User Documentation

Web Traffic Security

University of Stavanger

Table of content

UiS Web Traffic Security

Background

In accordance with the recommendations from the UiS Risk and Vulnerability Assessment (RVA), UiS has acquired a product for safe web browsing, Trend Micro InterScan Web Security Virutal Appliance (IWSVA)

Trend Micro IWSVA will be used by UiS to prevent malware from the internet reaching UiS users' workstations through web browsing of file transfers.

Infection with malicious code through web browsing may occur if a user accesses a web site infected with spyware, hidden redirection to a second web site, hidden malicious Java or ActiveX code, cross-site scripting or other advanced malware.

The majority of web sites that are infected with malware are legitimate web sites which have been compromised.

Why is UiS introducing Web Traffic Security?

Today's threat profile for hacker attack via the internet is characterized by organized crime, which have used the development of the internet to create a robust underground economy. Two main challenges characterize today's security solutions:

- A dramatic shift in the treat profile has produced much more complex threats.

- An explosion in the number of threats has meant that traditional protection against malware based on downloading of signature files, such as anti-virus software, often is too slow to detect and protect against new and sophisticated malware, and demands increasingly frequent downloads.

A solution is therefore required which rapidly stops new malware, and which is capable of recognizing behavior which in isolation may appear harmless, but can be recognized as threats or attack by correlation with other information.

How does Web Traffic Security work?

Web Traffic Security works by intercepting user traffic to the internet and sending this to UiS Internet Gateway (Trend Micro IWSVA servers). The Trend IWSVA servers verify the URL against its Web Reputation Filter and stops traffic to a web site recognized as containing malicious code. Return traffic from a web site is also checked for malware, and any malware is removed or stopped before it reaches the users workstation.

UiS Internet Gateway servers will be configured to stop malicious code only, and will not filter which web sites a user may access.

What does the user need to do?

Web traffic to the internet from UiS users will automatically be sent via UiS Internet Gateway and no action or configuration is required for the user to be able to use safer web browsing.

How does Trend IWSVA work?

Trend Micro InterScan Web Security Virtual Appliance (IWSVA) uses both local and distributed (in-the-cloud) security components. The distributed security components are located in Trend Micro Smart Protection Network.

A. Distributed Security Components- Trend Micro Smart Protection Network

Trend Micro Smart Protection Network consists of the following main components:

1. Web Reputation Service
2. Email Reputation
3. File Reputation
4. Correlation with Behaviour Analysis
5. Smart Feedback
6. Threat Intelligence

1. Web Reputation Service (WRS)

WRS is a cloud based service which uses domain reputation databases to score the security risk for a given web domain (for example uis.no), web pages and objects on a web page based on age, how often a domain is moved between Internet Service Providers (ISPs), and indications of suspicious activity trough typical malware behavioral pattern.

The Web Reputation service is continuously updated, and contents from web pages that have a bad score are stopped before it reaches the users network or workstation.

The reply from a web server is further scanned according to HTTP and FTP scan rules configured on the local Trend IWSVA server before it is sent to the user. Local IWSVA scanning and filter services include URL Filtering, Antivirus and Spyware,

The Trend IWSVA server uses a Web Reputation Cache in order to reduce the need to query the cloud based service, this minimizes delay and reduces the time it takes to make a HTTP lookup.

If no score exists for a requested content, and the Trend IWSVA server receives a score of "unknown", the following two processes are activated:

- Trend Micro's cloud based Web Reputation service starts an automatic process that crawls through the requested web page and analyses the content. The Trend Web Reputation Database is updated with the results and the next request for the same web content is serviced by the Web Reputation service.

- The Trend IWSVA server scans the unknown web content with its local scan service. The scan results are sent back to the cloud based Web Reputation service through the Page Analysis and Feedback loop.

2. File Reputation

Cyber criminals often move indvidual files with malicious code from one web page to another to avoid discovery. This makes checking the file's reputation an important security component. File Reputation technology verifies the file reputation against the

Trend File Reputation cloud based service prior to allowing a user to download the file. File Reputation verification also applies to files sent as attachment in emails.

3. Correlation and Behavior Analysis
Correlation and Behavior analysis is a Trend Micro background service which correlates activities from different Smart Protection Network components to see if a pattern indicating malicious intent can be found.

4. Smart Feedback
Trend Micro products installed at customer sites send information about newly identified threats back to the Trend Smart Protection Network.

B. Local Security Components:

The following local security components are used by the Trend IWSVA Scan Engine.

1. URL Filtrering
   URL Filtrering is based on classification of URLs. Trend IWSVAs URL Filtering service correlates its Security Categories with Trend’s Web Reputation Service database. This means that the classification of URLs is continuously updated with new information.
2. AntiVirus
3. Spyware
4. Heuristics
5. True File Type
6. Applet & ActiveX
7. Others

Protocols and traffic flow

UiS Web Traffic Security using Trend WSVA will protect the following internet traffic:

- **HTTP**

Tabell 1 Protocols and traffic flow

Web access methode	Description	What does Trend IWSVA do?
http	Unencrypted connection to a web page, data is sent in the clear between the user and the web page. It is the web page (URL) which defines the access method used, either unencrypted using http or encrypted using https.	1) http requests are checked either against local cache or against Trend Smart Protection Network. 2) Depending on the result, the request is sent to the internet web server. 3) Return traffic from the web server is scanned by the Trend IWSVA server before it is sent to the user.

What type of malware that will be stopped?

Some types of malware are listed below:

Phishing

If Trend IWSVA recognizes a web page as a Phishing URL, the user's traffic is stopped before it reaches the web page.

Phishing definition: A fraudulent collection of confidential information. This can be done by offering an email message or Web site that poses as a communication from a legitimate business, which requests information for the purpose of identity theft.

Spyware

If Trend IWSVA recognizes that a web page contains a program that secretly collects confidential information about the user, the users traffic to this program is stopped.

Spyware definition: A hidden but legal program that secretly collects confidential information. Spyware monitors a user's computing habits and personal information, and then sends this information to third parties without the user's approval.

Virus accomplice

If Trend IWSVA recognizes malicious behaviour in a users's outgoing HTTP request, then this is a sign that the user's workstation is infected with spyware or trojans, and the traffic is stopped.

Virus accomplice definition: An outbound HTTP request due to known behavior of malicious code—the malicious code could either send the information out or download further components from a certain URL. These are the symptoms of a spyware or Trojan infection.

Disease Vector

If Trend IWSVA recognizes that a web page is set up with the sole purpose of spreading malware, then traffic to this web page is stopped.

Disease vector definition: A Web site that exists only for a malicious purpose

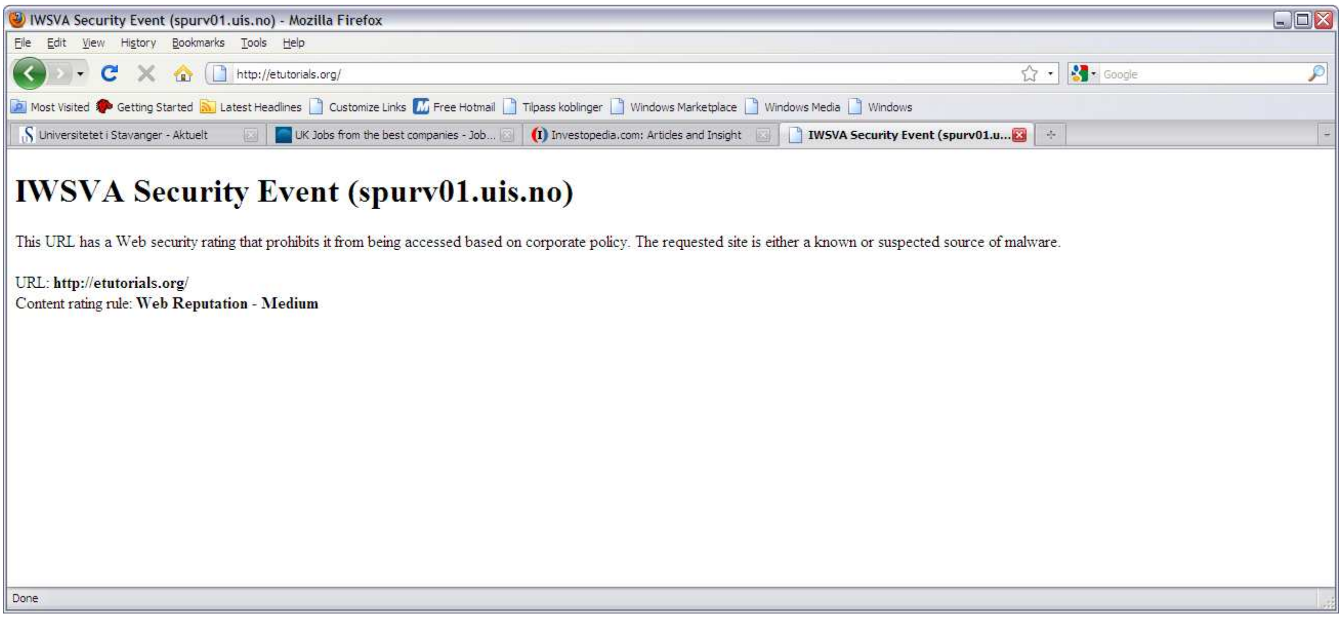
What messages may a user receive?

The user will be notified in his/her web browser if Trend IWSVA discovers malicious code in a web page.

The notification that is given will vary depending on the type of malicious code that is detected.

Exampel : URL blocking based on- Web Reputation

If a user attempts to go to a web page which contains malicious code, then a message similar to the one shown in the figure below will be sent to the user.


IWSVA Security Event (spurv01.uis.no) - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://etutorials.org/
Google
Most Visited Getting Started Latest Headlines Customize Links Free Hotmail Tilpass koblinger Windows Marketplace Windows Media Windows
Universitetet i Stavanger - Aktuelt
UK Jobs from the best companies - Job...
Investopedia.com: Articles and Insight
IWSVA Security Event (spurv01.u...
Done

IWSVA Security Event (spurv01.uis.no)

This URL has a Web security rating that prohibits it from being accessed based on corporate policy. The requested site is either a known or suspected source of malware.

URL: **http://etutorials.org/**
Content rating rule: **Web Reputation - Medium**

Are there other changes?

File Download

When a user downloads a file from the internet, the Trend IWSVA servers will scan the file for virus or other malware. This means that the user sometimes may see a short pause in the download while the scanning takes place, the file is subsequently downloaded as normal.