Integration Guide
Sourcefire® and NT OBJECTives™

Scope of Document

This Integration Guide covers the following models:

Sourcefire	Sourcefire 3D® Sensors running 4.9 and above Sourcefire Defense Center® running 4.9 and above
NT OBJECtives	NTOSpider Web Application Security Scanner

Guide Overview

- Scope of Document
- Functionality Added
- Assumptions and Prerequisites
- Caveats and Restrictions
- Integration Workflow
- Integration Validation
- Troubleshooting and Performance Monitoring
- Obtaining Support and Additional Resources

Functionality Added

Web applications can be a gateway for hackers targeting company confidential information, client records, and other sensitive data. Typically custom-built and modified often, web applications are not effectively protected by traditional web application vulnerability scanners that have a “one-size-fits-all” approach to rules.

NTOSpider is an active vulnerability scanner for web applications that identifies application vulnerabilities as well as site exposure risk and ranks their threat priority. NTOSpider also scans site structure, content, and configuration to identify inherent exposure to future or emerging threats.

Sourcefire IPS™ provides contextual awareness to accurately identify real threats, an open architecture to enable customization for a customer’s unique environment, and intelligent automation for impact assessment and IPS tuning.

When used together, scans from NTOSpider automatically generate precise content and application-specific Snort® rules for the vulnerabilities identified by the scan. Based on NTOSpider’s knowledge of the application and its inherent vulnerabilities, the NTOSpider/Snort rules are much more aggressive and effective than “one-size-fits-all” rules.

This creates an intrusion policy that does not just protect the web application’s hosting infrastructure but also protects the application itself from exploitable content such as forms, cookies, scripts, SQL strings and ODBC connectors, authentication, applets/objects, and hidden fields.

Assumptions and Prerequisites

For best results in protecting a production web application, the Sourcefire 3D® Sensor needs to be in inline IPS mode within the hosting infrastructure.

A licensed copy of NTOSpider and NTODefend is required.

No additional licenses are required to enable the integration itself.

Caveats and Restrictions

The integrated Sourcefire/NT OBJECTives solution is not classified as a Web Application Firewall (WAF). However, when integrated, the use of Sourcefire and NT OBJECTives provides a solution that may augment, eliminate the need for, or, in some cases, be superior to a standalone WAF.

It is up to the individual customers to decide whether this solution is suitable for their own environment and specific needs. For example, the Payment Card Industry Data Security Standard (PCI DSS) does not state that a WAF is required; however “compensating control” is required. Customers are encouraged to consult their PCI auditor to determine whether this integrated solution can be used as a “compensating control” in place of a WAF.

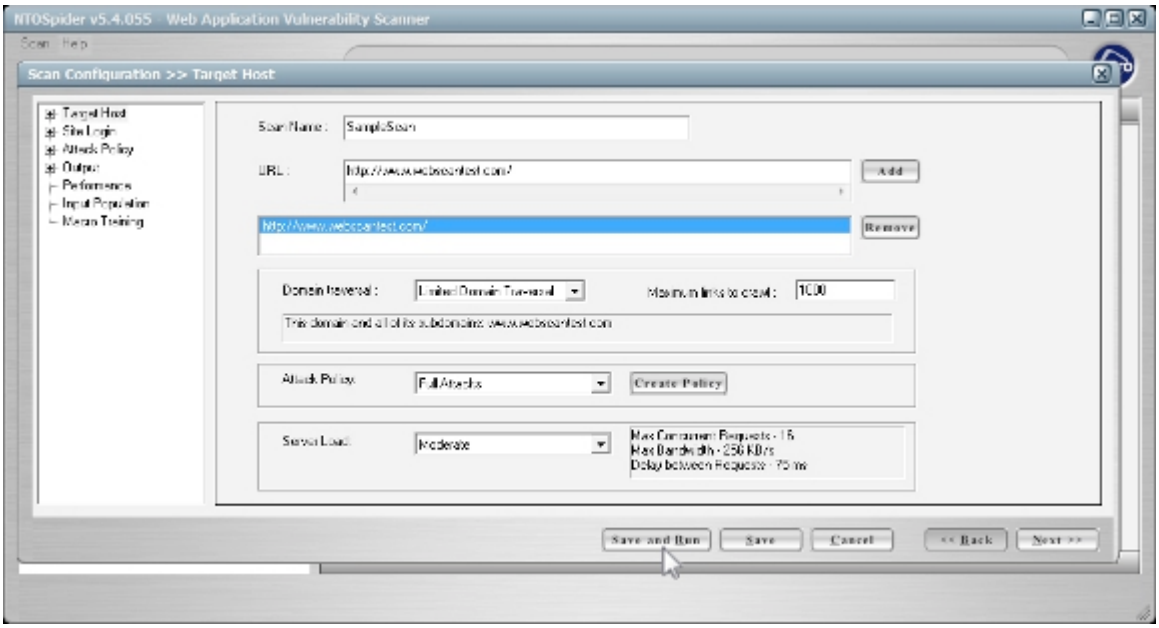
Because of the precise nature of the rules generated by this integration process, follow the steps outlined in this document whenever changes to the protected web application are made.

Integration Workflow

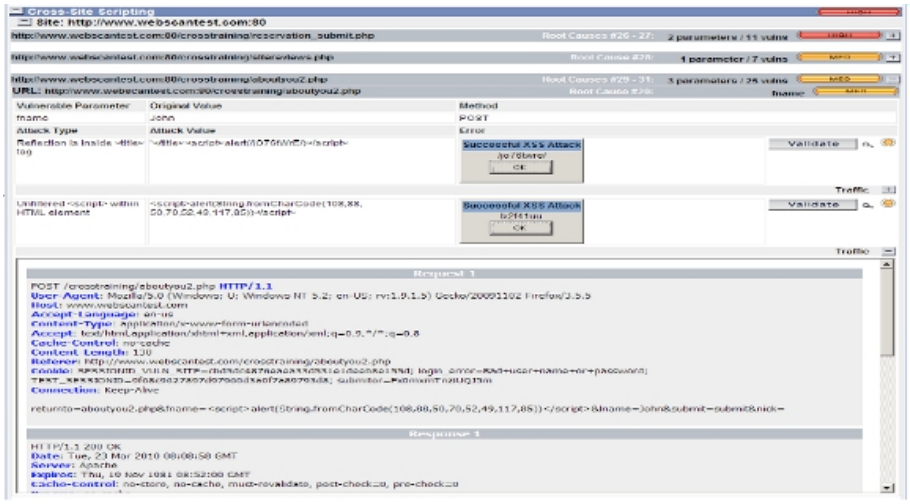
Using the Sourcefire/NT OBJECTives solution is a three-step process:

Step 1: Use the NTOSpider to discover vulnerabilities in the web application.

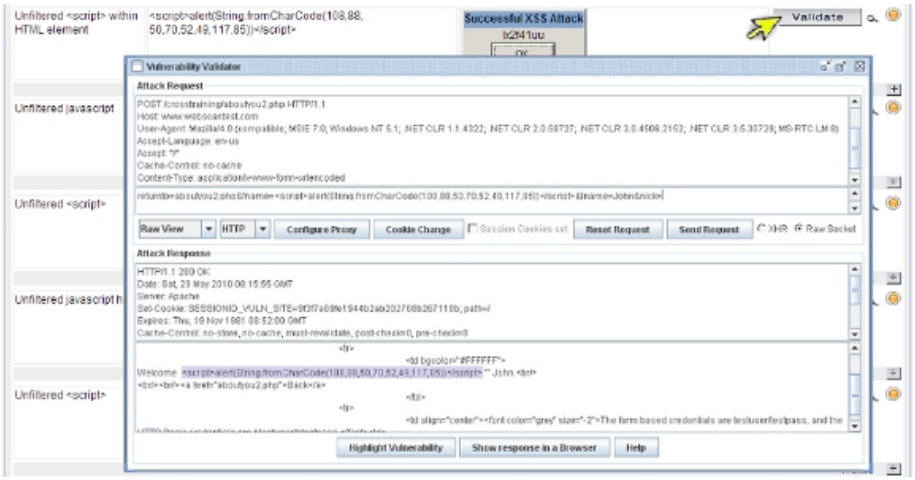
This normally only requires the URL of the site to be scanned.



Once complete, the NTOSpider report provides details of the vulnerabilities and remediation procedures for developers.



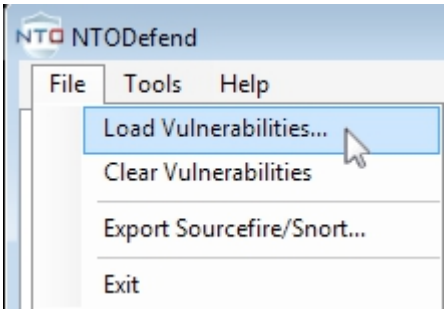
The reporting feature also includes the ability to reproduce the vulnerabilities for auditors to verify the findings and aid developers in remediation.



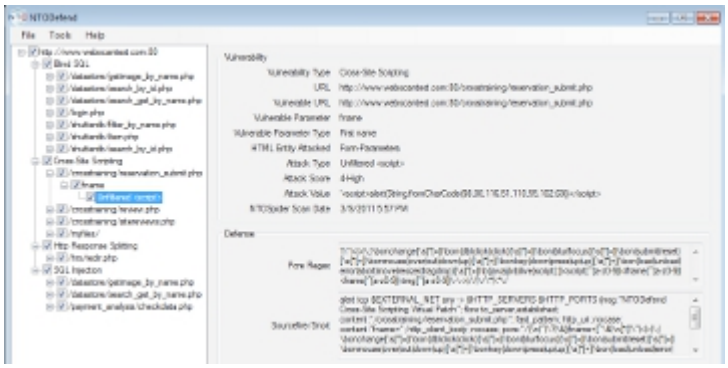
Step 2: Use NTODefend to review and generate rules.

The NTODefend tool provides a process for reviewing, approving and generating Snort rules.

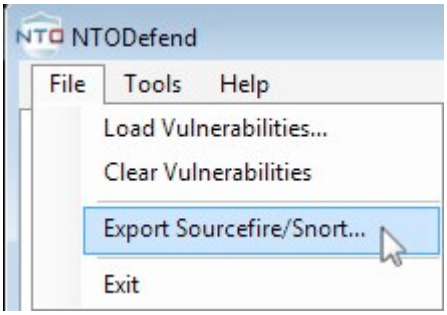
Import the vulnerabilities from NTOSpider into NTODefend. The `VulnerabilitiesSummary.xml` file is located in the report directory of the scan.



Review the vulnerabilities and preview the suggested rules.



Generate the Snort rules.



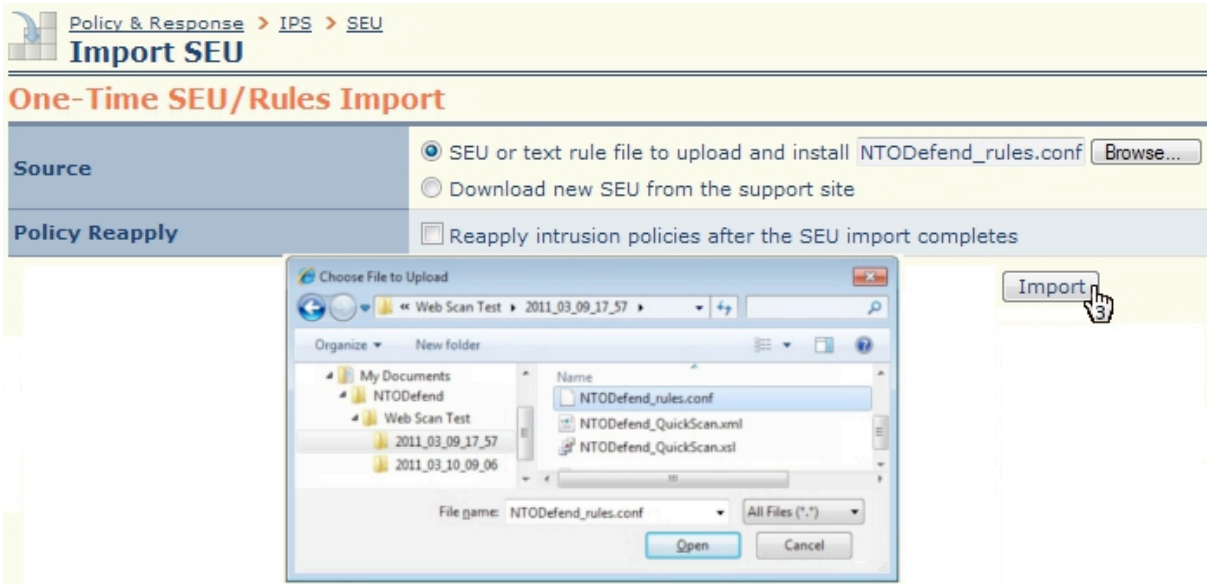
The resulting rules are completely custom and targeted to respond to the specific locations in the application that were found to be vulnerable.

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS
  (msg:"NTOSpider Blind SQL attack attempt"; flow:to_server,established;
   content:"/shutterdb/search_get_by_id2.php"; fast_pattern; http_uri; nocase;
   content:"id="; http_uri; nocase;
   pcre:"/(\n|^|\?|\&)(id=[^\&|\n]*('|\"|\de\d\d|%[a-fA-F]\d%[a-fA-F]\d|%.\d%.\d|\)|%|_|\-\-|#|\/\*))/Ui";
   metadata:service,http; classtype:web-application-attack; resp:icmp_host; sid:2000002; rev:1; )
  )
```

Step 3: Import Rules into the Sourcefire 3D System.

Log onto the Sourcefire Defense Center® as an administrator and go to the Import Rules screen.

Import the rule file that NTDefend generated in \My Documents\NTODefend\



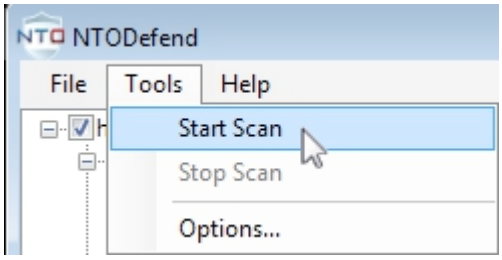
Once loaded, apply the rules to the Sourcefire 3D Sensors protecting the web application.

Your web application is now protected by the Sourcefire 3D System.

Integration Validation

Validate the integration by running another full scan using NTOSpider, which will also generate a new report to use for compliance reporting.

Use NTODefend's QuickScan feature to get an immediate check of the basic effectiveness of the new rules.



Troubleshooting and Performance Monitoring

If the functionality or performance of your Sourcefire 3D System diminishes after integrating the NTOBECTives rules, please contact Sourcefire support for troubling shooting and assistance.

Obtaining Support and Additional Resources

- Sourcefire Support: https://support.sourcefire.com
- NT OBJECTives Support: support@ntobjectives.com