Web Base Network Participation (WBNP) and Sender Base Network Participation (SBNP)

Contents

Introduction

The Cisco Web and Email Content Security products can provide telemetry data back to Cisco and Talos to increase the efficacy of web categorization in the Web Security Appliance (WSA) and connecting IP reputation for the Email Security Appliance (ESA).

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

The data is transmitted via binary encoded SSL encrypted packets. The included attachments provide insight into the data, specific formatting and descriptions for the data that is being transmitted. 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, and does not collect or use personal or confidential information such as usernames and passphrases. Additionally, the file names and URL attributes included with the hostname are obfuscated to ensure confidentiality.

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

For complete information, please review the WSA User Guide for the version of AsyncOS for Web Security currently running on your appliance. Please see "The Cisco SensorBase Network" in the User Guide.

ESA - SenderBase Network Participation

Customers participating in the SenderBase Network allow Cisco to collect aggregated email traffic statistics about their organization, increasing the utility of the service for all who use it. Participation is voluntary. Cisco only collects summary data on message attributes and information about how different types of messages were handled by Cisco appliances. For example, Cisco does not collect the message body or the message subject. Personally identifiable information and information that identifies your organization is kept confidential.

For complete information, please review the ESA User Guide for the version of AsyncOS for ESA Security currently running on your appliance. Please see the "SenderBase Network Participation" chapter in the User Guide.

General Security Concerns FAQ

Question:	Where is the data collected stored?
Answer:	Appliance telemetry is stored in Cisco US-based data centers.
Question:	Who has access to the data collected and stored?
Answer:	Access is limited to Cisco SBG personnel who analyze/use the data to create actionable intelligence.
Question:	What is the retention time of the data collected?
Answer:	There is no data retention/expiration policy regarding appliance telemetry. Data can be kept indefinitely or can be deleted for various reasons including but not limited to down-sampling/aggregation, storage management, age, relevance to current/future threats, and so on.
Question:	Are customer serial number(s) or public IP address(es) stored in the Talos categorization database?
Answer:	No, only URL and categories are retained. The WBNP packet does not contain source IP information.

Operation

This section details operation, the type of data (by description), and a sample data to demonstrate the information that would be transmitted:

- SBNP - Specific data types (fields) and sample data related to Email Security
- WBNP - Specific data types (fields) and sample data related to Web Security
- Threat Detection Operation - General overview of Threat Detection from a operational perspective

SenderBase (Email) Network Participation

Statistics shared per Emailappliance

Item	Sample Data
MGA Identifier	MGA 10012
Timestamp	Data from 8 AM to 8:05 AM on July 1, 2005

Software Version Numbers	MGA Version 4.7.0
Rule Set Version Numbers	Anti-Spam Rule Set 102
Anti-virus Update Interval	Updates every 10 minutes
Quarantine Size	500 MB
Quarantine Message Count	50 messages currently in quarantine
Virus Score Threshold	Send messages to quarantine at threat level 3 or higher
Sum of Virus Scores for messages entering quarantine	120
Count of messages entering quarantine	30 (yields average score of 4)
Maximum quarantine time	12 hours
Count of Outbreak quarantine messages broken down by why they entered and exited quarantine, correlated with Anti-Virus result	50 entering quarantine due to .exe rule 30 leaving quarantine due to manual release, and all 30 were virus positive
Count of Outbreak quarantine messages broken down by what action was taken upon leaving quarantine	10 messages had attachments stripped after leaving quarantine
Sum of time messages were held in quarantine	20 hours

Statistics shared per IP address

Item	**Sample Data**	**Standard Participation**	**Limited Participation**
Message count at various stages within the appliance	Seen by Anti-Virus engine: 100 Seen by Anti-Spam engine: 80		
Sum of Anti-Spam and Anti-Virus scores and verdicts	2,000 (sum of anti-spam scores for all messages seen)		
Number of messages hitting different Anti-Spam and Anti-Virus rule combinations	100 messages hit rules A and B 50 messages hit rule A only		
Number of Connections	20 SMTP Connections		
Number of Total and Invalid Recipients	50 total recipients 10 invalid recipients		
Hashed Filename(s): (a)	A file <one-way-hash>.pif was found inside an archive attachment called <one-way-hash>.zip.	Unobfuscated Filename	Hashed Filename
Obfuscated Filename(s): (b)	A file aaaaaaa0.aaa.pif was found inside a file aaaaaaa.zip.	Unobfuscated Filename	Obfuscated Filename

URL Hostname (c)	There was a link found inside a message to www.domain.com	Unobfuscated URL Hostname	Obfuscated URL Hostname
Obfuscated URL Path (d)	There was a link found inside a message to hostname www.domain.com, and had path aaa000aa/aa00aaa.	Unobfuscated URL Path	Obfuscated URL Path
Number of Messages by Spam and Virus Scanning Results	10 Spam Positive 10 Spam Negative 5 Spam Suspect 4 Virus Positive 16 Virus Negative 5 Virus Unscannable		
Number of messages by different Anti-Spam and Anti-Virus verdicts	500 spam, 300 ham		
Count of Messages in Size Ranges	125 in 30K-35K range		
Count of different extension types	300 “.exe” attachments		
Correlation of attachment types, true file type, and container type	100 attachments that have a “.doc” extension but are actually “.exe” 50 attachments are “.exe” extensions within a zip		
Correlation of extension and true file type with attachment size	30 attachments were “.exe” within the 50-55K range		
Number of messages by Stochastic Sampling results	14 messages skipped sampling 25 messages queued for sampling 50 messages scanned from sampling		
Number of messages that have failed DMARC verification	34 messages have failed DMARC verification		

Notes:

(a) Filenames are encoded in a 1-way hash (MD5).

(b) Filenames are sent in an obfuscated form, with all lowercase ASCII letters ([a-z]) replaced with “a,” all uppercase ASCII letters ([A-Z]) replaced with “A,” any multi-byte UTF-8 characters replaced with “x” (to provide privacy for other character sets), all ASCII digits ([0-9]) replaced.

(c) URL hostnames point to a web server providing content, much as an IP address does. No confidential information, such as usernames and passwords, are included.

(d) URL information included with the hostname is obfuscated to ensure that any personal information of the user is not revealed.

Statistics Shared per SDS Client

Item	**Sample Data**
TimeStamp	
Client version	
Number of requests made to the Client	
Number of requests made from the SDS Client	
Time results for DNS Lookups	
Server response time results	
Time to establish connection to server	
Number of connections established	
Number of concurrent open connections to server	
Number of service requests to WBRS	
Number of requests which hit local WBRS cache	
Size of local WBRS cache	
Response time results from remote WBRS	

AMP SBNP telemetry data

Format	Sample Data
amp_verdicts' : { ("verdict", "spyname", "score", "uploaded", "file_name"),	
("verdict", "spyname", "score", "uploaded", "file_name"),	
("verdict", "spyname", "score", "uploaded", "file_name"),	
……….	
("verdict", "spyname", "score", "uploaded", "file_name"),	
}	
Description	
Verdict - of the AMP reputation query	malicious/clean/unknown
Spyname- Name of the malware detected	[Trojan-Test]
Score - AMP assigned reputation score	[1-100]
Upload - AMP cloud indicated to upload the file	1
File Name - Name of the file attachment	abcd.pdf

WebBase (Web) Network Participation

Statistics shared per web request

Item	**Sample Data**	**Standard Participation**	**Limited Participation**
Version	coeus 7.7.0-608		

Serial Number			
SBNP sampling factor (Volume)			
SBNP sampling factor (Rate)	1		
Destination IP & Port		unobfuscated URL path segments	hashed URL path segments
Anti-Spyware chosen malware category	Skipped		
WBRS Score	4.7		
McAfee malware category verdict			
Referer URL		unobfuscated URL path segments	hashed URL path segments
Content Type ID			
ACL Decision Tag	0		
Legacy Web Categorization			
CIWUC Web Category and decision source	{'src': 'req', 'cat': '1026'}		
AVC App Name	Ads and Tracking		
AVC App Type	Ad Networks		
AVC App Behavior	Unsafe		
Internal AVC Result Tracking	[0,1,1,1]		
User agent tracking via indexed data structure	3		

Advanced Malware Statistics per web request

AMP Statistics	
Verdict - of the AMP reputation query	malicious/clean/unknown
Spyname- Name of the malware detected	[Trojan-Test]
Score - AMP assigned reputation score	[1-100]
Upload - AMP cloud indicated to upload the file	1
File Name - Name of the file attachment	abcd.pdf

End User Feedback statistics feed

Statistics Shared per End User Miscategorization Feedback	
Item	**Sample Data**
Engine ID (numeric)	0
Legacy Web Categorization code	
CIWUC Web Categorization Source	‘resp’ / ‘req’
CIWUC Web Category	1026

Example data provided – Standard participation

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

```
# uncategorized
"http://fake.example.com": {    "fs": {
      "cat": "-"
    },
}
```

Example data provided – Limited participation

- Original request from client: www.gunexams.com/Non-Restricted-FREE-Practice-Exams
- Message logged (in telemetry server): http://www.gunexams.com/76bd845388e0

Full WBNP Decode

Statistics Shared per Cisco Appliance

Item	**Sample Data**
Version	coeus 7.7.0-608
Serial number	0022190B6ED5-XYZ1YZ2
Model	S660
Webroot enabled	1
AVC enabled	1
Sophos enabled	0
Response Side Categorization enabled	1
Anti-Spyware Engine enabled	default-2001005008
Anti-Spyware SSE version	default-2001005008
Anti-Spyware Spycat Definitions version	default-8640
Anti-Spyware URL Blocklist DAT version	
Anti-Spyware URL Phishing DAT version	

Anti-Spyware Cookies DAT version	
Anti-Spyware Domain Blocking enabled	0
Anti-Spyware Threat Risk Threshold	90
McAfee enabled	0
McAfee Engine version	
McAfee DAT version	default-5688
WBNP Detail Level	2
WBRS Engine version	freebsd6-i386-300036
WBRS component versions	categories=v2-1337979188,ip=default-1379460997,keyword=v2-1312487822,prefixcat=v2-1379460670,rule=default-1358979215
WBRS Blocklist Threshold	-6
WBRS Allowlist Threshold	6
WBRS enabled	1

Secure Mobility enabled	0
L4 Traffic Monitor enabled	0
L4 Traffic Monitor Blocklist version	default-0
L4 Traffic Monitor Admin Blocklist	
L4 Traffic Monitor Admin Blocklist ports	
L4 Traffic Monitor Allowlist	

L4 Traffic Monitor Allowlist ports	
SBNP sampling factor	0.25
SBNP sampling factor (Volume)	0.1
SurfControl SDK version (legacy)	default-0
SurfControl Full Database version (legacy)	default-0
SurfControl Local Incremental Accumulation file version (legacy)	default-0
Firestone Engine version	default-210016
Firestone DAT version	v2-310003
AVC Engine version	default-110076
AVC DAT version	default-1377556980
Sophos Engine version	default-1310963572
Sophos DAT version	default-0
Adaptive Scanning enabled	0
Adaptive Scanning Risk Score Threshold	[10, 6, 3]
Adaptive Scanning Load Factor Threshold	[5, 3, 2]
SOCKS enabled	0
Total Transactions	

Total Transactions	

Total Allowed Transactions	
Total Malware Detected Transactions	
Total Transactions blocked by Admin Policy	
Total Transactions blocked by WBRS Score	
Total High Risk Transactions	
Total Transactions detected by Traffic Monitor	
Total Transactions with IPv6 clients	
Total Transactions with IPv6 servers	
Total Transactions using SOCKS proxy	
Total Transactions from remote users	
Total Transactions from local users	
Total Transactions allowed using SOCKS proxy	
Total Transactions from local users allowed using SOCKS proxy	
Total transactions from remote users allowed using SOCKS proxy	
Total transactions blocked using SOCKS proxy	
Total transactions from local users blocked using SOCKS proxy	
Total transactions from remote users blocked using SOCKS proxy	

Seconds since last restart	2843349

CPU Utilization (%)	9.9
RAM Utilization (%)	55.6
Hard Disk Utilization (%)	57.5
Bandwidth Utilization (/sec)	15307
Open TCP connections	2721
Transactions per second	264
Client Latency	163
Cache Hit Rate	21
Proxy CPU Utilization	17
WBRS WUC CPU Utilization	2.5
Logging CPU Utilization	3.4
Reporting CPU Utilization	3.9
Webroot CPU Utilization	0
Sophos CPU Utilization	0
McAfee CPU Utilization	0
vmstat utility output (vmstat –z, vmstat –m)	
Number of access policies configured	32
Number of configured custom web categories	32
Authentication Provider	Basic, NTLMSSP

Authentication Realms	Authentication Provider Hostname, Protocol & other configuration elements

Statistics shared per web request

Item	**Sample Data**	**Standard Participation**	**Limited Participation**
Version	coeus 7.7.0-608		
Serial Number			
SBNP sampling factor (Volume)			
SBNP sampling factor (Rate)	1		
Destination IP & Port		unobfuscated URL path segments	hashed URL path segments
Anti-Spyware chosen malware category	Skipped		
WBRS Score	4.7		
McAfee malware category verdict			
Referer URL		unobfuscated URL path segments	hashed URL path segments
Content Type ID			
ACL Decision Tag	0		
Legacy Web Categorization			
CIWUC Web Category and decision source	{'src': 'req', 'cat': '1026'}		
AVC App Name	Ads and Tracking		

AVC App Type	Ad Networks		
AVC App Behavior	Unsafe		
Internal AVC Result Tracking	[0,1,1,1]		
User agent tracking via indexed data structure	3		

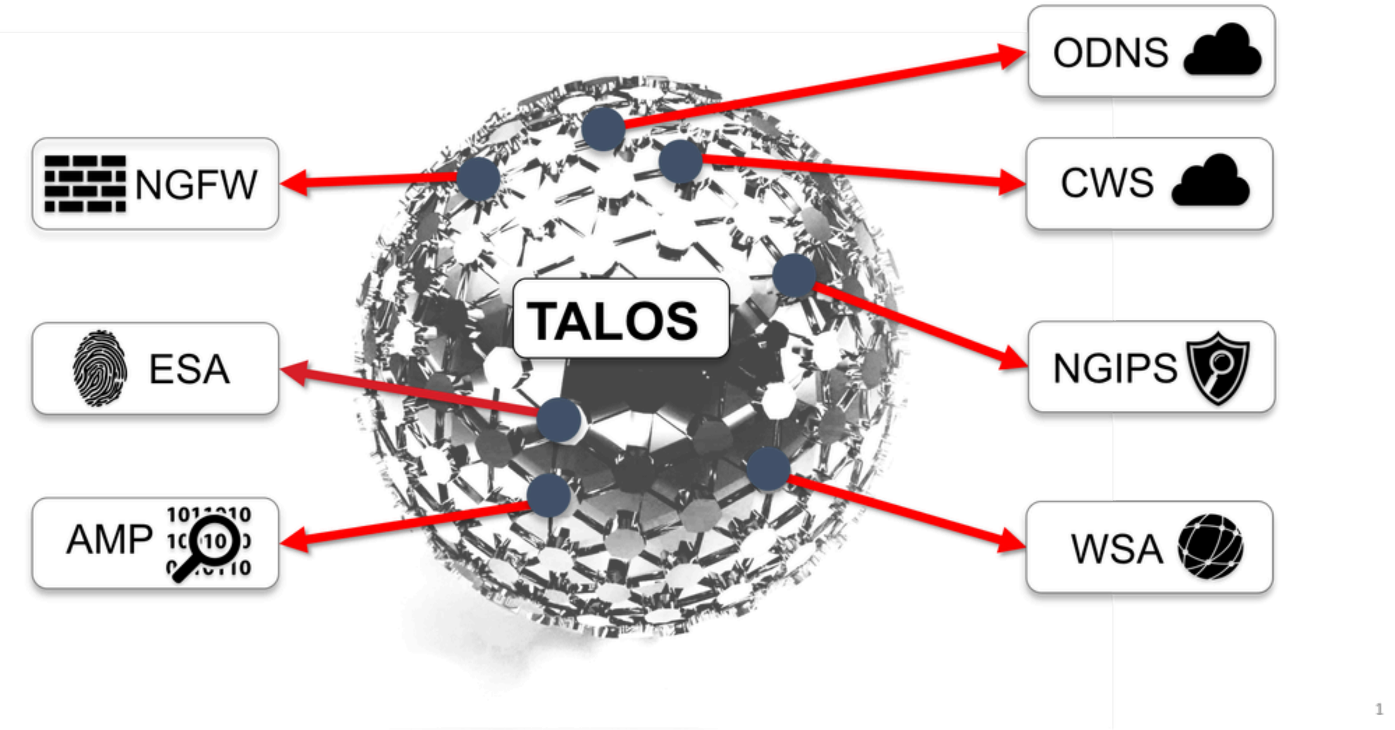
Advanced Malware Statistics per web request

AMP Statistics	
Verdict - of the AMP reputation query	malicious/clean/unknown
Spyname- Name of the malware detected	[Trojan-Test]
Score - AMP assigned reputation score	[1-100]
Upload - AMP cloud indicated to upload the file	1
File Name - Name of the file attachment	abcd.pdf

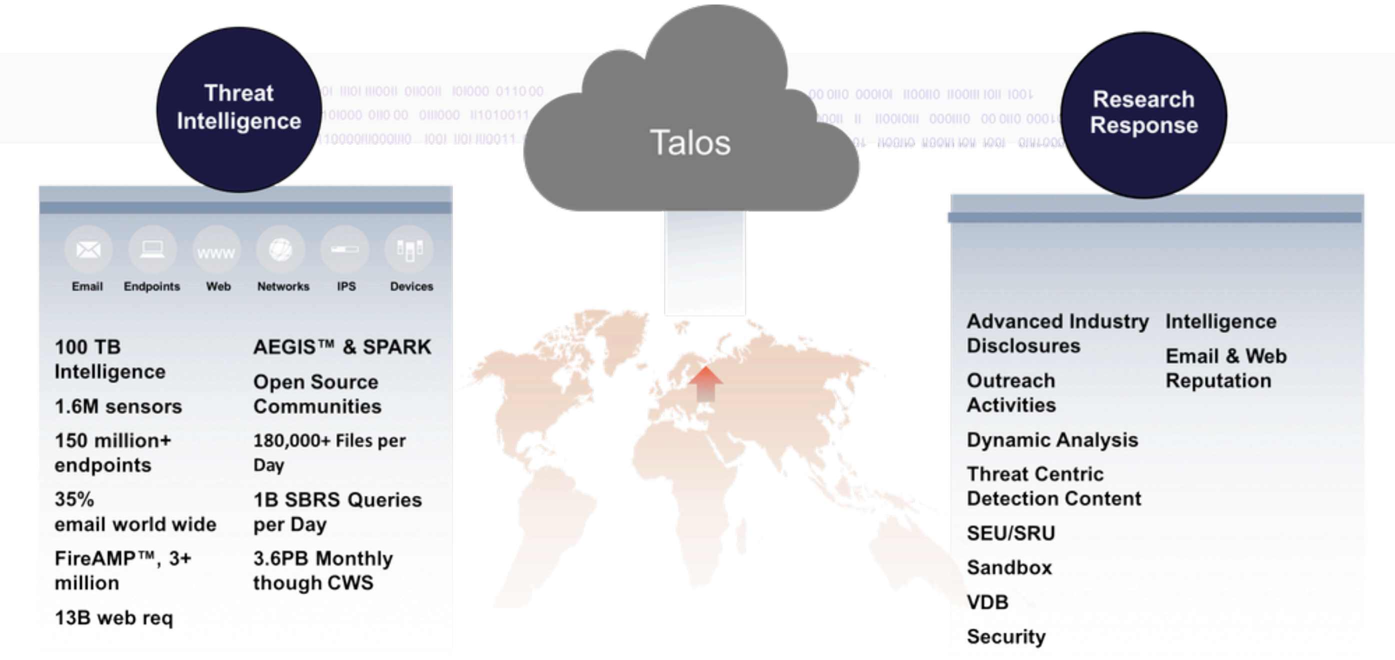
End User Feedback statistics feed

Statistics Shared per End User Miscategorization Feedback	
Item	**Sample Data**
Engine ID (numeric)	0
Legacy Web Categorization code	
CIWUC Web Categorization Source	‘resp’ / ‘req’
CIWUC Web Category	1026

Talos Detection Content



Threat Focused



100 TB Intelligence

1.6M sensors

150 million+ endpoints

35% email world wide

FireAMP™, 3+ million

13B web req

AEGIS™ & SPARK

Open Source Communities

180,000+ Files per Day

1B SBRS Queries per Day

3.6PB Monthly though CWS

Advanced Industry Disclosures

Outreach Activities

Dynamic Analysis

Threat Centric Detection Content

SEU/SRU

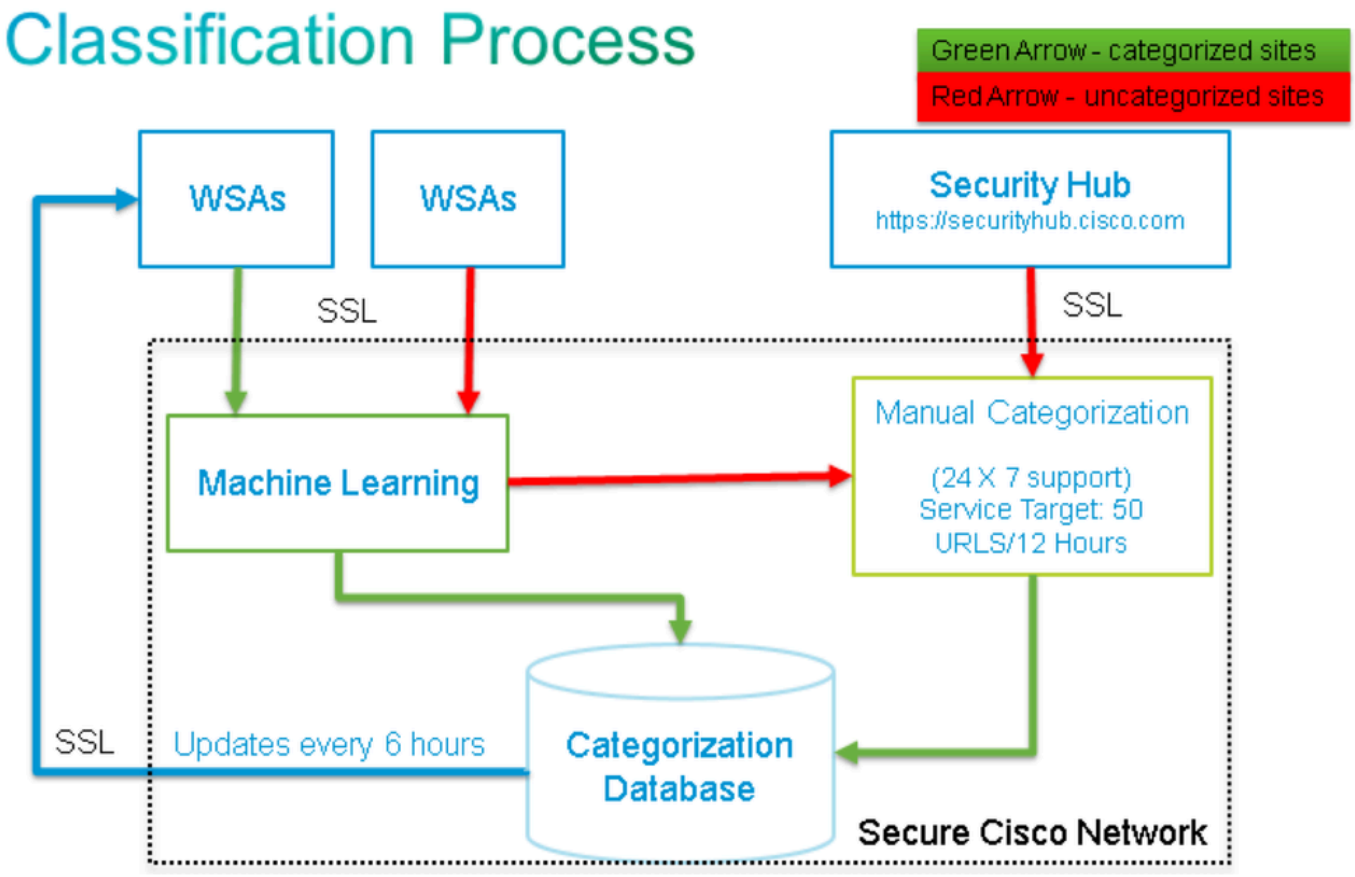
Sandbox

VDB

Security

Intelligence

Email & Web Reputation



Related Information

- Cisco Web Security Appliance - Product Page
- Cisco Email Security Appliance - Product Page
- Technical Support & Documentation - Cisco Systems