Cisco Success Network-Telemetry Data

Cisco Success Network-Telemetry Data

Cisco Success Network is an always-on usage information and metrics collection feature in the Secure Firewall migration tool, which collects and trasmits usage statistics through a secure cloud connection between the migration tool and the Cisco cloud. These statistics help us provide additional support on unused features and also improve our products. When you initiate a migration process in the Secure Firewall migration tool, the corresponding telemetry data file is generated and stored in a fixed location.

When you push the migrated FDM-managed device configuration to management center, the push service reads the telemetry data file from the location and deletes it after the data is successfully uploaded to the cloud.

The migration tool provides two options to choose from, for streaming telemetry data—**Limited** and **Extensive**.

With **Cisco Success Network** set to **Limited**, the following telemetry data points are collected:

Table 1: Limited Telemetry

Data Point	Description	Example Value
Time	The time and date when the telemetry data is collected	2023-04-25 10:39:19
Source Type	The source device type	ASA
Device Model Number	Model number of ASA	ASA5585-SSP-10, 5969 MB RAM, CPU Xeon 5500 series 2000 MHz, 1 CPU (4 cores)
Source Version	Version of ASA	9.2 (1)
Target Management Version	The target version of management center	6.5 or later
Target Management Type	The type of target management device, namely, management center	Management Center
Target Device Version	The version of target device	75

Data Point	Description	Example Value
Target Device Model	The model of target device	Cisco Secure Firewall Threat Defense for VMware
Migration Tool Version	The version of the migration tool	1.1.0.1912
Migration Status	The status of the migration of ASA configuration to management center	SUCCESS

The following tables provide information on the telemetry data points, their descriptions, and sample values, when **Cisco Success Network** is set to **Extensive**:

Table 2: System Information

Data Point	Description	Example Value
Operating System	Operating system that runs the Secure Firewall migration tool. It could be Windows7/Windows10 64-bit/macOS High Sierra	Windows 7
Browser	Browser used to launch the Secure Firewall migration tool. It could be Mozilla/5.0 or Chrome/68.0.3440.106 or Safari/537.36	Mozilla/5.0

Table 3: Source FDM-managed device Information

Data Point	Description	Example Value
Source Type	The source device type	FDM
Source Device Serial Number	Serial number of FDM-managed device	Cisco Firepower Threat Defense for VMware
Source Device Version	Version of FDM-managed device	7.2.0-8.0
Firewall Mode	The firewall mode configured on FDM-managed device - routed or transparent	ROUTED
Context Mode	The context mode of FDM-managed device. This can be single or multi-context.	SINGLE
FDM-Managed Device Config Statistics:		
ACL Counts	The number of ACLs which are attached to access group	46
Access Rules Counts	The total number of access rules	46
NAT Rule Counts	The total number of NAT rules	17
Network Object Counts	The number of network objects configured in FDM-managed device	34

Data Point	Description	Example Value
Network Object Group Counts	The number of network object groups in FDM-managed device	6
Port Object Counts	The number of port objects	85
Port Object Group Counts	The number of port object groups	37
Unsupported Access Rules Count	The total number of unsupported access rules	3
Unsupported NAT Rule Count	The total number of unsupported NAT access rules	0
FQDN Based Access Rule Counts	The number of FQDN -based access rules	7
Time range Based Access Rule Counts	The number of time range based access rules	1
SGT Based Access Rule Counts	The number of SGT-based access rules	0
Summary of Config lines that Tool is not able to parse		
Unparsed Config Count	The number of config lines that are unrecognized by the parser	68
Total Unparsed Access Rule Counts	The total number of unparsed access rules	3
More FDM-Managed Device config details...		
Is RA VPN Configured	Whether RA VPN is configured on FDM-managed device	false
Is S2S VPN Configured	Whether Site-to-Site VPN is configured on FDM-managed device	false
Is BGP Configured	Whether BGP is configured on FDM-managed device	false
Is EIGRP Configured	Whether EIGRP is configured on FDM-managed device	false
Is OSPF Configured	Whether OSPF is configured on FDM-managed device	false
Local Users Counts	The number of local users configured	0

Table 4: Target Management Device (Management Center) Information

Data Point	Description	Example Value
Target Management Type	The type of target management device, namely, management center	Management Center
Target Device Version	The version of target device	75

Data Point	Description	Example Value
Target Device Model	The model of target device	Cisco Secure Firewall Threat Defense for VMware

Table 5: Migration Summary

Data Point	Description	Example Value
Access Control Policy		
Name	The name of access control policy	Doesn't Exist
Partially Migrated ACL Rule Counts	The total number of partially migrated ACL rules	3
Expanded ACP Rule Counts	The number of expanded ACP rules	0
NAT Policy		
Name	The name of NAT policy	Doesn't Exist
NAT Rule Counts	The total number of migrated NAT rules	0
Partially Migrated NAT Rule Counts	The total number of partially migrated NAT rules	0
More migration details...		
Interface Counts	The number of updated interfaces	0
Sub Interface Counts	The number of updated subinterfaces	0
Static Routes Counts	The number of static routes	0
Objects Counts	The number of objects created	34
Object Group Counts	The number of object groups created	6
Security Zone Counts	The number of security zones created	3
Network Object Reused Counts	The number of objects reused	21
Network Object Rename Counts	The number of objects that are renamed	1
Port Object Reused Counts	The number of port objects that are reused	0
Port Object Rename Counts	The number of port objects that are renamed	0

Table 6: Secure Firewall Migration Tool Performance Data

Data Point	Description	Example Value
Conversion Time	The time taken to parse FDM-managed device configuration lines (in minutes)	14

Data Point	Description	Example Value
Migration Time	The total time taken for end-to-end migration (in minutes)	592
Config Push Time	The time taken to push the final configuration (in minutes)	7
Migration Status	The status of the migration of FDM-managed device configuration to management center	SUCCESS
Error Message	The error message as displayed by the Secure Firewall migration tool	null
Error Description	The description about the stage when the error has occurred and the possible root cause	nul

Telemetry FDM Example File

Thefollowing is an example of a telemetry data file on the migration of FDM-managed device configuration to threat defense:

```
{
"metadata": {
"contentType": "application/json", "topic": "migrationtool.telemetry"
},
"payload": { "FDM_config_stats": {
"access_rules_counts": 46,
"acl_counts": 46,
"fqdn_based_access_rule_counts": 7, "is_bgp_configured": false, "is_eigrp_configured":
false, "is_multicast_configured": false, "is_ospf_configured": false, "is_pbr_configured":
 false, "is_ra_vpn_configured": false, "is_s2s_vpn_configured": false, "is_snmp_configured":
 false, "local_users_counts": 0,
"nat_rule_counts": 17,
"network_object_counts": 34,
"network_object_group_counts": 6,
"port_object_counts": 85,
"port_object_group_counts": 37,
"sgt_based_access_rules_count": 0,
"timerange_based_access_rule_counts": 1,
"total_unparsed_access_rule_counts": 3,
"unparsed_config_count": 68,

"unsupported_access_rules_count": 3,
"unsupported_nat_rule_count": 0
},
"context_mode": "SINGLE", "error_description": null, "error_message": null, "firewall_mode":
 "ROUTED", "migration_status": "SUCCESS", "migration_summary": {
"access_control_policy": [ [
{
"access_rule_counts": 0,
"expanded_acp_rule_counts": 0, "name": "Doesn't Exist",
"partially_migrated_acl_rule_counts": 3
}
]
],
"interface_counts": 0,
"interface_group_counts": 0, "nat_Policy": [
[
{
"NAT_rule_counts": 0, "name": "Doesn't Exist",
"partially_migrated_nat_rule_counts": 0
}
]
],
"network_object_rename_counts": 1,
"network_object_reused_counts": 21,
"object_group_counts": 6,
"objects_counts": 34,
"port_object_rename_counts": 0,
"port_object_reused_counts": 0,
"security_zone_counts": 3,
"static_routes_counts": 0,
"sub_interface_counts": 0
},
"migration_tool_version": "1.1.0.1912",
"source_config_counts": 504,
"source_device_model_number": " FDM5585-SSP-10, 5969 MB RAM, CPU Xeon 5500 series 2000 MHz,
 1 CPU (4 cores)",
"source_device_serial_number": "JAF1528ACAD", "source_device_version": "9.6(2)",
"source_type": "FDM",
"system_information": {
"browser": "Chrome/69.0.3497.100", "operating_system": "Windows NT 10.0; Win64; x64"
},
"target_device_model": "Cisco Firepower Threat Defense for VMWare", "target_device_version":
 "75",
"target_management_type": "Management Center", "target_management_version": "6.2.3.3 (build
 76)",
"time": "2018-09-28 18:17:56",
"tool_performance": { "config_push_time": 7,
"conversion_time": 14,
"migration_time": 592
}
},
"version": "1.0"
```