NethServer 6 - Enhancement #2967
Transparent proxy: switch iplementation from TPROXY to REDIRECT

11/28/2014 03:44 AM - Giacomo Sanchietti

Status:	CLOSED	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:	nethserver-squid		
Target version:	v6.5		
Resolution:		**NEEDINFO:**	No

Description

Current implementation of transparent proxy is based on TPROXY.
TPROXY does not modify the IP header so the firewall can be use in bridged mode to scan all passing traffic without modifying any network configuration in the target environment.
But this implementation has some drawbacks:

- it can't correctly handle squidGuard redirect directives (#2958)
- it's hard to create transparent bypass based on source and destination (#2503)

The REDIRECT implementation will largely simplify firewall configuration and it will address above problems.
Thus, this implementation can't be used in bridged mode, but this scenario is not supported from the underlying system for now.

Related issues:

Related to NethServer 6 - Feature # 2503: Web proxy: bypass rules based on de...	**CLOSED**
Related to NethServer 6 - Enhancement # 2958: squidGuard: support multiple pr...	**CLOSED**

Associated revisions

Revision 20f4ae1b - 11/28/2014 09:29 AM - Giacomo Sanchietti

templates: remove TPROXY use REDIRCT. Refs #2967

Revision 17d867b1 - 12/10/2014 03:18 AM - Giacomo Sanchietti

shorewall: redirect https to port 3130. Refs #2967

History

#1 - 11/28/2014 03:44 AM - Giacomo Sanchietti

- Status changed from NEW to TRIAGED
- Target version set to v6.5
- % Done changed from 0 to 20

#2 - 11/28/2014 03:52 AM - Giacomo Sanchietti

- Related to Feature #2503: Web proxy: bypass rules based on destination and source added

#3 - 11/28/2014 03:53 AM - Giacomo Sanchietti

- Related to Enhancement #2958: squidGuard: support multiple profiles added

#4 - 11/28/2014 04:11 AM - Giacomo Sanchietti

- Category changed from nethserver-squid to <multiple packages>
- Status changed from TRIAGED to ON_DEV
- Assignee set to Giacomo Sanchietti
- % Done changed from 20 to 30

#5 - 11/28/2014 04:54 AM - Giacomo Sanchietti

- Subject changed from Transparent proxy: switch iplementation from TPROXY to DNAT to Transparent proxy: switch iplementation from TPROXY to REDIRECT

- Description updated

#6 - 11/28/2014 10:19 AM - Giacomo Sanchietti

- Status changed from ON_DEV to MODIFIED

- % Done changed from 30 to 60

#7 - 12/01/2014 08:06 AM - Giacomo Sanchietti

- Status changed from MODIFIED to ON_QA

- Assignee deleted (Giacomo Sanchietti)

- % Done changed from 60 to 70

Package in nethserver-testing:

- ~~nethserver-squid-1.2.0-18.0gitcfbd3944.ns6.noarch.rpm~~
- nethserver-squid-1.2.0-20.0git1a759fc7.ns6.noarch.rpm

Test case

- Enable proxy in transparent mode on green interface
- Enable proxy in transparent mode on blue interface
- Check clients on both networks can surf through the proxy

#8 - 12/02/2014 04:05 AM - Giacomo Sanchietti

- Category changed from <multiple packages> to nethserver-squid

#9 - 12/10/2014 03:18 AM - Giacomo Sanchietti

From Filippo on #2958:

In squid.conf https port is 3130, but shorewall redirects to 3129.

```
--- 90squid    2014-12-05 15:49:52.000000000 +0100
+++ /etc/e-smith/templates/etc/shorewall/rules/90squid    2014-12-04 20:02:19.230206865 +0100
@@ -64,7 +64,7 @@
            $OUT.="REDIRECT\tloc$bypass_src_str\t3129\ttcp\t80\t-\t$bypass_dst_str\n";
            if ($green_mode =~ /ssl/) {
                $OUT .="?COMMENT transparent proxy on green for port 443\n";
-               $OUT.="REDIRECT\tloc$bypass_src_str\t3129\ttcp\t443\t-\t$bypass_dst_str\n";
+               $OUT.="REDIRECT\tloc$bypass_src_str\t3130\ttcp\t443\t-\t$bypass_dst_str\n";
            }

        }
@@ -84,7 +84,7 @@
            $OUT.="REDIRECT\tblue$bypass_src_str\t3129\ttcp\t80\t-\t$bypass_dst_str\n";
            if ($blue_mode =~ /ssl/) {
                $OUT .="?COMMENT transparent proxy on blue for port 443\n";
-               $OUT.="REDIRECT\tloc$bypass_src_str\t3129\ttcp\t443\t-\t$bypass_dst_str\n";
+               $OUT.="REDIRECT\tloc$bypass_src_str\t3130\ttcp\t443\t-\t$bypass_dst_str\n";
            }
        }
    }
```

#10 - 12/10/2014 03:19 AM - Giacomo Sanchietti

New package in nethserver-testing:

- nethserver-squid-1.2.1.1-1.ns6.noarch.rpm

#11 - 12/11/2014 11:22 AM - Filippo Carletti

- Status changed from ON_QA to VERIFIED

- % Done changed from 70 to 90

Tested with transparent on green, I can surf.
iptables nat table has a redirect to port 3129 for port 80 and 3130 for port 443.
Looking at templates, I think that blue will work, but not tested.

#12 - 01/20/2015 03:45 AM - Giacomo Sanchietti

- Status changed from VERIFIED to CLOSED

- % Done changed from 90 to 100

Released in nethserver-updates:

- squid-3.3.13-1.el6.x86_64.rpm
- nethserver-squid-1.3.0-1.ns6.noarch.rpm