www.intentflow.co

Intentflow Verify - Verification report

22 of 22 device configurations fully analyzed.

PREPARED FOR	**Atlas Networks**
ASSESSMENT DATE	**September 7, 2026 20:42 UTC**

RESULT

PASS WITH ISSUES

Critical	**0**
Medium	**4 issue groups - 42 instances**
Informational	**1 issue group - 2 instances**

Contents

Executive summary

Intentflow Verify analyzed the supplied network configurations to identify routing, reachability, redundancy, policy and configuration risks.

PASS WITH ISSUES

Critical	**0**
Medium	**4 issue groups - 42 instances**
Informational	**1 issue group - 2 instances**

The assessment identified **44** finding instances across **5** consolidated issue groups, including **4** medium-severity. None of these prevent the network from operating as configured.

Most important findings:

MEDIUM [V-001] One device's failure would disconnect part of the network - hub01

MEDIUM [V-002, V-003, V-004 +16 more] SSH (TCP/22) is blocked on a path that is otherwise working (19 instances) - branch01, branch02, branch03, +17 more

MEDIUM [V-005, V-012, V-017] HTTPS (TCP/443) is blocked on a path that is otherwise working (3 instances) - branch03, branch11, branch15, +1 more

MEDIUM [V-024 - V-042] An access-list denies encrypted management access but permits the cleartext one (19 instances) - branch01, branch02, branch03, +16 more

INFORMATIONAL [V-043 - V-044] One device behaves differently from its structural peers (2 instances) - branch03, branch07, branch11, +1 more

Scope and method

What was assessed, how much of it could be analyzed, and how far the results should be trusted.

What was assessed

Devices analyzed: **22**
Fully analyzed: **22**
Platforms represented: Cisco IOS/IOS-XE (**22**)
Finding confidence: **25** high, **19** medium, **0** inferred

Exposure and coverage

22/22 device configurations analyzed - **100%** fully parsed.

Supported analysis

This assessment covered:

- configuration parsing and vendor recognition
- routing protocol relationships (BGP, OSPF, IPsec)
- forwarding behavior and reachability between devices

- access-list and route-policy behavior
- cross-device configuration consistency
- IP addressing and physical-link consistency, where topology data was supplied

Not assessed

The following were outside the available evidence and were not assessed:

- real-time interface counters, packet loss or optical power levels
- hardware failure state
- application-layer behavior
- device state or dynamic behavior not represented in the configuration snapshot
- business intent - whether the configuration matches what your organization meant to build

Findings describe behavior modelled from the uploaded configuration. A passing result means a tested property holds within that model and the evidence available - it is not an unrestricted guarantee about the running network.

Discovered network model

What the supplied configuration describes. Nothing here is a finding.

What the supplied configuration describes, before anything is assessed about it. These are counts of what the network states about itself.

Devices	**22**
Connected LANs	**21**
Routed prefixes	**65**

Segmentation and routing domains

OSPF area: 0

Comparable devices

Devices grouped by identical structure. This establishes only which devices are alike enough to be compared with each other - it makes no claim that any of them is misconfigured, and no behaviour has been compared here.

Devices	Count	Shared structure	Comparison strength
branch01, branch02, branch03, branch04, +17 more	21	1 LAN; 1 transit; 1 loopback; OSPF	high

Comparison strength reflects how specific the shared structure is: devices matching only on having one interface and no routing protocols are alike in a way that says very little, so a difference between them means less.

1 device had no structural peer in this upload, so no peer comparison is possible for it.

Forwarding paths

0 routed prefixes have more than one forwarding path
65 routed prefixes have a single next hop
A single next hop is normal for access and spoke networks; this is a description of the topology, not a finding about it.

Assessment results

Every finding counted by what it puts at risk, and what was actually tested.

Intentflow executed a set of network correctness and behavior checks across the supplied configuration snapshot. Every check that ran is listed in Appendix D, including those that found nothing.

Risk area	Status	Critical	Medium	Informational	Total
Availability	Review	0	23	0	23
Security	Review	0	19	0	19
Correctness	Healthy	0	0	2	2

Domain	Scope	Result
Routing	21 OSPF adjacencies	21 passed, 0 with findings
Forwarding	231 reachability pairs	231 passed, 0 with findings
Forwarding	21 local networks	21 reachable, 0 with findings
Policy	15 checks executed *	1 produced findings

** Policy checks evaluate configuration objects whose total population the model does not enumerate. The figure shown is the number of checks executed, not objects examined.*

Section	Status
Routing	PASS
Policy	19 Medium
Forwarding	23 Medium, 2 Informational

Change since the previous assessment

Compared against this environment's previous Verify run.

Metric	Previous	Current
Verdict	PASS WITH ISSUES	PASS WITH ISSUES
Coverage	100%	100%
Critical	0	0
Medium	39	42

Metric	Previous	Current
Informational	1	2

Forwarding behaviour

1,260 relationships were present in both runs and could be compared. Of those, **3** changed state - **3** newly unreachable, **0** newly reachable.

From	To	Protocol	Was	Now
10.103.0.0/24	10.200.0.0/24	HTTPS (TCP/443)	Reachable	Blocked
10.111.0.0/24	10.200.0.0/24	HTTPS (TCP/443)	Reachable	Blocked
10.115.0.0/24	10.200.0.0/24	HTTPS (TCP/443)	Reachable	Blocked

Findings

Every finding, most severe first. Findings sharing the same check and problem across multiple links, peers, or devices are shown once with every instance listed, rather than as repeated near-identical cards.

Correlated observations

Relationships between findings that individual checks cannot see. Every finding below is still reported and counted individually; nothing here replaces or re-rates one.

19 devices have findings from more than one verification check. branch03 has **4** findings across **3** checks.

MEDIUM **[V-001] One device's failure would disconnect part of the network - hub01**

Risk area: Availability

With hub01 unavailable, 2 of 21 discovered destinations stop being reachable.

Why: The dataplane was re-simulated with hub01 deactivated, and these destinations had no remaining path: 10.101.0.0, 10.102.0.0. Every other discovered destination still had one, so this is about redundancy for these specific destinations rather than the device being important in general.

Impact: Anything depending on those destinations would be offline for the duration of the outage, with no alternate path to fail over to.

Suggested action: Confirm whether a single path to these destinations via hub01 is intended - single-homing is often a deliberate cost decision. If it isn't, a second path or a backup route removes the dependency. Coverage: 15 of 22 devices were simulated.

MEDIUM **[V-002, V-003, V-004 +16 more] SSH (TCP/22) is blocked on a path that is otherwise working (19 instances) - branch01, branch02, branch03, +17 more**

Risk area: Availability

Found in 19 places - see the table below for each one.

Why: Basic connectivity to this network is confirmed working, so the path itself is fine. Tracing SSH (TCP/22) specifically: traffic was denied by an outbound filter. Re-tracing the same packet with all access-lists ignored delivers it successfully, which isolates the cause to a filter rather than to routing.

Impact: Anything relying on this service across this path will fail while ordinary connectivity tests keep passing - which is what makes it easy to miss and slow to diagnose. 21 of 21 discovered source networks have a route toward this destination, and 22 of 22 devices route toward it. 19 were verified by probe to actually reach it. The prefix spans 256 addresses.

Suggested action: Look for the access-list along this path that matches this traffic - the routing is already confirmed correct, so no routing change is needed.

Ref	Devices	Destination	Cause	Verified
V-002	branch01, mgmt01	10.200.0.254	Denied out	19
V-003	branch02, mgmt01	10.200.0.254	Denied out	19
V-004	branch03, mgmt01	10.200.0.254	Denied out	19
V-006	branch04, mgmt01	10.200.0.254	Denied out	19
V-007	branch05, mgmt01	10.200.0.254	Denied out	19
V-008	branch06, mgmt01	10.200.0.254	Denied out	19
V-009	branch08, mgmt01	10.200.0.254	Denied out	19
V-010	branch09, mgmt01	10.200.0.254	Denied out	19
V-011	branch10, mgmt01	10.200.0.254	Denied out	19
V-013	branch11, mgmt01	10.200.0.254	Denied out	19
V-014	branch12, mgmt01	10.200.0.254	Denied out	19
V-015	branch13, mgmt01	10.200.0.254	Denied out	19
V-016	branch14, mgmt01	10.200.0.254	Denied out	19
V-018	branch15, mgmt01	10.200.0.254	Denied out	19
V-019	branch16, mgmt01	10.200.0.254	Denied out	19
V-020	branch17, mgmt01	10.200.0.254	Denied out	19
V-021	branch18, mgmt01	10.200.0.254	Denied out	19
V-022	branch19, mgmt01	10.200.0.254	Denied out	19
V-023	branch20, mgmt01	10.200.0.254	Denied out	19

MEDIUM **[V-005, V-012, V-017] HTTPS (TCP/443) is blocked on a path that is otherwise working (3 instances) - branch03, branch11, branch15, +1 more**

Risk area: Availability

Found in 3 places - see the table below for each one.

Why: Basic connectivity to this network is confirmed working, so the path itself is fine. Tracing HTTPS (TCP/443) specifically: traffic was denied by an outbound filter. Re-tracing the same packet with all access-lists ignored delivers it successfully, which isolates the cause to a filter rather than to routing.

Impact: Anything relying on this service across this path will fail while ordinary connectivity tests keep passing - which is what makes it easy to miss and slow to diagnose. 21 of 21 discovered source networks have a route toward this destination, and 22 of 22 devices route toward it. 19 were verified by probe to actually reach it. The prefix spans 256 addresses.

Suggested action: Look for the access-list along this path that matches this traffic - the routing is already confirmed correct, so no routing change is needed.

Ref	Devices	Destination	Cause	Verified

Ref	Devices	Destination	Cause	Verified
V-005	branch03, mgmt01	10.200.0.254	Denied out	19
V-012	branch11, mgmt01	10.200.0.254	Denied out	19
V-017	branch15, mgmt01	10.200.0.254	Denied out	19

MEDIUM **[V-024 - V-042] An access-list denies encrypted management access but permits the cleartext one (19 instances) - branch01, branch02, branch03, +16 more**

Risk area: Security

Found in 19 places - see the table below for each one.

Why: Telnet carries credentials and session content in cleartext, and SSH is the encrypted equivalent of the same access. A filter that blocks the encrypted one and admits the other is the opposite of what either rule was presumably for.

Impact: Anyone able to observe this path can read the credentials used over Telnet. Both lines are in the same filter, so this is a difference between the two protocols rather than a filter that blocks a destination outright.

Suggested action: Check which of the two lines is wrong. If management access is meant to be blocked here, Telnet needs blocking too; if it is meant to be allowed, SSH is the one to allow.

Confidence: medium

Ref	Devices
V-024	branch01
V-025	branch02
V-026	branch03
V-027	branch04
V-028	branch05
V-029	branch06
V-030	branch08
V-031	branch09
V-032	branch10
V-033	branch11
V-034	branch12
V-035	branch13
V-036	branch14
V-037	branch15
V-038	branch16
V-039	branch17
V-040	branch18
V-041	branch19

Ref	Devices
V-042	branch20

INFORMATIONAL **[V-043 - V-044] One device behaves differently from its structural peers (2 instances) - branch03, branch07, branch11, +1 more**

Risk area: Correctness

Found in 2 places - see the table below for each one.

Why: The reason varies by instance - see the table below for each one.

Impact: Unknown from configuration alone. If the majority behaviour is intended, this device is an exception worth correcting; if the exception is intended, the others may be. Verify cannot tell which without a stated intent to check against.

Suggested action: The suggested action varies by instance - see the table below for each one.

Ref	Devices	Destination
V-043	branch03, branch11, branch15	10.200.0.0/24
V-044	branch07	10.200.0.0/24

Potential impact

Observed scope of each finding, widest first.

22 of 44 findings carry a measured scope, covering 2 affected destinations. Scope describes what was observed - how many discovered sources hold a route toward the affected destination, and how large that destination is - not how many hosts exist there or how much traffic is flowing. It is a separate axis from severity and does not re-rank anything above.

Ref	Finding	Destination	Severity	Sources routing toward	Verified
V-005	HTTPS (TCP/443) is blocked on a path that is otherwise working	10.200.0.254 (management LAN)	Medium	21 of 21 networks	19
V-002	SSH (TCP/22) is blocked on a path that is otherwise working	10.200.0.254 (management LAN)	Medium	21 of 21 networks	19

Sources routing toward is what the routing tables permit; Verified is what a modeled probe demonstrated. They are different measurements and are never added together.

Recommended remediation

Ordered by severity. Addressing the Critical items first is the intended reading.

Ref	Severity	Action

Ref	Severity	Action
V-001	Medium	Confirm whether a single path to these destinations via hub01 is intended - single-homing is often a deliberate cost decision. If it isn't, a second path or a backup route removes the dependency. Coverage: 15 of 22 devices were simulated.
V-002, V-003, V-004 +16 more (19)	Medium	Look for the access-list along this path that matches this traffic - the routing is already confirmed correct, so no routing change is needed.
V-005, V-012, V-017 (3)	Medium	Look for the access-list along this path that matches this traffic - the routing is already confirmed correct, so no routing change is needed.
V-024 - V-042 (19)	Medium	Check which of the two lines is wrong. If management access is meant to be blocked here, Telnet needs blocking too; if it is meant to be allowed, SSH is the one to allow.
V-043 - V-044 (2)	Informational	Action varies by instance - see the Findings section above (2 instances).

Technical appendices

Everything from here on is supporting evidence for the assessment above - the full per-file parse outcome, the raw technical data behind every finding, and the complete check catalog. Nothing past this point changes the result; it is what the result is built on.

Appendix A - coverage detail

Per-file parse outcome behind the coverage figure.

File	Status	Format
configs/branch01.cfg	PASSED	CISCO_IOS
configs/branch02.cfg	PASSED	CISCO_IOS
configs/branch03.cfg	PASSED	CISCO_IOS
configs/branch04.cfg	PASSED	CISCO_IOS
configs/branch05.cfg	PASSED	CISCO_IOS
configs/branch06.cfg	PASSED	CISCO_IOS
configs/branch07.cfg	PASSED	CISCO_IOS
configs/branch08.cfg	PASSED	CISCO_IOS
configs/branch09.cfg	PASSED	CISCO_IOS
configs/branch10.cfg	PASSED	CISCO_IOS
configs/branch11.cfg	PASSED	CISCO_IOS
configs/branch12.cfg	PASSED	CISCO_IOS
configs/branch13.cfg	PASSED	CISCO_IOS
configs/branch14.cfg	PASSED	CISCO_IOS
configs/branch15.cfg	PASSED	CISCO_IOS
configs/branch16.cfg	PASSED	CISCO_IOS
configs/branch17.cfg	PASSED	CISCO_IOS
configs/branch18.cfg	PASSED	CISCO_IOS
configs/branch19.cfg	PASSED	CISCO_IOS
configs/branch20.cfg	PASSED	CISCO_IOS
configs/hub01.cfg	PASSED	CISCO_IOS
configs/mgmt01.cfg	PASSED	CISCO_IOS

Appendix B - network reachability

Observed forwarding between discovered network segments. Nothing here is a finding.

21 source segments x **21** candidate destinations over ICMP, HTTPS (TCP/443), SSH (TCP/22); **63** self-relations excluded - **1,260** relationships analyzed, complete for this scope.

How to read this: each cell is the observed forwarding result from the source network toward a representative address in the destination prefix, for the protocol shown. A reachable result does not mean every address or service in the destination is reachable.

ICMP

420 relationships analyzed: **420** reachable, **0** not. Every relationship was evaluated; the reachable ones are counted rather than listed, and all **0** that were not reachable appear below.

HTTPS (TCP/443)

420 relationships analyzed: **417** reachable, **3** not. Every relationship was evaluated; the reachable ones are counted rather than listed, and all **3** that were not reachable appear below.

From	To		State	Disposition
10.103.0.0/24	10.200.0.0/24	[X]	Blocked	DENIED_OUT
10.111.0.0/24	10.200.0.0/24	[X]	Blocked	DENIED_OUT
10.115.0.0/24	10.200.0.0/24	[X]	Blocked	DENIED_OUT

[OK] reachable [X] blocked by a filter [-] no route [~] path-dependent (some paths succeed, some do not) [!] forwarding failure [?] not determined

SSH (TCP/22)

420 relationships analyzed: **401** reachable, **19** not. Every relationship was evaluated; the reachable ones are counted rather than listed, and all **19** that were not reachable appear below.

From	To		State	Disposition
10.101.0.0/24	10.200.0.0/24	[X]	Blocked	DENIED_OUT
10.102.0.0/24	10.200.0.0/24	[X]	Blocked	DENIED_OUT
10.103.0.0/24	10.200.0.0/24	[X]	Blocked	DENIED_OUT
10.104.0.0/24	10.200.0.0/24	[X]	Blocked	DENIED_OUT
10.105.0.0/24	10.200.0.0/24	[X]	Blocked	DENIED_OUT
10.106.0.0/24	10.200.0.0/24	[X]	Blocked	DENIED_OUT
10.108.0.0/24	10.200.0.0/24	[X]	Blocked	DENIED_OUT
10.109.0.0/24	10.200.0.0/24	[X]	Blocked	DENIED_OUT
10.110.0.0/24	10.200.0.0/24	[X]	Blocked	DENIED_OUT
10.111.0.0/24	10.200.0.0/24	[X]	Blocked	DENIED_OUT

From	To		State	Disposition
10.112.0.0/24	10.200.0.0/24	[X]	Blocked	DENIED_OUT
10.113.0.0/24	10.200.0.0/24	[X]	Blocked	DENIED_OUT
10.114.0.0/24	10.200.0.0/24	[X]	Blocked	DENIED_OUT
10.115.0.0/24	10.200.0.0/24	[X]	Blocked	DENIED_OUT
10.116.0.0/24	10.200.0.0/24	[X]	Blocked	DENIED_OUT
10.117.0.0/24	10.200.0.0/24	[X]	Blocked	DENIED_OUT
10.118.0.0/24	10.200.0.0/24	[X]	Blocked	DENIED_OUT
10.119.0.0/24	10.200.0.0/24	[X]	Blocked	DENIED_OUT
10.120.0.0/24	10.200.0.0/24	[X]	Blocked	DENIED_OUT

[OK] reachable [X] blocked by a filter [-] no route [~] path-dependent (some paths succeed, some do not) [!] forwarding failure [?] not determined

What these segments are

Read from the uploaded configuration - the VRF each interface sits in, the access-lists bound to it, and its description. Shown exactly as configured; nothing here is interpreted.

Segment	What it is	Devices	VRF	Filters
10.101.0.0/24	branch LAN	branch01	default	
10.102.0.0/24	branch LAN	branch02	default	
10.103.0.0/24	branch LAN	branch03	default	
10.104.0.0/24	branch LAN	branch04	default	
10.105.0.0/24	branch LAN	branch05	default	
10.106.0.0/24	branch LAN	branch06	default	
10.107.0.0/24	branch LAN	branch07	default	
10.108.0.0/24	branch LAN	branch08	default	
10.109.0.0/24	branch LAN	branch09	default	
10.110.0.0/24	branch LAN	branch10	default	
10.111.0.0/24	branch LAN	branch11	default	
10.112.0.0/24	branch LAN	branch12	default	
10.113.0.0/24	branch LAN	branch13	default	
10.114.0.0/24	branch LAN	branch14	default	
10.115.0.0/24	branch LAN	branch15	default	

Segment	What it is	Devices	VRF	Filters
10.116.0.0/24	branch LAN	branch16	default	
10.117.0.0/24	branch LAN	branch17	default	
10.118.0.0/24	branch LAN	branch18	default	
10.119.0.0/24	branch LAN	branch19	default	
10.120.0.0/24	branch LAN	branch20	default	
10.200.0.0/24	management LAN	mgmt01	default	

Appendix C - technical evidence

Finding references (V-001…) are local to this document and are reassigned on every run. The finding id is stable across runs for the same underlying issue.

V-001 One device's failure would disconnect part of the network - hub01

Finding ID: 3cfdf8abb2cef900
Device: hub01
Destinations Lost: 10.101.0.0, 10.102.0.0
Destinations Considered: 21
Devices Simulated: 15
Devices Discovered: 22

V-002 SSH (TCP/22) is blocked on a path that is otherwise working - branch01, mgmt01

Finding ID: edea4c2bb63a8425
Trace: DENIED_OUT
1. node: branch01
ORIGINATED(default)
FORWARDED(Forwarded out interface: GigabitEthernet0/0 with resolved next-hop IP: 10.0.1.2, Routes: [ospf (Network: 10.200.0.0/24, Next Hop: interface GigabitEthernet0/0 ip 10.0.1.2)])
DENIED(BLOCK-MGMT-SSH (EGRESS_FILTER))
Hops: branch01
Destination: 10.200.0.254
Protocol: TCP
Port: 22
Blocked By Filter: True
Source networks routing toward: 21 of 21 discovered
Source devices routing toward: 22 of 22 discovered
Source devices verified by probe: 19
Destination prefix spans: 256 addresses
Observed scope: HIGH

V-003 SSH (TCP/22) is blocked on a path that is otherwise working - branch02, mgmt01

Finding ID: 83dbec1fd6ce458b
Trace: DENIED_OUT
1. node: branch02
ORIGINATED(default)
FORWARDED(Forwarded out interface: GigabitEthernet0/0 with resolved next-hop IP: 10.0.2.2, Routes: [ospf (Network: 10.200.0.0/24, Next Hop: interface GigabitEthernet0/0 ip 10.0.2.2)])
DENIED(BLOCK-MGMT-SSH (EGRESS_FILTER))
Hops: branch02
Destination: 10.200.0.254
Protocol: TCP
Port: 22
Blocked By Filter: True
Source networks routing toward: 21 of 21 discovered

Source devices routing toward: 22 of 22 discovered
Source devices verified by probe: 19
Destination prefix spans: 256 addresses
Observed scope: HIGH

V-004 SSH (TCP/22) is blocked on a path that is otherwise working - branch03, mgmt01

Finding ID: 19d53efde853eec6
Trace: DENIED_OUT
1. node: branch03
ORIGINATED(default)
FORWARDED(Forwarded out interface: GigabitEthernet0/0 with resolved next-hop IP: 10.0.3.2, Routes: [ospf (Network: 10.200.0.0/24, Next Hop: interface GigabitEthernet0/0 ip 10.0.3.2)])
DENIED(BLOCK-MGMT-SSH (EGRESS_FILTER))
Hops: branch03
Destination: 10.200.0.254
Protocol: TCP
Port: 22
Blocked By Filter: True
Source networks routing toward: 21 of 21 discovered
Source devices routing toward: 22 of 22 discovered
Source devices verified by probe: 19
Destination prefix spans: 256 addresses
Observed scope: HIGH

V-005 HTTPS (TCP/443) is blocked on a path that is otherwise working - branch03, mgmt01

Finding ID: 1dbe4f31a3567874
Trace: DENIED_OUT
1. node: branch03
ORIGINATED(default)
FORWARDED(Forwarded out interface: GigabitEthernet0/0 with resolved next-hop IP: 10.0.3.2, Routes: [ospf (Network: 10.200.0.0/24, Next Hop: interface GigabitEthernet0/0 ip 10.0.3.2)])
DENIED(BLOCK-MGMT-SSH (EGRESS_FILTER))
Hops: branch03
Destination: 10.200.0.254
Protocol: TCP
Port: 443
Blocked By Filter: True
Source networks routing toward: 21 of 21 discovered
Source devices routing toward: 22 of 22 discovered
Source devices verified by probe: 19
Destination prefix spans: 256 addresses
Observed scope: HIGH

V-006 SSH (TCP/22) is blocked on a path that is otherwise working - branch04, mgmt01

Finding ID: db67326e2db88abf
Trace: DENIED_OUT
1. node: branch04
ORIGINATED(default)
FORWARDED(Forwarded out interface: GigabitEthernet0/0 with resolved next-hop IP: 10.0.4.2, Routes: [ospf (Network: 10.200.0.0/24, Next Hop: interface GigabitEthernet0/0 ip 10.0.4.2)])
DENIED(BLOCK-MGMT-SSH (EGRESS_FILTER))
Hops: branch04
Destination: 10.200.0.254
Protocol: TCP
Port: 22
Blocked By Filter: True
Source networks routing toward: 21 of 21 discovered
Source devices routing toward: 22 of 22 discovered
Source devices verified by probe: 19
Destination prefix spans: 256 addresses
Observed scope: HIGH

V-007 SSH (TCP/22) is blocked on a path that is otherwise working - branch05, mgmt01

Finding ID: c0125d86949e5f37
Trace: DENIED_OUT

1. node: branch05
ORIGINATED(default)
FORWARDED(Forwarded out interface: GigabitEthernet0/0 with resolved next-hop IP: 10.0.5.2, Routes: [ospf (Network: 10.200.0.0/24, Next Hop: interface GigabitEthernet0/0 ip 10.0.5.2)])
DENIED(BLOCK-MGMT-SSH (EGRESS_FILTER))
Hops: branch05
Destination: 10.200.0.254
Protocol: TCP
Port: 22
Blocked By Filter: True
Source networks routing toward: 21 of 21 discovered
Source devices routing toward: 22 of 22 discovered
Source devices verified by probe: 19
Destination prefix spans: 256 addresses
Observed scope: HIGH

V-008 SSH (TCP/22) is blocked on a path that is otherwise working - branch06, mgmt01

Finding ID: d9659e399afe7387
Trace: DENIED_OUT
1. node: branch06
ORIGINATED(default)
FORWARDED(Forwarded out interface: GigabitEthernet0/0 with resolved next-hop IP: 10.0.6.2, Routes: [ospf (Network: 10.200.0.0/24, Next Hop: interface GigabitEthernet0/0 ip 10.0.6.2)])
DENIED(BLOCK-MGMT-SSH (EGRESS_FILTER))
Hops: branch06
Destination: 10.200.0.254
Protocol: TCP
Port: 22
Blocked By Filter: True
Source networks routing toward: 21 of 21 discovered
Source devices routing toward: 22 of 22 discovered
Source devices verified by probe: 19
Destination prefix spans: 256 addresses
Observed scope: HIGH

V-009 SSH (TCP/22) is blocked on a path that is otherwise working - branch08, mgmt01

Finding ID: 849b0398174bcdcc
Trace: DENIED_OUT
1. node: branch08
ORIGINATED(default)
FORWARDED(Forwarded out interface: GigabitEthernet0/0 with resolved next-hop IP: 10.0.8.2, Routes: [ospf (Network: 10.200.0.0/24, Next Hop: interface GigabitEthernet0/0 ip 10.0.8.2)])
DENIED(BLOCK-MGMT-SSH (EGRESS_FILTER))
Hops: branch08
Destination: 10.200.0.254
Protocol: TCP
Port: 22
Blocked By Filter: True
Source networks routing toward: 21 of 21 discovered
Source devices routing toward: 22 of 22 discovered
Source devices verified by probe: 19
Destination prefix spans: 256 addresses
Observed scope: HIGH

V-010 SSH (TCP/22) is blocked on a path that is otherwise working - branch09, mgmt01

Finding ID: 6f31d06f36a98f9c
Trace: DENIED_OUT
1. node: branch09
ORIGINATED(default)
FORWARDED(Forwarded out interface: GigabitEthernet0/0 with resolved next-hop IP: 10.0.9.2, Routes: [ospf (Network: 10.200.0.0/24, Next Hop: interface GigabitEthernet0/0 ip 10.0.9.2)])
DENIED(BLOCK-MGMT-SSH (EGRESS_FILTER))
Hops: branch09
Destination: 10.200.0.254

Protocol: TCP
Port: 22
Blocked By Filter: True
Source networks routing toward: 21 of 21 discovered
Source devices routing toward: 22 of 22 discovered
Source devices verified by probe: 19
Destination prefix spans: 256 addresses
Observed scope: HIGH

V-011 SSH (TCP/22) is blocked on a path that is otherwise working - branch10, mgmt01

Finding ID: 705f956b5297e104
Trace: DENIED_OUT
1. node: branch10
ORIGINATED(default)
FORWARDED(Forwarded out interface: GigabitEthernet0/0 with resolved next-hop IP: 10.0.10.2, Routes: [ospf (Network: 10.200.0.0/24, Next Hop: interface GigabitEthernet0/0 ip 10.0.10.2)])
DENIED(BLOCK-MGMT-SSH (EGRESS_FILTER))
Hops: branch10
Destination: 10.200.0.254
Protocol: TCP
Port: 22
Blocked By Filter: True
Source networks routing toward: 21 of 21 discovered
Source devices routing toward: 22 of 22 discovered
Source devices verified by probe: 19
Destination prefix spans: 256 addresses
Observed scope: HIGH

V-012 HTTPS (TCP/443) is blocked on a path that is otherwise working - branch11, mgmt01

Finding ID: bbf45c7ab7ffdd17
Trace: DENIED_OUT
1. node: branch11
ORIGINATED(default)
FORWARDED(Forwarded out interface: GigabitEthernet0/0 with resolved next-hop IP: 10.0.11.2, Routes: [ospf (Network: 10.200.0.0/24, Next Hop: interface GigabitEthernet0/0 ip 10.0.11.2)])
DENIED(BLOCK-MGMT-SSH (EGRESS_FILTER))
Hops: branch11
Destination: 10.200.0.254
Protocol: TCP
Port: 443
Blocked By Filter: True
Source networks routing toward: 21 of 21 discovered
Source devices routing toward: 22 of 22 discovered
Source devices verified by probe: 19
Destination prefix spans: 256 addresses
Observed scope: HIGH

V-013 SSH (TCP/22) is blocked on a path that is otherwise working - branch11, mgmt01

Finding ID: edb8cf61b52dff83
Trace: DENIED_OUT
1. node: branch11
ORIGINATED(default)
FORWARDED(Forwarded out interface: GigabitEthernet0/0 with resolved next-hop IP: 10.0.11.2, Routes: [ospf (Network: 10.200.0.0/24, Next Hop: interface GigabitEthernet0/0 ip 10.0.11.2)])
DENIED(BLOCK-MGMT-SSH (EGRESS_FILTER))
Hops: branch11
Destination: 10.200.0.254
Protocol: TCP
Port: 22
Blocked By Filter: True
Source networks routing toward: 21 of 21 discovered
Source devices routing toward: 22 of 22 discovered
Source devices verified by probe: 19
Destination prefix spans: 256 addresses

Observed scope: HIGH

V-014 SSH (TCP/22) is blocked on a path that is otherwise working - branch12, mgmt01

Finding ID: 154ea23f5eeabd3c
Trace: DENIED_OUT
1. node: branch12
ORIGINATED(default)
FORWARDED(Forwarded out interface: GigabitEthernet0/0 with resolved next-hop IP: 10.0.12.2, Routes: [ospf (Network: 10.200.0.0/24, Next Hop: interface GigabitEthernet0/0 ip 10.0.12.2)])
DENIED(BLOCK-MGMT-SSH (EGRESS_FILTER))
Hops: branch12
Destination: 10.200.0.254
Protocol: TCP
Port: 22
Blocked By Filter: True
Source networks routing toward: 21 of 21 discovered
Source devices routing toward: 22 of 22 discovered
Source devices verified by probe: 19
Destination prefix spans: 256 addresses
Observed scope: HIGH

V-015 SSH (TCP/22) is blocked on a path that is otherwise working - branch13, mgmt01

Finding ID: 387ecd5f148dd6f2
Trace: DENIED_OUT
1. node: branch13
ORIGINATED(default)
FORWARDED(Forwarded out interface: GigabitEthernet0/0 with resolved next-hop IP: 10.0.13.2, Routes: [ospf (Network: 10.200.0.0/24, Next Hop: interface GigabitEthernet0/0 ip 10.0.13.2)])
DENIED(BLOCK-MGMT-SSH (EGRESS_FILTER))
Hops: branch13
Destination: 10.200.0.254
Protocol: TCP
Port: 22
Blocked By Filter: True
Source networks routing toward: 21 of 21 discovered
Source devices routing toward: 22 of 22 discovered
Source devices verified by probe: 19
Destination prefix spans: 256 addresses
Observed scope: HIGH

V-016 SSH (TCP/22) is blocked on a path that is otherwise working - branch14, mgmt01

Finding ID: 51171d0b6e6a1ab7
Trace: DENIED_OUT
1. node: branch14
ORIGINATED(default)
FORWARDED(Forwarded out interface: GigabitEthernet0/0 with resolved next-hop IP: 10.0.14.2, Routes: [ospf (Network: 10.200.0.0/24, Next Hop: interface GigabitEthernet0/0 ip 10.0.14.2)])
DENIED(BLOCK-MGMT-SSH (EGRESS_FILTER))
Hops: branch14
Destination: 10.200.0.254
Protocol: TCP
Port: 22
Blocked By Filter: True
Source networks routing toward: 21 of 21 discovered
Source devices routing toward: 22 of 22 discovered
Source devices verified by probe: 19
Destination prefix spans: 256 addresses
Observed scope: HIGH

V-017 HTTPS (TCP/443) is blocked on a path that is otherwise working - branch15, mgmt01

Finding ID: 1ae07f3154104b48
Trace: DENIED_OUT
1. node: branch15
ORIGINATED(default)
FORWARDED(Forwarded out interface: GigabitEthernet0/0 with resolved next-hop IP: 10.0.15.2, Routes: [ospf (Network: 10.200.0.0/24,

Next Hop: interface GigabitEthernet0/0 ip 10.0.15.2)])
DENIED(BLOCK-MGMT-SSH (EGRESS_FILTER))
Hops: branch15
Destination: 10.200.0.254
Protocol: TCP
Port: 443
Blocked By Filter: True
Source networks routing toward: 21 of 21 discovered
Source devices routing toward: 22 of 22 discovered
Source devices verified by probe: 19
Destination prefix spans: 256 addresses
Observed scope: HIGH

V-018 SSH (TCP/22) is blocked on a path that is otherwise working - branch15, mgmt01

Finding ID: ac16d1a5e2f90670
Trace: DENIED_OUT
1. node: branch15
ORIGINATED(default)
FORWARDED(Forwarded out interface: GigabitEthernet0/0 with resolved next-hop IP: 10.0.15.2, Routes: [ospf (Network: 10.200.0.0/24,
Next Hop: interface GigabitEthernet0/0 ip 10.0.15.2)])
DENIED(BLOCK-MGMT-SSH (EGRESS_FILTER))
Hops: branch15
Destination: 10.200.0.254
Protocol: TCP
Port: 22
Blocked By Filter: True
Source networks routing toward: 21 of 21 discovered
Source devices routing toward: 22 of 22 discovered
Source devices verified by probe: 19
Destination prefix spans: 256 addresses
Observed scope: HIGH

V-019 SSH (TCP/22) is blocked on a path that is otherwise working - branch16, mgmt01

Finding ID: a668488e0f39c568
Trace: DENIED_OUT
1. node: branch16
ORIGINATED(default)
FORWARDED(Forwarded out interface: GigabitEthernet0/0 with resolved next-hop IP: 10.0.16.2, Routes: [ospf (Network: 10.200.0.0/24,
Next Hop: interface GigabitEthernet0/0 ip 10.0.16.2)])
DENIED(BLOCK-MGMT-SSH (EGRESS_FILTER))
Hops: branch16
Destination: 10.200.0.254
Protocol: TCP
Port: 22
Blocked By Filter: True
Source networks routing toward: 21 of 21 discovered
Source devices routing toward: 22 of 22 discovered
Source devices verified by probe: 19
Destination prefix spans: 256 addresses
Observed scope: HIGH

V-020 SSH (TCP/22) is blocked on a path that is otherwise working - branch17, mgmt01

Finding ID: 427836b2ffe72269
Trace: DENIED_OUT
1. node: branch17
ORIGINATED(default)
FORWARDED(Forwarded out interface: GigabitEthernet0/0 with resolved next-hop IP: 10.0.17.2, Routes: [ospf (Network: 10.200.0.0/24,
Next Hop: interface GigabitEthernet0/0 ip 10.0.17.2)])
DENIED(BLOCK-MGMT-SSH (EGRESS_FILTER))
Hops: branch17
Destination: 10.200.0.254
Protocol: TCP
Port: 22
Blocked By Filter: True

Source networks routing toward: 21 of 21 discovered
Source devices routing toward: 22 of 22 discovered
Source devices verified by probe: 19
Destination prefix spans: 256 addresses
Observed scope: HIGH

V-021 SSH (TCP/22) is blocked on a path that is otherwise working - branch18, mgmt01

Finding ID: f29988ed52bc2092
Trace: DENIED_OUT
1. node: branch18
ORIGINATED(default)
FORWARDED(Forwarded out interface: GigabitEthernet0/0 with resolved next-hop IP: 10.0.18.2, Routes: [ospf (Network: 10.200.0.0/24, Next Hop: interface GigabitEthernet0/0 ip 10.0.18.2)])
DENIED(BLOCK-MGMT-SSH (EGRESS_FILTER))
Hops: branch18
Destination: 10.200.0.254
Protocol: TCP
Port: 22
Blocked By Filter: True
Source networks routing toward: 21 of 21 discovered
Source devices routing toward: 22 of 22 discovered
Source devices verified by probe: 19
Destination prefix spans: 256 addresses
Observed scope: HIGH

V-022 SSH (TCP/22) is blocked on a path that is otherwise working - branch19, mgmt01

Finding ID: 1761bebd010d1096
Trace: DENIED_OUT
1. node: branch19
ORIGINATED(default)
FORWARDED(Forwarded out interface: GigabitEthernet0/0 with resolved next-hop IP: 10.0.19.2, Routes: [ospf (Network: 10.200.0.0/24, Next Hop: interface GigabitEthernet0/0 ip 10.0.19.2)])
DENIED(BLOCK-MGMT-SSH (EGRESS_FILTER))
Hops: branch19
Destination: 10.200.0.254
Protocol: TCP
Port: 22
Blocked By Filter: True
Source networks routing toward: 21 of 21 discovered
Source devices routing toward: 22 of 22 discovered
Source devices verified by probe: 19
Destination prefix spans: 256 addresses
Observed scope: HIGH

V-023 SSH (TCP/22) is blocked on a path that is otherwise working - branch20, mgmt01

Finding ID: b5ff2626ce6d853b
Trace: DENIED_OUT
1. node: branch20
ORIGINATED(default)
FORWARDED(Forwarded out interface: GigabitEthernet0/0 with resolved next-hop IP: 10.0.20.2, Routes: [ospf (Network: 10.200.0.0/24, Next Hop: interface GigabitEthernet0/0 ip 10.0.20.2)])
DENIED(BLOCK-MGMT-SSH (EGRESS_FILTER))
Hops: branch20
Destination: 10.200.0.254
Protocol: TCP
Port: 22
Blocked By Filter: True
Source networks routing toward: 21 of 21 discovered
Source devices routing toward: 22 of 22 discovered
Source devices verified by probe: 19
Destination prefix spans: 256 addresses
Observed scope: HIGH

V-024 An access-list denies encrypted management access but permits the cleartext one - branch01

Finding ID: 2fcd5f4380d6fbed

Filter Name: BLOCK-MGMT-SSH
Applied At: GigabitEthernet0/0 (outbound)
Denied Service: SSH
Denied Line: deny tcp any 10.200.0.0 0.0.0.255 eq 22
Permitted Service: Telnet
Permitted Line: permit ip any any

V-025 An access-list denies encrypted management access but permits the cleartext one - branch02

Finding ID: c6e5a24fa2e1a1d2
Filter Name: BLOCK-MGMT-SSH
Applied At: GigabitEthernet0/0 (outbound)
Denied Service: SSH
Denied Line: deny tcp any 10.200.0.0 0.0.0.255 eq 22
Permitted Service: Telnet
Permitted Line: permit ip any any

V-026 An access-list denies encrypted management access but permits the cleartext one - branch03

Finding ID: 443c3c80a619d39a
Filter Name: BLOCK-MGMT-SSH
Applied At: GigabitEthernet0/0 (outbound)
Denied Service: SSH
Denied Line: deny tcp any 10.200.0.0 0.0.0.255 eq 22
Permitted Service: Telnet
Permitted Line: permit ip any any

V-027 An access-list denies encrypted management access but permits the cleartext one - branch04

Finding ID: e9020c561545d062
Filter Name: BLOCK-MGMT-SSH
Applied At: GigabitEthernet0/0 (outbound)
Denied Service: SSH
Denied Line: deny tcp any 10.200.0.0 0.0.0.255 eq 22
Permitted Service: Telnet
Permitted Line: permit ip any any

V-028 An access-list denies encrypted management access but permits the cleartext one - branch05

Finding ID: 5824b09fb8f1bb3a
Filter Name: BLOCK-MGMT-SSH
Applied At: GigabitEthernet0/0 (outbound)
Denied Service: SSH
Denied Line: deny tcp any 10.200.0.0 0.0.0.255 eq 22
Permitted Service: Telnet
Permitted Line: permit ip any any

V-029 An access-list denies encrypted management access but permits the cleartext one - branch06

Finding ID: 4cd0d6ea912db058
Filter Name: BLOCK-MGMT-SSH
Applied At: GigabitEthernet0/0 (outbound)
Denied Service: SSH
Denied Line: deny tcp any 10.200.0.0 0.0.0.255 eq 22
Permitted Service: Telnet
Permitted Line: permit ip any any

V-030 An access-list denies encrypted management access but permits the cleartext one - branch08

Finding ID: b55e9872621c0e9c
Filter Name: BLOCK-MGMT-SSH
Applied At: GigabitEthernet0/0 (outbound)
Denied Service: SSH
Denied Line: deny tcp any 10.200.0.0 0.0.0.255 eq 22
Permitted Service: Telnet
Permitted Line: permit ip any any

V-031 An access-list denies encrypted management access but permits the cleartext one - branch09

Finding ID: 86f3606044ac7eb0
Filter Name: BLOCK-MGMT-SSH
Applied At: GigabitEthernet0/0 (outbound)

Denied Service: SSH
Denied Line: deny tcp any 10.200.0.0 0.0.0.255 eq 22
Permitted Service: Telnet
Permitted Line: permit ip any any

V-032 An access-list denies encrypted management access but permits the cleartext one - branch10

Finding ID: f58576c86aeecc9a
Filter Name: BLOCK-MGMT-SSH
Applied At: GigabitEthernet0/0 (outbound)
Denied Service: SSH
Denied Line: deny tcp any 10.200.0.0 0.0.0.255 eq 22
Permitted Service: Telnet
Permitted Line: permit ip any any

V-033 An access-list denies encrypted management access but permits the cleartext one - branch11

Finding ID: 5569a8c2f1d0aa7e
Filter Name: BLOCK-MGMT-SSH
Applied At: GigabitEthernet0/0 (outbound)
Denied Service: SSH
Denied Line: deny tcp any 10.200.0.0 0.0.0.255 eq 22
Permitted Service: Telnet
Permitted Line: permit ip any any

V-034 An access-list denies encrypted management access but permits the cleartext one - branch12

Finding ID: 1df079508e06b81a
Filter Name: BLOCK-MGMT-SSH
Applied At: GigabitEthernet0/0 (outbound)
Denied Service: SSH
Denied Line: deny tcp any 10.200.0.0 0.0.0.255 eq 22
Permitted Service: Telnet
Permitted Line: permit ip any any

V-035 An access-list denies encrypted management access but permits the cleartext one - branch13

Finding ID: 676452a78db9c15e
Filter Name: BLOCK-MGMT-SSH
Applied At: GigabitEthernet0/0 (outbound)
Denied Service: SSH
Denied Line: deny tcp any 10.200.0.0 0.0.0.255 eq 22
Permitted Service: Telnet
Permitted Line: permit ip any any

V-036 An access-list denies encrypted management access but permits the cleartext one - branch14

Finding ID: a33a5014932721b2
Filter Name: BLOCK-MGMT-SSH
Applied At: GigabitEthernet0/0 (outbound)
Denied Service: SSH
Denied Line: deny tcp any 10.200.0.0 0.0.0.255 eq 22
Permitted Service: Telnet
Permitted Line: permit ip any any

V-037 An access-list denies encrypted management access but permits the cleartext one - branch15

Finding ID: 0e41b2ad5ac66737
Filter Name: BLOCK-MGMT-SSH
Applied At: GigabitEthernet0/0 (outbound)
Denied Service: SSH
Denied Line: deny tcp any 10.200.0.0 0.0.0.255 eq 22
Permitted Service: Telnet
Permitted Line: permit ip any any

V-038 An access-list denies encrypted management access but permits the cleartext one - branch16

Finding ID: 72394bd89375abe0
Filter Name: BLOCK-MGMT-SSH
Applied At: GigabitEthernet0/0 (outbound)
Denied Service: SSH
Denied Line: deny tcp any 10.200.0.0 0.0.0.255 eq 22

Permitted Service: Telnet
Permitted Line: permit ip any any

V-039 An access-list denies encrypted management access but permits the cleartext one - branch17

Finding ID: 5c05ff8c0d4c0be6
Filter Name: BLOCK-MGMT-SSH
Applied At: GigabitEthernet0/0 (outbound)
Denied Service: SSH
Denied Line: deny tcp any 10.200.0.0 0.0.0.255 eq 22
Permitted Service: Telnet
Permitted Line: permit ip any any

V-040 An access-list denies encrypted management access but permits the cleartext one - branch18

Finding ID: fb3faed9aa526bea
Filter Name: BLOCK-MGMT-SSH
Applied At: GigabitEthernet0/0 (outbound)
Denied Service: SSH
Denied Line: deny tcp any 10.200.0.0 0.0.0.255 eq 22
Permitted Service: Telnet
Permitted Line: permit ip any any

V-041 An access-list denies encrypted management access but permits the cleartext one - branch19

Finding ID: 21676a91c4e47f7a
Filter Name: BLOCK-MGMT-SSH
Applied At: GigabitEthernet0/0 (outbound)
Denied Service: SSH
Denied Line: deny tcp any 10.200.0.0 0.0.0.255 eq 22
Permitted Service: Telnet
Permitted Line: permit ip any any

V-042 An access-list denies encrypted management access but permits the cleartext one - branch20

Finding ID: 2d749a1e6031a958
Filter Name: BLOCK-MGMT-SSH
Applied At: GigabitEthernet0/0 (outbound)
Denied Service: SSH
Denied Line: deny tcp any 10.200.0.0 0.0.0.255 eq 22
Permitted Service: Telnet
Permitted Line: permit ip any any

V-043 One device behaves differently from its structural peers - branch03, branch11, branch15

Finding ID: 0db645ebb5f26869
Cohort Members: branch01, branch02, branch03, branch04, branch05, branch06, branch07, branch08, branch09, branch10, branch11, branch12, branch13, branch14, branch15, branch16, branch17, branch18, branch19, branch20, mgmt01
Cohort Size: 21
Grouping Confidence: high
Cohort Signature: vrfs: ['default'], runs_bgp: False, runs_ospf: True, loopback_interfaces: 1, transit_interfaces: 1, lan_interfaces: 1
Destination: 10.200.0.0/24
Protocol: HTTPS (TCP/443)
Dominant State: REACHABLE
Dominant Count: 17
Deviant Count: 3
Deviant Members: branch03, branch11, branch15
Evaluated: 20
Agreement Ratio: 0.85
Is Violation: False

V-044 One device behaves differently from its structural peers - branch07

Finding ID: 7c67540a4ac357c2
Cohort Members: branch01, branch02, branch03, branch04, branch05, branch06, branch07, branch08, branch09, branch10, branch11, branch12, branch13, branch14, branch15, branch16, branch17, branch18, branch19, branch20, mgmt01
Cohort Size: 21
Grouping Confidence: high
Cohort Signature: vrfs: ['default'], runs_bgp: False, runs_ospf: True, loopback_interfaces: 1, transit_interfaces: 1, lan_interfaces: 1
Destination: 10.200.0.0/24
Protocol: SSH (TCP/22)

Dominant State: BLOCKED
Dominant Count: 19
Deviant Count: 1
Deviant Members: branch07
Evaluated: 20
Agreement Ratio: 0.95
Is Violation: False

Appendix D - what was checked

The full check catalog, including checks that found nothing. Severity levels shown as printed here; the web console labels Medium as "Warning".

Check	Section	Risk area	Severity
Traffic takes a different path back than it took out.	Forwarding	Correctness	Informational
One device's failure would disconnect part of the network.	Forwarding	Availability	Medium
A device is configured to discard traffic toward a specific prefix.	Forwarding	Availability	Informational, Medium
Forwarding loop.	Forwarding	Availability	Critical
A single device is your only physical path between two parts of the network.	Forwarding	Availability	Medium
Equal-cost paths don't agree.	Forwarding	Availability	Critical
One device behaves differently from its structural peers.	Forwarding	Correctness	Informational
Two devices can't reach each other.	Forwarding	Availability	Critical
Traffic gets there, but the reply can't get back.	Forwarding	Availability	Critical
A device can't reach a destination that only exists in the routing table.	Forwarding	Availability	Critical, Medium
A network segment has no route to anywhere else.	Forwarding	Availability	Informational
A service is blocked on a path that otherwise works.	Forwarding	Availability	Medium
A device can't reach a local network it should.	Forwarding	Availability	Critical
An access-list line can never take effect.	Policy	Security	Critical, Informational
A BGP export policy advertises more than the device originates.	Policy	Security	Medium, Informational
A route-map used as a BGP filter can never permit anything.	Policy	Availability	Medium

Check	Section	Risk area	Severity
EVPN routed segment disagrees between switches.	Policy	Correctness	Critical
First-hop-redundancy members disagree on the virtual IP.	Policy	Availability	Critical
An access-list in use denies every packet.	Policy	Availability	Critical
An access-list in use permits every packet.	Policy	Security	Medium
An access-list denies encrypted management access but permits the cleartext one.	Policy	Security	Medium
Duplicate IP address.	Policy	Availability	Critical
IP/subnet mismatch on a physical link.	Policy	Availability	Critical
Physically connected, but nothing running.	Policy	Hygiene	Informational
Native VLAN mismatch on a trunk.	Policy	Security	Medium
MTU mismatch across a link.	Policy	Availability	Medium
VRF mismatch across a link.	Policy	Correctness	Medium
A configuration reference points at something that doesn't exist.	Policy	Correctness	Medium
Unused configuration objects.	Policy	Hygiene	Informational
Remote access line isn't tied to centralized authentication.	Policy	Security	Medium
VXLAN segment maps to different VLANs.	Policy	Correctness	Critical
A BGP session is up but carrying no routes.	Routing	Availability	Medium
BGP peer configuration is ambiguous.	Routing	Correctness	Medium
BGP peer configuration is incomplete.	Routing	Availability	Critical
BGP peer not found in this upload.	Routing	Hygiene	Informational
BGP peer configured on only one side.	Routing	Availability	Critical
BGP session appears established, but the path is blocked.	Routing	Availability	Critical
BGP session cannot form.	Routing	Availability	Critical
BGP session is configured correctly but didn't come up.	Routing	Availability	Critical, Medium
IPsec tunnel isn't established.	Routing	Availability	Critical
OSPF configured on a shut interface.	Routing	Hygiene	Informational

Check	Section	Risk area	Severity
OSPF adjacency didn't form.	Routing	Availability	Critical

Methodology

How the network is modeled

Intentflow Verify builds a behavioral model of the network from the supplied configurations and evaluates configuration and forwarding properties across the modeled network as a whole, rather than one device at a time in isolation. Nothing is deployed, changed, or contacted: the analysis runs entirely on the configuration provided.

How findings are correlated

A finding is rarely the output of a single test. Several underlying checks are combined into one plain-language result, so that a symptom is reported alongside its cause rather than as a list of separate warnings. Where multiple findings concern the same network locus or share an evidence-backed condition, they are correlated for investigation without suppressing the underlying findings - each one stays individually visible and individually counted.

How to read confidence

Confidence reflects how direct the underlying evidence is, not how serious the problem is. High means the finding is a directly observed fact. Medium means the evidence supports a reasonable but not certain reading. Inferred means a pattern is suspicious rather than confirmed - a design that is usually deliberate, occasionally not. Severity and confidence answer different questions and are shown separately for that reason.

How findings are categorized

Findings are categorized by:

- severity
- risk area
- affected scope
- confidence
- potential operational impact
- supporting evidence

Every finding is generated from the supplied configuration alone, never from live traffic or device state - nothing about this assessment requires or grants access to the running network. Findings are structural and behavioral: this is not a vulnerability scan and does not claim to be one.