NVC

メールヘッダ内へSBRS値を埋め込む設定について
(個別のメールにて確認する方法)

2009年7月16日

株式会社 ネットワークバリューコンポネンツ

設定補足

本設定はmessagefilterの機能を用いて実現します

Messagefilterの設定はCLIからのみの設定となります

作業手順 1

SSHクライアントもしくはシリアル接続等にてIronportへCLIログインします

作業手順 2

コマンド「 filters new 」を実行し、

“Enter filter script. Enter '.' on its own line to end.”

という表示がされたら、以下のスクリプトを入力してください。

```
---- ここから ----
CheckSBRS: if true {
                insert-header("X-SBRS", "$Reputation");
           }
.
---- ここまで ----
```

入力後、“1 filters added.”という表示がされることを確認してください。

作業手順 3

コマンド「 filters list 」を実行し、以下のように設定したフィルタが一覧に表示されることを確認してください。

```
Num Active Valid Name
  1   Y      Y   CheckSBRS
```

作業手順 4

コマンド「 commit 」を実行し、

“Please enter some comments describing your changes:”

という表示がされたら、必要に応じコメントを記載し

Enterキーを押下してください。

Enterキー押下後、“Changes committed: ”という表示がされることを

確認してください。

作業手順 5

外部から内部のメールアドレスに対して、メールを送信してください。

その後、メールログから該当メールのログを抽出し、送信元の

SBRSの値を確認してください。

以下はgmailからメールを送信した例です。

```
Thu Jul 16 15:32:33 2009 Info: New SMTP ICID 2679 interface Data 2 (172.16.27.32) address 209.85.210.195 reverse dns hos
t mail-yx0-f195.google.com verified yes
Thu Jul 16 15:32:33 2009 Info: ICID 2679 ACCEPT SG UNKNOWNLIST match sbrs[-1.0:10.0] SBRS 4.5 ← SBRSの値
Thu Jul 16 15:32:33 2009 Info: Start MID 255 ICID 2679
Thu Jul 16 15:32:33 2009 Info: MID 255 ICID 2679 From: <[redacted]@gmail.com>
Thu Jul 16 15:32:33 2009 Info: MID 255 ICID 2679 RID 0 To: <[redacted]@technvc.com>
Thu Jul 16 15:32:33 2009 Info: MID 255 Message-ID '<29920c340907152332t284ee05ck33405b87217ce3df@mail.gmail.com>'
Thu Jul 16 15:32:33 2009 Info: MID 255 Subject 'test from gmail'
Thu Jul 16 15:32:33 2009 Info: MID 255 ready 1570 bytes from <[redacted]@gmail.com>
Thu Jul 16 15:32:33 2009 Info: MID 255 matched all recipients for per-recipient policy DEFAULT in the inbound table
Thu Jul 16 15:32:33 2009 Info: MID 255 interim verdict using engine: CASE spam negative
Thu Jul 16 15:32:33 2009 Info: MID 255 using engine: CASE spam negative
Thu Jul 16 15:32:33 2009 Info: MID 255 interim AV verdict using Sophos CLEAN
Thu Jul 16 15:32:33 2009 Info: MID 255 antivirus negative
Thu Jul 16 15:32:33 2009 Info: MID 255 queued for delivery
Thu Jul 16 15:32:33 2009 Info: New SMTP DCID 338 interface 172.16.27.32 address 172.16.27.125 port 25
Thu Jul 16 15:32:33 2009 Info: Delivery start DCID 338 MID 255 to RID [0]
Thu Jul 16 15:32:33 2009 Info: Message done DCID 338 MID 255 to RID [0]
Thu Jul 16 15:32:33 2009 Info: MID 255 RID [0] Response '2.0.0 Ok: queued as C41768EC28'
Thu Jul 16 15:32:33 2009 Info: Message finished MID 255 done
Thu Jul 16 15:32:39 2009 Info: DCID 338 close
```

作業手順 6

受信したメールのヘッダを確認し、“X-SBRS”というヘッダが存在すること

を確認してください。

以下はgmailからのメールの例です。

```
Return-Path: <r                    @gmail.com>
X-Original-To:                     @technvc.com
Delivered-To:                      @technvc.com
Received: from c160.technvc.com (unknown [172.16.27.32])
    by mail.technvc.com (Postfix) with ESMTP id C41768EC28
    for <                  @technvc.com>; Thu, 16 Jul 2009 15:34:26 +0900 (JST)
X-SBRS: 4.5          <- この部分にIronportで設定したフィルタの結果が入ります
X-IronPort-Anti-Spam-Filtered: true
X-IronPort-Anti-Spam-Result: AtICAMdlXkrRVdLDkWdsb2JhbACYej8BAQEBCQkMBxGkZYEbkQQBAwIEhAcF
X-IronPort-AV: E=Sophos;i="4.42,409,1243782000";
   d="scan'208";a="255"
Received: from mail-yx0-f195.google.com ([209.85.210.195])
  by c160.technvc.com with ESMTP; 16 Jul 2009 15:32:33 +0900
Received: by yxe33 with SMTP id 33so7131150yxe.28
        for <                  @technvc.com>; Wed, 15 Jul 2009 23:32:31 -0700 (PDT)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=gamma;
        h=domainkey-signature:mime-version:received:date:message-id:subject
         :from:to:content-type:content-transfer-encoding;
        bh=g3zLYH4xKxcPrHOD18z9YfpQcnk/GaJedfustWU5uGs=;
```

注意点

新たに取得されたIPアドレスなど、メール配送が行われていない
アドレスをもった送信元からのメールの場合、SenderBaseの評価対象
となっていないために、SBRSの値が入らない場合があります。
この場合、メールログのSBRSの値は“None”となります。