



Fox DataDiode

secure one-way communication

Application-Sheet Nagios

How to use Nagios to monitor the entire (classified and unclassified) network efficiently, without degrading security?

Nagios provides an industry standard IT infrastructure monitoring system capable of watching hosts and services in a network. The system enables organizations to identify and resolve network problems before they affect business processes.

Organizations with classified and unclassified networks are forced to run at least two separate Nagios monitoring systems, one in the Black and one in the Red network.

This sheet describes a centralized solution to provide a bird's eye view of the status of the entire network using Nagios and the Fox DataDiode.

Business Benefits

Monitoring the status of the entire network is cumbersome because you have to check the status on multiple systems. As a result, the availability of the systems can be threatened. The benefit of a centralized Nagios solution is that it provides a higher availability of the network.



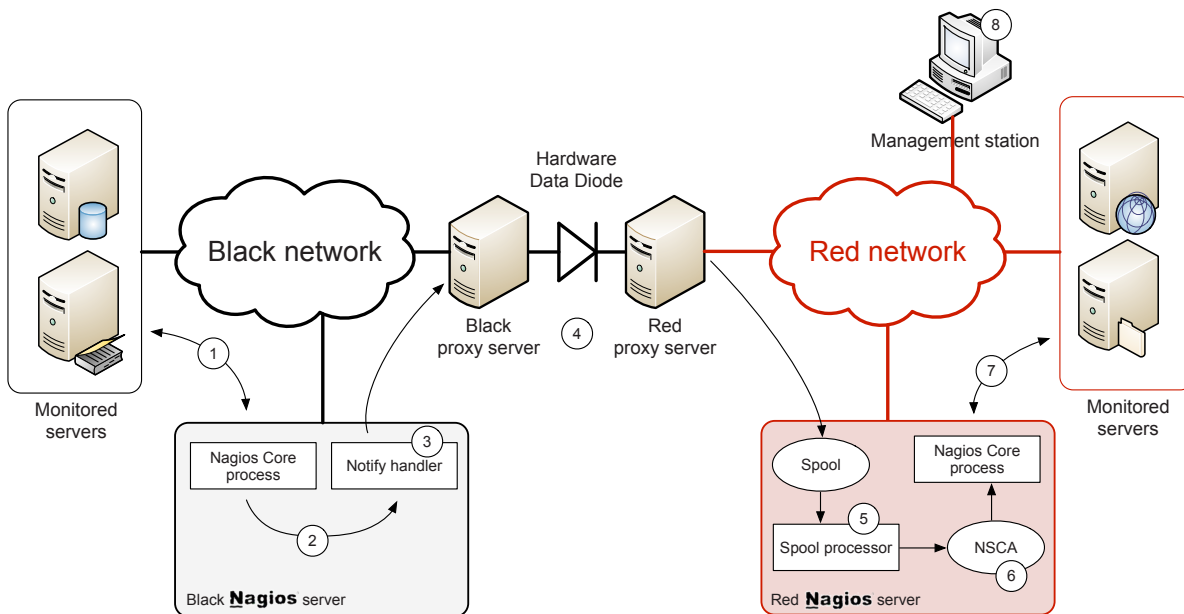
Prerequisites

- Nagios server in the Black network
- Nagios server in the Red network
- The Fox DataDiode must be configured to transmit FTP

Technical Details

The first step is to configure the red and black Nagios systems to monitor their respective networks using active checks (1, 7). The Red Nagios instance must also have host and service entries corresponding to the Black Nagios server. These entries must accept passive check results. [For more information on configuring Nagios see link 1]. On the Red Nagios server NSCA must be installed, both the daemon and the client. [For instructions on configuring NSCA see link 2].

When host or service goes down on the Black network a 'notify' command will be executed (2). This 'notify' command (3) puts the check results in a text file with a unique name, suitable for input by NSCA [2].



This file is then transferred via FTP through the Data Diode (4) to a spool directory on the Red Nagios server. The spool directory on the Red Nagios server is checked periodically for new files by a spool processor (5). The check results in the new files are sent via 'send_nsca' to the Nagios Core process (6). The web interface displayed on a management station (8) will display the status information for systems in both the Red and Black networks in one view.

The Fox DataDiode, a perfect 100% secure solution, transfers data -online, in real-time and continuously- between two networks of varying security levels without compromising the security of the receiving network.

What do you need?

- Nagios Server(s) in the unclassified network(s)
- Nagios server in the classified network
- Fox DataDiode solution:
 - Fox DataDiode software
 - Two proxy servers
 - Hardware Data Diode

Links

1. Nagios: <http://www.nagios.org>
2. NSCA: http://nagios.sourceforge.net/download/contrib/documentation/misc/NSCA_Setup.pdf

CONTACT

Fox-IT
Olof Palmestraat 6 P.O Box 638
2616 LM Delft 2600 AP Delft
The Netherlands

t +31 (0)15 284 79 99
f +31 (0)15 284 79 90
e datadiode@fox-it.com

www.datadiode.eu