送信者検証を使用したスプーフィング保護

内容

概要

デフォルトでは、Cisco Eメールセキュリティアプライアンス(ESA)は、同じドメインから同じドメインに「送信」されるメッセージの着信配信を妨げることはありません。これにより、顧客と正規のビジネスを行う外部の企業によってメッセージが「スプーフィング」される可能性があります。一部の企業は、医療、旅行代理店などの企業の代理として、サードパーティの組織にEメールを送信するように依頼しています。

送信者検証を使用したスプーフィング保護

メールフローポリシー(MFP)の設定

1. GUI で次の手順を実行します。**[Mail Policies] > [Mail Flow Policies] > [Add Policy...]**
2. SPOOF_ALLOW
3. [Sender Verification]セクションで、[Use Sender Verification Exception Table]*の設定を[Use Default]から[OFF]に*変更**します**。
4. [メール**ポリシー] > [メールフローポリシー] > [既定のポリシーパラメータ]**で、[送信者確認*例外テーブルの設定を*オンに設定**します**。

HATの設定

1. GUIから：**[Mail Policies] > [HAT Overview] > [Add Sender Group...]**
2. 以前に作成したMFP(SPOOF_ALLOW)に応じて名前を設定します。
3. ALLOWLISTとBLOCKLISTの送信者グループの上に順序を設定します。
4. この送信者グル**ープ設定にSPOOF_ALLOW**ポリシーを割り当てます。
5. [送信**して送信者を追加...]をクリックします。**
6. 内部ドメインのスプーフィングを許可する外部パーティのIPまたはドメインを追加します。

例外テーブルの設定

1. GUI で次の手順を実行します。 **[Mail Policies] > [Exception Table] > [Add Sender Verification Exception...]**
2.
3. **[Reject]**

確認

この時点では、*送信者が送信者グループSPOOF_ALLOWにリストされている場合を除きに、your.domainからyour.domainに送られるメールは拒否されます*。送信者の確認例外テーブルを使用しないMFPに関連付けられます。

この例は、リスナーへの手動telnetセッションを完了することで表示されます。

```
$ 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、上記の手順でESAで設定した例外テーブルからの直接応答です。

メールログから、192.168.0.9のIPアドレスが正しい送信者グループの有効なIPアドレスにないことが分かります。

```
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
```

上記の手順の設定例と一致する許可IPアドレスは、次のようになります。

```
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