Cisco Success Network Telemetry Data Collected from Cisco Firepower Management Center, Version 6.5

First Published: 2022-05-31

Last Modified: 2024-12-13

Cisco Success Network Telemetry Data Collected from Cisco Secure Firewall Management Center

Cisco Success Network allows enrolled FMC to continuously stream real-time configuration and operating state information to the Cisco Success Network cloud. This document provides a list of the collected and monitored data.

Enrolled FMC Data

When you enroll the FMC in Cisco Success Network, selected telemetry data about the enrolled FMC is streamed to the Cisco cloud. The following table describes the collected and monitored data about the enrolled FMC. The data includes feature-specific information about intrusion policies (both system-provided and custom) and malware detection for enrolled FMC.

Table 1: Enrolled FMC Telemetry Data

Data Point	Example Value
Device Name	Management Center East
Device UUID	24fd0ccf-1464- 491f-a503- d241317bb327
HA Peer UUID	24fe0ccd-1564- 491h-b802- d321317cc827
Device Model	Cisco Firepower Management Center 4000 Cisco Firepower Management Center for VMware
Serial Number	9AMDESQP6UN
System Uptime	99700000
Product Identifier	FS-VMW-SW-K9
Smart License PIID	24fd0ccf-1464- 491f-a503- d241317bb327
Virtual Account Identifier	CiscoSVStemp

Data Point	Example Value
Smart LicenseVirtual Account Name	FTD-ENG-SJC

Software Version Data

Cisco Success Network collects software information that pertains to the enrolled FMC device, including software version, rule update version, geolocation database version, and vulnerability database version information. The following table describes the collected and monitored software information about the enrolled device.

Table 2: Software Version Telemetry Data

Data Point	Example Value
FMC Software Version	{ type: "SOFTWARE", version: "x.x.x.x" }
Rule Update Version	{version: "2016-11-29-001-vrt", lastUpdated: 1468606837000 }
Vulnerability Database (VDB) Version	{version: "271", lastUpdated: 1468606837000 }
Geolocation Database Version	{version: "850" }

Managed Device Data

Cisco Success Network collects information about all the managed devices associated with an enrolled FMC. The following table describes the collected and monitored information about managed devices. This includes feature-specific policy and licensing information, such as URL filtering, intrusion prevention, and malware detection for managed devices.

Table 3: Managed Device Telemetry Data

Data Point	Example Value
Managed Device Name.	firepower
Managed Device Version.	6.2.3-10616
Managed Device Manager.	FMC
Managed Device Model.	Cisco Firepower 2130 NGFW Appliance Cisco FTD VMware
Managed Device Serial Number.	9AMDESQP6UN
Managed Device PID.	FPR2130-NGFW-K9 NGFWv
Is URL Filtering License Used for Device?	True
AC Rules with URL Filtering Per Device.	An integer value of 0 or greater.

Data Point	Example Value
Number of AC Rules with URL Filtering That Use URL Filtering License.	An integer value of 0 or greater.
Number of AC Rules with URL Filtering That Use Threat License.	An integer value of 0 or greater.
Is Threat License Used for Device?	True
Does AC Policy Have Intrusion Rule Attached?	True
Number of AC Rules with Intrusion Policies.	An integer value of 0 or greater.
Is Malware License Used for Device?	True
Number of AC Rules with Malware Policy.	An integer value of 0 or greater.
Number of AC Rules with Malware Policy That Use Malware License.	An integer value of 0 or greater.
Is Threat Intelligence Director (TID) Used for Device?	True
Count of local URL items.	`{"url": "/api/local/fmc_config/v1/domain/{domainUUID}/object/networks", "count": 10}, {"url": "/api/local/fmc_platform/v1/info/serverversion", "count": 2}`

Cisco Success Network collects information about the FTD upgrade process, upgrade failures, and the time taken for each upgrade script to run. Cisco uses this data to improve the upgrade process and enhance the customer upgrade experience. The following table shows the information collected regarding the FTD upgrade.

Table 4: Upgrade Status Telemetry Data

Data Point	Example Value
Hot fixes applied	Cisco_FTD_SSP_FP3K_Hotfix_W-7.3.1.2-5.sh.REL.tar
Base version	7.4.0-10
Target version	7.4.0-38
Upgrade package file name	Cisco_FTD_Upgrade-7.4.0-38.sh.REL.tar
Upgrade type	major

Data Point	Example Value
Displays detailed status of the canceled upgrade such as status, start and end time, and elapsed time.	{ "status": "COMPLETED", "message": "Device returned to previous version: 7.5.0-10.", "startTime": "Tue, 07 Mar 2023 06:10:37 UTC", "endTime": "Tue, 07 Mar 2023 06:10:40 UTC", "elapsedTimeInSeconds": 3 }
Detailed status of the upgrade, such as details of the failed script, start and end time, and elapsed time.	{ "status": "COMPLETED", "message": "Installation completed successfully. Upgraded applications are started.", "startTime": "Tue, 07 Mar 2023 06:08:45 UTC", "endTime": "Tue, 07 Mar 2023 06:10:35 UTC", "elapsedTimeInSeconds": 110,
Failed script	"/ngfw/var/sf/upgrade-scripts/7.5.1/200_pre/001_check_reg.pl"
The execution time for individual scripts in the upgrade process.	{ "name": "000_start/000_00_run_cli_kick_start.sh", "executionTime": 1 },

Deployment Information

After you configure your deployment, you must deploy the changes to the affected devices. The following table describes the collected and monitored data about configuration deployment, such as the number of devices affected and the status of deployments, including success and failure information.

Table 5: Deployment Information

Data Point	Example Value
Job ID.	8589936079
Number of Devices Selected for Deployment.	3
Number of Devices with Deployment Failure.	1
Number of Devices with Deployment Success.	2
End Time (in Unix Epoch format).	1523993913001
Start Time (in Unix Epoch format).	1523993840445
Status..	SUCCEEDED
Target Device UUID.	4f14f644-41e0 -11e8-9354- cf32315d7095

Data Point	Example Value
Policy Types Deployed.	NetworkDiscovery NGFWPolicy DeviceConfiguration
Last Deployment Job ID Collected in Current Run.	8589936079
Container Type (Standalone or HA Pair)..	STANDALONE
Container UUID.	5e006633-30fe-11e9-8a70-cd88086eeac0
Device Model.	Cisco FTD for VMWare
Device Version.	6.4.0
Policy Bundle Size.	3588153
Count of CSPA.	An integer value of 0 or greater.
Count of CSPA query.	An integer value of 0 or greater.
Count of CSPA group query.	An integer value of 0 or greater.

TLS/SSL Inspection Event Data

By default, the Firepower Threat Defense cannot inspect traffic encrypted with the Secure Socket Layer (SSL) protocol or its successor, the Transport Layer Security (TLS) protocol. TLS/SSL inspection enables you to either block encrypted traffic without inspecting it, or inspect encrypted or decrypted traffic with access control. The following tables describe statistics shared with Cisco Success Network about encrypted traffic.

Handshake Process

When the system detects a TLS/SSL handshake over a TCP connection, it determines whether it can decrypt the detected traffic. As the system handles encrypted sessions, it logs details about the traffic.

Table 6: TLS/SSL Inspection - Handshake Telemetry Data

Data Point	Example Value
The system reports the following applied actions when the traffic **cannot be decrypted** and is: • Blocked. • Blocked with a TCP reset. • Not decrypted.	An integer value of 0 or greater.

Data Point	Example Value
The system reports the following applied actions when the traffic **can be decrypted**: • With a known private key. • With a replacement key only. • By resigning a self-signed certificate. • By resigning the server certificate.	An integer value of 0 or greater.

Cache Data

After a TLS/SSL handshake completes, the managed device caches encrypted session data, which allows session resumption without requiring the full handshake. The managed device also caches server certificate data, which allows faster handshake processing in subsequent sessions.

Table 7: TLS/SSL Inspection - Cache Telemetry Data

Data Point	Example Value
The system caches encrypted session data and server certificate data, and reports on the cache per SSL connections, specifically: • The number of times SSL session information was cached. • The number of times the SSL certificate validation cache was hit. • The number of times the SSL certificate validation cache lookup missed. • The number of times the SSL original certificate cache was hit. • The number of times the SSL original certificate cache lookup missed. • The number of times the SSL resigned certificate cache was hit. • The number of times the SSL resigned certificate cache lookup missed. • The number of times the session ID cache was hit. • The number of times the session ID cache miss	An integer value of 0 or greater.
Is SSL Usage enabled on the FMC?	True

Certificate Status

The system evaluates encrypted traffic and reports the certificate status of the encrypting server.

Table 8: TLS/SSL Inspection - Certificate Status Telemetry Data

Data Point	Example Value
The system evaluates encrypted traffic based on the certificate status of the encrypting server, and reports. • Number of connections where the SSL certificate is valid. • Number of connections where the SSL certificate is expired. • Number of connections where the SSL certificate has an invalid issuer. • Number of connections where the SSL certificate has an invalid signature. • Number of connections where the SSL certificate is not checked. • Number of connections where the SSL certificate is not yet valid. • Number of connections where the SSL certificate is revoked. • Number of connections where the SSL certificate is self-signed. • Number of connections where the SSL certificate is unknown.	An integer value of 0 or greater.

Failure Reason

The system evaluates encrypted traffic and reports the failure reason when the system fails to decrypt traffic.

Table 9: TLS/SSL Inspection - Failure Telemetry Data

Data Point	Example Value
The system evaluates encrypted traffic and reports the failure reason when the system fails to decrypt traffic due to: • A decryption error. • Making a policy verdict during the handshake. • Making a policy verdict before the handshake. • Compression being negotiated. • An uncached session. • An interface in passive mode. • An unknown cipher suite. • An unsupported cipher suite.	An integer value of 0 or greater.

Version

The system evaluates encrypted traffic and reports the negotiated TLS/SSL version per connection.

Table 10: TLS/SSL Inspection - Version Telemetry Data

Data Point	Example Value
The system evaluates encrypted traffic and reports the negotiated version per SSL connections where: • SSLv2 was negotiated. • SSLv3 was negotiated. • An unknown version was negotiated. • TLSv1.0 was negotiated. • TLSv1.1 was negotiated. • TLSv1.2 was negotiated. • TLSv1.3 was negotiated.	An integer value of 0 or greater.

Snort Restart Data

When the traffic inspection engine, referred to as the Snort process, on a managed device restarts, inspection is interrupted until the process resumes. Creating or deleting a user-defined application, or activating or deactivating a system or custom application detector, immediately restarts the Snort process without going through the deploy process. The system warns you that continuing restarts the Snort process and allows you to cancel. The restart occurs on any managed device in the current domain or in any of its child domains. The following table describes the collected and monitored data about the Snort restart.

Table 11: Snort Restart Telemetry Data

Data Point	Example Value
Count of snort restarts when you enable or disable a custom application detector.	An integer value of 0 or greater
Count of snort restarts when you create or modify a custom application detector.	An integer value of 0 or greater

Contextual Cross-Launch Data

The contextual cross-launch feature allows you to quickly find more information about potential threats in web-based resources outside of the FMC. You can click directly from an event in the event viewer or dashboard in the FMC to the relevant information in an external resource. This lets you quickly gather context around a specific event based on its IP addresses, ports, protocol, domain, and/or SHA 256 hash.

Table 12: Contextual Cross-Launch Telemetry Data

Data Point	Example Value
The count of the Contextual Cross-Launch resources configured on the FMC.	An integer value of 0 or greater.
The count of the Contextual Cross-Launch resources enabled on the FMC.	An integer value of 0 or greater.
The count of Contextual Cross-Launch instances containing a domain variable.	An integer value of 0 or greater.
The count of Contextual Cross-Launch instances containing an IP variable.	An integer value of 0 or greater.
The count of Contextual Cross-Launch instances containing a SHA 256 variable.	An integer value of 0 or greater.
Count of users using the **Legacy** theme.	An integer value of 0 or greater.
Count of users using the **Light** theme.	An integer value of 0 or greater.

Telemetry Example File

The following is an example of a Cisco Success Network telemetry file for streaming policy and deployment information about a FMC and its managed devices:

```
{
  "version" : "1.0",
  "metadata" : {
    "topic" : "fmc.telemetry",
    "contentType" : "application/json"
  },
  "payload" : {
    "recordType" : "CST_FMC",
    "recordVersion" : "6.5.0",
    "recordedAt" : 1570468542867,
```

```
"fmc" : {
  "deviceInfo" : {
    "deviceModel" : "Cisco Firepower Management Center for VMWare",
    "deviceName" : "firepower",
    "deviceUuid" : "42f78a4c-e4ce-11e9-bd7d-5965f67ed43a",
    "serialNumber" : "None",
    "smartLicenseProductInstanceIdentifier" : "b3439793-951a-4bd4-bbdd-0bce45cff701",
    "smartLicenseVirtualAccountName" : "FMC_SSE-Integration-Dev-test",
    "systemUptime" : 477555000,
    "udiProductIdentifier" : "FS-VMW-SW-K9"
  },
  "versions" : {
    "items" : [
      {
        "type" : "SOFTWARE",
        "version" : "6.5.0-120"
      },
      {
        "lastUpdated" : 0,
        "type" : "SNORT_RULES_DB",
        "version" : "2019-08-12-001-vrt"
      },
      {
        "lastUpdated" : 1569991503000,
        "type" : "VULNERABILITY_DB",
        "version" : "309"
      },
      {
        "type" : "GEOLOCATION_DB",
        "version" : "2019-09-29-002"
      }
    ]
  }
},
"managedDevices" : {
  "items" : [
    {
      "deviceInfo" : {
        "deviceManager" : "FMC",
        "deviceModel" : "Cisco Firepower Threat Defense for VMWare",
        "deviceName" : "FTD_4",
        "deviceVersion" : "6.5.0-120",
        "serialNumber" : "9AUG1DNTFLN"
      },
      "malware" : {
        "malwareLicenseUsed" : false,
        "numberOfACRulesNeedMalwareLicense" : 0,
        "numberOfACRulesWithMalware" : 0
      },
      "sslUsage" : {
        "isSSLEnabled" : false
      },
      "threat" : {
        "acPolicyHasIntrusion" : false,
        "acRulesWithIntrusion" : 0,
        "isTIDEnabled" : false,
        "numberOfACRulesNeedThreatLicense" : 0,
        "threatLicenseUsed" : false
      },
      "urlFiltering" : {
        "acRulesWithURLFiltering" : 0,
        "numberOfACRulesNeedThreatLicense" : 0,
        "numberOfACRulesNeedURLLicense" : 0,
        "urlFilteringLicenseUsed" : false
```

```
      }
    },
    {
      "deviceInfo" : {
        "deviceManager" : "FMC",
        "deviceModel" : "Cisco Firepower Threat Defense for VMWare",
        "deviceName" : "FTD_3",
        "deviceVersion" : "6.5.0-120",
        "serialNumber" : "9AG01XAV5GW"
      },
      "malware" : {
        "malwareLicenseUsed" : true,
        "numberOfACRulesNeedMalwareLicense" : 10,
        "numberOfACRulesWithMalware" : 20
      },
      "sslUsage" : {
        "isSSLEnabled" : false
      },
      "threat" : {
        "acPolicyHasIntrusion" : true,
        "acRulesWithIntrusion" : 20,
        "isTIDEnabled" : true,
        "numberOfACRulesNeedThreatLicense" : 20,
        "threatLicenseUsed" : true
      },
      "urlFiltering" : {
        "acRulesWithURLFiltering" : 16,
        "numberOfACRulesNeedThreatLicense" : 0,
        "numberOfACRulesNeedURLLicense" : 16,
        "urlFilteringLicenseUsed" : true
      }
    }
  ]
},
"deploymentData" : { },
"analysis" : {
  "crossLaunchInfo" : {
    "count" : 28,
    "enabledCount" : 28,
    "iocInfo" : [
      {
        "domain" : 10,
        "ip" : 9,
        "sha256" : 9
      }
    ]
  }
},
"theme" : {
  "legacy" : 1
},
"SSLStats" : {
  "action" : {
    "block" : 0,
    "block_with_reset" : 0,
    "decrypt_resign_self_signed" : 0,
    "decrypt_resign_self_signed_replace_key_only" : 0,
    "decrypt_resign_signed_cert" : 0,
    "decrypt_with_known_key" : 0,
    "do_not_decrypt" : 0
  },
  "cache_status" : {
    "cached_session" : 0,
    "cert_validation_cache_hit" : 0,
```

```
          "cert_validation_cache_miss" : 0,
          "orig_cert_cache_hit" : 0,
          "orig_cert_cache_miss" : 0,
          "resigned_cert_cache_hit" : 0,
          "resigned_cert_cache_miss" : 0,
          "session_cache_hit" : 0,
          "session_cache_miss" : 0
        },
        "cert_status" : {
          "cert_expired" : 0,
          "cert_invalid_issuer" : 0,
          "cert_invalid_signature" : 0,
          "cert_not_checked" : 0,
          "cert_not_yet_valid" : 0,
          "cert_revoked" : 0,
          "cert_self_signed" : 0,
          "cert_unknown" : 0,
          "cert_valid" : 0
        },
        "failure_reason" : {
          "decryption_error" : 0,
          "handshake_error_before_verdict" : 0,
          "handshake_error_during_verdict" : 0,
          "ssl_compression" : 0,
          "uncached_session" : 0,
          "undecryptable_in_passive_mode" : 0,
          "unknown_cipher_suite" : 0,
          "unsupported_cipher_suite" : 0
        },
        "version" : {
          "ssl_v20" : 0,
          "ssl_v30" : 0,
          "ssl_version_unknown" : 0,
          "tls_v10" : 0,
          "tls_v11" : 0,
          "tls_v12" : 0,
          "tls_v13" : 0
        }
      },
      "snortRestart" : {
        "appDetectorSnortRestartCnt" : 0,
        "appSnortRestartCnt" : 0
      }
    }
  }
```

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.