CIS VMware NSX 4.x Tier-0 Gateway Router STIG Benchmark

v1.0.0 - 08-19-2025

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-0 Gateway Router 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-0 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

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-0 Gateway Router

Recommendations

1 STIG RULES

VMware NSX

VMware NSX 4.x Tier-0 Gateway Router Secure Technical Implementation Guide (STIG)

Version: 1 Release: 2 Benchmark

Date: 30 Jan 2025

CLASSIFICATION unclassified

1.1 NT0R-4X-000013 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The NSX Tier-0 Gateway router must be configured to disable Protocol Independent Multicast (PIM) on all interfaces that are not required to support multicast routing.

```
GROUP ID: V-265390
RULE ID: SV-265390r994520
```

Rationale:

If multicast traffic is forwarded beyond the intended boundary, it could be intercepted by unauthorized or unintended personnel. Limiting where within the network a given multicast group's data is permitted to flow is an important first step in improving multicast security.

A scope zone is an instance of a connected region of a given scope. Zones of the same scope cannot overlap while zones of a smaller scope will fit completely within a zone of a larger scope. For example, Admin-local scope is smaller than Site-local scope, so the administratively configured boundary fits within the bounds of a site. According to RFC 4007 IPv6 Scoped Address Architecture (section 5), scope zones are also required to be "convex from a routing perspective"; that is, packets routed within a zone must not pass through any links that are outside of the zone. This requirement forces each zone to be one contiguous island rather than a series of separate islands.

As stated in the DOD IPv6 IA Guidance for MO3, "One should be able to identify all interfaces of a zone by drawing a closed loop on their network diagram, engulfing some routers and passing through some routers to include only some of their interfaces." Therefore, it is imperative that the network engineers have documented their multicast topology and thereby knows which interfaces are enabled for multicast. Once this is done, the zones can be scoped as required.

Audit:

From the NSX Manager web interface, go to Networking >> Connectivity >> Tier-0 Gateways.

For every Tier-0 Gateway, expand the Tier-0 Gateway >> Interfaces and GRE Tunnels, and click on the number of interfaces present to open the interfaces dialog.

Expand each interface that is not required to support multicast routing, then expand "Multicast" and verify PIM is disabled.

If PIM is enabled on any interfaces that are not supporting multicast routing, this is a finding.

Remediation:

Disable multicast PIM routing on interfaces that are not required to support multicast by doing the following:

From the NSX Manager web interface, go to Networking >> Connectivity >> Tier-0 Gateways and expand the target Tier-0 gateway.

Expand "Interfaces and GRE Tunnels", click on the number of interfaces present to open the interfaces dialog, and then select "Edit" on the target interface.

Expand "Multicast", change PIM to "disabled", and then click "Save".

1.2 NT0R-4X-000016 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The NSX Tier-0 Gateway router must be configured to have all inactive interfaces removed.

```
GROUP ID: V-265393
RULE ID: SV-265393r994529
```

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-0 Gateways.

For every Tier-0 Gateway, expand the Tier-0 Gateway >> Interfaces and GRE Tunnels, and click on the number of interfaces present to open the interfaces dialog.

Review each interface present to determine if they are not in use or inactive.

If there are any interfaces present on a Tier-0 Gateway that are not in use or inactive, this is a finding.

Remediation:

Remove unused interfaces by doing the following:

From the NSX Manager web interface, go to Networking >> Connectivity >> Tier-0 Gateways and expand the target Tier-0 gateway.

Expand "Interfaces and GRE Tunnels", then click on the number of interfaces present to open the interfaces dialog.

Select "Delete" on the unneeded interface, and then click "Delete" again to confirm.

1.3 NT0R-4X-000027 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The NSX Tier-0 Gateway router must be configured to have the Dynamic Host Configuration Protocol (DHCP) service disabled if not in use.

```
GROUP ID: V-265404
RULE ID: SV-265404r999914
```

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-0 Gateways.

For every Tier-0 Gateway, expand the Tier-0 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-0 Gateways and edit the target Tier-0 gateway.

Click "Set DHCP Configuration", select "No Dynamic IP Address Allocation", and then click "Save". Close "Editing".

1.4 NT0R-4X-000029 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The NSX Tier-0 Gateway router must be configured to use encryption for Open Shortest Path First (OSPF) routing protocol authentication.

```
GROUP ID: V-265406
RULE ID: SV-265406r994568
```

Rationale:

A rogue router could send a fictitious routing update to convince a site's perimeter router to send traffic to an incorrect or even a rogue destination. This diverted traffic could be analyzed to learn confidential information about the site's network or used to disrupt the network's ability to communicate with other networks. This is known as a "traffic attraction attack" and is prevented by configuring neighbor router authentication for routing updates. However, using clear-text authentication provides little benefit since an attacker can intercept traffic and view the authentication key. This would allow the attacker to use the authentication key in an attack.

This requirement applies to all IPv4 and IPv6 protocols that are used to exchange routing or packet forwarding information; this includes all Interior Gateway Protocols (such as OSPF, Enhanced Interior Gateway Routing Protocol [EIGRP], and Intermediate System to Intermediate System [IS-IS]) and exterior gateway protocols (such as Border Gateway Protocol [BGP]), multiprotocol label switching (MPLS)-related protocols (such as Label Distribution Protocol [LDP]), and multicast-related protocols.

Typically routing protocols must be setup on both sides so knowing the authentication key does not necessarily mean an attacker would be able to setup a rogue router and peer with a legitimate one and inject malicious routes.

Audit:

If the Tier-0 Gateway is not using OSPF, this is Not Applicable.

To verify OSPF areas are using authentication with encryption, do the following:

From the NSX Manager web interface, go to Networking >> Connectivity >> Tier-0 Gateways.

For every Tier-0 Gateway, expand the "Tier-0 Gateway".

Expand "OSPF", click the number next to "Area Definition", and view the "Authentication" field for each area.

If OSPF area definitions do not have the "Authentication" field set to "MD5" and a "Key ID" and "Password" configured, this is a finding.

Remediation:

To set authentication for OSPF area definitions, do the following:

From the NSX Manager web interface, go to Networking >> Connectivity >> Tier-0 Gateways, and expand the target Tier-0 gateway.

Expand "OSPF", click the number next to "Area Definition". Select "Edit" on the target OSPF Area Definition.

Change the Authentication drop-down to MD5, enter a Key ID and Password, and then click "Save".

Note: The MD5 password can have a maximum of 16 characters.

1.5 NT0R-4X-000051 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The NSX Tier-0 Gateway router must be configured to restrict it from accepting outbound IP packets that contain an illegitimate address in the source address field by enabling Unicast Reverse Path Forwarding (uRPF).

```
GROUP ID: V-265428
RULE ID: SV-265428r994634
```

Rationale:

A malicious platform can use a compromised host in an enclave 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 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. When uRPF is enabled in strict mode, the packet must be received on the interface that the device would use to forward the return packet; thereby mitigating IP source address spoofing.

Audit:

From the NSX Manager web interface, go to Networking >> Connectivity >> Tier-0 Gateways.

For every Tier-0 Gateway, expand Tier-0 Gateway >> Interfaces and GRE Tunnels, and then click on the number of interfaces present to open the interfaces dialog.

Expand each interface to view the URPF Mode configuration.

If URPF Mode is not set to "Strict" on any interface, this is a finding.

Remediation:

Enable strict URPF mode on interfaces by doing the following:

From the NSX Manager web interface, go to Networking >> Connectivity >> Tier-0 Gateways and expand the target Tier-0 gateway.

Expand "Interfaces and GRE Tunnels", click on the number of interfaces present to open the interfaces dialog, and then select "Edit" on the target interface.

From the drop-down, set the URPF mode to "Strict" and then click "Save".

1.6 NT0R-4X-000055 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The NSX Tier-0 Gateway must be configured to use a unique password for each autonomous system (AS) with which it peers.

```
GROUP ID: V-265432
RULE ID: SV-265432r994646
```

Rationale:

If the same keys are used between External Border Gateway Protocol (eBGP) neighbors, the chance of a hacker compromising any of the BGP sessions increases. It is possible that a malicious user exists in one autonomous system who would know the key used for the eBGP session. This user would then be able to hijack BGP sessions with other trusted neighbors.

Audit:

If the Tier-0 Gateway is not using BGP, this is Not Applicable.

Since the NSX Tier-0 Gateway does not reveal the current password, interview the router administrator to determine if unique passwords are being used.

If unique passwords are not being used for each AS, this is a finding.

Remediation:

To set authentication for BGP neighbors, do the following:

From the NSX Manager web interface, go to Networking >> Connectivity >> Tier-0 Gateways, and expand the target Tier-0 gateway.

Expand BGP. Next to "BGP Neighbors", click on the number present to open the dialog, then select "Edit" on the target BGP Neighbor.

Expand "BGP", click the number next to "BGP Neighbors". Select "Edit" on the target BGP neighbor.

Under Timers & Password, enter a password up to 20 characters that is different from other autonomous systems, and then click "Save".

1.7 NT0R-4X-000054 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The NSX Tier-0 Gateway router must be configured to implement message authentication for all control plane protocols.

```
GROUP ID: V-265431
RULE ID: SV-265431r994643
```

Rationale:

A rogue router could send a fictitious routing update to convince a site's perimeter router to send traffic to an incorrect or a rogue destination. This diverted traffic could be analyzed to learn confidential information about the site's network or used to disrupt the network's ability to communicate with other networks. This is known as a "traffic attraction attack" and is prevented by configuring neighbor router authentication for routing updates.

This requirement applies to all IPv4 and IPv6 protocols that are used to exchange routing or packet forwarding information. This includes Border Gateway Protocol (BGP), Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Intermediate System to Intermediate System (IS-IS) and Label Distribution Protocol (LDP).

Satisfies: SRG-NET-000230-RTR-000001, SRG-NET-000230-RTR-000002

Audit:

If the Tier-0 Gateway is not using BGP or OSPF, this is Not Applicable.

Since the router does not reveal if a BGP password is configured, interview the router administrator to determine if a password is configured on BGP neighbors.

If BGP neighbors do not have a password configured, this is a finding.

To verify OSPF areas are using authentication, do the following:

From the NSX Manager web interface, go to Networking >> Connectivity >> Tier-0 Gateways.

For every Tier-0 Gateway expand the "Tier-0 Gateway".

Expand "OSPF", click the number next to "Area Definition", and view the "Authentication" field for each area.

If OSPF area definitions do not have Password or MD5 set for authentication, this is a finding.

Remediation:

To set authentication for BGP neighbors, do the following:

From the NSX Manager web interface, go to Networking >> Connectivity >> Tier-0 Gateways, and expand the target Tier-0 gateway.

Expand BGP. Next to BGP Neighbors, click on the number present to open the dialog, then select "Edit" on the target BGP Neighbor.

Under Timers & Password, enter a password up to 20 characters, and then click "Save".

To set authentication for OSPF Area definitions, do the following:

From the NSX Manager web interface, go to Networking >> Connectivity >> Tier-0 Gateways, and expand the target Tier-0 gateway.

Expand OSPF. Next to "Area Definition", click on the number present to open the dialog, and then select "Edit" on the target OSPF Area.

Change the Authentication drop-down to Password or MD5, enter a Key ID and/or Password, and then click "Save".

1.8 NT0R-4X-000064 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The NSX Tier-0 Gateway router must be configured to have Internet Control Message Protocol (ICMP) unreachable notifications disabled on all external interfaces.

```
GROUP ID: V-265441
RULE ID: SV-265441r999915
```

Rationale:

The ICMP supports IP traffic by relaying information about paths, routes, and network conditions. Routers automatically send ICMP messages under a wide variety of conditions. Host unreachable ICMP messages are commonly used by attackers for network mapping and diagnosis.

Audit:

If the Tier-0 Gateway is deployed in an Active/Active HA mode, this is Not Applicable.

From the NSX Manager web interface, go to Security >> Policy Management >> Gateway Firewall >> Gateway Specific Rules, and choose each Tier-0 Gateway in the drop-down.

Review each Tier-0 Gateway Firewall rule to verify one exists to drop ICMP unreachable messages.

If a rule does not exist to drop ICMP unreachable messages, this is a finding.

Remediation:

To configure a shared rule to drop ICMP unreachable messages, do the following:

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

Click "Add Rule" (add a policy first, if needed) and under "Services", select "ICMP Destination Unreachable" and "Apply".

Enable logging and under the "Applied To" field select the target Tier-0 gateways and click "Publish" to enforce the new rule.

Note: A rule can also be created under Gateway Specific Rules to meet this requirement.

1.9 NT0R-4X-000065 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The NSX Tier-0 Gateway router must be configured to have Internet Control Message Protocol (ICMP) mask replies disabled on all external interfaces.

```
GROUP ID: V-265442
RULE ID: SV-265442r999916
```

Rationale:

The ICMP supports IP traffic by relaying information about paths, routes, and network conditions. Routers automatically send ICMP messages under a wide variety of conditions. Mask Reply ICMP messages are commonly used by attackers for network mapping and diagnosis.

Audit:

If the Tier-0 Gateway is deployed in an Active/Active HA mode, this is Not Applicable.

From the NSX Manager web interface, go to Security >> Policy Management >> Gateway Firewall >> Gateway Specific Rules, and choose each Tier-0 Gateway in the drop-down menu.

Review each Tier-0 Gateway Firewall rule to verify one exists to drop ICMP mask replies.

If a rule does not exist to drop ICMP mask replies, this is a finding.

Remediation:

To configure a shared rule to drop ICMP unreachable messages, do the following:

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

Click "Add Rule" (add a policy first if needed). Under "Services", select the custom service that identifies ICMP mask replies, and then click "Apply".

Enable logging, under the "Applied To" field select the target Tier-0 gateways' external interfaces, and then select "Publish" to enforce the new rule.

Note: A rule can also be created under Gateway Specific Rules to meet this requirement.

Note: A pre-created service for ICMP mask replies does not exist by default and may need created.

1.10 NT0R-4X-000066 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The NSX Tier-0 Gateway router must be configured to have Internet Control Message Protocol (ICMP) redirects disabled on all external interfaces.

```
GROUP ID: V-265443
RULE ID: SV-265443r999917
```

Rationale:

The ICMP supports IP traffic by relaying information about paths, routes, and network conditions. Routers automatically send ICMP messages under a wide variety of conditions. Redirect ICMP messages are commonly used by attackers for network mapping and diagnosis.

Audit:

If the Tier-0 Gateway is deployed in an Active/Active HA mode, this is Not Applicable.

From the NSX Manager web interface, go to Security >> Policy Management >> Gateway Firewall >> Gateway Specific Rules, and choose each Tier-0 Gateway in the drop-down menu.

Review each Tier-0 Gateway Firewalls rules to verify one exists to drop ICMP redirects.

If a rule does not exist to drop ICMP redirects, this is a finding.

Remediation:

To configure a shared rule to drop ICMP unreachable messages, do the following:

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

Click "Add Rule" (add a policy first if needed). Under "Services", select "ICMP Redirect", and then click "Apply".

To enable logging, under the "Applied To" field, select the target Tier-0 gateways' external interfaces, and then click "Publish" to enforce the new rule.

Note: A rule can also be created under Gateway Specific Rules to meet this requirement.

1.11 NT0R-4X-000067 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The NSX Tier-0 Gateway router must be configured to use the Border Gateway Protocol (BGP) maximum prefixes feature to protect against route table flooding and prefix de-aggregation attacks.

```
GROUP ID: V-265444
RULE ID: SV-265444r994682
```

Rationale:

The effects of prefix de-aggregation can degrade router performance due to the size of routing tables and also result in black-holing legitimate traffic. Initiated by an attacker or a misconfigured router, prefix de-aggregation occurs when the announcement of a large prefix is fragmented into a collection of smaller prefix announcements.

In 1997, misconfigured routers in the Florida Internet Exchange network (AS7007) de-aggregated every prefix in their routing table and started advertising the first /24 block of each of these prefixes as their own. Faced with this additional burden, the internal routers became overloaded and crashed repeatedly. This caused prefixes advertised by these routers to disappear from routing tables and reappear when the routers came back online. As the routers came back after crashing, they were flooded with the routing table information by their neighbors. The flood of information would again overwhelm the routers and cause them to crash. This process of route flapping served to destabilize not only the surrounding network but also the entire internet. Routers trying to reach those addresses would choose the smaller, more specific /24 blocks first. This caused backbone networks throughout North America and Europe to crash.

Maximum prefix limits on peer connections combined with aggressive prefix-size filtering of customers' reachability advertisements will effectively mitigate the de-aggregation risk. BGP maximum prefix must be used on all eBGP routers to limit the number of prefixes that it should receive from a particular neighbor, whether customer or peering autonomous system (AS). Consider each neighbor and how many routes they should be advertising and set a threshold slightly higher than the number expected.

Audit:

If the Tier-0 Gateway is not using BGP, this is Not Applicable.

From the NSX Manager web interface, go to Networking >> Connectivity >> Tier-0 Gateways.

For every Tier-0 Gateway with BGP enabled, expand the Tier-0 Gateway.

Expand BGP, click on the number next to "BGP Neighbors", and then view the router filters for each neighbor.

If "Maximum Routes" is not configured, or a route filter does not exist for each BGP neighbor, this is a finding.

Remediation:

To set maximum prefixes for BGP neighbors, do the following:

From the NSX Manager web interface, go to Networking >> Connectivity >> Tier-0 Gateways and expand the target Tier-0 gateway.

Expand BGP. Next to "BGP Neighbors", click on the number present to open the dialog, and then select "Edit" on the target BGP Neighbor.

Click "Router Filter", add or edit an existing router filter, enter a number for "Maximum Routes", and then click "Add".

Click "Apply", then click "Save" to finish the configuration.

1.12 NT0R-4X-000102 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The NSX Tier-0 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-265479
RULE ID: SV-265479r994787
```

Rationale:

The Neighbor Discovery (ND) 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-0 Gateways.

For every Tier-0 Gateway, expand Tier-0 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-0 Gateways >> edit the target Tier-0 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.

1.13 NT0R-4X-000091 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The NSX Tier-0 Gateway router must be configured to use its loopback address as the source address for Internal Border Gateway Protocol (IBGP) peering sessions.

```
GROUP ID: V-265468
RULE ID: SV-265468r994754
```

Rationale:

Using a loopback address as the source address offers a multitude of uses for security, access, management, and scalability of the Border Gateway Protocol (BGP) routers. It is easier to construct appropriate ingress filters for router management plane traffic destined to the network management subnet since the source addresses will be from the range used for loopback interfaces instead of a larger range of addresses used for physical interfaces. Log information recorded by authentication and syslog servers will record the router’s loopback address instead of the numerous physical interface addresses.

The routers within the iBGP domain should also use loopback addresses as the source address when establishing BGP sessions.

Audit:

If the Tier-0 Gateway is not using iBGP, this is Not Applicable.

From the NSX Manager web interface, go to Networking >> Connectivity >> Tier-0 Gateways.

For every Tier-0 Gateway with BGP enabled, expand the Tier-0 Gateway.

Expand BGP, click on the number next to BGP Neighbors, then view the source address for each neighbor.

If the Source Address is not configured as the Tier-0 Gateway loopback address for the iBGP session, this is a finding.

Remediation:

To configure a loopback interface, do the following:

From the NSX Manager web interface, go to Networking >> Connectivity >> Tier-0 Gateways and expand the target Tier-0 gateway.

Expand interfaces and click "Add Interface".

Enter a name, select "Loopback" as the Type, enter an IP address, select an Edge Node for the interface, then click "Save".

Note: More than one loopback may need to be configured depending on the routing architecture.

To set the source address for BGP neighbors, do the following:

From the NSX Manager web interface, go to Networking >> Connectivity >> Tier-0 Gateways >> expand the target Tier-0 gateway.

Expand BGP >> next to BGP Neighbors, click on the number present to open the dialog >> select "Edit" on the target BGP Neighbor.

Under Source Addresses, configure the source address with the loopback address and click "Save".

1.14 NT0R-4X-000106 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The NSX Tier-0 Gateway router must be configured to have routing protocols disabled if not in use.

```
GROUP ID: V-265483
RULE ID: SV-265483r999918
```

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-0 Gateways.

For every Tier-0 Gateway, expand the Tier-0 Gateway to view if border gateway protocol (BGP) or Open Shortest Path First (OSPF) is enabled.

If BGP and/or OSPF is enabled and not in use, this is a finding.

Remediation:

If not used in the implementation, then disable BGP, do the following:

From the NSX Manager web interface, go to Networking >> Connectivity >> Tier-0 Gateways and edit the target Tier-0 gateway.

Expand BGP, change from "On" to "Off", and then click "Save".

If not used in the implementation, then disable OSPF, do the following:

From the NSX Manager web interface, go to Networking >> Connectivity >> Tier-0 Gateways and edit the target Tier-0 gateway.

Expand OSPF, change from "Enabled" to "Disabled", and then click "Save".

1.15 NT0R-4X-000107 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The NSX Tier-0 Gateway router must be configured to have multicast disabled if not in use.

```
GROUP ID: V-265484
RULE ID: SV-265484r999919
```

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-0 Gateways.

For every Tier-0 Gateway, expand the Tier-0 Gateway, then expand "Multicast" to view the multicast configuration.

If multicast is enabled and not in use, this is a finding.

Remediation:

If not used, disable Multicast by doing the following:

From the NSX Manager web interface, go to Networking >> Connectivity >> Tier-0 Gateways and edit the target Tier-0 gateway.

Expand Multicast, change from "Enabled" to "Disabled", and then click "Save".

1.16 NT0R-4X-000108 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The NSX Tier-0 Gateway router must be configured to use encryption for border gateway protocol (BGP) routing protocol authentication.

```
GROUP ID: V-265485
RULE ID: SV-265485r994805
```

Rationale:

A rogue router could send a fictitious routing update to convince a site's perimeter router to send traffic to an incorrect or even a rogue destination. This diverted traffic could be analyzed to learn confidential information about the site's network or used to disrupt the network's ability to communicate with other networks. This is known as a "traffic attraction attack" and is prevented by configuring neighbor router authentication for routing updates. However, using clear-text authentication provides little benefit since an attacker can intercept traffic and view the authentication key. This would allow the attacker to use the authentication key in an attack.

This requirement applies to all IPv4 and IPv6 protocols that are used to exchange routing or packet forwarding information; this includes all Interior Gateway Protocols (such as Open Shortest Path First [OSPF], Enhanced Interior Gateway Routing Protocol [EIGRP], and Intermediate System to Intermediate System [IS-IS]) and Exterior Gateway Protocols (such as BGP), multiprotocol label switching (MPLS)-related protocols (such as Label Distribution Protocol [LDP]), and multicast-related protocols.

Audit:

If the Tier-0 Gateway is not using BGP, this is Not Applicable.

To verify BGP neighbors are using authentication with encryption, do the following:

From the NSX Manager web interface, go to Networking >> Connectivity >> Tier-0 Gateways.

For every Tier-0 Gateway, expand the "Tier-0 Gateway".

Expand "BGP", click the number next to "BGP Neighbors" and expand each BGP neighbor.

Expand the "Timers and Password" section and review the Password field.

If any BGP neighbors do not have a password configured, this is a finding.

Remediation:

To set authentication for BGP neighbors, do the following:

From the NSX Manager web interface, go to Networking >> Connectivity >> Tier-0 Gateways, and expand the target Tier-0 gateway.

Expand BGP. Next to "BGP Neighbors", click on the number present to open the dialog, then select "Edit" on the target BGP Neighbor.

Expand "BGP", click the number next to "BGP Neighbors". Select "Edit" on the target BGP neighbor.

Under Timers & Password, enter a password up to 20 characters, and then click "Save".

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	NT0R-4X-000013 (Manual)	☐	☐
1.2	NT0R-4X-000016 (Manual)	☐	☐
1.3	NT0R-4X-000027 (Manual)	☐	☐
1.4	NT0R-4X-000029 (Manual)	☐	☐
1.5	NT0R-4X-000051 (Manual)	☐	☐
1.6	NT0R-4X-000055 (Manual)	☐	☐
1.7	NT0R-4X-000054 (Manual)	☐	☐
1.8	NT0R-4X-000064 (Manual)	☐	☐
1.9	NT0R-4X-000065 (Manual)	☐	☐
1.10	NT0R-4X-000066 (Manual)	☐	☐
1.11	NT0R-4X-000067 (Manual)	☐	☐
1.12	NT0R-4X-000102 (Manual)	☐	☐
1.13	NT0R-4X-000091 (Manual)	☐	☐
1.14	NT0R-4X-000106 (Manual)	☐	☐
1.15	NT0R-4X-000107 (Manual)	☐	☐
1.16	NT0R-4X-000108 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
08-19-2025	1.0.0	Initial CIS Release