DMARC Verification

https://campus.barracuda.com/doc/73722698/

If you make setting changes, allow a few minutes for the changes to take effect.

Domain-based Message Authentication, Reporting, and Conformance (DMARC) is a sender email authentication mechanism that provides protection against phishing attacks, and improves spam accuracy by blocking spam in spoofed messages.

The Link Protection feature in the Barracuda Email Security Service will change the body hash of the email as the body is changed. If you are using DMARC inspection on the mail server side, disable Link Protection in the Barracuda Email Security Service.

Domain-Based Message Authentication, Reporting, and Conformance

DMARC is built on top of the email authentication mechanisms Sender Policy Framework (SPF) and DomainKeys Inspection (DKIM); you must have both an SPF and a DKIM record published for the domain to set DMARC policies.

Important

DMARC overrides DKIM and SPF settings if the following conditions are true:

- DMARC is enabled
- The sender's domain is not exempted from DMARC
- The sender's domain has a valid DMARC DNS TXT record (_dmarc.*example.com*)
- The policy specified by the sender's DMARC record indicates **block** or **quarantine**

Specify DMARC policy settings on the **Inbound Settings > Sender Authentication** page:

- **Enable DMARC** – When set to **Yes**, DMARC enables a sending domain to specify policy for messages that fail DKIM or SPF. When set to **No**, the Barracuda Email Security Service does not run DMARC checks for inbound messages and the SPF and DKIM policy settings are used to verify the IP address range and sending domain.

Additionally, you can select to exempt specific domains from DMARC verification.

Sender Policy Framework

SPF is a sender authentication tool works by having domains publish IP addresses or hostnames that identify machines designated as mail sending machines for that domain. When receiving a message from a domain, the Barracuda Email Security Service can check those records to make sure mail is coming from a designated sending machine. This setting applies only to inbound mail.

For more information on SPF, including how to add the Barracuda Email Security Service outbound IP ranges to your SPF records, see How to Configure Sender Policy Framework.

Specify SPF policy settings on the **Inbound Settings > Sender Authentication** page:

- **Block FAIL** – The SPF FAIL (also referred to as Hard FAIL) response indicates that the IP address of the message sender does not match the IP address or range of IP addresses specified in the sending domain name's SPF record, and that the real owner of the domain has specifically indicated that such messages should be rejected (blocked) as spoofed.
- **Block FAIL, SOFTFAIL** – The SPF SOFTFAIL response indicates that the message sender's IP address does not match the IP address or range of IP addresses specified in the sending domain name's SPF record. A SOFTFAIL means that the domain owner did not specify how such messages should be handled.
- When set to **Off**, the Barracuda Email Security Service does not query DNS for an SPF record for the sending domain to verify whether the sender is the true owner of that domain. If you are concerned about domain spoofing, enable of of the SPF options.

Additionally, you can select to exempt specific IP ranges from SPF verification.

DomainKeys Inspection

The DKIM email authentication method allows a sending domain to cryptographically sign outgoing messages. When a message is received from a domain, the Barracuda Email Security Service verifies that the message is from the sending domain and that the message has not been tampered with.

DKIM uses a public and private key-pair system. An encrypted public key is published to the sending server's DNS records, and each outgoing message is then signed by the server using the corresponding private key. For incoming messages, when the Barracuda Email Security Service sees that message is signed, it retrieves the public key from the sending server's DNS records and uses that key to validate the messages's DKIM signature.

Specify DKIM policy settings on the **Inbound Settings > Sender Authentication** page:

- **Block** – Messages from a domain that fails DKIM verification are blocked.
- **Quarantine** – Messages from a domain that fails DKIM verification are quarantined.
- **Off** – When set to Off, the Barracuda Email Security Service does not run DKIM checks for inbound messages. This is the default setting.

Additionally, you can select to exempt specific domains from DKIM verification.