Wie konfiguriere ich die ESA, um Antispam- und/oder Antivirus-Scans für meine vertrauenswürdigen Absender zu überspringen?

Inhalt

Frage

Wie konfiguriere ich die ESA, um Antispam- und/oder Antivirus-Scans für meine vertrauenswürdigen Absender zu überspringen?

Antwort

AsyncOS bietet drei Haupttools, mit denen Sie die Anti-Spam- oder Virenprüfung für Ihre vertrauenswürdigsten Absender überspringen können. Bitte beachten Sie, dass die ESA nicht empfiehlt, die Virenprüfung aufgrund der Möglichkeit einer unbeabsichtigten Virusinfektion zu überspringen, auch nicht für Ihre vertrauenswürdigsten Absender. Im Folgenden werden die drei Möglichkeiten erläutert, wie Sie die Anti-Spam-Prüfung für einen Teil des Nachrichtenflusses überspringen können.

Das erste Tool, das Ihnen zur Verfügung steht, sind die Mail Flow Policies der Host Access Table (HAT). Mithilfe von Mail Flow Policies können Sie Absender nach IP-Adresse (entweder numerische IP-Adressen oder PTR-DNS-Namen), nach SenderBase-Score oder nach einer lokalen DNS-Zulässigkeit oder Blocklist identifizieren. Nachdem Sie die Absender in einer Absendergruppe in der HAT als vertrauenswürdig identifiziert haben, können Sie diese Absendergruppe markieren, um die Anti-Spam-Prüfung zu überspringen.

Nehmen wir an, Sie wollten einen bestimmten Geschäftspartner, BEISPIEL.COM, identifizieren, der in seiner E-Mail keine Anti-Spam-Prüfung durchführen sollte. Sie müssten die IP-Adressen des Mailservers (oder DNS-Zeigerdatensätze) von SCU.COM herausfinden. Nehmen wir in diesem Fall an, dass BEISPIEL.COM über Mail-Server verfügt, die über IP-Adressen mit DNS-PTR-Datensätzen von "smtp1.mail.scu.com" bis "smtp4.mail.scu.com" verfügen. Denken Sie in diesem Fall daran, dass wir den PTR-Datensatz (manchmal auch Reverse DNS genannt) für die Mail-Server betrachten. Dies hat nichts mit dem Domänennamen zu tun, den die Leute bei SCU.COM für ausgehende E-Mails verwenden.

Sie können eine neue Absendergruppe (oder eine vorhandene Absendergruppe, z. B. ALLOWLIST) mit Mail-Policys > Übersicht > Absendergruppe hinzufügen erstellen. Lassen Sie uns eine "NotSpammer" erstellen. Nachdem Sie diese Seite gesendet haben, kehren Sie zum Bildschirm Mail Policies>Overview (Mail-Policys > Übersicht) zurück, wo Sie eine neue Richtlinie für diese Absendergruppe hinzufügen können. Wenn Sie auf "Richtlinie hinzufügen" klicken, erhalten Sie die Möglichkeit, eine neue Richtlinie zu erstellen. In diesem Fall möchten wir die Standardrichtlinie nur in einem Bereich überschreiben: Erkennung von Spam Geben Sie der

Richtlinie einen Namen, und legen Sie das Verbindungsverhalten auf "Akzeptieren" fest. Scrollen Sie dann nach unten zum Abschnitt "Spam-Erkennung", und legen Sie diese Richtlinie so fest, dass die Spam-Überprüfung übersprungen wird. Reichen Sie diese neue Richtlinie ein, und vergessen Sie nicht, "Änderungen bestätigen".

Ein alternativer Ansatz besteht darin, die Anti-Spam-Prüfung mit den Richtlinien für eingehende E-Mails zu überspringen. Der Unterschied zwischen den HAT- und den Richtlinien für eingehende E-Mails besteht darin, dass die HAT vollständig auf den IP-Informationen des Absenders basiert: die echte IP-Adresse, die IP-Adresse, wie sie im DNS wiedergegeben wird, das SenderBase-Ergebnis (das auf der IP-Adresse basiert) oder ein DNS-Zulässigkeits- oder Sperrlisteneintrag, der auf der IP-Adresse basiert. Richtlinien für eingehende E-Mails basieren auf den Informationen für den Nachrichtenumschlag: wer die Nachricht ist oder von wem sie stammt. Das bedeutet, dass sie anfällig dafür sind, von jemandem getäuscht zu werden, der einen Absender der Nachricht imitiert. Wenn Sie jedoch die Anti-Spam-Prüfung für eingehende E-Mails von Personen überspringen möchten, die E-Mail-Adressen haben, die in "@beispiel.com" enden, können Sie dies ebenfalls tun.

Um eine solche Richtlinie zu erstellen, gehen Sie zu **Mail-Policys > Richtlinien für eingehende E-Mails > Richtlinie hinzufügen**. Dadurch können Sie eine Richtlinie hinzufügen, die eine Gruppe von Absendern (oder Empfängern) definiert. Sobald Sie die Richtlinie für eingehende E-Mails definiert haben, wird sie im Übersichtsbildschirm angezeigt (Mail-Policys > Mail-Policys für eingehende E-Mails). Sie können dann auf die Spalte "Anti-Spam" klicken und die spezifischen Einstellungen für den Spam-Schutz für diesen Benutzer bearbeiten.

Die Anti-Spam-Einstellungen für eine bestimmte Richtlinie haben viele Optionen, aber in diesem Fall wollen wir einfach die Anti-Spam-Prüfung überspringen. Beachten Sie hier einen weiteren Unterschied zwischen HAT-basierten Richtlinien und eingehenden Mail-Policys: Mit der HAT können Sie das Anti-Spam-Scanning nur überspringen oder nicht überspringen, während die Richtlinien für eingehende E-Mails viel mehr Kontrolle haben. Sie können beispielsweise Spam von bestimmten Absendern unter Quarantäne stellen und Spam von anderen Absendern löschen.

Die dritte Option zum Überspringen der Anti-Spam-Prüfung besteht in der Konfiguration und Verwendung eines Nachrichtenfilters.

> **Hinweis**: Content-Filter können hierfür nicht verwendet werden, da Content-Filter nach dem bereits erfolgten Anti-Spam-Scanning auftreten.

Eine der Aktionen in Nachrichtenfilter ist "skip-spamcheck". Der Nachrichtenfilter unten überspringt die Antispam-Prüfung für Absender, die eine bestimmte IP-Adresse haben oder von einem bestimmten Domänennamen stammen:

```
SkipSpamcheckFilter:
   if ( (remote-ip == '192.168.195.101') or
        (mail-from == '@example\\.com$')      )
   {
       skip-spamcheck();
   }
```

Weitere Informationen zur Verwendung von Nachrichtenfiltern finden Sie im Benutzerhandbuch für Ihre AsyncOS-Version.

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems