Deep Security Vulnerability Protection Summary

Trend Micro, Incorporated

This documents outlines the process behind rules creation and answers common questions about vulnerability coverage for Deep Security

Version 2.2

April 2015

1. Purpose of this note

The Deep Security Vulnerability Labs team is the Trend Micro team that researches vulnerabilities and threats and provides protection via various protection modules in Deep Security. This document explains the process of threat monitoring, rule creation and quality assurance of rules. A list of answers to Frequently Asked Questions (FAQ) is included in Section 3 of the document.

While this document is focused on Deep Security, the process outlined in this document also applies to the protection provided by Trend Micro Vulnerability Protection (formerly Intrusion Defense Firewall).

2. Rule Development Process

The process involves 3 primary stages:

- Monitoring for vulnerabilities and threats
- Vulnerability research and rule development
- Quality assurance and delivery of rules to customers in a Deep Security Rule Update.

2.1 Monitoring for Vulnerabilities and Threats

The entire rule development process starts with monitoring for the latest vulnerabilities and threats. The Deep Security Vulnerability Labs team monitors threats 24/7 from various different sources. These sources include:

- Subscriptions to vulnerability research sources
- Programs with software vendors such as Microsoft Active Protections Program (MAPP)
- Trend Micro sources, including malware and attack information from customers (through the Trend Micro Smart Protection Network), honeypots, and other sources.
- Public information

The Deep Security Vulnerability Labs team is a member of the TrendLabs team, which is a global team that monitors emerging threats. This team monitors and disseminates key threat information company-wide so that all products can provide protection with the threat defense technologies included in each product.

2.2 Vulnerability Research and Rules Development Criteria

The focus of vulnerability research is on the server and desktop software likely to exist within end customer environments. This includes operating systems such as Microsoft Windows, Linux, and Unix, as well as enterprise software, including web browsers, web servers, application servers, backup software and databases. Deep Security does not provide protection for network devices, since Deep Security is not in a position to protect those devices.

Primarily, it is **remote** vulnerabilities and exploits which Deep Security provides protection for. This means that the vulnerabilities can be exploited **over the network** from an attacking computer. The primary protection provided by Deep Security is very similar to a network Intrusion Detection and Prevention (IDS/IPS) system, however it is applied at the host for more granular and specific security.

While there are many software vulnerabilities disclosed on a daily basis, Deep Security only provides protection for a subset of these vulnerabilities. The criteria used to determine if protection is provided:

1. Is the vulnerability in enterprise software that many of our customers depend on and for which Deep Security is in a position to protect?

2. Can the vulnerability be protected by network inspection (Deep Packet Inspection)?
3. Is the vulnerability information available and sufficient to be able to develop an Intrusion Prevention rule for the vulnerability?
4. Is the vulnerability CVSS severity level significant enough to warrant coverage? Typically, a CVSS score of 4.0 is required, although coverage for CVSS score lower than 4.0 is sometimes provided.

It is often the lack of vulnerability information that prevents Deep Security (and all network security companies) from delivering protection for a specific vulnerability. The criteria for developing an Intrusion Prevention (IDS/IPS) rule is shown in Figure 1 below.

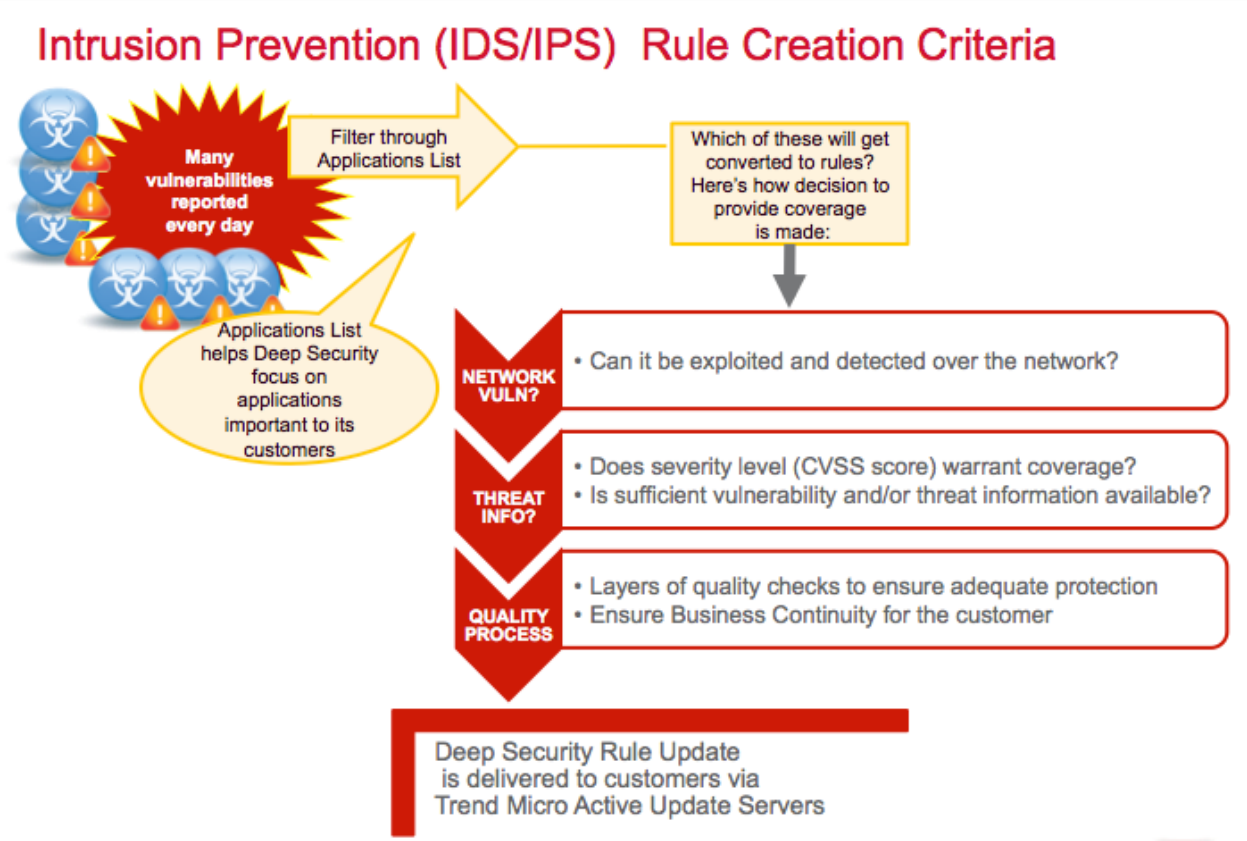


Figure 1: Intrusion Prevention (IDS/IPS) Rule Criteria for Coverage

2.3 Vulnerability Research and Rules Development

Once it has been determined that a specific rule can be developed, a rigorous rule development process is followed in order to develop the rule, including tests for potential False Negative and False Positive conditions. A False Negative is when a rule does not detect certain attack condition and a False Positive is when a rule identifies legitimate traffic as an attack.

A rule is created based on all threat information available. The vulnerabilities are imported into a vulnerability tracking system and pushed into the research queue after being subjected to a triage process. The research team selects vulnerabilities from the top of the research queue and researches and collects all relevant threat information. This information is used to develop an Intrusion Prevention (IDS/IPS) rule. Developing a rule is similar to writing a small software program. An Intrusion Prevention (IDS/IPS) rule is very different from an Antivirus Signature. It is not just a pattern but a series of checks that look deep into the protocol, looking for very specific fields and structures in a protocol and/or file.

Once an Intrusion Prevention (IDS/IPS) rule is developed, it is subjected to various unit tests to ensure that it covers all aspects of the vulnerability and doesn't cause false positives. These tests are carried out by the developer of the rule, and also a member of the quality assurance team.

After Unit Testing is completed, the rule undergoes a Peer Review.

Figure 2 summarizes the Intrusion Prevention (IDS/IPS) rule development process:

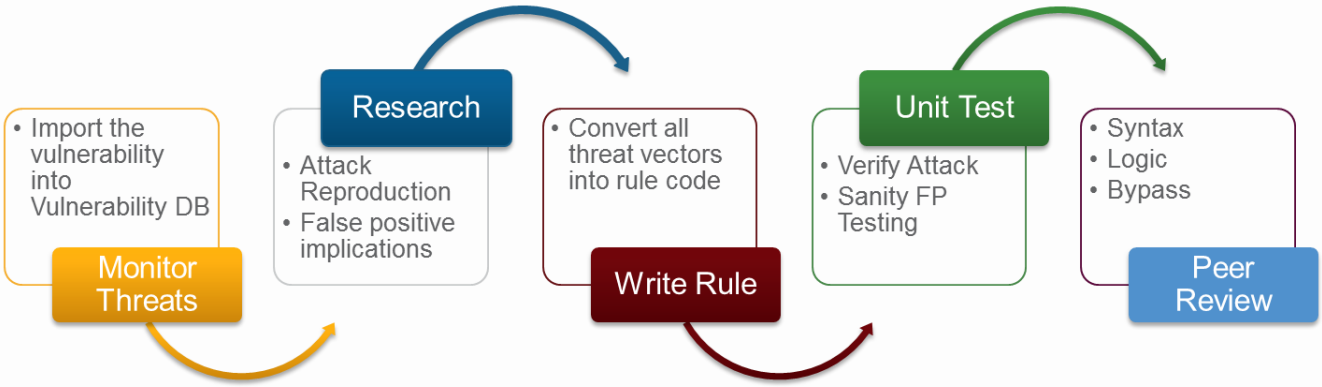


Figure 2 – Intrusion Prevention (IDS/IPS) Rule Development Process

In addition to the development of the specific rule, most IDS/IPS rules have a corresponding recommendation rule that identifies which software contains the vulnerability. The vulnerability labs team creates rules for the Recommendation Scan feature of Deep Security. This allows Recommendation Scan to ensure that the Intrusion Prevention (IDS/IPS) rule is deployed on the appropriate systems within a customer environment. These recommendation rules are verified against real applications and patches in most of the cases as a part of the rules development process.

2.4 Integration Testing

Once the Rule Development Process is completed for a rule, it is included in a potential rule update with other rules scheduled for release. This rule update is subjected to several integration tests to ensure that the entire update works as expected within product and simulated customer environments. This involves:

- **False Positive Tests:** With any IDS/IPS product, false positives are a significant concern. We ensure thorough false positive tests by running the rules through terabytes of 'good traffic'. The traffic has been generated based on thousands of test cases, and also collected from customer environments.

- **Regression Tests:** Ensuring that the rule doesn't have any impact on other rules. We accomplish this by replaying attacks against all rules that could be possibly impacted and making sure the rules prevent those attacks.
- **Performance Tests:** To ensure that there is minimal impact on network throughput, the rules are subjected to network performance tests using industry standard tools.
- **Staging Tests:** These are to ensure that the rule updates work fine with *all* supported versions of Deep Security.
- **Soak Tests:** A rule update is released to an internal production operational environment within Trend Micro to ensure that the rule update does not have any negative operational impact.
- **Security Update Testing:** Before a rule update is released to the customers, our team ensures that the rule update is posted and there are no issues importing them in the product via the Active Update servers.

Once the above process is complete, the rules are delivered and available to a customer. In many cases, such as the ShellShock and Heartbleed vulnerabilities, this is all done within 24 hours of the vulnerability being disclosed publicly.

Figure 3 is a summary of the Rule Update Integration Testing process:

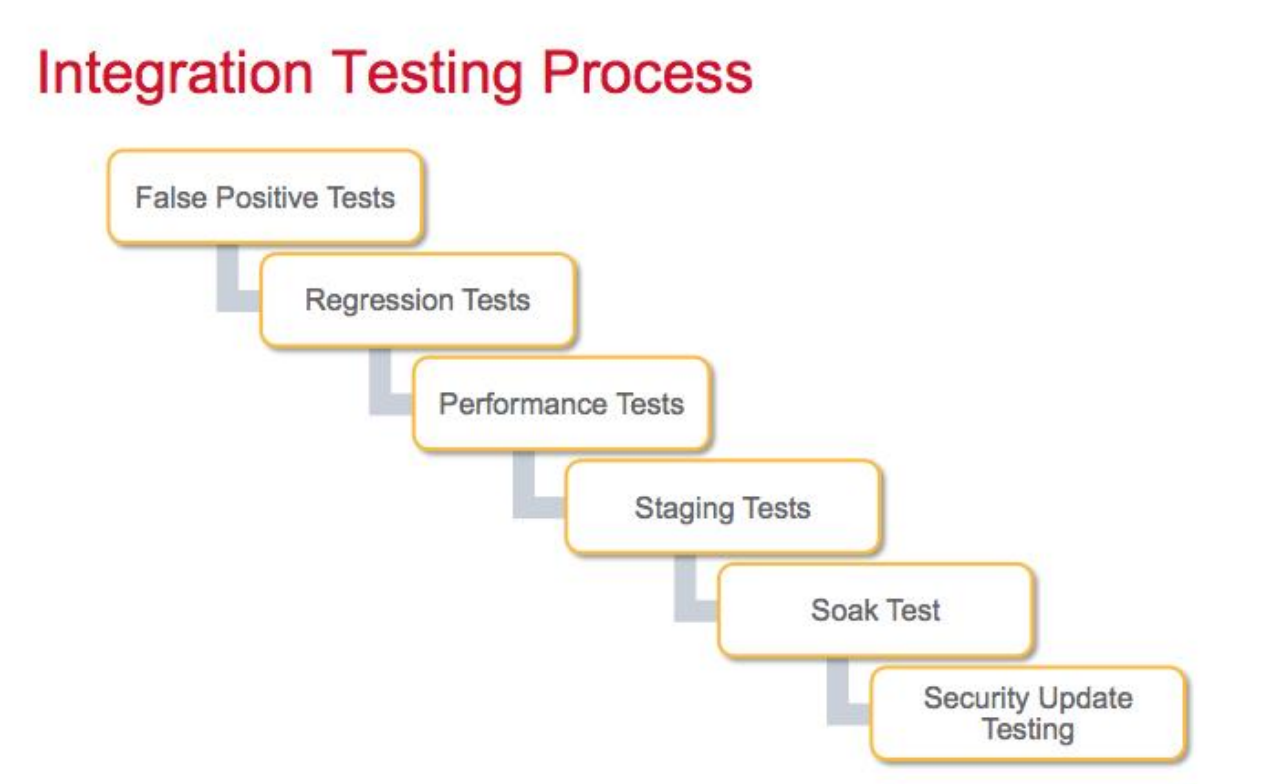


Figure 3 – Rule Update Integration Testing Process

3. Frequently Asked Questions (FAQ)

3.1 What are the various sources of threat information used to create rules?

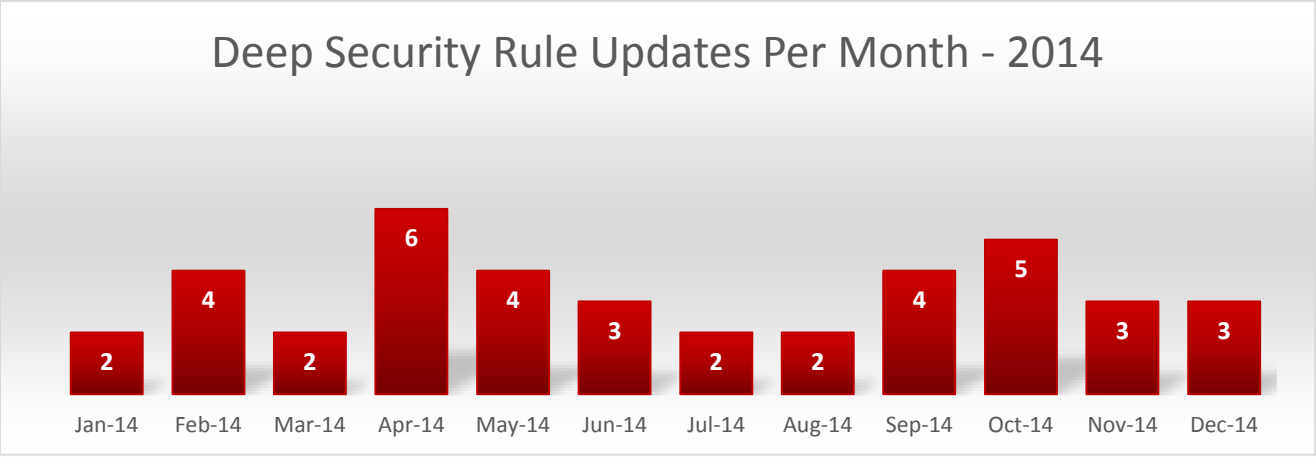
A. Deep Security Intrusion Prevention (IDS/IPS) rules are created based on vulnerability research and threat intelligence collected from several different sources, internal and external. These include:

- Subscriptions to vulnerability research sources
- Programs with software vendors such as Microsoft Active Protections Program (MAPP)
- Trend Micro sources, including malware and attack information from customers, honeypots, and other sources.
- Public information

3.2 What is the frequency of Deep Security Rule Updates (DSRUs)?

- Deep Security Rule Updates are scheduled for 2nd and 4th Tuesdays of the month. The first update is aligned with the Microsoft Patch Tuesday Updates
- Microsoft Patch Tuesday updates are available within 4-6 hours of the Microsoft patch release.
- Often out-of-band updates are released for vulnerabilities with wide spread impact and active exploitation. These are shipped within 12-48 hrs.

Table below summarizes the frequency of updates for the year 2014.



Deep Security Rule Update Frequency

3.3 What time frame are Deep Security Rule Updates made available for various vulnerabilities?

A. Development and delivery of Intrusion Prevention rule are provided on a best effort basis, based on type of software, remote exploitability, available of vulnerability information and severity.

Delivery Targets for Security Updates:	Criteria	Typical Time Frame
Microsoft Patch Tuesday	Microsoft Monthly security updates (Patch Tuesday)	Typically within 4-6 hours
Emergency Updates	Emergency updates for serious vulnerabilities in widespread software (Microsoft out of band patches, Heartbleed, Shellshock)	Typically within 24 hours
Scheduled Updates	Vulnerabilities with CVSS 9.0 - 10	Next scheduled Rule Update
	Vulnerabilities with CVSS 7.0 – 9.0	Within 2 Rule Updates from the date of publication
	Vulnerabilities with CVSS 4.0 – 7.0	Within 3 Rule Updates from the date of publication

3.4 Which software vulnerabilities does Deep Security provide protection for?

A. As described in this document, multiple criteria are used to determine if protection is provided for a specific software vulnerability. The following table provides a summary of the software categories Deep Security has provided protection for in the past.

	2013-14	Before 2013	Total
Platforms	**119**	**458**	**577**
Windows OS and Core Services	49	295	**344**
Non-Windows OS and Core Services	70	163	**233**
Server Applications	**185**	**965**	**1150**
Web Servers	13	142	**155**
Application Servers	73	121	**194**
Web Console/Management Interfaces	31	141	**172**
Database Servers	10	99	**109**
DHCP, FTP, DNS servers	8	41	**49**
Mail Server	6	94	**100**
Directory Server/Services	2	22	**24**
HP Products	25	54	**79**
Backup Software	8	52	**60**
News, Media Streaming	-	5	**5**
PPTP Server	-	1	**1**
Anti Spam Server	1	7	**8**
Other Applications (best effort)	8	186	**194**

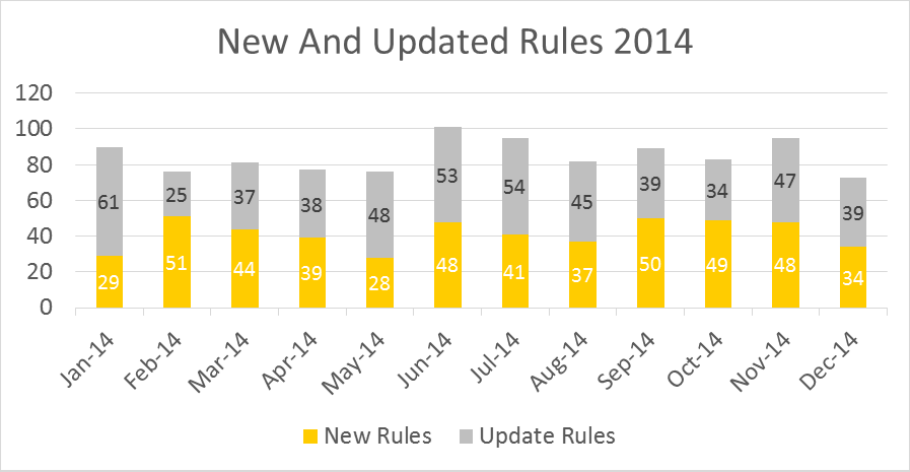
Desktop Applications	411	1106	1517
Miscellaneous/Generic Detection	6	67	**73**
Browsers	227	406	**633**
DHCP, DNS, FTP Clients	-	40	**40**
PDF Readers	36	72	**108**
Browser Plugins and media players	94	227	**321**
Dependent Libraries	10	8	**18**
Microsoft Office	22	177	**199**
Media Client	7	44	**51**
Microsoft products (other than office)	6	18	**24**
Others (best effort)	3	47	**50**

Application Control	72	72
File Sharing software/P2P	20	
Miscellaneous	8	
Instant Messaging	15	
Email clients/protocols	10	
Remote Administration Tools	8	
Web Browsers	6	
Web Media	5	

3.5 How many rules are shipped every month?

A. Every month we ship, on average, 40 new rules and update about the same every month. Rules are updated when more threat information is available, or to fix any discovered issues.

The following graph summarizes the number of new and updated rules in 2014.



3.6 Does Deep Security provide protection for unsupported/end of life Operating Systems (e.g. Windows XP and Windows 2000) and Applications? Will Trend Micro Deep Security support Windows 2003 after End Of Life on July 14, 2015?

A. Yes. This is one of the advantages of the Deep Security platform. Its host- based Intrusion Prevention capabilities help to detect and prevent threats even before the malicious network packets reach your applications. It helps you protect against new vulnerabilities that are uncovered in these platforms and applications, and discover when malicious changes happen on your systems.

While you plan your transition from these platforms, Deep Security helps mitigate vulnerabilities and reduce your exposure via:

- Intrusion Prevention System shielding against new vulnerabilities.
- Integrity Monitoring System – which keeps an eye on your platform and application assets e.g. files, data, registry, installed software etc. and alert you about its integrity.
- Anti-Malware module keeps your system clear of any malware, spyware or backdoors, remote access Trojans etc.

This, additionally, helps you maintain your compliance requirements by shielding vulnerabilities and threats and buys you time for migration.

3.7 How long will the above (e.g.: Windows 2003) be supported?

A. Support for the specified unsupported platforms (Windows XP, Windows 2000, and Windows 2003) will be supported at least until 2017. This will allow organizations to make a secure transition to a new platform.