Windows Update using llnwi.net URLs

Our Windows servers access the internet through a Squid HTTP proxy. This is done because some of them are running on IPv6-only, and a proxy enables them to reach content on the old internet, such as Windows Update, CRL/OSCP URLs, etc.

If we're using a proxy anyway, this is the perfect place to carefully allow what can be accessed from the big bad internets.

So we have a few ACL lines, based on https://technet.microsoft.com/en-us/library/cc708605(WS.10).aspx.

Since 11 Feb 2015 one of our Windows 2008 R2 boxes started to receive redirects from au.download.windowsupdate.com.

So a HEAD request to this URL:

http://au.download.windowsupdate.com/d/msdownload/update/software/updt/2015/01/windows6.1-kb3005788-x64-express_fd385da8462d27efb7bb326b86fd8808887f1c55.cab

was redirected to:

http://ic.91000226.1100bf.1.msftsrvcs.vo.llnwi.net/d/msdownload/update/software/updt/2015/01/windows6.1-kb3005788-x64-express_fd385da8462d27efb7bb326b86fd8808887f1c55.cab

That llnwi.net wasn't in the accesslist, so it was rejected.

After some searching I concluded that this is a legitimate redirect.

Based on what BITS requested so far:

```
http://ic.91000226.00af17.1.msftsrvcs.vo.llnwi.net/c/msdownload/update/software/secu/2015/01/windows6.1-kb3023562-
x64-express_a68363518e54e54666d7cb116462abb17114bdd3.cab
http://ic.91000226.01556b.1.msftsrvcs.vo.llnwi.net/d/msdownload/update/software/defu/2015/02/mpas-
fe_bd_37a87ccdb6a96ab15424a728cf9fbcbe6d6d9c20.exe
http://ic.91000226.024efb.1.msftsrvcs.vo.llnwi.net/d/msdownload/update/software/updt/2015/01/windows6.1-kb3020338-
x64-express_6a333b9cac01a79054a8516fd58066a3c16a9175.cab
http://ic.91000226.033e6f.1.msftsrvcs.vo.llnwi.net/c/msdownload/update/software/secu/2015/01/ie11-windows6.1-
kb3021952-x64-express_732b6304f691ea9e1bdc3a7ecc287b3ec1b6b611.cab
http://ic.91000226.04a879.1.msftsrvcs.vo.llnwi.net/c/msdownload/update/software/secu/2014/12/windows6.1-kb3004361-
x64-express_15b5da31dd4dbdb1241dc7b0a60960c6a800ee11.cab
http://ic.91000226.04b0d8.1.msftsrvcs.vo.llnwi.net/d/msdownload/update/software/updt/2015/01/windows6.1-kb3004394-
v2-x64-express_7423fc8202bf2d663f3251a2fc39bf0c23debd4c.cab
http://ic.91000226.06d0f6.1.msftsrvcs.vo.llnwi.net/d/msdownload/update/software/secu/2015/01/windows6.1-kb3013455-
x64-express_cf5cbf8735147c2514fc0c5621f5eff4a917bca4.cab
http://ic.91000226.0a7048.1.msftsrvcs.vo.llnwi.net/c/msdownload/update/software/defu/2015/02/mpas-d_bd_1.
191.4500.0_1421f6758ae7c0df89b1cc047f160d17819009a6.exe
http://ic.91000226.0a9837.1.msftsrvcs.vo.llnwi.net/c/msdownload/update/software/secu/2015/01/windows6.1-kb3004375-
v3-x64-express_01a90d22730c18d82a90e92340327cfe76a195e5.cab
http://ic.91000226.0a9c30.1.msftsrvcs.vo.llnwi.net/c/msdownload/update/software/uprl/2015/02/windows-kb890830-x64-
v5.21-delta_a4dc652001ee45f5a03466fe6f3403d272d5fd38.exe
http://ic.91000226.0b361c.1.msftsrvcs.vo.llnwi.net/c/msdownload/update/software/secu/2015/01/windows6.1-kb3031432-
x64-express_f84fbb47409bfc2d2cd19444d55efa65577f276c.cab
http://ic.91000226.0bdf57.1.msftsrvcs.vo.llnwi.net/c/msdownload/update/software/secu/2015/01
/mpsyschk_cb1fefac0669ab60ac983bda2202780a80a84d32.exe
http://ic.91000226.0cf75b.1.msftsrvcs.vo.llnwi.net/c/msdownload/update/software/secu/2015/01/windows6.1-kb3029944-
x64-express_27c4b120fc6bd56c5fe429fa7bae34de9f7ae900.cab
http://ic.91000226.1100bf.1.msftsrvcs.vo.llnwi.net/d/msdownload/update/software/updt/2015/01/windows6.1-kb3005788-
x64-express_fd385da8462d27efb7bb326b86fd8808887f1c55.cab
http://ic.91000226.132660.1.msftsrvcs.vo.llnwi.net/c/msdownload/update/software/secu/2015/01
/mpsyschk_b2f2b1fe31b7ecec4ea43004bc4e2c7b7171b74f.exe
http://ic.91000226.14fb1b.1.msftsrvcs.vo.llnwi.net/c/msdownload/update/software/secu/2015/01/windows6.1-kb3023607-
x64-express_e76e10fe041a23f31017dab2ed817b3e5f5d7bb7.cab
```

I've come up with this ACL:

```
dstdom_regex ^ic\.91000226\.[0-9a-z]{6}\.1\.msftsrvcs\.vo\.llnwi\.net$
```

Let's see how that goes.