Kann ich die Ablaufzeit von sicheren Umschlägen vorschreiben, die von einer Cisco E-Mail Security Appliance mit CRES generiert werden?

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Ablaufzeit für sichere Umschläge festgelegt wird, die von einer Cisco E-Mail Security Appliance (ESA) generiert werden, die den Cisco Registered Envelope Service (RES) implementiert.

Kann ich die Ablaufzeit von sicheren Umschlägen vorschreiben, die von einer Cisco E-Mail Security Appliance mit RES generiert werden?

Ja, Sie können den ausgehenden Nachrichten SMTP-Header hinzufügen, die zur Verschlüsselung markiert werden. Dies schließt den Header 'X-PostX-ExpirationDate' ein.

Im Folgenden sehen Sie einen Auszug aus dem Benutzerhandbuch der E-Mail Security Appliance.

Einfügen von Verschlüsselungs-Headern in Nachrichten

AsyncOS ermöglicht es Ihnen, einer Nachricht Verschlüsselungseinstellungen hinzuzufügen, indem Sie einen SMTP-Header mithilfe eines Content-Filters oder eines Nachrichtenfilters in eine Nachricht einfügen. Der Verschlüsselungs-Header kann die im zugehörigen

Verschlüsselungsprofil definierten Verschlüsselungseinstellungen überschreiben und bestimmte Verschlüsselungsfunktionen auf Nachrichten anwenden.

Vorgehensweise

Schritt 1	Gehen Sie zu Mail-Policys > Outgoing Content FilterorIncoming Content Filters.
Schritt 2	Klicken Sie im Bereich Filters (Filter) auf Filter hinzufügen.
Schritt 3	Klicken Sie im Bereich Aktionen auf Aktion hinzufügen, und wählen Sie Header hinzufügen/bearbe aus, um einen Verschlüsselungs-Header in die Nachrichten einzufügen, um eine zusätzliche Verschlüsselungseinstellung anzugeben. Wenn z. B. ein registrierter Umschlag 24 Stunden nach dem Senden ablaufen soll, geben Sie X-P ExpirationData als Headernamen und +24:00:00 als Headerwert ein.

Nächste Schritte

Verwandte Themen

- Weitere Informationen zum Erstellen eines Filters für verschlüsselte Inhalte finden Sie unter Verschlüsseln und Sofortige Zustellen von Nachrichten mithilfe eines Content-Filters.
- Informationen zum Einfügen eines Headers mithilfe eines Nachrichtenfilters finden Sie unter Verwenden von Nachrichtenfiltern zum Erzwingen von E-Mail-Richtlinien.

Verschlüsselungs-Header

In der folgenden Tabelle werden die Verschlüsselungs-Header angezeigt, die Sie Nachrichten hinzufügen können.

Tabelle 3: E-Mail-Verschlüsselungs-Header

MIME-Header	Beschreibung	Wert
`X-PostX-Reply-Enabled`	Gibt an, ob eine sichere Antwort für die Nachricht aktiviert werden soll, und zeigt die Schaltfläche Antworten in der Nachrichtenleiste an. Dieser Header fügt der Nachricht eine Verschlüsselungseinstellung hinzu.	Ein Boolean, um festzul ob die Schaltfläche Antworten angezeigt we soll. Legen Sie true fest die Schaltfläche anzuze Der Standardwert ist fal
`X-PostX-Reply-All-Enabled`	Gibt an, ob die sichere "Antwort an alle" für die Nachricht aktiviert werden soll und zeigt die Schaltfläche Alle antworten in der Nachrichtenleiste an. Dieser Header überschreibt die Standardprofileinstellung.	Eine Boolean-Methode, festzulegen, ob die Schaltfläche Alle antwo angezeigt werden soll. L Sie true fest, um die Schaltfläche anzuzeige Standardwert ist false.
`X-PostX-Forward-Enabled`	Gibt an, ob die sichere Nachrichtenweiterleitung aktiviert werden	Ein Boolean, um festzul ob die Schaltfläche

	soll, und zeigt die Weiterleitungstaste in der Nachrichtenleiste an. Dieser Header überschreibt die Standardprofileinstellung.	Weiterleiten angezeigt werden soll. Legen Sie fest, um die Schaltfläche anzuzeigen. Der Standardwert ist false.
X-PostX-Send-Return-Receipt	Gibt an, ob Lesebestätigungen aktiviert werden sollen. Der Absender erhält eine Quittung, wenn Empfänger den sicheren Umschlag öffnen. Dieser Header überschreibt die Standardprofileinstellung.	Ein boolescher Code für Senden einer Lesebestätigung. Legen true fest, um die Schaltf anzuzeigen. Der Standardwert ist false.
X-PostX-ExpirationDate	Definiert das Ablaufdatum eines registrierten Umschlags, bevor dieser gesendet wird. Der Schlüsselserver beschränkt den Zugriff auf den registrierten Umschlag nach dem Ablaufdatum. Der registrierte Umschlag zeigt eine Meldung an, dass die Nachricht abgelaufen ist. Dieser Header fügt der Nachricht eine Verschlüsselungseinstellung hinzu. Wenn Sie den Cisco Registered Envelope Service verwenden, können Sie sich bei der Website unter http://res.cisco.com anmelden und die Nachrichtenverwaltungsfunktionen verwenden, um das Ablaufdatum von Nachrichten nach dem Senden festzulegen, anzupassen oder zu löschen.	Ein Zeichenfolgenwert, das relative Datum oder relative Uhrzeit enthält. Verwenden Sie das For +HH:MM:SS für relative Stunden, Minuten und Sekunden und das Form +D für relative Tage. Standardmäßig gibt es k Ablaufdatum.
X-PostX-ReadNotificationDate	Definiert das "Read by"-Datum des registrierten Umschlags, bevor dieser gesendet wird. Der lokale Schlüsselserver generiert eine Benachrichtigung, wenn der registrierte Umschlag bis zu diesem Datum nicht gelesen wurde. Registrierte Umschläge mit diesem Header funktionieren nicht mit dem Cisco Registered Envelope Service, sondern nur mit einem lokalen Schlüsselserver. Dieser Header fügt der Nachricht eine Verschlüsselungseinstellung hinzu.	Ein Zeichenfolgenwert, das relative Datum oder relative Uhrzeit enthält. Verwenden Sie das For +HH:MM:SS für relative Stunden, Minuten und Sekunden und das Form +D für relative Tage. Standardmäßig gibt es k Ablaufdatum.
X-PostX-Suppress-Applet-For-Open	Gibt an, ob das Entschlüsselungs-Applet deaktiviert werden soll. Das Entschlüsselungs-Applet bewirkt, dass Nachrichtenanhänge in der Browserumgebung geöffnet werden. Durch das Deaktivieren des Applets wird die Nachrichtenanbindung am Schlüsselserver entschlüsselt. Wenn Sie diese Option deaktivieren, dauert das Öffnen von Nachrichten möglicherweise	Ein boolesches Objekt, festzulegen, ob das Entschlüsselungs-Apple deaktiviert werden soll. Legen Sie true fest, um Applet zu deaktivieren. Standardwert ist false.

	länger, jedoch nicht abhängig von der Browserumgebung. Dieser Header überschreibt die Standardprofileinstellung.	
X-PostX-Use-Script	Gibt an, ob JavaScript-freie Umschläge gesendet werden sollen. Ein JavaScript-freier Umschlag ist ein registrierter Umschlag, der das JavaScript nicht enthält, mit dem Umschläge lokal auf dem Computer des Empfängers geöffnet werden. Der Empfänger muss entweder die Methode "Online öffnen" oder die Methode "Öffnen durch Weiterleiten" verwenden, um die Nachricht anzuzeigen. Verwenden Sie diesen Header, wenn das Gateway einer Empfängerdomäne JavaScript entfernt und die verschlüsselte Nachricht unopfbar macht. Dieser Header fügt der Nachricht eine Verschlüsselungseinstellung hinzu.	Eine Boolean-Methode, festzulegen, ob das JavaScript-Applet eingeschlossen werden Legen Sie false fest, um einen JavaScript-freien Umschlag zu senden. D Standardwert ist true.
X-PostX-Remember-Envelope-Key-Checkbox	Gibt an, ob für das Offline-Öffnen von Umschlägen eine Envelope-spezifische Schlüssel-Caching zugelassen werden soll. Beim Caching von Umschlagschlüsseln wird der Entschlüsselungsschlüssel für einen bestimmten Umschlag auf dem Computer des Empfängers zwischengespeichert, wenn der Empfänger die richtige Passphrase eingibt und das Kontrollkästchen "Kennwort für diesen Umschlag speichern" aktiviert. Danach muss der Empfänger keine Passphrase mehr eingeben, um den Umschlag auf dem Computer erneut zu öffnen. Dieser Header fügt der Nachricht eine Verschlüsselungseinstellung hinzu.	Eine Boolescher Ausdru der festlegt, ob die Zwischenspeicherung v Umschlagschlüsseln ak und das Kontrollkästche "Kennwort für diesen Umschlag speichern" aktiviert werden soll. De Standardwert ist false.

Beispiele für Verschlüsselungs-Header

Dieser Abschnitt enthält Beispiele für Verschlüsselungsheader.

Aktivieren der Umschlagschlüsselzwischenspeicherung für Offline-Öffnen

Um einen registrierten Umschlag mit aktivierter Envelope Key-Caching zu senden, fügen Sie die folgende Überschrift in die Nachricht ein:

```
X-PostX-Remember-Envelope-Key-Kontrollkästchen: wahr
```

Das Kontrollkästchen "Kennwort für diesen Umschlag speichern" wird auf dem registrierten Umschlag angezeigt.

JavaScript-freie Umschläge aktivieren

Um einen registrierten Umschlag ohne JavaScript zu senden, fügen Sie die folgende Überschrift in die Nachricht ein:

```
X-PostX-Use-Script: falsch
```

Wenn der Empfänger die Anlage securedoc.html öffnet, wird der registrierte Umschlag mit dem Link "Online öffnen" angezeigt, und die Schaltfläche "Öffnen" ist deaktiviert.

Aktivieren des Ablaufs von Nachrichten

Um eine Nachricht so zu konfigurieren, dass sie 24 Stunden nach dem Senden abläuft, fügen Sie den folgenden Header in die Nachricht ein:

```
X-PostX-Ablaufdatum: +24:00:00
```

Der Empfänger kann den Inhalt der verschlüsselten Nachricht während des 24-Stunden-Zeitraums nach dem Senden öffnen und anzeigen. Danach zeigt der registrierte Umschlag eine Meldung an, dass der Umschlag abgelaufen ist.

Deaktivieren des Entschlüsselungs-Applets

Um das Entschlüsselungs-Applet zu deaktivieren und die Nachrichtenanbindung am Schlüsselserver entschlüsseln zu lassen, fügen Sie den folgenden Header in die Nachricht ein:

```
X-PostX-Suppress-Applet-For-Open: wahr
```

> **Hinweis**: Wenn Sie das Entschlüsselungs-Applet deaktivieren, dauert das Öffnen der Nachricht möglicherweise etwas länger, sie ist jedoch nicht von der Browserumgebung abhängig.