# Endace Fusion Connector for Cisco Stealthwatch

## Introduction

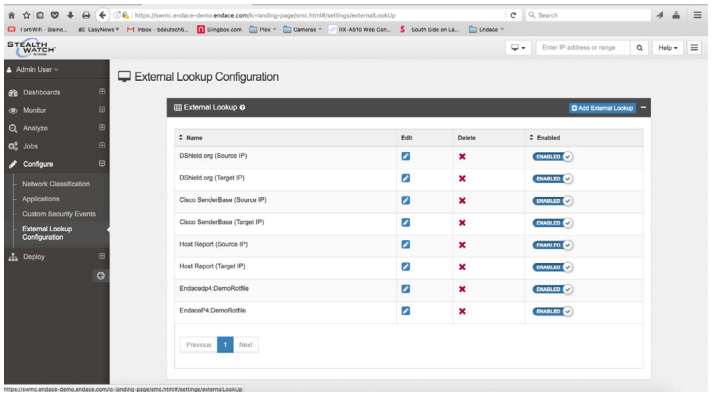
Cisco Stealthwatch is a comprehensive, network telemetry-based security monitoring and analytics solution that streamlines incident response through behavioral analysis; detecting denial of service attacks, anomalous behaviour, malicious activity and insider threats. Based on a scalable enterprise architecture, Stealthwatch provides near real- time situational awareness of all users and devices on the network.

EndaceProbe Network Recorders provide the perfect complement to Stealthwatch by capturing, recording and indexing all traffic on the network down to the nanosecond level. Access to historical network traffic provides context and deterministic root cause for security events flagged by Stealthwatch.

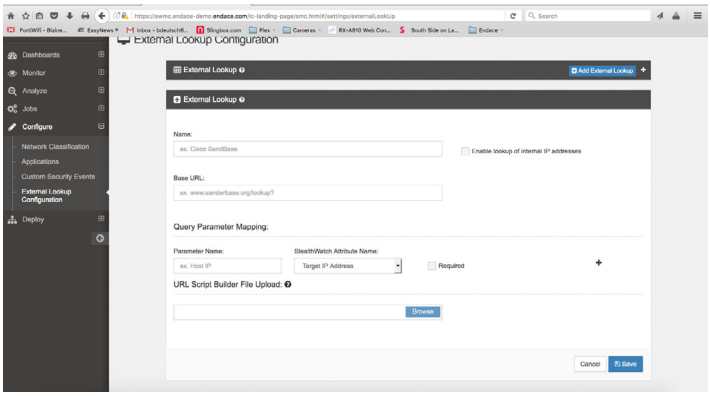
Using the External Lookup feature in the Stealthwatch Management Console (SMC), analysts can seamlessly pivot from an event in SMC through to the associated packet data on the EndaceProbe.

## Creating a Fusion connector through External Lookups

Begin by logging into the Stealthwatch system and navigate to



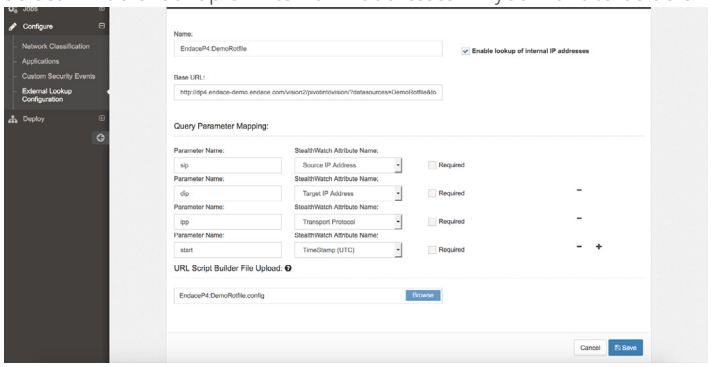

"External Lookup Configuration"




In the upper right hand select the blue "Add External Lookup" button to create a new lookup.

Provide a name that will detail the source of this lookup. The Stealthwatch External Lookup API allows for a query to be sent to multiple Endace Probe and RotationFile systems and processed in parallel. Each combination must have its own external lookup and should be named so as to enable easy identification back to Stealthwatch..

Select "Enable lookup of internal IP addresses" if you want to be able




to query based on internal IP's. This is necessary to investigate internal traffic. Otherwise lookups will only be performed on external public addressing.

The "Base URL" field is critical. In this example the base URL is:

http://dp4.endace-demo.endace.com/vision2/pivotintovision/?datasources=DemoRotfile&tools=trafficOverTime_by_prot&

This example uses the DNS name of the target probe, initiates a vision investigation using Vision2, defines the datasource as a specific "rotation file" and creates the first graph using a "Traffic Breakdown over Time" tool. You can choose any of the Vision2 tools to start with but one must be selected. It is also necessary to add the "&" at the end of the URL to properly form the query. See EDM09-123v5 EndaceVision v2 User Guide page 65 for more details on the Pivot to Vision URL parameters.

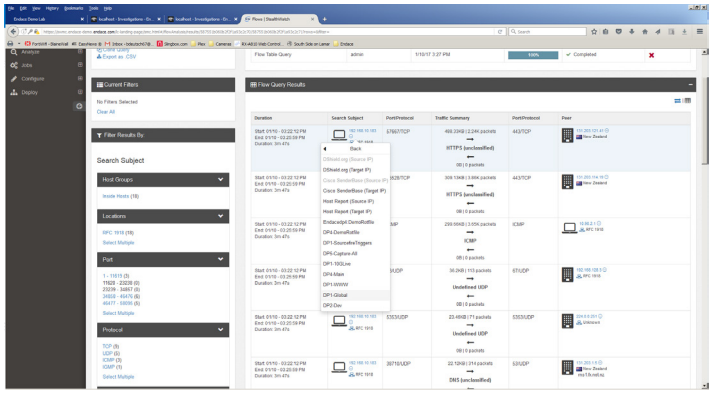
The following Query Parameter Mapping fields allow attributes from the report that the external lookup is triggered from to be mapped to the Endace Pivot to Vision API and automatically appended to the base URL. At least one of Source or Target IP and the Timestamp attribute are required in order for EndaceVision to display useful information.

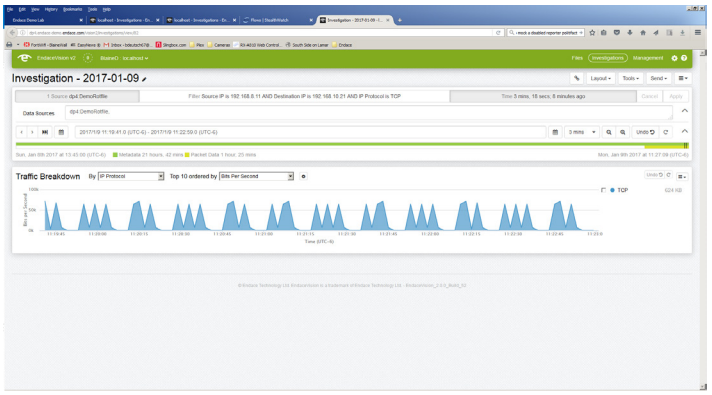
The Endace Pivot to Vision API requires start and end time parameters but Stealthwatch provides a single event time called "TimeStamp", which contains both the start and end time of the event. In order to extract both of these values a script is provided that can be uploaded

through the "URL Script Builder Upload" dialog. Copy and paste this code into notepad and name it the same as the External Lookup, then upload accordingly. Alternatively you can request a copy of the script from product.management@endace.com.

```
import java.text.SimpleDateFormat

def thisTime = new Date();
def String query = "";
int loop = 0;

vendorValues.each { valueOperand ->

 query += (query != "" ? "&" : "");
 if (loop == 0) {
          query += valueOperand.getName() + "=";
 } else if (loop == 1 ) {
  query += "end=";
}
 def String convertedStr = "";
 if (valueOperand.getFromValue() instanceof String || valueOperand.
getFromValue() instanceof Integer) {
  convertedStr = valueOperand.getFromValue().toString();
 } else if (valueOperand.getFromValue() instanceof Date &&
valueOperand.getName() == "start" ) {
          thisTime = valueOperand.getFromValue().time;
convertedStr = new SimpleDateFormat("yyyy-MM-dd'T'HH:mm:ss");

format(thisTime);

  loop += 1;
 }
 String.valueOf('java.lang.Integer');
 query += URLEncoder.encode(convertedStr,"UTF-8");
};

query = baseUrl + query;
return query;
```

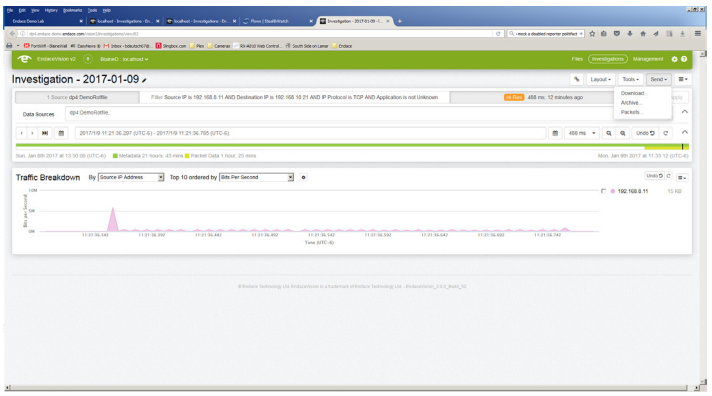
Click Save and repeat this process for each target probe and rotationfile that you plan to run queries against.





## Utilizing the External Lookup

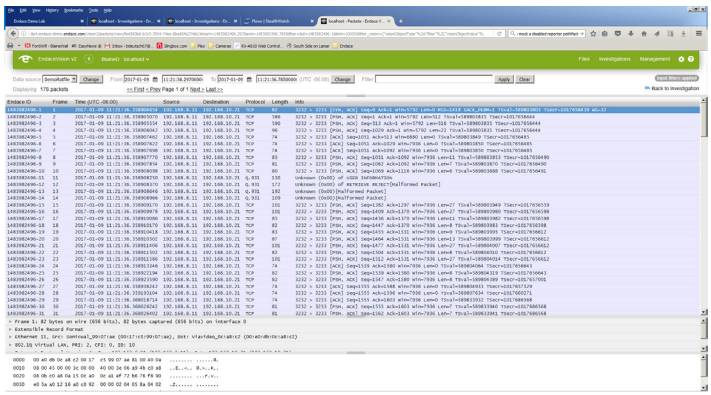
After doing a flow query within Stealthwatch you can right click on an IP and select External Lookup. Choose the appropriate probe and rotationfile and then click to begin the investigation within Vision2.



Once Vision2 launches the resulting lookup can be further refined based on various parameters that will aid in the investigation. Once you have isolated the suspect traffic, a PCAP can be analyzed within Vision2 and/or downloaded and further analyzed with a suitable packet analyzer of your preference.

Select download to get a PCAP file and save to your local PC

Select "Packets" to use the EndacePackets™ analyzer, a built-in, browser-based packet decode similar to Wireshark™, for onboard packet analysis without the need to download packet capture files.





For more information on the Endace portfolio of products, visit: endace.com/products

For further information, email: info@endace.com