MANRS+ Controls

Control Domain	Control Title	Control ID	Control Specification	Auditing Guidelines (Auditing levels: Self declared, Measured, Audited)	Ownership	Comments
Routing Security						
Routing Security	RPKI Route Origin Validation	RS-01	Any announcement received from a BGP neighbor or generated internally that is invalidated by an existing RPKI ROA is discarded and not announced to other BGP neigbours.	1. Check metrics from the measurement system indicating occurrence of incidents violating the control. Ensure that the metrics are within the defined range. [Measured] 2. Examine documentation which includes information about RPKI processes including which RPKI Trust Anchors are used to import ROAs, how often updates to ROAs are imported, and how often these updates are published to their routers. Ensure that the documented procedures reflect best practices for ROV. [Self-declared][Audited]	Connectivity Provider (CP)	Efficacy of RS-01 depends on the implementation of controls RI-01 and RI-03 by the Enterprise Customers (EC).
Routing Security	IRR Filtering of Direct Customers	RS-02	Announcements received from a direct Enterprise customer and its customer cone (if exists) are filtered using a whitelist (allow-list) generated from the IRR.	1. Check metrics from the measurement system indicating occurrence of incidents violating the control. Ensure that the metrics are within the defined range. [Measured] 2. Examine documentation of the process for configuring new customer connections, which includes description of how IRR direct customer cone prefix-lists are generated and applied, including which IRRs and what objects are used, and how often these prefix-lists are published to their routers. This must include templates or description of the automation process used to generate and apply the prefix-lists.[Self-declared][Audited]	CP	Efficacy of RS-02 depends on the implementation of controls RI-02 and RI-03 by the Enterprise Customers (EC).
Routing Security	Assistance with RPKI or IRR maintenance for a customer	RS-03	Assist a customer with implementing controls RI-01, RI-02 and RI-03.	1. Examine a list of the RPKI and IRR maintenance operations that the provider can perform at customer's request on their behalf.[Self-declared][Audited]	CP	
DDoS Attack Prevention						
DDoS Attack Prevention	Detection of volumetric DDoS attack traffic	DA-01	Traffic is monitored for a set of IP addresses and malicious traffic can be detected and reported.	1. Examine documentation describing detection capabilities and its parameters [Self-declared][Audited]	CP	
DDoS Attack Prevention	Rate limiting of malicious traffic	DA-02	Malicious traffic can be rate limited.	1. Examine documentation describing rate limiting capabilities and its parameters [Self-declared][Audited]	CP	
DDoS Attack Prevention	Scrubbing of malicious traffic	DA-03	Malicious traffic can be scrubbed and clean, legitimate traffic is delivered to the customer.	1. Examine documentation describing scrubbing capabilities and its parameters [Self-declared][Audited]	CP	
DDoS Attack Prevention	RTBH (Remotely Triggered Blackholing)	DA-04	Selective filtering based on RTBH is supported and a customer can request it	1. Check metrics from the measurement system for the positive tests of FlowSpec-based filtering. [Measured] 2. Examine documentation describing scrubbing capabilities and its parameters [Self-declared][Audited]	CP (Shared?)	
DDoS Attack Prevention	FlowSpec	DA-05	Selective filtering based on Flowspec is supported and a customer can request it	1. Check metrics from the measurement system for the positive tests of RTBH-based filtering. [Measured] 2. Examine documentation describing scrubbing capabilities and its parameters [Self-declared][Audited]	CP (Shared?)	
Anti-spoofing Protection						
Anti-spoofing Protection	uRPF	AS-01	For single-homed enterprise customers either a uRPF strict mode or an ACL permitting only traffic with source IP addresses from an Enterprise Customer is enabled on corresponding PE router interfaces	1. Check for a negative Spoofer test from a customer network (Alt: Check metrics from the measurement system confirming ingress source address validation) [Measured] 2. Examine documentation for the deployed anti-spoofing controls [Self-declared][Audited]	CP	
Anti-spoofing Protection	ACLs	AS-02	ACLs permitting only traffic with source IP addresses from IP ranges used by an enterprise customer	1. Check for a negative Spoofer test from a customer network (Alt: Check metrics from the measurement system confirming ingress source address validation) [Measured] 2. Examine documentation for the deployed anti-spoofing controls [Self-declared][Audited]	CP	
Anti-spoofing Protection	Source Address Verification (SAV)	AS-03	For CMTS-connected enterprise customers, SAV (DOCSIS 3) is enabled.	1. Check for a negative Spoofer test from a customer network (Alt: Check metrics from the measurement system confirming ingress source address validation) [Measured] 2. Examine documentation for the deployed anti-spoofing controls [Self-declared][Audited]		
Maintaining Routing Information						
Maintaining Routing Information	ROA registration	RI-01	1. ROAs cover all announcements to other BGP neighbours originated in the CP network 2. Published ROAs do not invalidate legitimate announcements	1. Compare route announcements using externally visible the BGP information (RIS, RouteViews) with the ROAs in the RPKI repository. Ensure that all announcements are properly covered. [Measured] 2. Check that none of the ROAs invalidates legitimate announcements originated by the CP. [Measured] 3. Examine the documentation to ensure that ROA maintenance follows best practices. [Self-declared][Audited]	Shared	Corresponding control - RS-03
Maintaining Routing Information	IRR route object registration	RI-02	1. IRR objects are published in the RIR IRR authoritative for the corresponding address space 2. IRR route objects cover all announcements originated in the CP network 3. IRR route objects cover announcements originated in the customer cone networks 4. There are no conflicts among the RIR IRRs and RPKI as far as route objects related to CP announcements are concerned	1. Compare route announcements using externally visible the BGP information (RIS, RouteViews) with the IRR registrations. Ensure that all announcements are properly covered. [Measured] 2. Check that the route object corresponding to an announcement is registered in the correct IRR (the one authoritative for the corresponding address block) and there are no conflicting records in the RPKI.[Measured] 3. Examine the documentation to ensure that ROA maintenance follows best practices. [Self-declared][Audited]	Shared	Corresponding control - RS-03
Maintaining Routing Information	AS-SET registration	RI-03	1. AS-SET uses the IRR::ASN:AS-NAME notation and lists the CP customer cone members (ASNs and AS-SETs) 2. AS-SET is registered in the PeeringDB and the RIR IRR authoritative for the CP ASN.	1. Check the records in the Peering DB and the IRR hosting the ASN to ensure the proper format.[Measured]	Shared	Corresponding control - RS-03
Facilitate global operational communication and coordination						
Facilitate global operational communication and coordination	Valid contact email	GC-01	1. Contact information is publicly available 2. Contact email is valid	1. Check that contact information is available in one of the databases (RIR/NIR or PeeringDB) [Measured] 2. Check the address is valid and responsive by sending a test e-mail and expecting a human response within predefined time. [Measured][Self-declared][Audited]	CP	
Security services						
Security services	Secure configuration	SS-01	1. Secure configuration for customer devices facing the provider is available and the deployment can be assisted on request	1. Check that secure configuration templates (e.g. CIS benchmarks) are available [Self-declared][Audited] 2. Examine documentation for the process of deployment of such configurations on customer's request.[Self-declared][Audited]	Shared	
Security services	Monitoring and reporting	SS-02	1. Monitoring and reporting if a customer announcement is invalidated by ROAs 2. Monitoring and reporting if a customer announcement is being hijacked (or more general - if the routing policy was violated) outside the control of the connectivity provider	1. Examine documentation for the monitoring and reporting service. [Self-declared][Audited]	Shared	
Security services	Assistance in registration	SS-03	1. Offer assistance in the registration of customer's routing information in the IRR and RPKI systems.	1. Examine documentation of the registration assistance service.[Self-declared][Audited]	Shared	
Supply chain transparency (experimental)						
Supply chain transparency	ASPA registration (when available, experimental requirement)	ST-01	1. All upstream providers are documented in RPKI using ASPA objects	1. Check the RPKI for the existence of ASPA objects and corroborate this with AS relationship data (e.g. CAIDA AS relationship, or RIPEStat)		This is just a suggestion for a future control

Learn more: https://www.manrs.org/about/manrs-working-group

MANRS