS

1 Introduction

This document describes how to forward IP addresses of client machines whilst surfing the internet via a Squid Cache / Finjan NG combination.

This document only describes the required setting in the Squid Cache configuration file and any necessary changes to be made to the NG appliances settings.

This document does not describe how to configure Squid or any other part of the Squid configuration. This document is for competent administrators of Squid servers and of Finjan NG appliances.

2 Squid Settings

To enable the IP addresses of client machines to be seen in the log window of the NG appliance after being proxied forward by the Squid Cache.

It must be noted that Squid is an Open Source tool and does not support the forwarding of NTLM credentials to another upstream device in proxy mode. However NTLM credentials can be used in ICAP mode. Please be advised that this configuration is not a supported by Finjan.

Please follow the instructions below.

⇨ **Editing the Squid Configuration:**

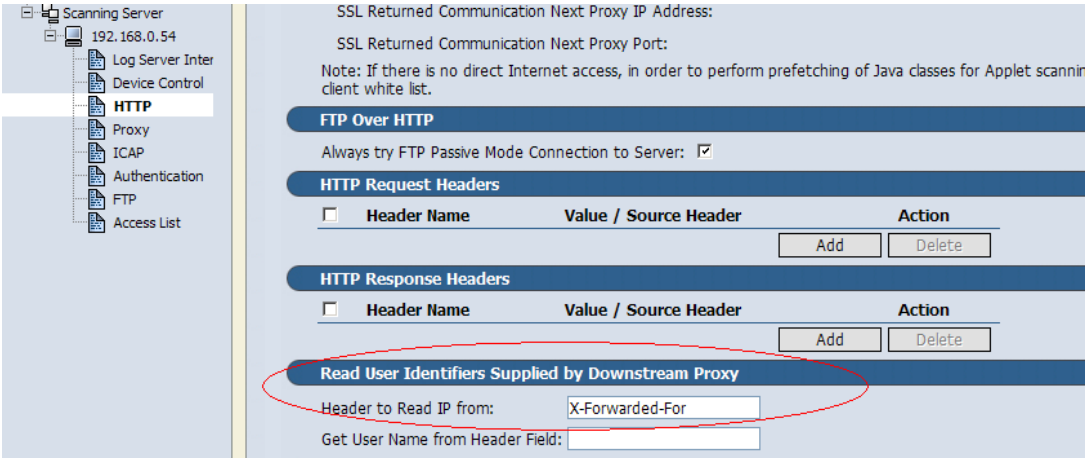
1. Log into the Squid cache appliance and switch user to the "root" account
2. Edit the file: squid.conf using "vi" or a similar editor
3. Change the parameter for the X-Forwarded-For section to "forwarded_for on" (please see example 1 below, the relevant parameter is highlighted in red)
4. Save the changes to the file.
5. Restart the squid proxy by using the relevant scripts: Example: - /etc/init.d/squid restart
6. Edit the Finjan NG appliance to accept and use the "X-Forwarded-For" headers - Please review Examples 2, 3 and 4 for explanations on how to set different versions (8.4.3, 8.5.0 and 9.0).
7. Apply and commit the changes to the Finjan NG
8. Test the solution and check in the log window that the Squid Cache is forwarding the IP address of the client machine.

2.1 Example 1: Squid.conf Settings

```
# TAG: follow_x_forwarded_for
#       Allowing or Denying the X-Forwarded-For header to be followed to
#       find the original source of a request.
#
#       Requests may pass through a chain of several other proxies
#       before reaching us.  The X-Forwarded-For header will contain a
#       comma-separated list of the IP addresses in the chain, with the
#       rightmost address being the most recent.
#
#       If a request reaches us from a source that is allowed by this
#       configuration item, then we consult the X-Forwarded-For header
#       to see where that host received the request from.  If the
#       X-Forwarded-For header contains multiple addresses, and if
#       acl_uses_indirect_client is on, then we continue backtracking
#       until we reach an address for which we are not allowed to
#       follow the X-Forwarded-For header, or until we reach the first
#       address in the list.  (If acl_uses_indirect_client is off, then
#       it's impossible to backtrack through more than one level of
#       X-Forwarded-For addresses.)
#
#       The end result of this process is an IP address that we will
#       refer to as the indirect client address.  This address may
#       be treated as the client address for access control, delay
#       pools and logging, depending on the acl_uses_indirect_client,
#       delay_pool_uses_indirect_client and log_uses_indirect_client
#       options.
#
#       SECURITY CONSIDERATIONS:
#
#               Any host for which we follow the X-Forwarded-For header
#               can place incorrect information in the header, and Squid
#               will use the incorrect information as if it were the
#               source address of the request.  This may enable remote
#               hosts to bypass any access control restrictions that are
#               based on the client's source addresses.
#
#       For example:
#
#               acl localhost src 127.0.0.1
#               acl my_other_proxy srcdomain .proxy.example.com
#               follow_x_forwarded_for allow localhost
#               follow_x_forwarded_for allow my_other_proxy
#
#Default:
forwarded_for on
```

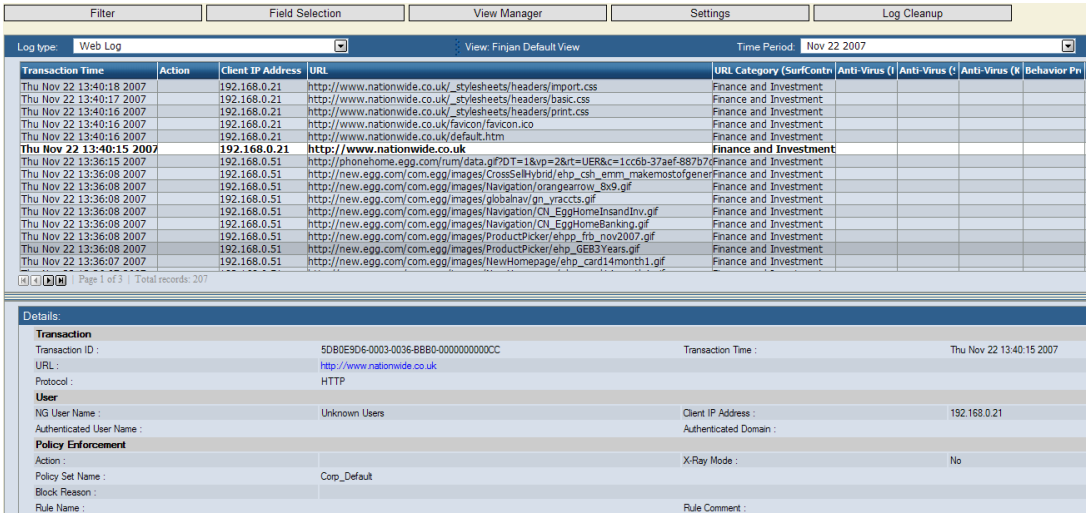
2.2 Example 2: NG 8.4.3 Settings

Navigate to Settings > Devices > HTTP and add “X-Forwarded-For” to the Read User Identifiers Supplied by the Downstream Proxy.



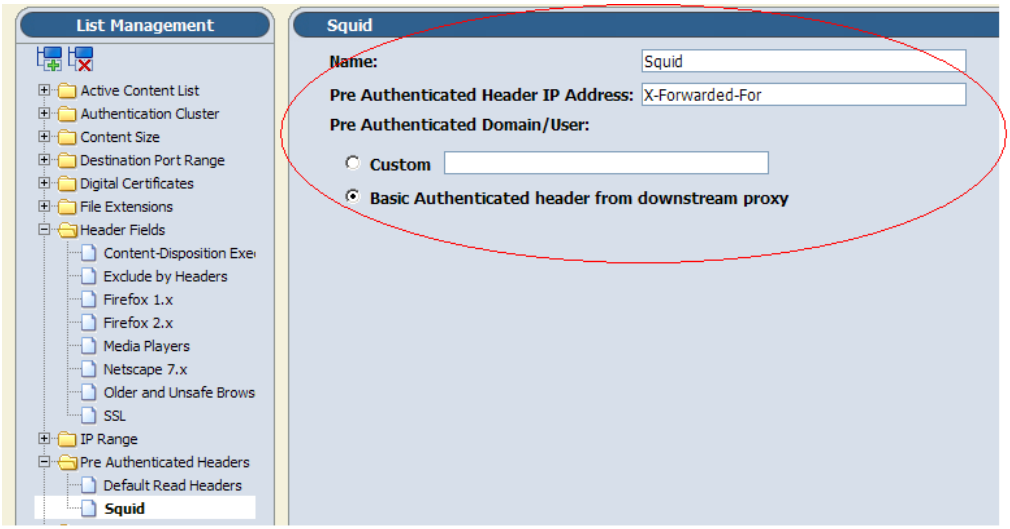
Click the apply button and then commit the changes.

Check log window after test

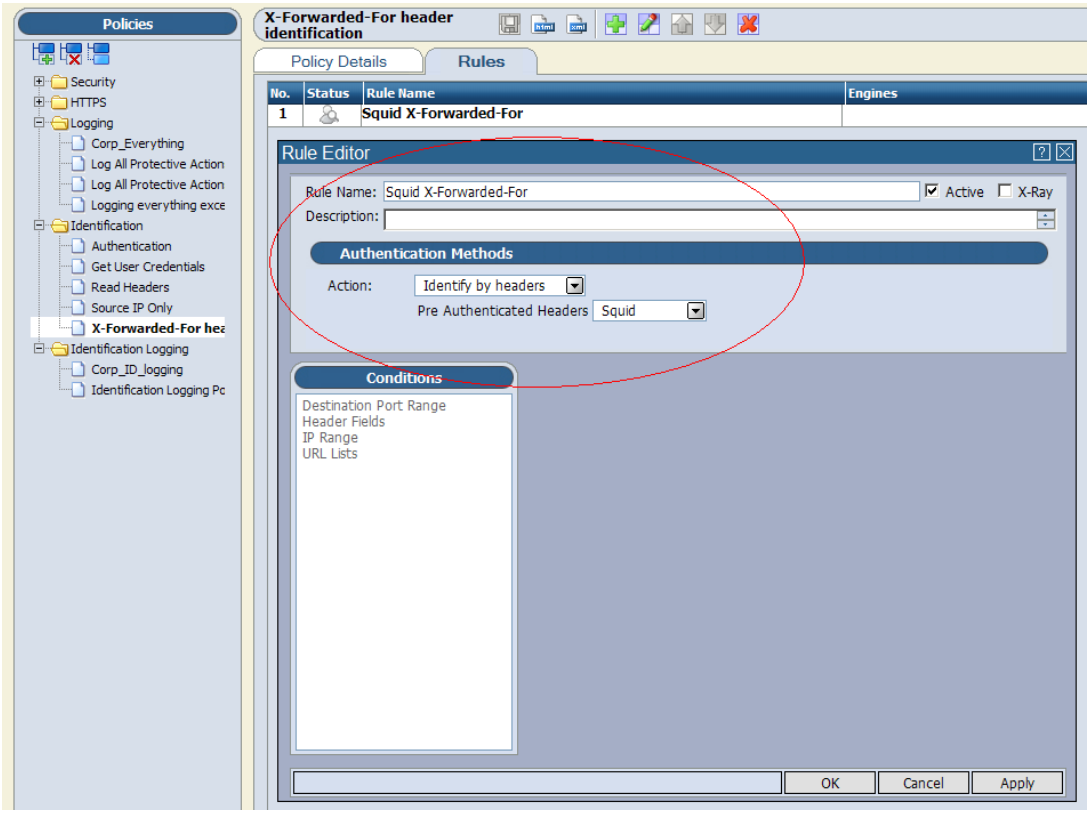


2.3 Example 3: NG 8.5.0 Settings

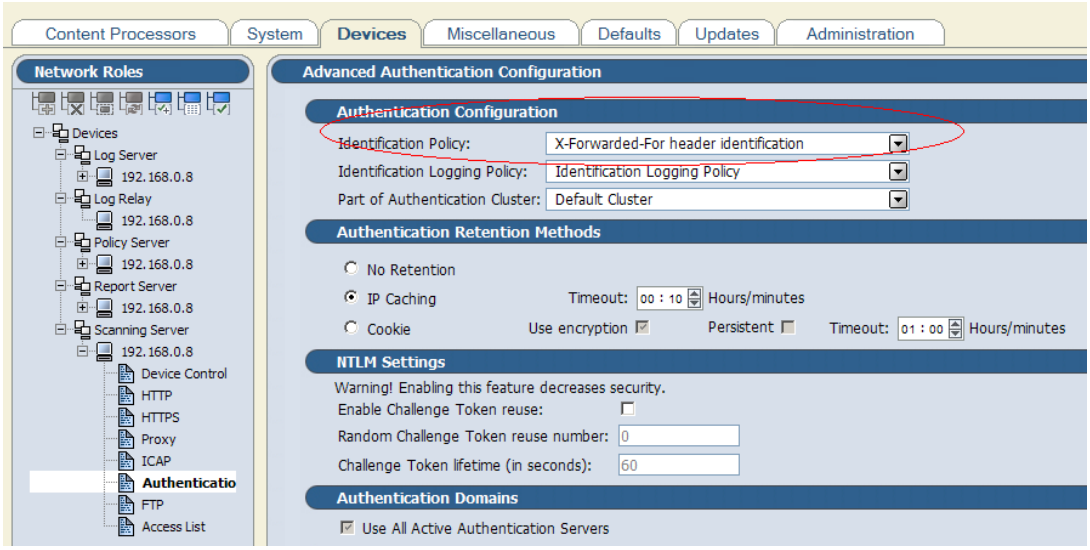
Navigate to Lists > List Management > Header Fields > Pre Authenticated Headers and Create a new header field “Squid”. Add an entry in the Pre Authenticated Header IP address: “X-Forwarded-For” and click the Basic Authenticated header from downstream proxy.



Apply all changes in this page and then navigate to Polices > Identification and then add an entry "X-Forward-For" then edit the Identification policy and change the action to "Identify by Headers" and choose the created "Pre Authentication Headers" to Squid. Change the rule name to reflect its status.

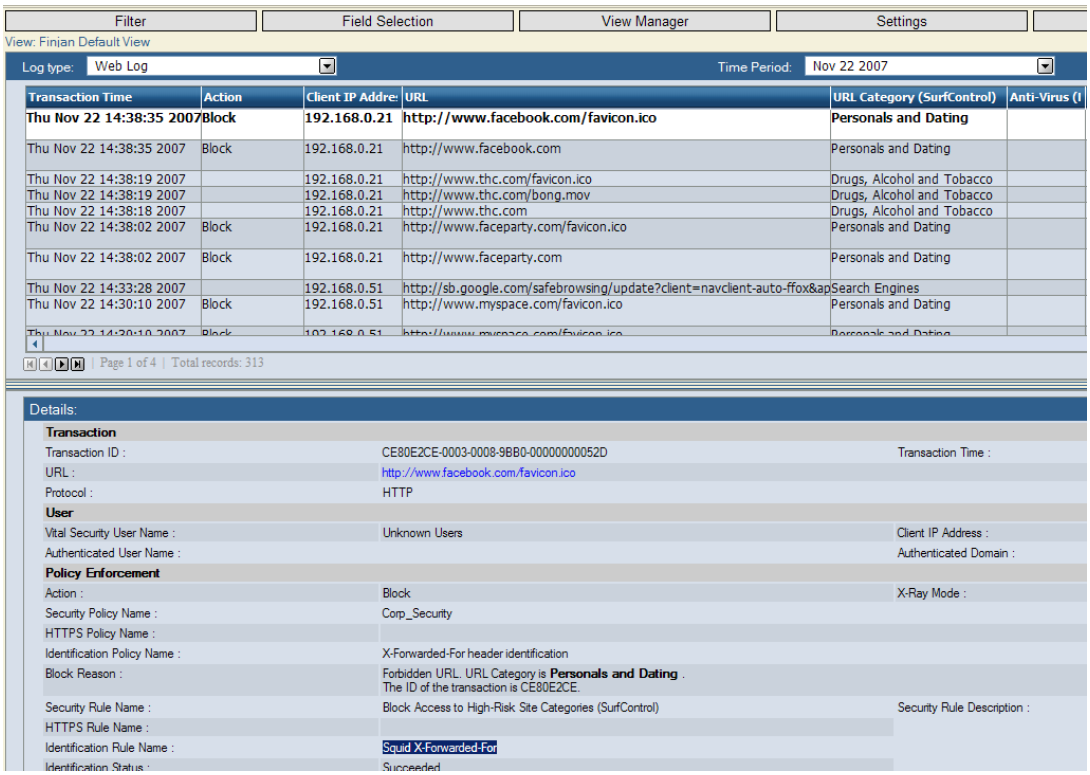


Navigate to Settings > Devices > Authentication and select the “X-Forwarded-Header Identification that you have created in the previous step. Apply and commit all changes.



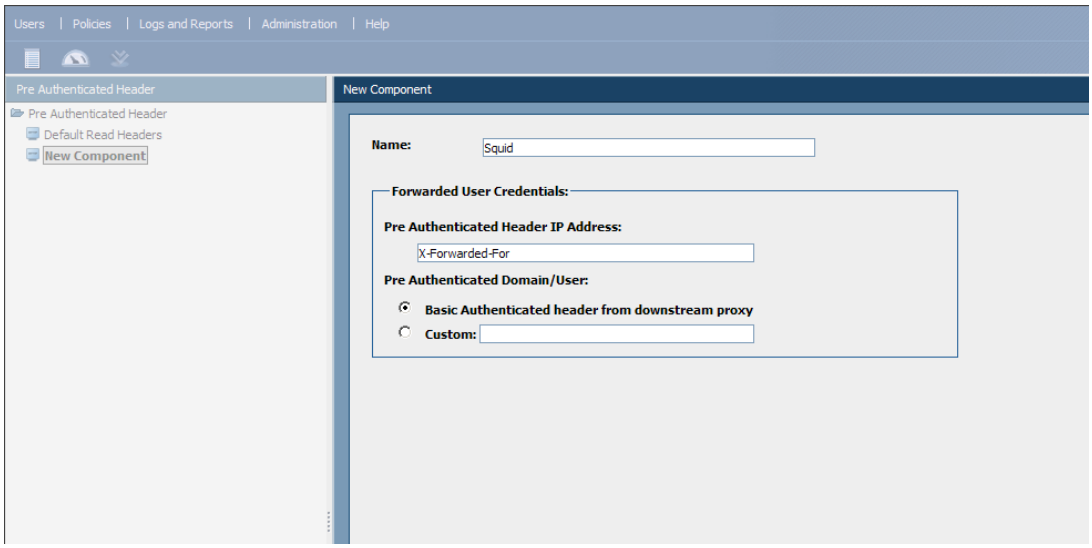
Apply and commit all changes.

Check log window after test.

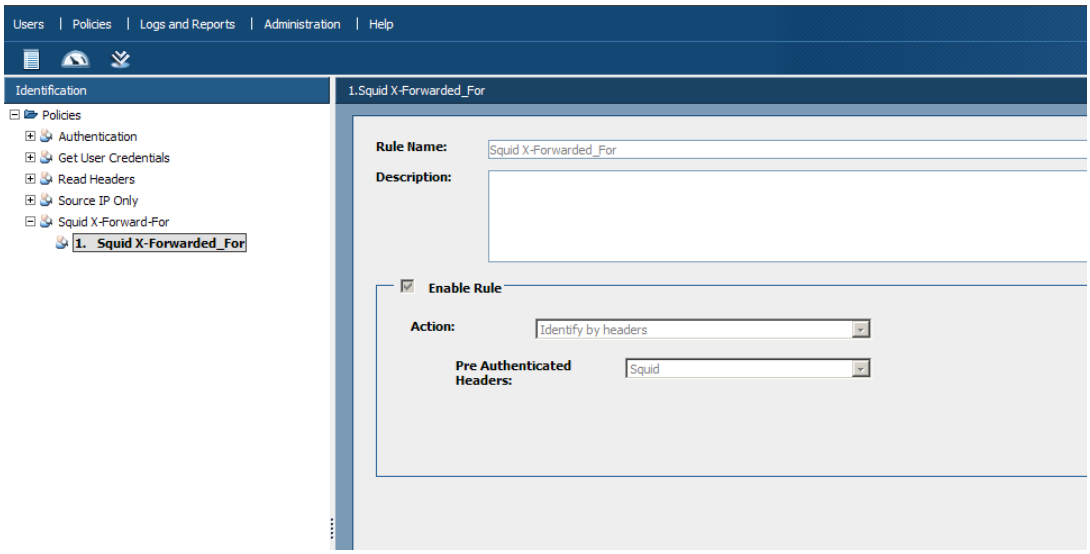


2.4 Example 4: NG 9.x Settings

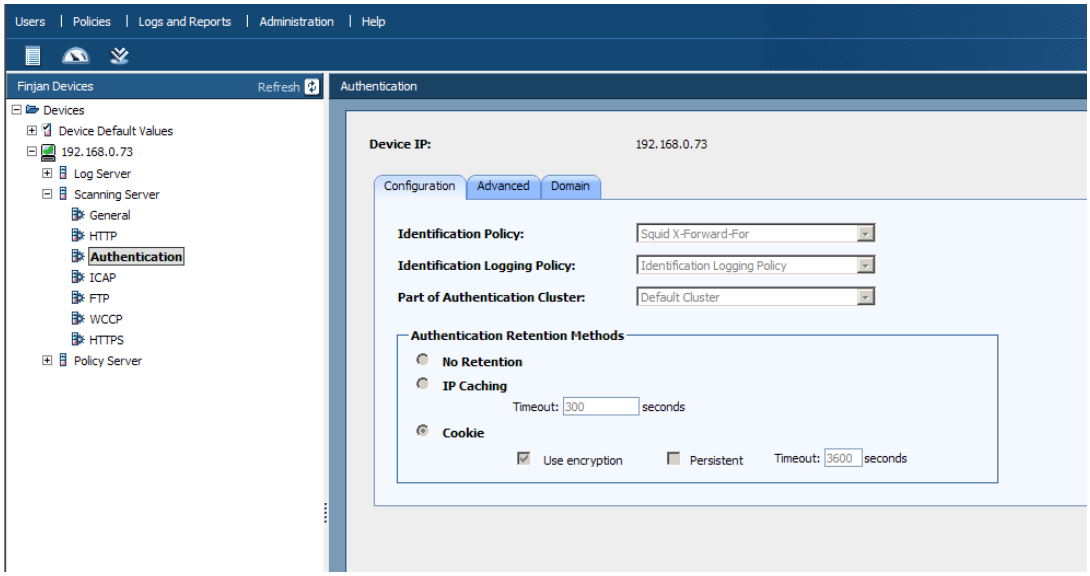
Policies > Condition Settings > Pre Authenticated Headers and Create a new header field “Squid”. Add an entry in the Pre Authenticated Header IP address: “X-Forwarded-For” and click the Basic Authenticated header from downstream proxy.



Apply all changes in this page and then navigate to Polices > Identification and then add an entry “X-Forward-For” then edit the Identification policy and change the action to “Identify by Headers” and choose the created “Pre Authentication Headers” to Squid. Change the rule name to reflect its status.



Navigate to Administration > System Settings > Finjan Devices, Select the scanner and then go to the Authentication section and select the “X-Forwarded-Header Identification that you have created in the previous step. Apply and commit all changes.



Apply and commit all changes.

Check log window after test.