VMware NSX Network Detection and Response ICAP Integration

Contents

VMware NSX Network Detection and Response ICAP Integration

ICAP Integration enables the Sensor to offload the analysis and blocking of malicious content.

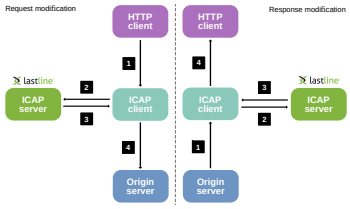
About ICAP Integration

The VMware NSX Network Detection and Response integration allows a third party proxy server or security appliance to use the *Internet Content Adaptation Protocol (ICAP)* (https://tools.ietf.org/html/rfc3507) protocol to offload its HTTP traffic to the Sensor for the analysis and blocking of malicious content.

VMware officially supports integration with *Squid* (http://www.squid-cache.org//) proxies (*version 3.5.x* (http://www.squid-cache.org/Versions/v3/3.5/)). Any third-party proxy that correctly implements *RFC 3507* (https://tools.ietf.org/html/rfc3507) should be able to leverage the ICAP integration without issues.

ICAP Concepts

The following figure shows an ICAP transaction.



Two endpoints are involved in the transaction:

- ICAP client — A third party proxy or security appliance that is forwarding HTTP data between an internal host and an external origin server serving the content.
- ICAP server — The Sensor leveraging ICAP communication to monitor the HTTP traffic relayed by the client.

The *ICAP specification* (http://www.icap-forum.org/documents/specification/rfc3507.txt) defines two basic operation modes for an ICAP client.

- Request modification (REQMOD) — An ICAP client setup to use `REQMOD` requests will relay to the ICAP server all the incoming HTTP requests before relaying them to the origin server. The Sensor has the capability to use this type of request to prevent infected clients from exfiltrating data to low reputation hosts. The Sensor also has the capability to inspect files and documents being pushed towards external services in the context of HTTP `POST` submissions.
- Response modification (RESPMOD) — When set in this mode, an ICAP client will share the HTTP response with the Sensor generated by the origin server before delivering it back to the ICAP client. Most ICAP client implementations deliver in a `RESPMOD` request both the HTTP client request and its response. In this scenario, the Sensor has the opportunity to inspect the HTTP request that has been sent out to the server as well as the server response.

The Sensor can handle both `REQMOD` and `RESPMOD` requests at the same time, offering the maximum level of protection. Most third party appliances support the configuration of both operation modes on the same ICAP endpoint. Where this was not possible, each request mode offers different types of protection:

Requirement	Request type
Prevent clients from exfiltrating data towards low reputation domains.	`REQMOD`
Prevent submission of malicious documents to APIs by means of HTTP `POST` requests.	`REQMOD`

Requirement	Request type
Prevent clients from downloading malicious documents.	`RESPMOD`
Detect interactions towards low reputation domains. Note that in this case, `RESPMOD` is unable to prevent requests from reaching the remote endpoint, so it will not block the exfiltration itself.	`REQMOD`, `RESPMOD`

The Sensor supports *ICAP Preview* (https://tools.ietf.org/html/rfc3507#section-4.5), if implemented by the client. Rather than delivering the entire HTTP transaction to the ICAP service, a client can start by delivering the beginning of such transaction to the ICAP service. The ICAP service then decides whether the transaction should be skipped or fully delivered. The ICAP implementation has the capability to derive the file type of the document being served from preview content. From this, it can determine whether the file type is of potential security interest.

Configure ICAP integration

Configuration Steps

ICAP integration is configured on the PROXY tab of the User Portal/Manager Web UI.

Procedure

Step 1: Login to the Web UI

Using your Web browser, login to the User Portal at *https://user.lastline.com/* (https://user.lastline.com/) (for EMEA customers *https://user.emea.lastline.com/* (https://user.emea.lastline.com/)) for a hosted deployment or the Manager Web UI for an On-Premises installation.

Step 2: Navigate to the Admin page

From the Main navigation menu, click **[Admin]**. On the Admin page, select **[Appliances]** from left sidebar menu. For most users, the Appliances → Overview tab is initially displayed by default.

Step 3: Select the Configuration tab

Click the Configuration tab. You are prompted to select an appliance for configuration. Click the **[Appliance:]** link at the top of the page and select an appliance from the Select Appliance pop-up. Select an appropriate appliance: ICAP integration is supported on the Sensor only.

Step 4: Select the Proxy tab and then enable ICAP

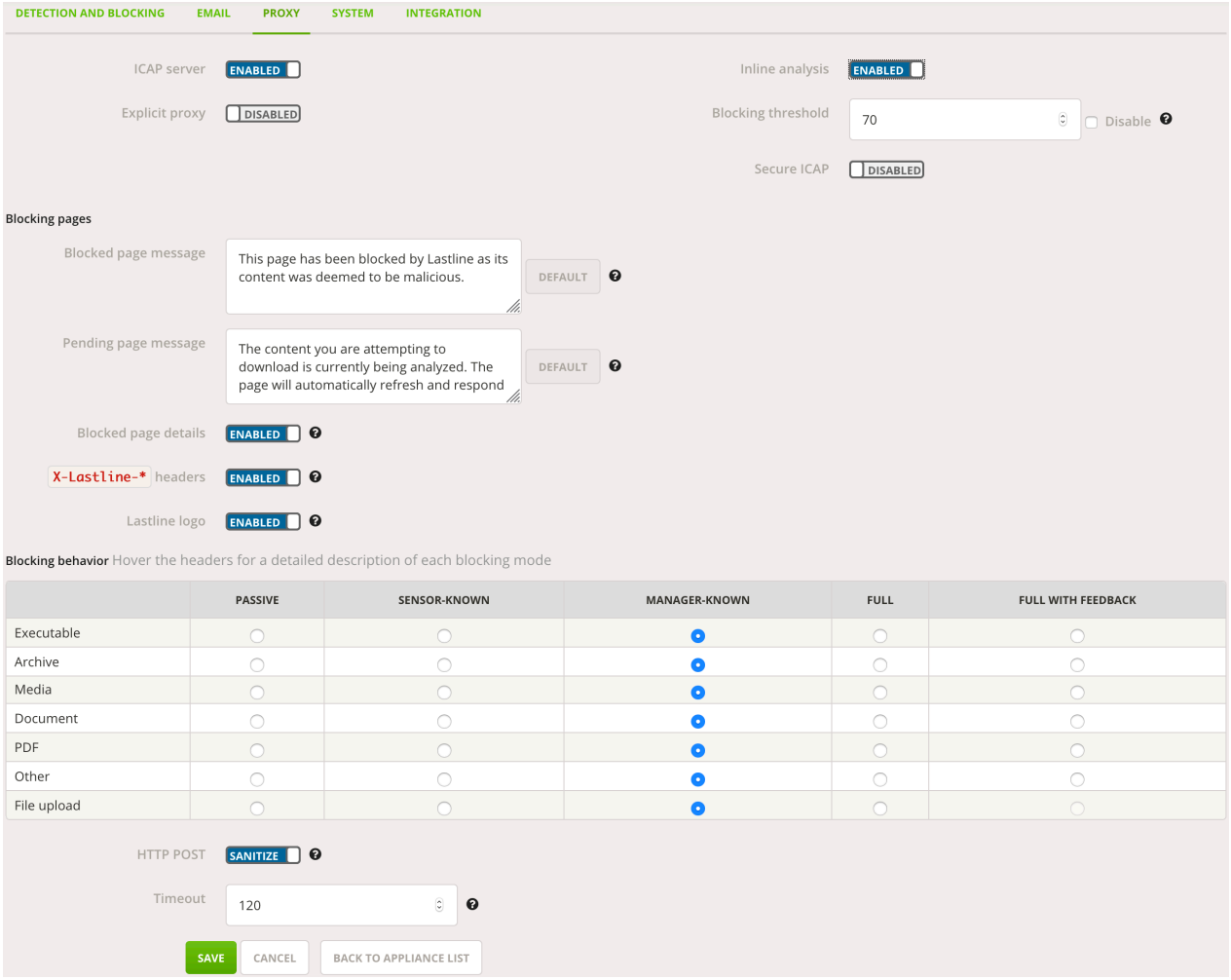
Click the PROXY tab. By default, ICAP server is **[DISABLED]**. Click the button to toggle it to **[ENABLED]**.

Step 5: Enable inline analysis

If INLINE ANALYSIS is **[ENABLED]**, the ICAP capability can act upon the transfer of malicious files. You should enable this option. It is only accessible after you enable ICAP server.

Step 6: Set other ICAP options

There are a number of other options you can set on the PROXY tab:



SECURE ICAP — If **[ENABLED]**, the option allows ICAP-aware HTTP proxies to connect to the Sensor by means of a secure connection. The default port is 11344.

Blocking threshold — Sets a threshold value. Any content with a score above that value will be sanitized. You can disable the clocking threshold.

Blocking pages — When the Sensor blocks a transaction deemed to be malicious, it replaces the original content with simple self-contained HTML pages providing details of its reasons. There are two options: BLOCKED PAGE MESSAGE and PENDING PAGE MESSAGE. Each can be customized. Enabling BLOCKED PAGE DETAILS inserts the details into the pages. You can also enable X-LASTLINE-* HEADERS which include details in the metadata.

Blocking behavior — You can configure the blocking policy to be applied by the ICAP daemon for each type of file. The file types are Executable, Archive, Media, Document , PDF, Other, and File upload. The following policies can be applied:

- PASSIVE — No blocking is attempted on this type of file, but any relevant content will be analyzed.
- SENSOR-KNOWN — Block all artifacts known to be malicious by the Sensor (listed in its local cache). This method offers the lowest levels of protection but ensures minimal lag.
- MANAGER-KNOWN — Block all artifacts known to be malicious by the Manager. These data are listed in the Manager cache and shared across all managed appliances.
- FULL — This mode allows the proxy to stall an ICAP request for as long as necessary to provide a verdict on the file, within the limits set by the ICAP timeout. Depending on the client implementation, this may cause the transaction to appear as unresponsive for long periods of time (in the order of minutes in some cases).

  This blocking mode is particularly suitable for the integration with third party proxies that implement mechanisms to improve the user experience. Such mechanisms may include data trickling or “patience pages”, providing feedback to the user.
- FULL WITH FEEDBACK — This mode will generate “patience pages” that provide feedback to the user on the analysis progress. These mechanisms have been tested exclusively with the squid proxy. They may lead to unwanted side-effects when using third-party proxies, which may implement caching mechanisms that disrupt the VMware NSX Network Detection and Response operation. Such third party proxies often implement their own mechanisms to improve user experience, and therefore may perform better with the Full blocking mode.

HTTP POST — Determines what the Sensor does with malicious content. If **[BLOCK]**, the Blocked page message is sent to the destination. If **[SANITIZE]**, the Sensor removes the malicious content before it forwards the request to its destination.

TIMEOUT — Sets the maximum time in seconds that the proxy server is allowed to delay the request.

Step 7: Save the Proxy configuration

When you are done, click the **[SAVE AND DEPLOY]** button to enable your changes. The Sensor will start an ICAP service which is accessed at the following URI:

```
icap://<sensor_IP>:1344/lastline
```

Note: The Select Appliance pop-up lists the IP address of the Sensor.

Configure ICAP Client

ICAP configuration for the client side strongly depends on the vendor. The following example is a working configuration to integrate *Squid 3.5.x* (http://www.squid-cache.org/Versions/v3/3.5/) with the Sensor in ICAP mode:

```
icap_enable on
icap_log /var/log/squid3/icap.log
icap_preview_enable on
icap_preview_size 1024
icap_send_client_ip on
# The lastline-sensor has the ICAP service enabled and reachable on port 1344
icap_service service_lastline_reqmod reqmod_precache bypass=0 icap://lastline-
sensor:1344/lastline
icap_service service_lastline_respmod respmod_precache bypass=0 icap://lastline-
sensor:1344/lastline
adaptation_access service_lastline_reqmod allow all
adaptation_access service_lastline_respmod allow all
```

Note: *lastline-sensor* is the IP address of the Sensor, obtained from Select Appliance pop-up.

Whenever possible it is recommended to enable the capability to share both client and server IP addresses with the ICAP server. Support for this feature varies widely depending on the client implementation. For instance, the Squid proxy currently supports sharing the client IP address, but not the server IP address. When either information is not available, the associated field will be reported as "0.0.0.0" in the Web UI.

Troubleshoot ICAP

The server IP in the UI appears as 0.0.0.0

The ICAP protocol specifies extensions allowing a client to report the IP address of the client and the origin server involved in the HTTP transaction. However, not all ICAP implementations support it. If the information is provided by the ICAP client using the `X-Client-IP` and `X-Server-IP` headers, it will be correctly reported by the Sensor.

X-Lastline headers

Pages analyzed by the ICAP instance may contain additional information on the analysis status by means of additional HTTP headers. The presence of such headers can be disabled from the ICAP configuration, but are often useful to diagnose the blocking decisions.

X-Lastline-Status — Provides information on the state of the object at the time of analysis. The following values are possible:

- new — The specific file hash has not been recently analyzed by VMware NSX Network Detection and Response and a score is not currently available.
- known — The specific file is known and a score is associated to it.
- reputation list — The contacted remote endpoint has low reputation.
- timeout — The process reached its timeout while waiting for the analysis of the file.
- error — An error is preventing the analysis of the file.

X-Lastline-Score — The score currently associated with the file, if known, expressed as a value between 0 and 100.

X-Lastline-Task — The task UUID associated with the analysis of the file. It is possible to use this UUID in order to access the analysis details from the User Portal/Manager Web UI.

Further transaction information is available in the log files on the Sensor. All the available logs are located in the directory `/var/log/c-icap`. This includes the standard `access.log` file containing details on every HTTP transaction inspected by ICAP as well as the associated response code. A second more detailed `processing.log` file contains detailed information on the file processing performed on each HTTP transaction.

ICAP response codes

The following is the list of ICAP status codes that can be returned by the ICAP appliance in response to a client request.

Code	Explanation
`100 Continue`	Response to an ICAP preview in case the preview content was deemed to be interesting for analysis.
`200 OK`	Transaction was received by the ICAP service and analyzed.

Code	Explanation
`204 Unmodified`	The transaction was determined to be benign and can be delivered without modifications.
`400 Bad request`	Malformed or unparseable request.
`404 Service not found`	The service requested in the ICAP request was not found. The service must be `"lastline"`.
`405 Not allowed`	The ICAP method is not allowed by the service.
`408 Request timeout`	The ICAP service gave up waiting for a request and is terminating the connection.
`500 Server error`	The request triggered a bug in the service implementation.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com