

## Re: (NIS/NPF) Event log and other issues.

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-10/3802.html>

---

**From:**

**Date:** 07/04/02

Date: Thu, 4 Jul 2002 00:32:17 +0100

Hi Joseph V. Morris,

In n/g comp.security.firewalls you remarked...

- > *Hmmm, Tack, I remain a bit confused. How can you assert that it is, in*
- > *fact, connecting to the internet if you don't have any log entries? Are*
- > *you referring to your statement (from your site) that:*
- >
- > *"No logs are recorded for nmain.exe except for the usual...*
- >
- > *'An instance of "C:\PROGRAM FILES\COMMON FILES\SYMANTEC*
- > *SHARED\NMAIN.EXE" is preparing to access the Internet for the first*
- > *time' "*
- >
- > *If so, that doesn't indicate an actual internet connection; it's basically*
- > *just a notification that an Internet-enabled application has been loaded*
- > *(indeed, you should see that for LOTS of applications in your firewall*
- > *event log). (That's a very poorly worded event log entry because it's not*
- > *always true for all applications.)*

You may have missed this 'twig' amongst the 'branches'...

"NIS HAS NEVER PRESENTED ME WITH AN INTERNET ACCESS ALERT FOR  
`SYMANTEC NORTON PROGRAM INTEGRATOR` (NMAIN.EXE), yet, according to  
the Alert Tracker and the NIS Statistics window, NMAIN.EXE \*is\*  
connecting to the internet and transmitting data without my ever  
having to configure a rule to permit it."

Noticing nmain transmitting data in the statistics screen, made me  
think that it \*was\* actually connecting.

- > *Now, there ARE rules for nmain.exe in the NIS Rules Settings (especially*
- > *if you're running at High Security -- which you should be -- and allowed*
- > *Automatic Firewall Rule Creation (or whatever they're calling it today)).*
- > *Here's one:*
- > *\*\*\*\*\**
- > *Rule nnn Norton Program Integrator HTTP Rule*
- > *Category: General*

Re: (NIS/NPF) Event log and other issues.

comp.security.firewalls: Re: (NIS/NPF) Event log and other issues.

- > *Rule in use: YES*
- > *Logging: NO*
- > *Protocol: TCP*
- > *Action: Permit*
- > *Direction: Outbound*
- > *Application: (Symantec Norton Program Integrator)*
- > *.....Path: c:\...\nmain.exe*
- > *Local service: Any Service*
- > *Local Address: Any Address*
- > *Remote Service:*
- > *.....Port: 80*
- > *.....Port: 81*
- > *.....Port: 82*
- > *.....Port: 83*
- > *.....Port: 443*
- > *.....Port: 1080*