CIS VMware NSX 4.x Distributed 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 Distributed 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 Distributed 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

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

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 Distributed Firewall

Recommendations

1 STIG RULES

VMware NSX

VMware NSX 4.x Distributed Firewall Secure Technical Implementation Guide (STIG)

Version: 1 Release: 2 Benchmark

Date: 30 Jan 2025

CLASSIFICATION unclassified

1.1 NDFW-4X-000004 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The NSX Distributed Firewall must generate traffic log entries that can be sent by the ESXi hosts to the central syslog.

```
GROUP ID: V-265612
RULE ID: SV-265612r993933
```

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 utilization or capacity thresholds, or identifying an improperly configured network element.

Satisfies: SRG-NET-000074-FW-000009, 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, navigate to Security >> Policy Management >> Distributed Firewall >> All Rules.

For each rule, click the gear icon and verify the logging setting.

If logging is not enabled for any rule, this is a finding.

Remediation:

From the NSX Manager web interface, navigate to Security >> Policy Management >> Distributed Firewall >> Category Specific Rules.

For each rule that has logging disabled, click the gear icon, toggle the logging option to "Enable", and click "Apply".

or

For each Policy or Section, click the menu icon on the left and select "Enable Logging for All Rules".

After all changes are made, click "Publish".

NOTE: Syslog and alert monitoring procedure: Syslog configuration is in the vSphere ESXi STIG where there is a control to require syslog configuration. This is because the NSX Distributed Firewall data plane is not directly configured to communicate with the central log server/syslog. The firewall runs in a distributed manner across ESXi hosts, and the traffic logs for the DFW are located on each host for the traffic it processes and are forwarded from each host to a centralized syslog server. Thus, ESXi hosts must be configured to send the syslogs to the log server. In turn, the syslog must be configured to send all required alerts, including when unknown or out-of-order extension headers are detected in inbound and outbound IPv6 traffic.

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-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 NDFW-4X-000015 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The NSX Distributed Firewall must limit the effects of packet flooding types of denial-of-service (DoS) attacks.

```
GROUP ID: V-265618
RULE ID: SV-265618r993951
```

Rationale:

A firewall experiencing a DoS attack will not be able to handle production traffic load. The high utilization 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 utilization. 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, navigate to Security >> Settings >> General Settings >> Firewall >> Flood Protection to view Flood Protection profiles.

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

If the TCP Half Open Connection limit, UDP Active Flow Limit, ICMP Active Flow Limit, and Other Active Connection Limit are "not set" or SYN Cache and RST Spoofing is not Enabled on a profile, this is a finding.

For each distributed firewall flood protection profile, examine the "Applied To" field to view the workloads it is protecting.

If a distributed firewall flood protection profile is not applied to all workloads through one or more policies, this is a finding.

Remediation:

To create a new Flood Protection profile:

From the NSX Manager web interface, navigate 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.

Enable SYN Cache and RST Spoofing, configure the "Applied To" field with the appropriate security groups, and 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 NDFW-4X-000016 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The NSX Distributed Firewall must deny network communications traffic by default and allow network communications traffic by exception.

```
GROUP ID: V-265619
RULE ID: SV-265619r993954
```

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-000235-FW-000133

Audit:

From the NSX Manager web interface, navigate to Security >> Policy Management >> Distributed Firewall >> Category Specific Rules >> APPLICATION >> Default Layer3 Section >> Default Layer3 Rule >> Action.

If the Default Layer3 Rule is set to "ALLOW", this is a finding.

Remediation:

From the NSX Manager web interface, navigate to Security >> Policy Management >> Distributed Firewall >> Category Specific Rules >> APPLICATION >> Default Layer3 Section >> Default Layer3 Rule and change action to "Drop" or "Reject".

After all changes are made, click "Publish".

Note: Before enabling, ensure the necessary rules to whitelist approved traffic are created and published, or this change may result in loss of communication for workloads.

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-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

1.4 NDFW-4X-000027 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The NSX Distributed Firewall must be configured to inspect traffic at the application layer.

```
GROUP ID: V-265628
RULE ID: SV-265628r993981
```

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. By 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. By 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, navigate to Security >> Distributed Firewall >> All Rules.

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, navigate to Security >> Policy Management >> Distributed Firewall >> Category Specific Rules.

For 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".

Note: This control does not apply to Ethernet rules.

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

1.5 NDFW-4X-000029 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The NSX Distributed Firewall must configure SpoofGuard to restrict it from accepting outbound packets that contain an illegitimate address in the source address.

```
GROUP ID: V-265630
RULE ID: SV-265630r993987
```

Rationale:

A compromised host in an enclave can be used by a malicious platform to launch cyberattacks on third parties. This is a common practice in "botnets", which are a collection of compromised computers using malware to attack other computers or networks. Distributed denial-of-service (DDoS) attacks frequently leverage IP source address spoofing to send packets to multiple hosts that in turn will then send return traffic to the hosts with the IP addresses that were forged. This can generate significant amounts of traffic. Therefore, protection measures to counteract IP source address spoofing must be taken.

SpoofGuard is a tool that is designed to prevent virtual machines from sending traffic with an IP address from which it is not authorized to send traffic. In the instance that a virtual machine's IP address does not match the IP address on the corresponding logical port and segment address binding in SpoofGuard, the virtual machine's virtual network interface card (vNIC) is prevented from accessing the network entirely. SpoofGuard can be configured at the port or segment level. There are several reasons SpoofGuard might be used, but for the distributed firewall it will guarantee that rules will not be inadvertently (or deliberately) bypassed. For distributed firewall (DFW) rules created using IP sets as sources or destinations, the possibility always exists that a virtual machine could have its IP address forged in the packet header, thereby bypassing the rules in question.

Audit:

Identity SpoofGuard profiles in use by doing the following:

From the NSX Manager web interface, navigate to Networking >> Connectivity >> Segments >> NSX.

For each segment, expand view Segment Profiles >> SpoofGuard to note the profiles in use.

Review SpoofGuard profile configuration by doing the following:

From the NSX Manager web interface, navigate to Networking >> Connectivity >> Segments >> Profiles >> Segment Profiles.

Review the SpoofGuard profiles previously identified as assigned to segments to ensure the following configuration:

Port Bindings: Yes

If a segment is not configured with a SpoofGuard profile that has port bindings enabled, this is a finding.

Remediation:

To create a segment profile with SpoofGuard enabled, do the following:

From the NSX Manager web interface, navigate to Networking >> Connectivity >> Segments >> Profiles >> Segment Profiles >> Add Segment Profile >> SpoofGuard.

Enter a profile name and enable port bindings, then click "Save".

To update a segments SpoofGuard profile, do the following:

From the NSX Manager web interface, navigate to the Networking >> Connectivity >> Segments >> NSX, and click "Edit" from the drop-down menu next to the target segment.

Expand "Segment Profiles" then choose the new SpoofGuard profile from the drop-down list, and then click "Save".

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

1.6 NDFW-4X-000034 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The NSX Distributed Firewall must configure an IP Discovery profile to disable trust on every use method.

```
GROUP ID: V-265633
RULE ID: SV-265633r993996
```

Rationale:

A compromised host in an enclave can be used by a malicious platform to launch cyberattacks on third parties. This is a common practice in "botnets", which are a collection of compromised computers using malware to attack other computers or networks. Distributed denial-of-service (DDoS) attacks frequently leverage IP source address spoofing to send packets to multiple hosts that in turn will then send return traffic to the hosts with the IP addresses that were forged. This can generate significant amounts of traffic. Therefore, protection measures to counteract IP source address spoofing must be taken.

IP Discovery in NSX uses DHCP and DHCPv6 snooping, Address Resolution Protocol (ARP) snooping, Neighbor Discovery (ND) snooping, and VM Tools to learn MAC and IP addresses.

The discovered MAC and IP addresses are used to achieve ARP/ND suppression, which minimizes traffic between VMs connected to the same logical switch. The addresses are also used by the SpoofGuard and distributed firewall (DFW) components. DFW uses the address bindings to determine the IP address of objects in firewall rules.

By default, the discovery methods ARP snooping and ND snooping operate in a mode called trust on first use (TOFU). In TOFU mode, when an address is discovered and added to the realized bindings list, that binding remains in the realized list forever. TOFU applies to the first "n" unique <IP, MAC, VLAN> bindings discovered using ARP/ND snooping, where "n" is the configurable binding limit. Users can disable TOFU for ARP/ND snooping. The methods will then operate in trust on every use (TOEU) mode. In TOEU mode, when an address is discovered, it is added to the realized bindings list and when it is deleted or expired, it is removed from the realized bindings list. DHCP snooping and VM Tools always operate in TOEU mode.

Audit:

Identify IP Discovery profiles in use by doing the following:

From the NSX Manager web interface, navigate to Networking >> Connectivity >> Segments >> NSX.

For each segment, expand view Segment Profiles >> IP Discovery to note the profiles in use.

Review IP Discovery profile configuration by doing the following:

From the NSX Manager web interface, navigate to Networking >> Connectivity >> Segments >> Profiles >> Segment Profiles.

Review the IP Discovery profiles previously identified as assigned to segments to ensure the following configuration:

Duplicate IP Detection: Enabled

ARP Snooping: Enabled

ARP Binding Limit: 1

DHCP Snooping: Disabled

DHCP Snooping - IPv6: Disabled

VMware Tools: Disabled

VMware Tools - IPv6: Disabled

Trust on First Use: Enabled

If a segment is not configured with an IP Discovery profile that is configured with the settings above, this is a finding.

Remediation:

To create a segment profile for IP Discovery, do the following:

From the NSX Manager web interface, navigate to Networking >> Connectivity >> Segments >> NSX >> Profiles >> Segment Profiles >> Add Segment Profile >> IP Discovery.

Enter a profile name then configure the below settings:

Duplicate IP Detection: Enabled

ARP Snooping: Enabled

ARP Binding Limit: 1

DHCP Snooping: Disabled

DHCP Snooping - IPv6: Disabled

VMware Tools: Disabled

VMware Tools - IPv6: Disabled

Trust on First Use: Enabled

Click "Save".

Note: ND Snooping may be enabled if IPv6 is in use.

To update a segments IP Discovery profile, do the following:

From the NSX Manager web interface, navigate to the Networking >> Connectivity >> Segments >> NSX, and click "Edit" from the drop-down menu next to the target segment.

Expand "Segment Profiles" then choose the new IP Discovery profile from the drop-down list, and then click "Save".

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	NDFW-4X-000004 (Manual)	☐	☐
1.2	NDFW-4X-000015 (Manual)	☐	☐
1.3	NDFW-4X-000016 (Manual)	☐	☐
1.4	NDFW-4X-000027 (Manual)	☐	☐
1.5	NDFW-4X-000029 (Manual)	☐	☐
1.6	NDFW-4X-000034 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
08-27-2025	1.0.0	Initial CIS Release