White Paper

Transmitting Telemetry Data from Cisco Web and Email Security

As part of their function, the Cisco® Web and Email Security products can provide telemetry data back to Cisco. This data increases the efficacy of web categorization in the Cisco Web Security Appliance (WSA) and of connecting IP reputation for the Cisco Email Security Appliance (ESA).

The telemetry data is provided for the WSA and ESA on an opt-in basis.

Note: This capability is enabled by default during system setup.

The data is transmitted in binary-encoded SSL encrypted packets. The information below provides insight into the data along with specific formatting. WebBase Network Participation (WBNP) and SenderBase Network Participation (SBNP) data is not viewable in a direct log or file format. This data is transmitted in encrypted form. At no time is this data "at rest."

WSA WebBase Network Participation

Cisco recognizes the importance of maintaining your privacy. We do not collect or use personal or confidential information such as usernames and passphrases. Additionally, the file names and URL attributes that follow the hostname are obfuscated to help ensure confidentiality.

When it comes to decrypted HTTPS transactions, the SensorBase Network receives only the IP address, web reputation score, and URL category of the server name in the certificate.

Enabling and Disabling Participation in WBNP and SBNP

Step 1. Choose Security Services > SensorBase. Verify that SenderBase Network Participation is enabled.

If it is disabled, none of the data that the appliance collects is sent back to the SensorBase Network servers.

Step 2. In the Participation Level section, choose one of the following levels:

- **Limited:** Basic participation summarizes server name information and sends MD5-hashed path segments to the SensorBase Network servers.
- **Standard:** Enhanced participation sends the entire URL with unobfuscated path segments to the SensorBase Network servers. This option assists in providing a more robust database and continually improves the integrity of web reputation scores.

Step 3. In the Cisco AnyConnect® Network Participation field, choose whether to include information collected from clients that connect to the Web Security Appliance using the AnyConnect® client. AnyConnect clients send their web traffic to the appliance using the Secure Mobility feature.

Step 4. In the Excluded Domains and IP Addresses field, you may enter any domains or IP addresses to exclude from traffic sent to the SensorBase servers.

Step 5. Submit and commit your changes.

Example Data: Standard Participation

```
# categorized
"http://google.com/": {
    "wbrs": "5.8",
    "fs": {
          "src": "req",
          "cat": "1020"
    },
}
# uncategorized
"http://fake.example.com":{
    "fs": {
      "cat": "-"
    },
}
```

Example Data: Limited Participation

```
The original request from the client was:
http://www.gunexams.com/Non-Restricted-FREE-Practice-Exams
The logged message (in telemetry server) was:
http://www.gunexams.com/76bd845388e0
```

General Security Concerns FAQ

Q. Why should you choose Standard participation over Limited?

A. Cisco web security technologies are known for detecting and identifying new and emerging web exploitation techniques. The Angler exploit kit, for example, has a success rate of 40 percent. It is one of the most effective ways of compromising users on the Internet. Cisco Talos has insight into nearly 17 billion web requests each day, drawing on multiple protection methods, including Cisco AMP technology, to protect our users.

The core component of any holistic security strategy is solid, actionable intelligence. Over the past 10 years Talos has built one of the most comprehensive intelligence-gathering and analysis platforms in the industry. Through the ClamAV, Snort, Immunet, SpamCop, SenderBase, Threat Grid, and Talos user communities, Talos receives valuable intelligence that no other security research team can match. In addition, through collaboration with users and customers around the globe in our Crete (formerly SPARK) program, Talos is able to detect regionalized and language-specific threats as they emerge.

Standard participation on the WSA enriches the overall Talos threat intelligence process. Customers with Standard participation stand to benefit by being part of a larger threat intelligence community, sharing and consuming fast information about zero-day exploits, and fulfilling their goal of protecting their end users.

Q. Where is the data stored?

A. Appliance telemetry is stored in Cisco's U.S.-based data centers.

Q. Who has access to it?

A. Access is limited to Cisco Security Business Group personnel who analyze and use the data to create actionable intelligence.

Q. What is the retention time?

A. There is no data retention or expiration policy regarding appliance telemetry. Data may be kept indefinitely or may be deleted for various reasons, including but not limited to downsampling and aggregation, storage management, age, relevance to current and future threats, and so on.

Q. Is the customer serial number or public IP address stored in the Talos categorization database?

A. No. Only URLs and categories are retained. The WBNP packet does not contain source IP information.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-738822-00 04/17