送信者検証を使用したスプーフィング保護

目次

[はじめに](#)
[送信者検証を使用したスプーフィング保護](#)
[帽子を設定して下さい](#)
[例外表を設定して下さい](#)
[確認](#)
[関連情報](#)
[Cisco サポート コミュニティ - 特集対話](#)

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) は同じドメインに」行く同じドメインから「アドレス指定されるメッセージの受信配信を防ぎません。 これはメッセージが「顧客とのビジネスを正当化する外部会社によって」スプーフィングされるようにします。 いくつかの会社はサード パーティ組織にヘルスケア、旅行会社、先祖などのような会社に代わってメールを送信 するために頼ります

送信者検証を使用した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 > 帽子概要 > 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 Group Settings 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:

```
$ telnet example.com 25
Trying 192.168.0.189...
Connected to example.com.
Escape character is '^]'.
220 example.com ESMTP
helo example.com
250 example.com
mail from: <test@example.com>
553 Envelope sender <test@example.com> rejected
```

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:

```
Wed Aug 5 21:16:51 2015 Info: New SMTP ICID 2692 interface Management (192.168.0.189) address
192.168.0.9 reverse dns host my.host.com verified no
Wed Aug 5 21:16:51 2015 Info: ICID 2692 RELAY SG RELAY_SG match 192.168.0.0/24 SBRS not enabled
Wed Aug 5 21:17:02 2015 Info: ICID 2692 Address: <test@example.com> sender rejected, envelope
sender matched domain exception
```

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:

```
Wed Aug 5 21:38:19 2015 Info: New SMTP ICID 2694 interface Management (192.168.0.189) address
192.168.0.15 reverse dns host unknown verified no
Wed Aug 5 21:38:19 2015 Info: ICID 2694 ACCEPT SG SPOOF_ALLOW match 192.168.0.15 SBRS not
enabled
Wed Aug 5 21:38:29 2015 Info: Start MID 3877 ICID 2694
Wed Aug 5 21:38:29 2015 Info: MID 3877 ICID 2694 From: <test@example.com>
Wed Aug 5 21:38:36 2015 Info: MID 3877 ICID 2694 RID 0 To: <robert@example.com>
Wed Aug 5 21:38:50 2015 Info: MID 3877 Subject 'This is an allowed IP and email'
Wed Aug 5 21:38:50 2015 Info: MID 3877 ready 170 bytes from <test@example.com>
Wed Aug 5 21:38:50 2015 Info: MID 3877 matched all recipients for per-recipient policy DEFAULT
in the inbound table
Wed Aug 5 21:38:51 2015 Info: MID 3877 interim verdict using engine: CASE spam negative
Wed Aug 5 21:38:51 2015 Info: MID 3877 using engine: CASE spam negative
Wed Aug 5 21:38:51 2015 Info: MID 3877 interim AV verdict using Sophos CLEAN
Wed Aug 5 21:38:51 2015 Info: MID 3877 antivirus negative
Wed Aug 5 21:38:51 2015 Info: MID 3877 AMP file reputation verdict : CLEAN
Wed Aug 5 21:38:51 2015 Info: MID 3877 Outbreak Filters: verdict negative
Wed Aug 5 21:38:51 2015 Info: MID 3877 queued for delivery
Wed Aug 5 21:38:51 2015 Info: New SMTP DCID 354 interface 192.168.0.189 address 192.168.0.15
port 25
Wed Aug 5 21:38:51 2015 Info: Delivery start DCID 354 MID 3877 to RID [0]
Wed Aug 5 21:38:51 2015 Info: Message done DCID 354 MID 3877 to RID [0] [('X-IPAS-Result',
'A0GJMwA8usJV/w8AqMBbGQSEFRqFGKUygmUBkV2GMAKBcQEBAgEBAQOBB4QbKIEIhxuCQbxmoDcRAYNPAYE0AQSqSZB5gXA
```

```
BAQgCAYQjgT8DAgE'), ('X-IronPort-AV', 'E=Sophos;i="5.15,620,1432612800"; \r\n
d="scan\'";a="3877"')]
Wed Aug 5 21:38:51 2015 Info: MID 3877 RID [0] Response '2.0.0 Ok: queued as 1D74E1002A8'
Wed Aug 5 21:38:51 2015 Info: Message finished MID 3877 done
Wed Aug 5 21:38:56 2015 Info: DCID 354 close
```

関連情報

- ログを検索する Regex での ESA、SMA、WSA の Grep
- 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