

Inbound Email Precedence

<https://campus.barracuda.com/doc/51187924/>

Table 1. Inbound Email Precedence

Behavior/Setting	Antivirus Scanning?	Action	Reason
Unmanaged user and default unmanaged policy	No	blocked	Invalid recipient
More than 40 received headers	No	blocked	Possible mail loop
Account suspended	Yes	allowed	Account suspended
Client IP address is on redelivery allow list	No	allowed	-
Empty email body or 1 or 0 header	No	blocked	malformed mail
Sender policy is exempt and the sender is the recipient	Yes	allowed	Sender policies
Sender policy is set to quarantine	No	quarantined	Sender policies
User policy is set to exempt	Yes	allowed	Recipient policies
Default scan policy is set to exempt for all users	Yes	allowed	Recipient policies
Message content filter is set to allow	Yes	allowed	Message content filters: Subject Content Header Content Body Content Attachment Content
IP policy for valid first non-trusted forwarder is set to exempt	Yes	allowed	IP address policies
User policy is set to block	Yes	blocked	Recipient policies
IP policy for valid first non-trusted forwarder is set to block	Yes	blocked	IP address policies
Sender policy for valid first non-trusted forwarder is set to block	No	blocked	Sender policies
Attachment policy is set to block or quarantine	No	blocked / quarantined	Attachment filter
Block if attachments are encrypted	Yes	blocked	Content protected
Message content filter is set to block or quarantine	No	blocked / quarantined	Message content filters: Subject Content Header Content Body Content Attachment Content

Email category or IP/Domain database is set to allow / block / quarantine	Yes	allowed / blocked / quarantined	Email category
Bulk Email is set to block or quarantine	No	blocked / quarantined	Bulk email detected
Linked domain policy is set to block or quarantine	No	blocked / quarantined	Content URL
Linked domain policy is set to ignore	Yes	<i>dependent upon scanning results</i>	Content URL
Recipient blocked by reputation-based blocking	No	blocked	Reputation-based blocking
Rate control policy exempts account	Yes	deferred	Rate control, rate control exemptions
Recipient blocked based on real-time block list (RBL)	No	blocked	RBL
Deferred by Barracuda real-time system (BRTS)	Yes	deferred	BRTS System
Quarantine by BRTS	No	quarantine	BRTS System
Blocked by reputation check	No	blocked	Intent analysis
Deferred by Nameserver	Yes	deferred	Suspicious Nameserver
Blocked by local intent analysis check	No	blocked	Intent analysis
Blocked by multi-level intent analysis check	No	blocked	Intent analysis
Deferred by multi-level intent analysis check	Yes	deferred	Suspicious content
Blocked or quarantined by DomainKeys Identified Mail (DKIM) inspection	No	blocked / quarantined	DKIM inspection
Blocked due to no PTR record	No	blocked	No PTR record
Sender Policy Framework (SPF) check blocks client IP	No	blocked	SPF
Blocked by Barracuda Anti-Fraud Intelligence (BAFi) score check	No	blocked	Anti-fraud
Deferred by BAFi score check	Yes	deferred	Suspicious BAFi score
Blocked by image analysis	No	blocked	Image analysis
Deferred by antivirus scan	-	deferred	Suspicious
Blocked by antivirus scan	-	blocked	Antivirus
Blocked by Advanced Threat Detection (ATD)	No	blocked	ATD
Blocked based on Cloudscan scoring	No	blocked	Cloudscan score
Deferred by wait list check	No	deferred	Suspicious

© Barracuda Networks Inc., 2021 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.