Network Ten

Cisco Report

June 2022

purple.telstra.com

Document Development

**Preparation**

|  |  |  |  |
| --- | --- | --- | --- |
| Action | Name | Role | Date |
| Prepared By: | Chris Larkin | Technical Consultant | 1th July 2022 |
| Reviewed By: | Daniel Gonzalez | Technical Consultant | 11th July 2022 |

**Contact Details**

|  |  |
| --- | --- |
| Account Manager | |
| Name: | Nick Goodey |
| Phone: | +61 2 85761680 |
| Email: | Nick.Goodey@team.telstra.com |

**Distribution List**

|  |  |  |
| --- | --- | --- |
| Name | Title | Organisation |
| Costa Varvarigos | Communications Manager - Technology | Network Ten |

Table of Contents

[1 Executive Summary 4](#_Toc106280969)

[2 Incidents and Service Requests 5](#_Toc106280970)

[3 Firmware and Uptime Status 6](#_Toc106280971)

[3.1 Uptime 6](#_Toc106280972)

[3.2 Latest Firmware Revisions 7](#_Toc106280973)

[3.2.1 2900 and 3900 series routers 7](#_Toc106280974)

[3.2.2 ASR 1001-X 7](#_Toc106280975)

[3.3 Known critical Vulnerabilities 7](#_Toc106280976)

[4 Hardware EOL/EOS 7](#_Toc106280977)

[5 Recommendations 8](#_Toc106280978)

[6 Hardware Status 9](#_Toc106280979)

[6.1 Temperature Status 9](#_Toc106280980)

[6.2 Power Supply Status 10](#_Toc106280981)

[6.3 Fan Status 10](#_Toc106280982)

[7 Statistics 11](#_Toc106280983)

[7.1 ndw-ten-r01 11](#_Toc106280984)

[7.1.1 Interfaces 12](#_Toc106280985)

[7.2 ndw-ten-r02 14](#_Toc106280986)

[7.2.1 Interfaces 15](#_Toc106280987)

[7.3 ndw-atv-r01 17](#_Toc106280988)

[7.3.1 Interfaces 18](#_Toc106280989)

[7.4 ndw-atv-r02 20](#_Toc106280990)

[7.4.1 Interfaces 21](#_Toc106280991)

# Executive Summary

This report covers the availability and performance of the Cisco routers and switches within the Network Tenenvironment.

The report is summarized in the following dashboard.

|  |  |  |
| --- | --- | --- |
| Category | Comments | Status |
| Tickets | 7 Total: 7 Incidents + 0 Service Requests 0 Open, 7 Completed, 0 Cancelled | C:\InhouseApps\o2lib\Images\24x24\Tick.png |
| Firmware Status | There is newer firmware available, but there is no specific requirement to upgrade. | C:\InhouseApps\o2lib\Images\24x24\Tick.png |
| Uptime | No devices rebooted | C:\Users\robert.gruener\Downloads\1389264091_configure.png |
| Recommendations | No recommendations. | C:\InhouseApps\o2lib\Images\24x24\Tick.png |

|  |  |
| --- | --- |
| Symbol | Description |
| C:\InhouseApps\o2lib\Images\24x24\Tick.png | No issues of concern. |
|  | There are issues to be noted. |
| C:\Users\robert.gruener\Downloads\1389264091_configure.png | Work is required. |
| C:\InhouseApps\o2lib\Images\24x24\Exclamation.png | Important problems need to be fixed. |

# Incidents and Service Requests

| **ID** | **Type** | **Priority** | **Title** | **Opened** | **Closed** | **Status** | **Done** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| SNI2456125 | Incident | Moderate | [Ch10 Perth Studio]-[ndw-new-r01 - Monitor down] | 2022-06-23 19:36:04 | 03-07-2022  14:00:28 | Closed |  |
| SNI2456127 | Incident | Moderate | [Ch10 Sydney Studio]-[ndw-ten-r01 - Monitor down] | 2022-06-23 19:38:24 | 03-07-2022  14:00:24 | Closed |  |
| SNI2425217 | Incident | Moderate | Network TEN DVN2 Data link impact between NSW and WA at 28/05/22 3:50PM | 2022-05-28 5:58:49 | 2022-06-04 14:00:23 | Closed |  |
| SNI2427046 | Incident | Moderate | Multiple sites - multiple devices - monitor down | 2022-05-30 13:16:37 | 2022-06-05 14:00:22 | Closed |  |
| SNI2441318 | Incident | Moderate | INCIDENT #84121-#84123 [Ch10 Melbourne]-[ndw-atv-r01- Monitor down] | 2022-06-13 16:14:35 | 2022-06-19 14:00:28 | Closed |  |
| SNI2443357 | Incident | Moderate | INCIDENT #84129 [Ch10 Sydney Studio]-[ndw-ten-r02- Monitor down] | 2022-06-14 16:54:32 | 2022-06-20 14:00:33 | Closed |  |
| SNI2458515 | Incident | Moderate | [Ch10 Perth Studio]-[ndw-new-r01 - Monitor down] | 2022-06-25 7:48:35 | 2022-06-30 14:00:11 | Closed |  |

# Firmware and Uptime Status

Uptimes calculated on Friday, 1 July 2022

| **Name** | **Site** | **State** | **Address** | **Model** | **Serial Number** | **Firmware** | **Up Days** | **Status** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ndw-tvq-r01 | Brisbane Studio | QLD | 172.20.200.201 | ISR G2 3945E | FGL190511LH | 15.4(1)T3 | 2652 |  |
| ndw-tvq-r02 | Brisbane Studio | QLD | 172.20.200.202 | ISR G2 3945E | FGL190511LJ | 15.4(1)T3 | 2651 |  |
| ndw-gct-r01 | Gold Coast News Bureau | QLD | 172.20.200.205 | ISR 2921 | FGL190510RT | 15.3(3)M4 | 303 |  |
| ndw-gct-r02 | Gold Coast News Bureau | QLD | 172.20.200.206 | ISR 2921 | FGL190510Q0 | 15.3(3)M4 | 303 |  |
| ndw-atv-r01 | Melbourne Studio | VIC | 172.20.200.195 | ASR 1001-X | FXS1852Q1CC | 15.4(2r)S | 2571 |  |
| ndw-atv-r02 | Melbourne Studio | VIC | 172.20.200.196 | ASR 1001-X | FXS1847Q1Y1 | 15.4(2r)S | 2571 |  |
| txa-nws-r01 | Mt Lofty | SA | 172.20.200.213 | ISR 2901 | FGL190524WY | 15.4(3)M1 | 1115 |  |
| txa-crf-r01 | Mt Lofty (ex ADS/SAS) | SA | 172.20.200.211 | ISR 2901 | FGL190524WV | 15.4(3)M1 | 2662 |  |
| ndw-can-r01 | Parliament House | ACT | 172.20.200.203 | ISR 2921 | FTX1848AKM2 | 15.3(3)M4 | 159 |  |
| ndw-can-r02 | Parliament House | ACT | 172.20.200.204 | ISR 2921 | FGL190510Q1 | 15.3(3)M4 | 159 |  |
| ndw-new-r01 | Perth Studio | WA | 172.20.200.199 | ISR G2 3945E | FGL151111QA | 15.4(1)T3 | 101 |  |
| ndw-new-r02 | Perth Studio | WA | 172.20.200.200 | ISR G2 3945E | FGL190511KB | 15.4(1)T3 | 101 |  |
| ndw-ten-r01 | Sydney Studio | NSW | 172.20.200.193 | ASR 1001-X | FXS1852Q1FJ | 15.4(2r)S | 2569 |  |
| ndw-ten-r02 | Sydney Studio | NSW | 172.20.200.194 | ASR 1001-X | FXS1851Q1SG | 15.4(2r)S | 2569 |  |
| txa-art-r01 | TXA Artamon | NSW | 172.20.200.207 | ISR 2901 | FGL190524X2 | 15.4(3)M1 | 1428 |  |
| txa-bky-r01 | TXA Bickley | WA | 172.20.200.209 | ISR 2901 | FGL190524X1 | 15.4(3)M1 | 2520 |  |
| txa-cml-r01 | TXA Carmel | WA | 172.20.200.210 | ISR 2901 | FGL190524X0 | 15.4(3)M1 | 1709 |  |
| txa-eyr-r01 | TXA Mt Dandenong Backup | VIC | 172.20.200.212 | ISR 2901 | FGL190524X3 | 15.4(3)M1 | 2438 |  |
| txa-ota-r01 | TXA Mt Dandenong Primary | VIC | 172.20.200.214 | ISR 2901 | FGL190524WW | 15.4(3)M1 | 1247 |  |

## Uptime

No devices rebooted

## Latest Firmware Revisions

### 2900 and 3900 series routers

<https://software.cisco.com/download/home/282774229/type/280805680/>

<https://software.cisco.com/download/home/282774228/type/280805680/>

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Stream | Currently Installed Version | Suggested version | Latest Version | Release Date |
| **15.3M** | 15.3(3)M4 |  | 15.3.3M10(MD) | 31 Jul 2017 |
| **15.4T** | 15.4(1)T3 |  | 15.4.2T4(ED) | 15 Oct 2015 |
| **15.4M** | 15.4(3)M1 |  | 15.4.3M10(MD) | 10 Aug 2018 |
| **15.6M** |  | **15.6.3M9(MD)** | 15.6.3M9(MD) | 21 Sep 2020 |
| **15.7M** |  | **15.7.3M8(MD)** | 15.7.3M8(MD) | 09 Mar 2021 |

### ASR 1001-X

<https://software.cisco.com/download/home/284932298/type/282046477/release>

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Stream | Currently Installed Version | Suggested version | Latest Version | Release Date |
| **3.13** | 3.13.2S |  | 3.13.9S(MD) | 17 Mar 2018 |
| **16.6** |  |  | 16.6.9(MD) | 26 Feb 2021 |
| **16.12** |  | **16.12.5(MD)** | 16.12.7(MD) | 03 Feb 2022 |
| **17.3** |  | **17.3.5(MD)** | 17.3.5(MD) | 10 Feb 2022 |

## Known critical Vulnerabilities

There are known relevant critical vulnerabilities with the installed firmware.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Cisco IOS Software Release | Advisory ID | Security Advisories | Publication Date | First Fixed |
| 15.3(3)M4  15.4(1)T3  15.4(3)M1  3.13.2S | CVE-2015-6280 | [Cisco IOS and IOS XE Software SSH Version 2 RSA-Based User Authentication Bypass Vulnerability](http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150923-sshpk) | 2015 Sep 23 | 15.3(3)M10  15.5(3)M6  15.6(3)M2a  3.16.10S(MD) |
| 15.3(3)M4  15.4(1)T3  15.4(3)M1 | CVE-2017-12240 | [Cisco IOS and IOS XE Software DHCP Remote Code Execution Vulnerability](https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-dhcp) | 2017 Sep 27 | 15.3(3)M10  15.5(3)M6  15.6(3)M2a |
| 3.13.2S | CVE-2019-12643 | [Cisco REST API Container for IOS XE Software Authentication Bypass Vulnerability](https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190828-iosxe-rest-auth-bypass) | 2019 Aug 28 | 3.16.10S(MD) |

## Aruba

<Aruba>

|  |  |  |
| --- | --- | --- |
| SoftwareName | ReleaseDate | Version |
| DRT 1.0\_84965 | Released on Sep 5, 2022 | v1 |
| FIPS aruba-mibs\_6.5.4.24\_84939.tar.gz | Released on Aug 31, 2022 | v6.5 |
| FIPS standard-mibs\_6.5.4.24\_84939.tar.gz | Released on Aug 31, 2022 | v6.5 |
| ArubaOS\_70xx\_6.5.4.24\_84938 | Released on Aug 31, 2022 | v6.5 |
| aruba-mibs\_6.5.4.24\_84938.tar.gz | Released on Aug 31, 2022 | v6.5 |
| FIPS ArubaOS\_72xx\_6.5.4.24-FIPS\_84939 | Released on Aug 31, 2022 | v6.5 |
| standard-mibs\_6.5.4.24\_84938.tar.gz | Released on Aug 31, 2022 | v6.5 |
| FIPS ArubaOS\_7280\_6.5.4.24-FIPS\_84939 | Released on Aug 31, 2022 | v6.5 |
| ArubaOS\_72xx\_6.5.4.24\_84938 | Released on Aug 31, 2022 | v6.5 |
| FIPS ArubaOS\_70xx\_6.5.4.24-FIPS\_84939 | Released on Aug 31, 2022 | v6.5 |

|  |  |  |
| --- | --- | --- |
| SoftwareName | ReleaseDate | Version |
| DRT 1.0\_84965 | Released on Sep 5, 2022 | v1 |
| FIPS aruba-mibs\_6.5.4.24\_84939.tar.gz | Released on Aug 31, 2022 | v6.5 |
| FIPS standard-mibs\_6.5.4.24\_84939.tar.gz | Released on Aug 31, 2022 | v6.5 |
| ArubaOS\_70xx\_6.5.4.24\_84938 | Released on Aug 31, 2022 | v6.5 |
| aruba-mibs\_6.5.4.24\_84938.tar.gz | Released on Aug 31, 2022 | v6.5 |
| FIPS ArubaOS\_72xx\_6.5.4.24-FIPS\_84939 | Released on Aug 31, 2022 | v6.5 |
| standard-mibs\_6.5.4.24\_84938.tar.gz | Released on Aug 31, 2022 | v6.5 |
| FIPS ArubaOS\_7280\_6.5.4.24-FIPS\_84939 | Released on Aug 31, 2022 | v6.5 |
| ArubaOS\_72xx\_6.5.4.24\_84938 | Released on Aug 31, 2022 | v6.5 |
| FIPS ArubaOS\_70xx\_6.5.4.24-FIPS\_84939 | Released on Aug 31, 2022 | v6.5 |

## F5

<F5\_t1>

|  |  |  |  |
| --- | --- | --- | --- |
| Release Number | Release Type | Image Name | Release Date |
| 12.0.0 | Major | BIGIP-12.0.0.0.0.606 | 09/02/2015 |
| 12.0.0.1 | Hotfix | Hotfix-BIGIP-12.0.0.1.0.628-HF1 | 01/07/2016 |
| 12.0.0.2 | Hotfix | Hotfix-BIGIP-12.0.0.2.0.644-HF2 | 04/11/2016 |
| 12.0.0.3 | Hotfix | Hotfix-BIGIP-12.0.0.3.0.654-HF3 | 06/02/2016 |
| 12.0.0.4 | Hotfix | Hotfix-BIGIP-12.0.0.4.0.674-HF4 | 09/01/2016 |
|  |  |  |  |
| 12.1.0 | Minor / LTS | BIGIP-12.1.0.0.0.1434 | 05/18/2016 |
| 12.1.0-HF1 | Hotfix | Hotfix-BIGIP-12.1.0.1.0.1447-HF1 | 06/21/2016 |

<F5\_t2>

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Major Release and Long-Term Stability  Release versions | First customer ship | End of Software Development | End of Technical Support | Latest maintenance release |
| 17.0.x | April 26, 2022 | July 31, 2023 | July 31, 2023 | N/A |
| 16.1.x | July 7, 2021 | July 31, 2025 | July 31, 2025 | 16.1.3 |
| 15.1.x | December 11, 2019 | December 31, 2024 | December 31, 2024 | 15.1.6 |
| 14.1.x | December 11, 2018 | December 31, 2023 | December 31, 2023 | 14.1.5 |
| 13.1.x | December 19, 2017 | December 31, 2022 | December 31, 2023 | 13.1.5 |

|  |  |  |
| --- | --- | --- |
| Software version or branch | End of Software Development | End of Technical Support |
| 16.0.x | October 7, 2021 | October 7, 2021 |
| 15.0.x | August 23, 2020 | August 23, 2020 |
| 14.1.2.4 | May 11, 2020 | May 11, 2020 |
| 14.0.x | November 9, 2019 | November 9, 2019 |
| 13.0.x | May 22, 2018 | May 22, 2019 |
| 12.0.0 | December 2, 2016 | December 2, 2017 |
| 12.1.x | May 18, 2021 | May 18, 2022 |
| 11.6.x | May 10, 2021 | May 10, 2022 |

## Fortiguard

<Fortiguard>

|  |  |  |  |
| --- | --- | --- | --- |
| Name | ReleaseDate | firstItemVersions | fullDescription |
| FortiADC -- Read-Only user able to modify system files | Sep 06, 2022 | 6.3.0 | FortiDDoS-F 6.3.0 FortiADC 6.2.1, 6.2.0, 6.1.5, 6.1.4, 6.1.3, 6.1.2, 6.1.1, 6.1.0, 6.0.4, 6.0.3, 6.0.2, 6.0.1, 6.0.0, 5.4.5, 5.4.4, 5.4.3, 5.4.2, 5.4.1, 5.4.0, 5.3.7, 5.3.6, 5.3.5, 5.3.4, 5.3.3, 5.3.2, 5.3.1, 5.3.0 |
| FortiAP & FortiAP-S & FortiAP-W2 & FortiAP-U - Command injection in CLI | Sep 06, 2022 | 7.2.0, 7.0.3, 7.0.1, 7.0.0, 6.4.7, 6.4.6, 6.4.5, 6.4.4, 6.4.3, 6.4.2, 6.4.1, 6.4.0, 6.2.6, 6.2.5, 6.2.4, 6.2.3, 6.2.2, 6.2.1, 6.2.0, 6.0.6, 6.0.5, 6.0.4, 6.0.3, 6.0.2, 6.0.1, 6.0.0 | FortiAP-W2 7.2.0, 7.0.3, 7.0.1, 7.0.0, 6.4.7, 6.4.6, 6.4.5, 6.4.4, 6.4.3, 6.4.2, 6.4.1, 6.4.0, 6.2.6, 6.2.5, 6.2.4, 6.2.3, 6.2.2, 6.2.1, 6.2.0, 6.0.6, 6.0.5, 6.0.4, 6.0.3, 6.0.2, 6.0.1, 6.0.0 FortiAP-U 6.2.3, 6.2.2, 6.2.1, 6.2.0, 6.0.4, 6.0.3, 6.0.2, 6.0.1, 6.0.0, 5.4.6, 5.4.5, 5.4.4, 5.4.3, 5.4.0 FortiAP 7.2.0, 7.0.3, 7.0.2, 7.0.1, 7.0.0, 6.4.7, 6.4.6, 6.4.5, 6.4.4, 6.4.3, 6.0.6, 6.0.5, 6.0.4, 6.0.3, 6.0.2, 6.0.1, 6.0.0 FortiAP-S 6.4.7, 6.4.6, 6.4.5, 6.4.4, 6.4.3, 6.4.2, 6.4.1, 6.4.0, 6.2.6, 6.2.5, 6.2.4, 6.2.3, 6.2.2, 6.2.1, 6.2.0, 6.0.6, 6.0.5, 6.0.4, 6.0.3, 6.0.2, 6.0.1, 6.0.0 |
| FortiMail - Cross-site scripting (XSS) in Webmail | Sep 06, 2022 | 7.0.3, 7.0.2, 7.0.1, 7.0.0, 6.4.7, 6.4.6, 6.4.5, 6.4.4, 6.4.3, 6.4.2, 6.4.1, 6.4.0, 6.2.8, 6.2.7, 6.2.6, 6.2.5, 6.2.4, 6.2.3, 6.2.2, 6.2.1, 6.2.0, 6.0.9, 6.0.8, 6.0.7, 6.0.6, 6.0.5, 6.0.4, 6.0.3, 6.0.2, 6.0.12, 6.0.11, 6.0.10, 6.0.1, 6.0.0 | FortiMail 7.0.3, 7.0.2, 7.0.1, 7.0.0, 6.4.7, 6.4.6, 6.4.5, 6.4.4, 6.4.3, 6.4.2, 6.4.1, 6.4.0, 6.2.8, 6.2.7, 6.2.6, 6.2.5, 6.2.4, 6.2.3, 6.2.2, 6.2.1, 6.2.0, 6.0.9, 6.0.8, 6.0.7, 6.0.6, 6.0.5, 6.0.4, 6.0.3, 6.0.2, 6.0.12, 6.0.11, 6.0.10, 6.0.1, 6.0.0 |
| FortiManager & FortiAnalyzer - Inter ADOM information leakage | Sep 06, 2022 | 7.2.0, 7.0.3, 7.0.2, 7.0.1, 7.0.0, 6.4.8, 6.4.7, 6.4.6, 6.4.5, 6.4.4, 6.4.3, 6.4.2, 6.4.1, 6.4.0, 6.2.9, 6.2.8, 6.2.7, 6.2.6, 6.2.5, 6.2.4, 6.2.3, 6.2.2, 6.2.1, 6.2.0, 6.0.9, 6.0.8, 6.0.7, 6.0.6, 6.0.5, 6.0.4, 6.0.3, 6.0.2, 6.0.11, 6.0.10, 6.0.1, 6.0.0 | FortiManager 7.2.0, 7.0.3, 7.0.2, 7.0.1, 7.0.0, 6.4.8, 6.4.7, 6.4.6, 6.4.5, 6.4.4, 6.4.3, 6.4.2, 6.4.1, 6.4.0, 6.2.9, 6.2.8, 6.2.7, 6.2.6, 6.2.5, 6.2.4, 6.2.3, 6.2.2, 6.2.1, 6.2.0, 6.0.9, 6.0.8, 6.0.7, 6.0.6, 6.0.5, 6.0.4, 6.0.3, 6.0.2, 6.0.11, 6.0.10, 6.0.1, 6.0.0 FortiAnalyzer 7.2.0, 7.0.3, 7.0.2, 7.0.1, 7.0.0, 6.4.8, 6.4.7, 6.4.6, 6.4.5, 6.4.4, 6.4.3, 6.4.2, 6.4.1, 6.4.0, 6.2.9, 6.2.8, 6.2.7, 6.2.6, 6.2.5, 6.2.4, 6.2.3, 6.2.2, 6.2.1, 6.2.0, 6.0.9, 6.0.8, 6.0.7, 6.0.6, 6.0.5, 6.0.4, 6.0.3, 6.0.2, 6.0.11, 6.0.10, 6.0.1, 6.0.0 |
| FortiOS - Flaws over krb keytab encryption scheme | Sep 06, 2022 | 7.2.0, 7.0.5, 7.0.4, 7.0.3, 7.0.2, 7.0.1, 7.0.0, 6.4.9, 6.4.8, 6.4.7, 6.4.6, 6.4.5, 6.4.4, 6.4.3, 6.4.2, 6.4.1, 6.4.0, 6.2.9, 6.2.8, 6.2.7, 6.2.6, 6.2.5, 6.2.4, 6.2.3, 6.2.2, 6.2.11, 6.2.10, 6.2.1, 6.2.0, 6.0.9, 6.0.8, 6.0.7, 6.0.6, 6.0.5, 6.0.4, 6.0.3, 6.0.2, 6.0.14, 6.0.13, 6.0.12, 6.0.11, 6.0.10, 6.0.1, 6.0.0 | FortiOS 7.2.0, 7.0.5, 7.0.4, 7.0.3, 7.0.2, 7.0.1, 7.0.0, 6.4.9, 6.4.8, 6.4.7, 6.4.6, 6.4.5, 6.4.4, 6.4.3, 6.4.2, 6.4.1, 6.4.0, 6.2.9, 6.2.8, 6.2.7, 6.2.6, 6.2.5, 6.2.4, 6.2.3, 6.2.2, 6.2.11, 6.2.10, 6.2.1, 6.2.0, 6.0.9, 6.0.8, 6.0.7, 6.0.6, 6.0.5, 6.0.4, 6.0.3, 6.0.2, 6.0.14, 6.0.13, 6.0.12, 6.0.11, 6.0.10, 6.0.1, 6.0.0 |

## CISCO

N-1 Check Failed, currently version 15.4.3M10, is far below the latest version

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Stream | Currently Installed Version | Suggested version | Latest Version | Release Date |
|  |  | text |  |  |
|  |  | 15.7.3M8(MD) | 15.7.3M8(MD) | 09-Mar-2021 |
|  |  | 15.6.3M9(MD) | 15.6.3M9(MD) | 21-Sep-2020 |
|  |  |  | 15.5.3M10(MD) | 27-Sep-2019 |
|  |  |  | 15.4.3M10(MD) | 10-Aug-2018 |

## Azure

<Azure>

<AzureCV>

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Name | Health | Column1 | Alert A/ | SKU | Subsc...1. | Locati.... | Data Path Availability | Health Probe Status SNAT Connection Count SYN Count | 1 |
| sfdev2949054-lb |  |  | 0 | Standard | Infra-SF-EA | North Eur... |  |  |  |
| sfdev2949055-lb |  |  | 0 | Standard | Infra-SF-EA | North Eur... |  |  |  |
| sfdev2949069-lb |  |  | 0 | Standard | Infra-SF-EA | North Eur... |  |  |  |
| sfdev2949070-lb |  |  | 0 | Standard | Infra-SF-EA | West Euro... |  |  |  |
| sfdev2949091-lb |  |  | 0 | Standard | Infra-SF-EA | North Eur... |  |  |  |
| sfdev2949156-lb |  |  | 0 | Standard | Infra-SF-EA | Central US |  |  |  |
| sfdev2949161-lb |  |  | 0 | Standard | Infra-SF-EA | West Euro... |  |  |  |
| sfqamfup2022412949087-I1 |  |  | 0 | Standard | Infra-SF-EA | West Euro... |  |  |  |
| sfqamoup2022412949088-I |  |  | 0 | Standard | Infra-SF-EA | West Euro... |  |  |  |

# Hardware EOL/EOS

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Product | End Of Life | End of SW Maintenance | End of Service Contract Renewal | End Of Support | Link |
| 2900 and 3900 series | September 9, 2016 | December 9, 2020 | March 9, 2022 | December 31, 2022 | [Info Link](https://www.cisco.com/c/en/us/products/collateral/routers/2900-series-integrated-services-routers-isr/eos-eol-notice-c51-737831.html) |
| ASR 1001-X | January 31, 2022 | August 1, 2023 | October 27, 2024 | July 31, 2027 | [Info Link](https://www.cisco.com/c/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/asr1001-x-1002-x-eol.html) |

# Recommendations

For the critical vulnerabilities:

* CVE-2015-6280: Devices running a vulnerable version of Cisco IOS and Cisco IOS XE Software are affected if SSHv2 access is configured with RSA-based user authentication and at least one user is configured with a public key.

**Option not configured on devices, not affected.**

* CVE-2017-12240: This vulnerability affects Cisco devices that are running a vulnerable release of Cisco IOS Software or Cisco IOS XE Software and are configured as a DHCP relay agent.

**Devices are not configured as DHCP agent**, **not affected.**

* CVE-2019-12643: This vulnerability affects Cisco devices that are configured to use a vulnerable version of Cisco REST API virtual service container.

**Option not configured on devices, not affected.**

# Hardware Status

## Temperature Status

| **Device Name** | **Description** | **Status** |
| --- | --- | --- |
| ndw-ads-r02 | CPU | normal |
| ndw-ads-r02 | Intake Left | normal |
| ndw-ads-r02 | Intake Right | normal |
| ndw-ads-r02 | Exhaust Right | normal |
| ndw-ads-r02 | Exhaust Left | normal |
| ndw-ads-r02 | Power Supply 1 | normal |
| ndw-ads-r02 | Power Supply 2 | normal |
| ndw-ads-r01 | CPU | normal |
| ndw-ads-r01 | Intake Left | normal |
| ndw-ads-r01 | Intake Right | normal |
| ndw-ads-r01 | Exhaust Right | normal |
| ndw-ads-r01 | Exhaust Left | normal |
| ndw-ads-r01 | Power Supply 1 | normal |
| ndw-ads-r01 | Power Supply 2 | normal |
| ndw-tvq-r02 | CPU | normal |
| ndw-tvq-r02 | Intake Left | normal |
| ndw-tvq-r02 | Intake Right | normal |
| ndw-tvq-r02 | Exhaust Right | normal |
| ndw-tvq-r02 | Exhaust Left | normal |
| ndw-tvq-r02 | Power Supply 1 | normal |
| ndw-tvq-r01 | CPU | normal |
| ndw-tvq-r01 | Intake Left | normal |
| ndw-tvq-r01 | Intake Right | normal |
| ndw-tvq-r01 | Exhaust Right | normal |
| ndw-tvq-r01 | Exhaust Left | normal |
| ndw-tvq-r01 | Power Supply 1 | normal |
| ndw-new-r02 | CPU | normal |
| ndw-new-r02 | Intake Left | normal |
| ndw-new-r02 | Intake Right | normal |
| ndw-new-r02 | Exhaust Right | normal |
| ndw-new-r02 | Exhaust Left | normal |
| ndw-new-r02 | Power Supply 1 | normal |
| ndw-new-r01 | CPU | normal |
| ndw-new-r01 | Intake Left | normal |
| ndw-new-r01 | Intake Right | normal |
| ndw-new-r01 | Exhaust Right | normal |
| ndw-new-r01 | Exhaust Left | normal |
| ndw-new-r01 | Power Supply 1 | normal |
| txa-nws-r01 | CPU | normal |
| txa-nws-r01 | Exhaust Fan | normal |
| txa-nws-r01 | N/A | normal |
| txa-nws-r01 | Intake Right(Bezel) | normal |
| txa-nws-r01 | Intake Right | normal |
| txa-crf-r01 | CPU | normal |
| txa-crf-r01 | Exhaust Fan | normal |
| txa-crf-r01 | N/A | normal |
| txa-crf-r01 | Intake Right(Bezel) | normal |
| txa-crf-r01 | Intake Right | normal |
| txa-bky-r01 | CPU | normal |
| txa-bky-r01 | Exhaust Fan | normal |
| txa-bky-r01 | N/A | normal |
| txa-bky-r01 | Intake Right(Bezel) | normal |
| txa-bky-r01 | Intake Right | normal |
| txa-art-r01 | CPU | normal |
| txa-art-r01 | Exhaust Fan | normal |
| txa-art-r01 | N/A | normal |
| txa-art-r01 | Intake Right(Bezel) | normal |
| txa-art-r01 | Intake Right | normal |
| txa-cml-r01 | CPU | normal |
| txa-cml-r01 | Exhaust Fan | normal |
| txa-cml-r01 | N/A | normal |
| txa-cml-r01 | Intake Right(Bezel) | normal |
| txa-cml-r01 | Intake Right | normal |
| ndw-gct-r01 | CPU | normal |
| ndw-gct-r01 | Intake Left | normal |
| ndw-gct-r01 | Intake Right | normal |
| ndw-gct-r01 | Exhaust Left | normal |
| ndw-gct-r01 | Exhaust Right | normal |
| ndw-gct-r01 | Power Supply | normal |
| ndw-can-r01 | CPU | normal |
| ndw-can-r01 | Intake Left | normal |
| ndw-can-r01 | Intake Right | normal |
| ndw-can-r01 | Exhaust Left | normal |
| ndw-can-r01 | Exhaust Right | normal |
| ndw-can-r01 | Power Supply | normal |
| txa-eyr-r01 | CPU | normal |
| txa-eyr-r01 | Exhaust Fan | normal |
| txa-eyr-r01 | N/A | normal |
| txa-eyr-r01 | Intake Right(Bezel) | normal |
| txa-eyr-r01 | Intake Right | normal |
| ndw-gct-r02 | CPU | normal |
| ndw-gct-r02 | Intake Left | normal |
| ndw-gct-r02 | Intake Right | normal |
| ndw-gct-r02 | Exhaust Left | normal |
| ndw-gct-r02 | Exhaust Right | normal |
| ndw-gct-r02 | Power Supply | normal |
| ndw-can-r02 | CPU | normal |
| ndw-can-r02 | Intake Left | normal |
| ndw-can-r02 | Intake Right | normal |
| ndw-can-r02 | Exhaust Left | normal |
| ndw-can-r02 | Exhaust Right | normal |
| ndw-can-r02 | Power Supply | normal |
| txa-ota-r01 | CPU | normal |
| txa-ota-r01 | Exhaust Fan | normal |
| txa-ota-r01 | N/A | normal |
| txa-ota-r01 | Intake Right(Bezel) | normal |
| txa-ota-r01 | Intake Right | normal |
| txa-wil-r01 | CPU | normal |
| txa-wil-r01 | Exhaust Fan | normal |
| txa-wil-r01 | N/A | normal |
| txa-wil-r01 | Intake Right(Bezel) | normal |
| txa-wil-r01 | Intake Right | normal |

## Power Supply Status

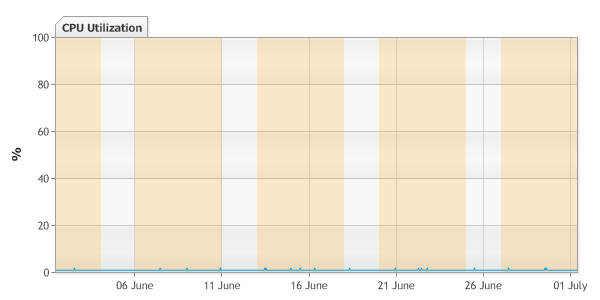
| **Device Name** | **Description** | **Status** |
| --- | --- | --- |
| ndw-ads-r02 | C3900 AC Power Supply 1 | normal |
| ndw-ads-r02 | C3900 AC Power Supply 2 | normal |
| ndw-ads-r01 | C3900 AC Power Supply 1 | normal |
| ndw-ads-r01 | C3900 AC Power Supply 2 | normal |
| ndw-tvq-r02 | C3900 AC Power Supply 1 | normal |
| ndw-tvq-r02 | Unknown | notPresent |
| ndw-tvq-r01 | C3900 AC Power Supply 1 | normal |
| ndw-tvq-r01 | Unknown | notPresent |
| ndw-new-r02 | C3900 AC Power Supply 1 | normal |
| ndw-new-r02 | Unknown | notPresent |
| ndw-new-r01 | C3900 AC Power Supply 1 | normal |
| ndw-new-r01 | Unknown | notPresent |
| txa-nws-r01 | C1941/C2901 AC Power Supply | normal |
| txa-crf-r01 | C1941/C2901 AC Power Supply | normal |
| txa-bky-r01 | C1941/C2901 AC Power Supply | normal |
| txa-art-r01 | C1941/C2901 AC Power Supply | normal |
| txa-cml-r01 | C1941/C2901 AC Power Supply | normal |
| ndw-gct-r01 | C2921/C2951 AC Power Supply | normal |
| ndw-gct-r01 | Redundant Power Supply | notPresent |
| ndw-can-r01 | C2921/C2951 AC Power Supply | normal |
| ndw-can-r01 | Redundant Power Supply | notPresent |
| txa-eyr-r01 | C1941/C2901 AC Power Supply | normal |
| ndw-gct-r02 | C2921/C2951 AC Power Supply | normal |
| ndw-gct-r02 | Redundant Power Supply | notPresent |
| ndw-can-r02 | C2921/C2951 AC Power Supply | normal |
| ndw-can-r02 | Redundant Power Supply | notPresent |
| txa-ota-r01 | C1941/C2901 AC Power Supply | normal |
| txa-wil-r01 | C1941/C2901 AC Power Supply | normal |

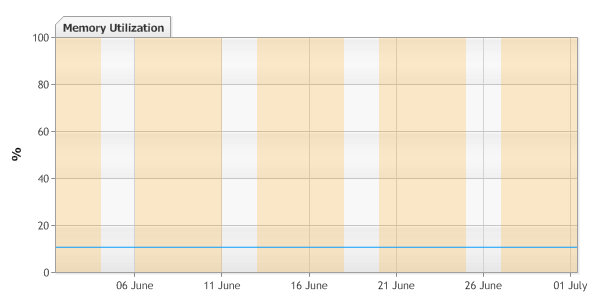
## Fan Status

| **Device Name** | **Description** | **Status** |
| --- | --- | --- |
| ndw-ads-r02 | Fan Tray | normal |
| ndw-ads-r02 | Fan 1 | normal |
| ndw-ads-r02 | Fan 2 | normal |
| ndw-ads-r02 | Fan 3 | normal |
| ndw-ads-r02 | Fan 4 | normal |
| ndw-ads-r02 | Fan 5 | normal |
| ndw-ads-r01 | Fan Tray | normal |
| ndw-ads-r01 | Fan 1 | normal |
| ndw-ads-r01 | Fan 2 | normal |
| ndw-ads-r01 | Fan 3 | normal |
| ndw-ads-r01 | Fan 4 | normal |
| ndw-ads-r01 | Fan 5 | normal |
| ndw-tvq-r02 | Fan Tray | normal |
| ndw-tvq-r02 | Fan 1 | normal |
| ndw-tvq-r02 | Fan 2 | normal |
| ndw-tvq-r02 | Fan 3 | normal |
| ndw-tvq-r02 | Fan 4 | normal |
| ndw-tvq-r02 | Fan 5 | normal |
| ndw-tvq-r01 | Fan Tray | normal |
| ndw-tvq-r01 | Fan 1 | normal |
| ndw-tvq-r01 | Fan 2 | normal |
| ndw-tvq-r01 | Fan 3 | normal |
| ndw-tvq-r01 | Fan 4 | normal |
| ndw-tvq-r01 | Fan 5 | normal |
| ndw-new-r02 | Fan Tray | normal |
| ndw-new-r02 | Fan 1 | normal |
| ndw-new-r02 | Fan 2 | normal |
| ndw-new-r02 | Fan 3 | normal |
| ndw-new-r02 | Fan 4 | normal |
| ndw-new-r02 | Fan 5 | normal |
| ndw-new-r01 | Fan Tray | normal |
| ndw-new-r01 | Fan 1 | normal |
| ndw-new-r01 | Fan 2 | normal |
| ndw-new-r01 | Fan 3 | normal |
| ndw-new-r01 | Fan 4 | normal |
| ndw-new-r01 | Fan 5 | normal |
| txa-nws-r01 | Fan Tray | normal |
| txa-nws-r01 | System Fan | normal |
| txa-crf-r01 | Fan Tray | normal |
| txa-crf-r01 | System Fan | normal |
| txa-bky-r01 | Fan Tray | normal |
| txa-bky-r01 | System Fan | normal |
| txa-art-r01 | Fan Tray | normal |
| txa-art-r01 | System Fan | normal |
| txa-cml-r01 | Fan Tray | normal |
| txa-cml-r01 | System Fan | normal |
| ndw-gct-r01 | Fan Tray | normal |
| ndw-gct-r01 | Fan 1 | normal |
| ndw-gct-r01 | Fan 2 | normal |
| ndw-gct-r01 | Fan 3 | normal |
| ndw-gct-r01 | Fan 4 | normal |
| ndw-can-r01 | Fan Tray | normal |
| ndw-can-r01 | Fan 1 | normal |
| ndw-can-r01 | Fan 2 | normal |
| ndw-can-r01 | Fan 3 | normal |
| ndw-can-r01 | Fan 4 | normal |
| txa-eyr-r01 | Fan Tray | normal |
| txa-eyr-r01 | System Fan | normal |
| ndw-gct-r02 | Fan Tray | normal |
| ndw-gct-r02 | Fan 1 | normal |
| ndw-gct-r02 | Fan 2 | normal |
| ndw-gct-r02 | Fan 3 | normal |
| ndw-gct-r02 | Fan 4 | normal |
| ndw-can-r02 | Fan Tray | normal |
| ndw-can-r02 | Fan 1 | normal |
| ndw-can-r02 | Fan 2 | normal |
| ndw-can-r02 | Fan 3 | normal |
| ndw-can-r02 | Fan 4 | normal |
| txa-ota-r01 | Fan Tray | normal |
| txa-ota-r01 | System Fan | normal |
| txa-wil-r01 | Fan Tray | normal |
| txa-wil-r01 | System Fan | normal |

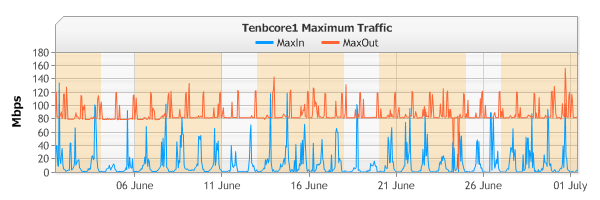
# Statistics

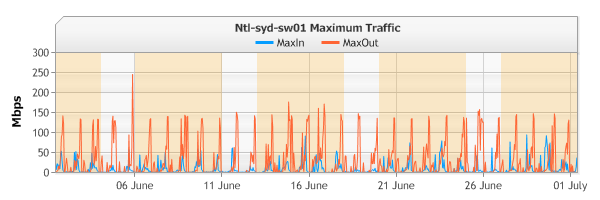
## ndw-ten-r01

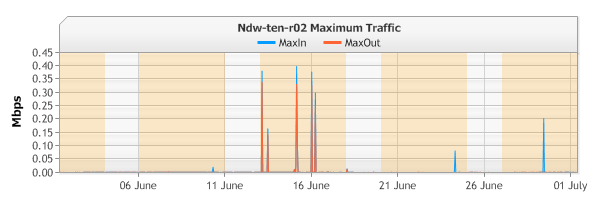


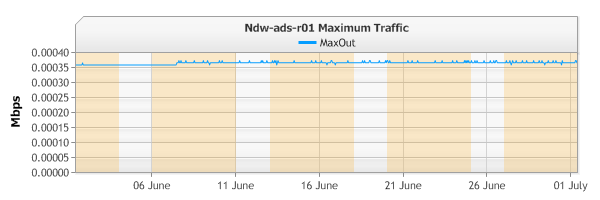


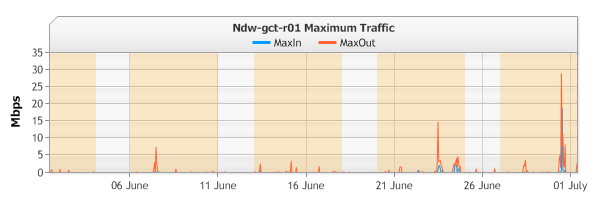
### Interfaces

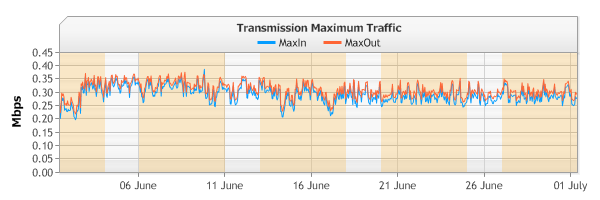


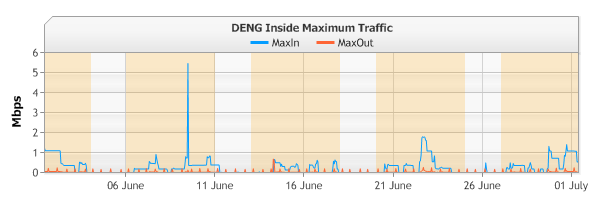




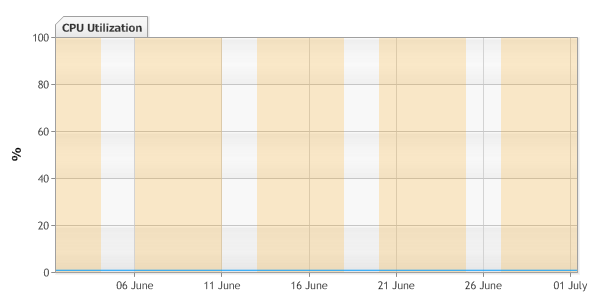


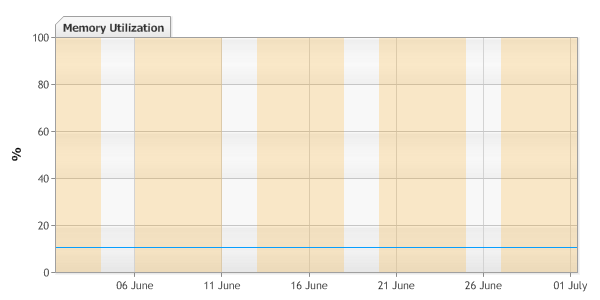




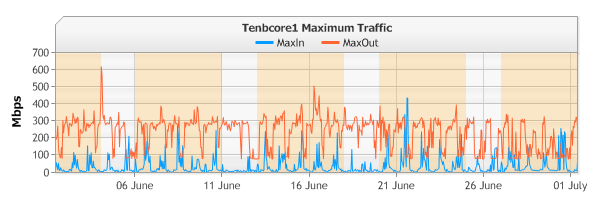


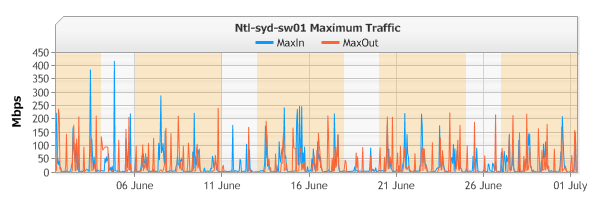
## ndw-ten-r02

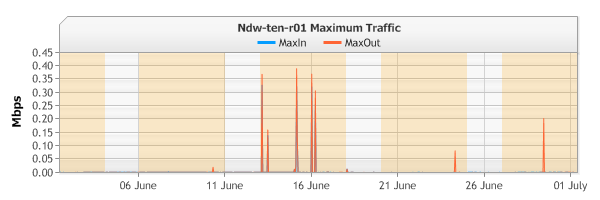


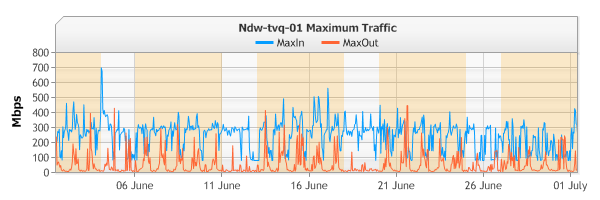


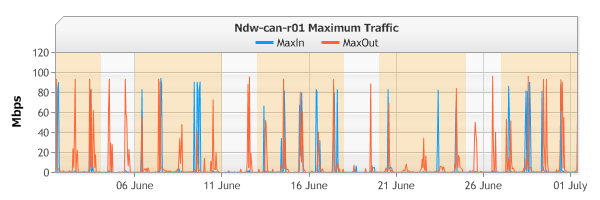
### Interfaces



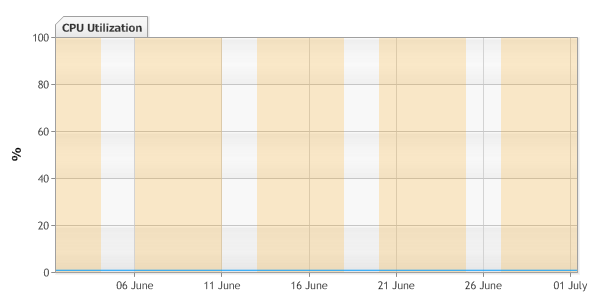


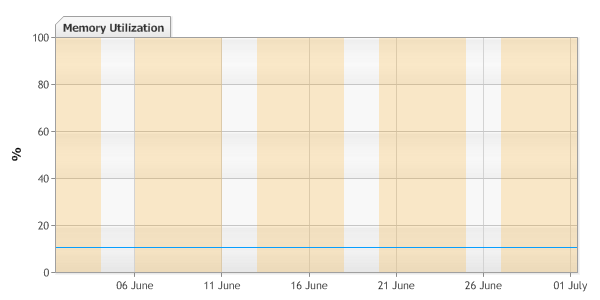




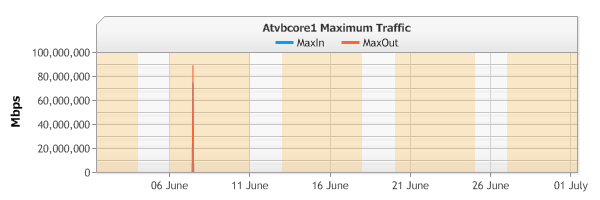


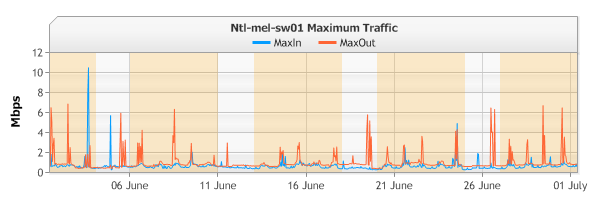
## ndw-atv-r01

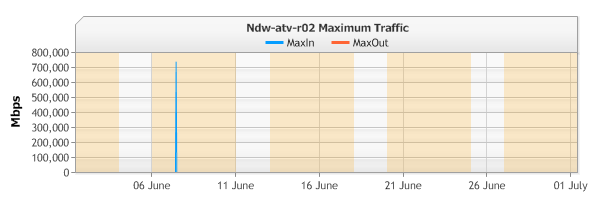


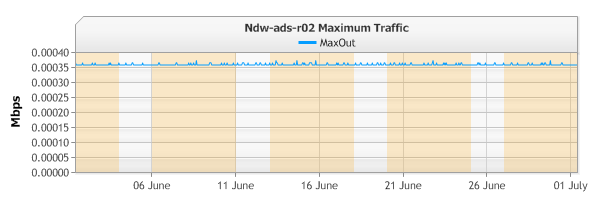


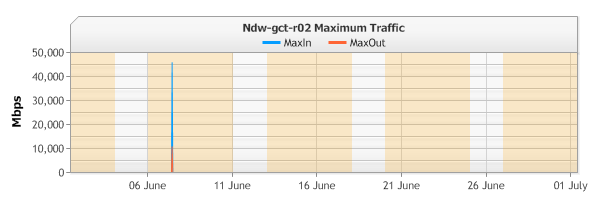
### Interfaces

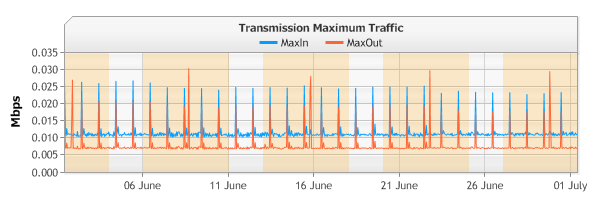


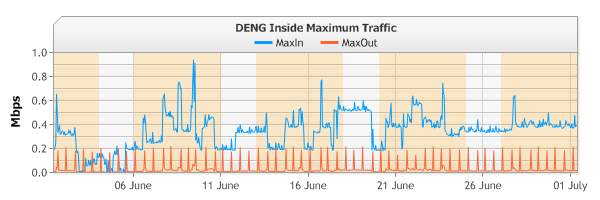


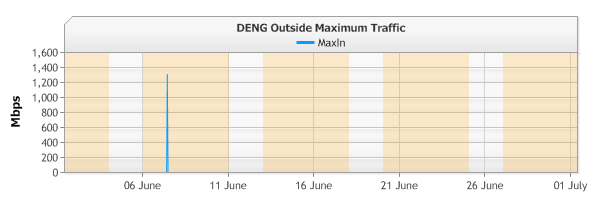




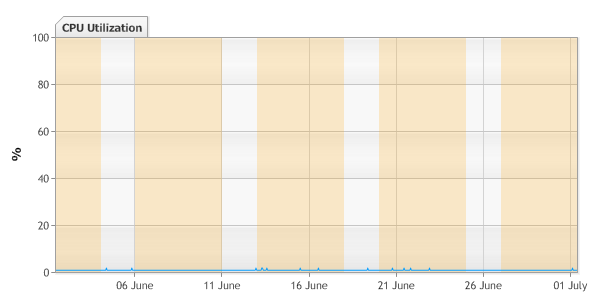


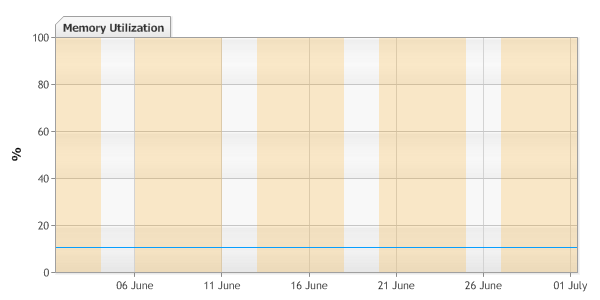




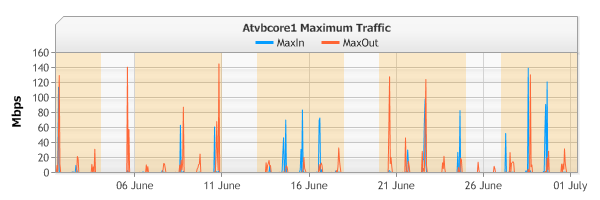


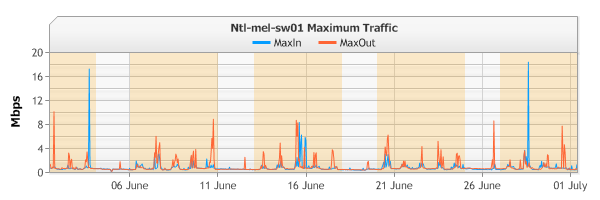
## ndw-atv-r02

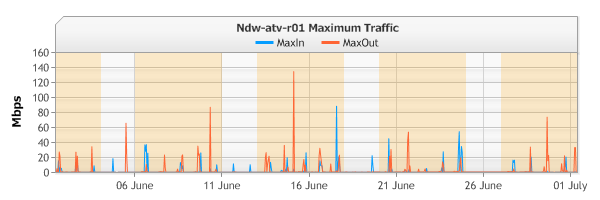


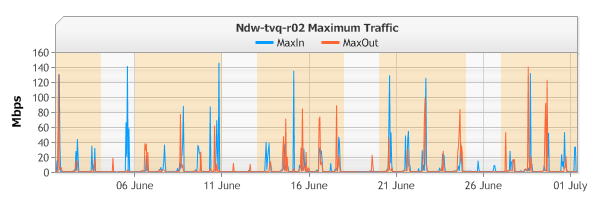


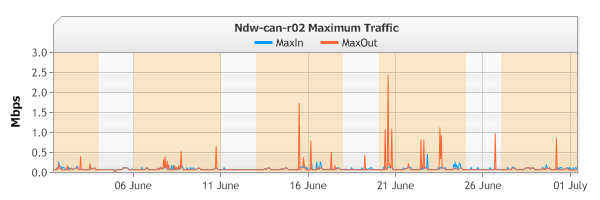
### Interfaces



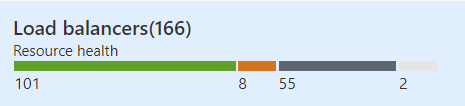
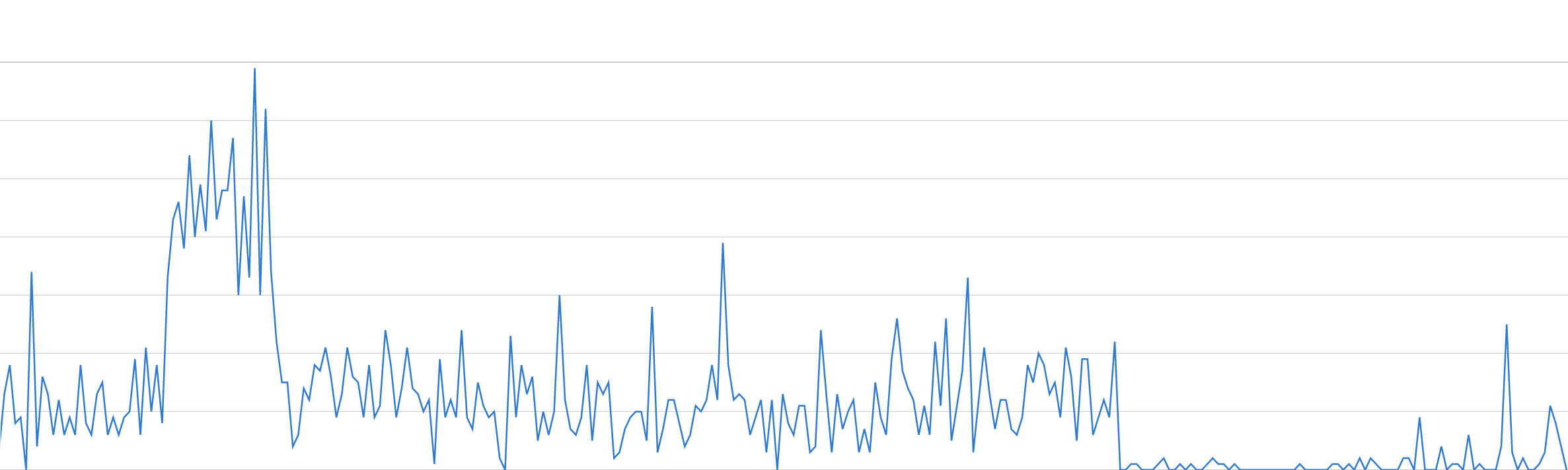








## More Charts

<charts>