CIS VMware NSX 4.x Tier-1 Gateway Firewall 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

Target Technology Details

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

Version: 1 Release: 2 Benchmark

Date: 30 Jan 2025

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 Firewall 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

Supplementary information that does not correspond to any other field but may be useful to the user.

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.

Acknowledgements

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

Recommendations

1 STIG RULES

VMware NSX

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

Version: 1 Release: 2 Benchmark

Date: 30 Jan 2025

CLASSIFICATION unclassified

1.1 NT1F-4X-000004 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The NSX Tier-1 Gateway firewall must generate traffic log entries.

```
GROUP ID: V-265488
RULE ID: SV-265488r994833
```

Rationale:

Without establishing what type of event occurred, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack.

Audit event content that may be necessary to satisfy this requirement includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Associating event types with detected events in the network element logs provides a means of investigating an attack, recognizing resource usage or capacity thresholds, or identifying an improperly configured network element.

Satisfies: SRG-NET-000074-FW-000009, SRG-NET-000061-FW-000001, SRG-NET-000075-FW-000010, SRG-NET-000076-FW-000011, SRG-NET-000077-FW-000012, SRG-NET-000078-FW-000013, SRG-NET-000492-FW-000006, SRG-NET-000493-FW-000007

Audit:

From the NSX Manager web interface, go to Security >> Policy Management >> Gateway Firewall >> Gateway Specific Rules.

For each Tier-1 Gateway and for each rule, click the gear icon and verify the logging setting.

If logging is not "Enabled", this is a finding.

Remediation:

From the NSX Manager web interface, go to Security >> Policy Management >> Gateway Firewall >> Gateway Specific Rules.

For each Tier-1 Gateway and for each rule with logging disabled, click the gear icon and enable logging, and then click "Apply".

After all changes are made, click "Publish".

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000067 Employ automated mechanisms to monitor remote access methods.

- NIST SP 800-53::AC-17 (1)
- NIST SP 800-53A::AC-17 (1).1
- NIST SP 800-53 Revision 4::AC-17 (1)
- NIST SP 800-53 Revision 5::AC-17 (1)

CCI-000131 Ensure that audit records containing information that establishes when the event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 b

CCI-000132 Ensure that audit records containing information that establishes where the event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 c

CCI-000133 Ensure that audit records containing information that establishes the source of the event.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 d

CCI-000134 Ensure that audit records containing information that establishes the outcome of the event.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3

- NIST SP 800-53 Revision 5::AU-3 e

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

1.2 NT1F-4X-000015 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The NSX Tier-1 Gateway firewall must manage excess bandwidth to limit the effects of packet flooding types of denial-of-service (DoS) attacks.

```
GROUP ID: V-265493
RULE ID: SV-265493r994848
```

Rationale:

A firewall experiencing a DoS attack will not be able to handle production traffic load. The high usage and CPU caused by a DoS attack will also have an effect on control keep-alives and timers used for neighbor peering resulting in route flapping and will eventually black hole production traffic.

The device must be configured to contain and limit a DoS attack's effect on the device's resource usage. The use of redundant components and load balancing are examples of mitigating "flood-type" DoS attacks through increased capacity.

Satisfies: SRG-NET-000193-FW-000030, SRG-NET-000192-FW-000029, SRG-NET-000362-FW-000028

Audit:

From the NSX Manager web interface, go to Security >> Settings >> General Settings >> Firewall >> Flood Protection to view Flood Protection profiles.

If there are no Flood Protection profiles of type "Gateway", this is a finding.

For each gateway flood protection profile, if TCP Half Open Connection limit, UDP Active Flow Limit, ICMP Active Flow Limit, and Other Active Connection Limit are set to "None", this is a finding.

For each gateway flood protection profile, examine the "Applied To" field to view the Tier-1 Gateways to which it is applied.

If a gateway flood protection profile is not applied to all Tier-1 Gateways through one or more policies, this is a finding.

Remediation:

To create a new Flood Protection profile, do the following:

From the NSX Manager web interface, go to Security >> Settings >> General Settings >> Firewall >> Flood Protection >> Add Profile >> Add Firewall Profile.

Enter a name and specify appropriate values for the following: TCP Half Open Connection limit, UDP Active Flow Limit, ICMP Active Flow Limit, and Other Active Connection Limit.

Configure the "Applied To" field to contain Tier-1 Gateways and then click "Save".

Additional Information:

CCI-001095 Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.

- NIST SP 800-53::SC-5 (2)
- NIST SP 800-53A::SC-5 (2).1
- NIST SP 800-53 Revision 4::SC-5 (2)
- NIST SP 800-53 Revision 5::SC-5 (2)

CCI-001094 Restrict the ability of individuals to launch organization-defined denial of service attacks against other systems.

- NIST SP 800-53::SC-5 (1)
- NIST SP 800-53A::SC-5 (1).1
- NIST SP 800-53 Revision 4::SC-5 (1)
- NIST SP 800-53 Revision 5::SC-5 (1)

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

1.3 NT1F-4X-000016 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The NSX Tier-1 Gateway firewall must deny network communications traffic by default and allow network communications traffic by exception.

```
GROUP ID: V-265494
RULE ID: SV-265494r994851
```

Rationale:

To prevent malicious or accidental leakage of traffic, organizations must implement a deny-by-default security posture at the network perimeter. Such rulesets prevent many malicious exploits or accidental leakage by restricting the traffic to only known sources and only those ports, protocols, or services that are permitted and operationally necessary.

As a managed boundary interface, the firewall must block all inbound and outbound network traffic unless a filter is installed to explicitly allow it. The allow filters must comply with the Ports, Protocols, and Services Management (PPSM) Category Assurance List (CAL) and Vulnerability Assessment (VA).

Satisfies: SRG-NET-000202-FW-000039, SRG-NET-000205-FW-000040, SRG-NET-000235-FW-000133, SRG-NET-000364-FW-000031, SRG-NET-000364-FW-000032

Audit:

From the NSX Manager web interface, go to Security >> Policy Management >> Gateway Firewall >> Gateway Specific Rules >> Choose each Tier-1 Gateway in drop-down >> Policy_Default_Infra Section >> Action.

If the default_rule is set to Allow, this is a finding.

Remediation:

From the NSX Manager web interface, go to Security >> Policy Management >> Gateway Firewall >> Gateway Specific Rules >> Choose each Tier-1 Gateway in drop-down >> Policy_Default_Infra Section >> Action >> change the Action to Drop or Reject and click "Publish".

Additional Information:

CCI-001109 Deny network communications traffic by default and allow network communications traffic by exception at managed interfaces; and/or for organization-defined systems.

- NIST SP 800-53::SC-7 (5)
- NIST SP 800-53A::SC-7 (5).1 (i) (ii)
- NIST SP 800-53 Revision 4::SC-7 (5)
- NIST SP 800-53 Revision 5::SC-7 (5)

CCI-001097 Monitor and control communications at the external managed interfaces to the system and at key managed interfaces within the system.

- NIST SP 800-53::SC-7 a
- NIST SP 800-53A::SC-7.1 (iii)
- NIST SP 800-53 Revision 4::SC-7 a
- NIST SP 800-53 Revision 5::SC-7 a

CCI-001190 Fail to an organization-defined known-system state for the list of organization-defined types of system failures on organization-defined system components on the indicated components while preserving organization-defined system state information in failure.

- NIST SP 800-53::SC-24
- NIST SP 800-53A::SC-24.1 (iv)
- NIST SP 800-53 Revision 4::SC-24
- NIST SP 800-53 Revision 5::SC-24

CCI-002403 Only allow incoming communications from organization-defined authorized sources routed to organization-defined authorized destinations.

- NIST SP 800-53 Revision 4::SC-7 (11)
- NIST SP 800-53 Revision 5::SC-7 (11)

1.4 NT1F-4X-000020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The NSX Tier-1 Gateway firewall must be configured to send traffic log entries to a central audit server.

```
GROUP ID: V-265496
RULE ID: SV-265496r994857
```

Rationale:

Without the ability to centrally manage the content captured in the traffic log entries, identification, troubleshooting, and correlation of suspicious behavior would be difficult and could lead to a delayed or incomplete analysis of an ongoing attack.

The DOD requires centralized management of all network component audit record content. Network components requiring centralized traffic log management must have the ability to support centralized management. The content captured in traffic log entries must be managed from a central location (necessitating automation). Centralized management of traffic log records and logs provides for efficiency in maintenance and management of records, as well as the backup and archiving of those records.

Ensure at least one syslog server is configured on the firewall.

If the product inherently has the ability to store log records locally, the local log must also be secured. However, this requirement is not met since it calls for a use of a central audit server.

Satisfies: SRG-NET-000333-FW-000014, SRG-NET-000098-FW-000021

Audit:

From an NSX Edge Node shell hosting the Tier-1 Gateway, run the following command:

```
get logging-servers
```

Note: This check must be run from each NSX Edge Node hosting a Tier-1 Gateway, as they are configured individually.

or

If Node Profiles are used, from the NSX Manager web interface, go to System >> Configuration >> Fabric >> Profiles >> Node Profiles.

Click "All NSX Nodes" and verify the syslog servers listed.

If any configured logging servers are configured with a protocol of "udp", this is a finding.

If any configured logging servers are not configured with a level of "info", this is a finding.

If no logging-servers are configured, this is a finding.

Remediation:

To configure a profile to apply syslog servers to all NSX Edge Nodes, do the following:

From the NSX Manager web interface, go to System >> Configuration >> Fabric >> Profiles >> Node Profiles.

Click "All NSX Nodes" and then under "Syslog Servers" click "Add".

Enter the syslog server details and choose "Information" for the log level and click "Add".

or

(Optional) From an NSX Edge Node shell, run the following command to clear any existing incorrect logging-servers:

```
clear logging-servers
```

From an NSX Edge Node shell, run the following command to configure a tcp syslog server:

```
set logging-server proto tcp level info
```

From an NSX Edge Node shell, run the following command to configure a primary and backup TLS syslog server:

```
set logging-server proto tls level info serverca ca.pem clientca ca.pem
certificate cert.pem key key.pem
```

From an NSX Edge Node shell, run the following command to configure a LI-TLS syslog server:

set logging-server proto li-tls level info serverca root-ca.crt

Note: If using the protocols TLS or LI-TLS to configure a secure connection to a log server, the server and client certificates must be stored in /var/vmware/nsx/file-store/ on each NSX Edge Node appliance.

Note: Configure the syslog or Simple Network Management Protocol (SNMP) server to send an alert if the events server is unable to receive events from the NSX-T and also if denial-of-service (DoS) incidents are detected. This is true if the events server is STIG compliant.

Additional Information:

CCI-001851 Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

- NIST SP 800-53 Revision 4::AU-4 (1)
- NIST SP 800-53 Revision 5::AU-4 (1)

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

1.5 NT1F-4X-000027 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The NSX Tier-1 Gateway firewall must be configured to inspect traffic at the application layer.

```
GROUP ID: V-265500
RULE ID: SV-265500r994869
```

Rationale:

Application inspection enables the firewall to control traffic based on different parameters that exist within the packets such as enforcing application-specific message and field length. Inspection provides improved protection against application-based attacks by restricting the types of commands allowed for the applications. Application inspection all enforces conformance against published RFCs.

Some applications embed an IP address in the packet that needs to match the source address that is normally translated when it goes through the firewall. Enabling application inspection for a service that embeds IP addresses, the firewall translates embedded addresses and updates any checksum or other fields that are affected by the translation. Enabling application inspection for a service that uses dynamically assigned ports, the firewall monitors sessions to identify the dynamic port assignments, and permits data exchange on these ports for the duration of the specific session.

Audit:

From the NSX Manager web interface, go to Security >> Policy Management >> Gateway Firewall >> Gateway Specific Rules.

For each Tier-1 Gateway, review rules that do not have a Context Profile assigned.

For example, if a rule exists to allow SSH by service or custom port then it should have the associated SSH Context Profile applied.

If any rules with services defined have an associated suitable Context Profile but do not have one applied, this is a finding.

Remediation:

From the NSX Manager web interface, go to Security >> Policy Management >> Gateway Firewall >> Gateway Specific Rules.

For each Tier-1 Gateway and each rule that should have a Context Profile enabled, click the pencil icon in the Context Profile column.

Select an existing Context Profile or create a custom one then click "Apply".

After all changes are made, click "Publish".

Not all App IDs will be suitable for use in all cases and should be evaluated in each environment before use.

A list of App IDs for application layer rules is available here: https://docs.vmware.com/en/NSX-Application-IDs/index.html.

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

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	NT1F-4X-000004 (Manual)	☐	☐
1.2	NT1F-4X-000015 (Manual)	☐	☐
1.3	NT1F-4X-000016 (Manual)	☐	☐
1.4	NT1F-4X-000020 (Manual)	☐	☐
1.5	NT1F-4X-000027 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
08-18-2025	1.0.0	Initial CIS Release