目次

概要

デフォルトで Cisco E メール セキュリティ アプライアンス (ESA) は当たる メッセージの受信配信を防ぎませんか。からか。 同じドメインに行く同じドメイン。 これはメッセージがあるようにしますか。スプーフィングされるか。 顧客とのビジネスを正当化する外部会社によって。 何人かの会社はサード パーティ 組織にヘルスケアのような会社、旅行会社、先祖などに代わって電子メールを送信 するために頼ります

送信側 確認を使用するスプーフィング保護

設定して下さいメール フロー ポリシー (MFP) を

1. GUI を使用する場合： **郵送して下さいポリシー > メール フロー ポリシー > Add ポリシーを…**
2. SPOOF_ALLOW のように関連している名前を使用して新しい MFP を作成して下さい
3. *送信側 確認* セクションでは、**使用 デフォルト**から **OFF** に *使用 送信側 確認 例外 表* 設定を変更して下さい。
4. **メール ポリシー > メール フロー ポリシー > デフォルトポリシー パラメータ**では、に *使用 送信側 確認 例外 表* 設定を設定 して下さい。

帽子を設定して下さい

1. GUI を使用する場合： **郵送して下さいポリシー > 帽子外観 > Add 送信側 グループを…**
2. 先に作成される MFP に名前をすなわち SPOOF_ALLOW それに応じて設定 して下さい。
3. 順序を設定 して下さいそうすればホワイトリスト下およびブラックリスト送信側の上にグループあります。
4. この送信側 グループ設定に **SPOOF_ALLOW** ポリシーを割り当てて下さい。
5. 『SUBMIT』 をクリック し、**追加して下さい送信側を…**
6. 内部 ドメインをスプーフィングすることを割り当てたいと思うことあらゆる外部パーティのための IP かドメインを追加して下さい。

例外 表を設定して下さい

1. GUI を使用する場合： **郵送して下さいポリシー > 例外 表 > Add 送信側 確認 例外を…**
2.
3.

確認

この時点で、*your.domain* から your.domainwould に来るメールは送信側 確認 例外 表を使用しない MFP に関連付けられるので送信側が送信側 グループ SPOOF_ALLOW にリストされていなければ拒否されます。

これの例はリスナーへの手動 Telnetセッションの完了によって見られます:

553 SMTP 応答は上記のステップからの ESA で設定されるように例外 表からの直接的な応答結果です。

メール ログから、192.168.0.9 の IP アドレスが正しい送信側 グループのための有効 な IP アドレスにないことを見ることができます:

上記のステップからのコンフィギュレーション例と一致する許可された IP アドレスは次の通り参照されます:

関連情報

- ログを検索する Regex の ESA、SMA および WSA グレップ
- ESA メッセージ破棄の判別
- テクニカルサポートとドキュメント - Cisco Systems