SPF-Konfiguration und Best Practices

Inhalt

Einführung

In diesem Dokument werden verschiedene Szenarien mit dem Sender Policy Framework (SPF) der Cisco E-Mail Security Appliance (ESA) beschrieben.

Voraussetzungen

Cisco empfiehlt, dass Sie die folgenden Themen kennen:

- Cisco ESA
- Alle Versionen von AsyncOS

Was ist SPF?

Sender Policy Framework (SPF) ist ein einfaches E-Mail-Validierungssystem zur Erkennung von E-Mail-Spoofing. Es bietet einen Mechanismus, mit dem Empfänger-Mail-Empfänger überprüfen können, ob eingehende E-Mails von einer Domäne von einem Host gesendet werden, der von den Administratoren dieser Domäne autorisiert wurde. Die Liste der autorisierten sendenden Hosts für eine Domäne wird in DNS-Datensätzen (Domain Name System) für diese Domäne in Form eines speziell formatierten TXT-Datensatzes veröffentlicht. E-Mail-Spam und Phishing verwenden häufig gefälschte Absenderadressen. Die Veröffentlichung und Überprüfung von SPF-Datensätzen kann daher als Antispam-Verfahren betrachtet werden.

Wird sich die Leistung der ESA erheblich auswirken?

Hinsichtlich der CPU-Leistung sind keine großen Auswirkungen auf die Leistung zu erwarten. Durch die Aktivierung der SPF-Verifizierung wird jedoch die Anzahl der DNS-Abfragen und des DNS-Datenverkehrs erhöht. Für jede Nachricht muss die ESA möglicherweise 1-3 SPF-DNS-Abfragen initiieren. Dies führt dazu, dass der DNS-Cache früher als zuvor abläuft. Aus diesem

Grund wird die ESA auch weitere Abfragen für die anderen Prozesse generieren.

Zusätzlich zu den vorherigen Informationen ist der SPF-Datensatz ein TXT-Datensatz, der größer sein kann als die normalen DNS-Datensätze und einen zusätzlichen DNS-Datenverkehr verursachen kann.

Wie wird der SPF aktiviert?

Diese Anleitungen finden Sie im erweiterten Benutzerhandbuch zum Einrichten der SPF-Überprüfung:

So aktivieren Sie das SPF/System Independent Data Format (SIDF) für die Standard-Mail-Flow-Richtlinie:

1. Klicken Sie auf **Mail-Policys > Mail Flow Policy**.
2. Klicken Sie auf **Standardrichtlinienparameter**.
3. In den Standardrichtlinienparametern sehen Sie den Abschnitt **Sicherheitsfunktionen**.
4. Klicken Sie im Abschnitt SPF/SIDF Verification (SPF/SIDF-Überprüfung) auf **Yes (Ja)**.
5. Legen Sie die Konformitätsstufe fest (die Standardeinstellung ist SIDF-kompatibel). Mit dieser Option können Sie festlegen, welcher Standard der SPF- oder SIDF-Verifizierung verwendet werden soll. Neben der SIDF-Konformität können Sie SIDF-kompatibel auswählen, die SPF und SIDF kombiniert. Einzelheiten zu den Konformitätsstufen finden Sie im *Endbenutzerleitfaden.*
6. Wenn Sie eine Kompatibilitätsstufe mit SIDF-Kompatibilität auswählen, legen Sie fest, ob bei der Überprüfung ein **Pass-**Ergebnis der PRA-Identität auf **None** herabgestuft wird, wenn Resent-Sender vorhanden ist: oder Resent-From: Header in der Nachricht vorhanden. Sie können diese Option aus Sicherheitsgründen auswählen.
7. Wenn Sie eine Konformitätsebene für SPF auswählen, legen Sie fest, ob ein Test mit der HELO-Identität durchgeführt werden soll. Sie können diese Option verwenden, um die Leistung zu verbessern, indem Sie die HELO-Prüfung deaktivieren. Dies kann nützlich sein, da die Spf-Passed-Filterregel zuerst die PRA oder die MAIL FROM Identities überprüft. Die Appliance führt nur die HELO-Prüfung für die SPF-Konformitätsebene durch.

Wenn Sie Aktionen für SPF-Verifizierungsergebnisse durchführen möchten, fügen Sie Content-Filter hinzu:

1. Erstellen Sie für jeden Typ der SPF/SIDF-Überprüfung einen Content-Filter mit spf-Status. Verwenden Sie eine Namenskonvention, um den überprüfungstyp anzugeben. Verwenden Sie z. B. **SPF-Passed** für Nachrichten, die die SPF/SIDF-Überprüfung übergeben, oder **SPF-TempErr** für Nachrichten, die aufgrund eines vorübergehenden Fehlers während der Überprüfung nicht übergeben wurden. Informationen zum Erstellen eines Inhaltsfilters mit spf-status finden Sie in der spf-status Content-Filterregel in der GUI.
2. Nachdem Sie einige SPF/SIDF-verifizierte Nachrichten verarbeitet haben, klicken Sie auf **Monitor > Content Filters**, um zu sehen, wie viele Meldungen die SPF/SIDF-verifizierten Content-Filter ausgelöst haben.

Was bedeutet "Helo Test" ein- und ausschalten? Was geschieht, wenn der Helo-Test in einer bestimmten Domäne fehlschlägt?

Wenn Sie eine Konformitätsebene für SPF auswählen, legen Sie fest, ob ein Test mit der HELO-Identität durchgeführt werden soll. Sie können diese Option verwenden, um die Leistung zu verbessern, indem Sie die HELO-Prüfung deaktivieren. Dies kann nützlich sein, da die Spf-Passed-Filterregel zuerst die PRA oder die MAIL FROM Identities überprüft. Die Appliance führt nur die HELO-Prüfung für die SPF-Konformitätsebene durch.

Gültige SPF-Datensätze

Um die SPF HELO-Prüfung zu bestehen, stellen Sie sicher, dass Sie für jede sendende MTA (separat von der Domäne) einen SPF-Datensatz angeben. Wenn Sie diesen Datensatz nicht angeben, wird die HELO-Prüfung wahrscheinlich zu einem **Keine** Urteil für die HELO-Identität führen. Wenn Sie bemerken, dass SPF-Absender in Ihrer Domäne eine große Anzahl von **Keine** Verdicts zurückgeben, haben diese Absender möglicherweise keinen SPF-Datensatz für jede sendende MTA enthalten.

Die Nachricht wird zugestellt, wenn keine Nachrichten-/Content-Filter konfiguriert sind. Auch hier können Sie bestimmte Aktionen mit Message-/Content-Filtern für jedes SPF/SIDF-Verdict durchführen.

Wie kann sie am besten für nur eine externe Domäne aktiviert werden?

Um den SPF für eine bestimmte Domäne zu aktivieren, müssen Sie möglicherweise eine neue Absendergruppe mit einer Mail-Flow-Richtlinie definieren, für die SPF aktiviert ist. erstellen Sie dann Filter wie oben erwähnt.

Können Sie eine SPF-Prüfung auf Spam-verdächtig aktivieren?

Cisco Anti-Spam berücksichtigt bei der Berechnung der Spam-Bewertungen eine ganze Reihe von Faktoren. Durch einen verifizierbaren SPF-Datensatz kann der Spam-Wert verringert werden, es besteht jedoch weiterhin die Möglichkeit, dass diese Nachrichten als Spam-verdächtig erfasst werden.

Die bestmögliche Lösung wäre, die Absender-IP-Adresse zuzulassen ODER einen Nachrichtenfilter zu erstellen, um die Spam-Prüfung mit mehreren Bedingungen (remote-ip, mail-from, X-skipspamcheck-header usw.) zu überspringen. Der Header kann vom sendenden Server hinzugefügt werden, um eine Art von Nachrichten von anderen zu identifizieren.

Zugehörige Informationen

- Cisco Email Security Appliance - Benutzerhandbücher
- Best Practices für die E-Mail-Authentifizierung - Einsatz von SPF/DKIM/DMARC
- Technischer Support und Dokumentation - Cisco Systems