CIS VMware NSX 4.x Tier-1 Gateway Router STIG Benchmark

v1.0.0 – 01-30-2025

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Overview

All CIS Benchmarks™ (Benchmarks) focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system and applications for vulnerabilities and quickly updating with the latest security patches.
- End-point protection (Antivirus software, Endpoint Detection and Response (EDR), etc.).
- Logging and monitoring user and system activity.

In the end, the Benchmarks are designed to be a key **component** of a comprehensive cybersecurity program.

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate VMware NSX 4.x Tier-1 Gateway Router and are looking to comply with the STIG guidance

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations (or rules) for securing a technology or a supporting platform. STIG Benchmark profiles are used to identify which Vulnerability Severity Category Code (CAT) each rule is associated with.

Description

The Rule Title from the STIG.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Additional Information

References from the STIG Rule if applicable.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **SEVERITY: CAT I**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be high severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT II**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be medium severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT III**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be low severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for VMware NSX 4.x Tier-1 Gateway Router

Contributor
Darren Stevenson

Recommendations

1 STIG RULES

VMware NSX

VMware NSX 4.x Tier-1 Gateway Router Secure Technical Implementation Guide (STIG)

Version: 1 Release: 2 Benchmark

Date: 30 Jan 2025

CLASSIFICATION unclassified

1.1 NT1R-4X-000016 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The NSX Tier-1 Gateway router must be configured to have all inactive interfaces removed.

```
GROUP ID: V-265518
RULE ID: SV-265518r999924
```

Rationale:

An inactive interface is rarely monitored or controlled and may expose a network to an undetected attack on that interface. Unauthorized personnel with access to the communication facility could gain access to a router by connecting to a configured interface that is not in use.

If an interface is no longer used, the configuration must be deleted and the interface disabled. For sub-interfaces, delete sub-interfaces that are on inactive interfaces and delete sub-interfaces that are themselves inactive. If the sub-interface is no longer necessary for authorized communications, it must be deleted.

Audit:

From the NSX Manager web interface, go to Networking >> Connectivity >> Tier-1 Gateways.
For every Tier-1 Gateway, expand the Tier-1 Gateway. Click on the number in the Linked Segments to review the currently linked segments.
For every Tier-1 Gateway, expand the Tier-1 Gateway. Expand Interfaces and GRE Tunnels, and click on the number of interfaces present to open the interfaces dialog. Review each interface or linked segment present to determine if they are not in use or inactive.
If there are any linked segments or service interfaces present on a Tier-1 Gateway that are not in use or inactive, this is a finding.

Remediation:

To remove a stale linked segment from a Tier-1 Gateway, do the following:
From the NSX Manager web interface, go to Networking >> Connectivity >> Segments and edit the target segment.
Under Connected Gateway, change to "None" and click "Save".
Note: The stale linked segment can also be deleted if there are no active workloads attached to it.
To remove a stale service interface from a Tier-1 Gateway, do the following:
From the NSX Manager web interface, go to Networking >> Connectivity >> Tier-1 Gateways >> Edit the target Tier-1 gateway.
Expand "Interfaces and GRE Tunnels", then click on the number of interfaces present to open the interfaces dialog.
On the stale service interface, select "Delete" and click "Delete" again to confirm.

Additional Information:

CCI-001414 Enforce approved authorizations for controlling the flow of information between connected systems based on organization-defined information flow control policies.

- NIST SP 800-53::AC-4
- NIST SP 800-53A::AC-4.1 (iii)
- NIST SP 800-53 Revision 4::AC-4
- NIST SP 800-53 Revision 5::AC-4

1.2 NT1R-4X-000027 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The NSX Tier-1 Gateway router must be configured to have the DHCP service disabled if not in use.

```
GROUP ID: V-265529
RULE ID: SV-265529r999926
```

Rationale:

A compromised router introduces risk to the entire network infrastructure, as well as data resources that are accessible via the network. The perimeter defense has no oversight or control of attacks by malicious users within the network. Preventing network breaches from within is dependent on implementing a comprehensive defense-in-depth strategy, including securing each device connected to the network. This is accomplished by following and implementing all security guidance applicable for each node type. A fundamental step in securing each router is to enable only the capabilities required for operation.

Audit:

From the NSX Manager web interface, go to Networking >> Connectivity >> Tier-1 Gateways.
For every Tier-1 Gateway expand the Tier-1 Gateway to view the DHCP configuration.
If a DHCP profile is configured and not in use, this is a finding.

Remediation:

From the NSX Manager web interface, go to Networking >> Connectivity >> Tier-1 Gateways and edit the target Tier-1 gateway.
Click "Set DHCP Configuration", select "No Dynamic IP Address Allocation", click "Save", and then close "Editing".

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

1.3 NT1R-4X-000102 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The NSX Tier-1 Gateway router must be configured to advertise a hop limit of at least 32 in Router Advertisement messages for IPv6 stateless auto-configuration deployments.

```
GROUP ID: V-265604
RULE ID: SV-265604r995285
```

Rationale:

The Neighbor Discovery protocol allows a hop limit value to be advertised by routers in a Router Advertisement message being used by hosts instead of the standardized default value. If a very small value was configured and advertised to hosts on the LAN segment, communications would fail due to the hop limit reaching zero before the packets sent by a host reached its destination.

Audit:

If IPv6 forwarding is not enabled, this is Not Applicable.
From the NSX Manager web interface, go to Networking >> Connectivity >> Tier-1 Gateways.
For every Tier-1 Gateway, expand Tier-1 Gateway >>Additional Settings.
Click on the ND profile name to view the hop limit.
If the hop limit is not configured to at least 32, this is a finding.

Remediation:

To configure the Neighbor Discovery hop limit, do the following:
From the NSX Manager web interface, go to Networking >> Connectivity >> Tier-1 Gateways >> edit the target Tier-1 gateway.
Expand Additional Settings and select an "ND Profile" from the drop down with a hop limit of 32 or more, then click "Close Editing".
Note: The default ND profile has a hop limit of 64 and cannot be edited. If required, create a new or edit another existing ND profile to use.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.4 NT1R-4X-000107 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The NSX Tier-1 Gateway router must be configured to have multicast disabled if not in use.

```
GROUP ID: V-265608
RULE ID: SV-265608r999927
```

Rationale:

A compromised router introduces risk to the entire network infrastructure, as well as data resources that are accessible via the network. The perimeter defense has no oversight or control of attacks by malicious users within the network. Preventing network breaches from within is dependent on implementing a comprehensive defense-in-depth strategy, including securing each device connected to the network. This is accomplished by following and implementing all security guidance applicable for each node type. A fundamental step in securing each router is to enable only the capabilities required for operation.

Audit:

From the NSX Manager web interface, go to Networking >> Connectivity >> Tier-1 Gateways.
For every Tier-1 Gateway, expand the Tier-1 Gateway then expand Multicast to view the Multicast configuration.
If Multicast is enabled and not in use, this is a finding.
If a Tier-1 Gateway is not linked to a Tier-0 Gateway, this is Not Applicable.

Remediation:

If not used, disable Multicast by doing the following:
From the NSX Manager web interface, go to Networking >> Connectivity >> Tier-1 Gateways and edit the target Tier-1 gateway.
Expand Multicast and change from "Enabled" to "Disabled" and then click "Save".

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	NT1R-4X-000016 (Manual)	☐	☐
1.2	NT1R-4X-000027 (Manual)	☐	☐
1.3	NT1R-4X-000102 (Manual)	☐	☐
1.4	NT1R-4X-000107 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
08-14-2025	1.0.0	Initial CIS Release