# Erstellen einer Whitelist-Richtlinie auf einer Cisco ESA für Phishing-Tests

### Inhalt

Einführung Voraussetzungen Anforderungen Hintergrundinformationen Konfigurieren Erstellen der Absendergruppe Erstellen des Nachrichtenfilters Überprüfen

# Einführung

In diesem Dokument wird beschrieben, wie eine Whitelist-Richtlinie für die Cisco Email Security Appliance (ESA) oder Cloud Email Security (CES)-Instanz erstellt wird, um Phishing-Schulungstests und -Kampagnen zu ermöglichen.

### Voraussetzungen

#### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Navigieren und Konfigurieren von Regeln für die Cisco ESA/CES auf der WebUI.
- Erstellen von Nachrichtenfiltern auf der Cisco ESA/CES in der Befehlszeilenschnittstelle (CLI).
- Kenntnis der für die Phishing-Kampagne/den Phishing-Test verwendeten Ressourcen

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Hintergrundinformationen

Administratoren, die Phishing-Tests oder -Kampagnen durchführen, erhalten E-Mails mit Informationen, die den aktuellen Talos-Regeln für die Regelsätze für Anti-Spam und/oder Outbreak-Filter entsprechen. In einem solchen Fall erreichen die Phishing-Kampagnen-E-Mails keine Endbenutzer und werden von der Cisco ESA/CES selbst verklagt, wodurch der Test zum Erliegen kommt. Administratoren müssen sicherstellen, dass die ESA/CES ihre Kampagne/Tests über diese E-Mails durchführen kann.

### Konfigurieren

**Warnung**: Der Standpunkt von Cisco zu Anbietern von Whitelisting-Phishing-Simulationen und -Schulungen weltweit ist nicht zulässig. Wir empfehlen Administratoren, mit dem Phishing-Simulator-Dienst zu arbeiten *(z. B.: PhishMe)*, um ihre IPs abzurufen, und fügen sie dann lokal zur Whitelist hinzu. Cisco muss seine ESA-/CES-Kunden vor diesen IP-Adressen schützen, wenn sie jemals die Hände wechseln oder eine Bedrohung darstellen.

**Vorsicht**: Administratoren sollten diese IPs während des Tests nur in einer Whitelist-Liste speichern. Wenn externe IPs eine längere Zeit nach dem Testen auf einer Whitelist verbleiben, können unerwünschte oder schädliche E-Mails an Endbenutzer gesendet werden, wenn diese IPs kompromittiert werden.

Erstellen Sie auf der Cisco E-Mail Security Appliance (ESA) eine neue Absendergruppe für Ihre Phishing-Simulation, und weisen Sie sie der \$TRUSTED Mail Flow-Richtlinie zu. Auf diese Weise können alle Phishing-Simulations-E-Mails an Endbenutzer gesendet werden. Mitglieder dieser neuen Absendergruppe unterliegen keiner Ratenbeschränkung, und der Inhalt dieser Absender wird nicht von der Cisco IronPort Anti-Spam-Engine gescannt, sondern wird weiterhin von der Anti-Virus-Software gescannt.

Hinweis: Standardmäßig ist Anti-Virus in der \$TRUSTED Mail Flow-Richtlinie aktiviert, aber Anti-Spam deaktiviert.

#### Erstellen der Absendergruppe

- 1. Klicken Sie auf die Registerkarte Mail-Policys.
- 2. Wählen Sie im Abschnitt *Host Access Table* (*Hostzugriffstabelle*) die Option *HAT Overview* (*HAT-Übersicht*) aus.

	cisco	Ernail Sec	C100V curity Virtual Appliance							
٨	N	Ionitor	Mail Policies	Security Sen	vices		٩	letw	ork	Syste
	HAT Find Se	Overviev enders Find Sen	Email Security Manag Incoming Mail Policies Incoming Content Filters Outgoing Mail Policies Outgoing Content Filters Mail Policy Settings Host Access Table (Ha	er ; ; ()						
	Sender	Groups (List	Mail Flow Policies	25	)	ĺ.				
	Add S	ender Group	Exception Table Address Lists		tation	Conro	۲			E-town of Theorem
	Order	Sender Grou	Recipient Access Table (	RAT) D	2	4	6	8	+10	Sources Appli
	1	WHITELIST	Destination Controls						- E	None applied
	2	BLACKLIST	Bounce Verification	1	- 10 -	51	З <u>г</u> .	16	1	None applied
		01/0000000000	Data Loss Descention	(010)					11	

3. Vergewissern Sie sich rechts, dass der InboundMail-Listener aktuell ausgewählt ist.

4. Klicken Sie in der Spalte *Absendergruppe* unten auf *Absendergruppe hinzufügen..,* 

Add S	ender Group													In	nport HAT
Order	Sender Group	-10	-8	Ser -6	nderBa	ase™ -2	Reput	ation 2	Scor 4	e ?	8	+10	External Threat Feed Sources Applied	Mail Flow Policy	Delete
1	WHITELIST	1	1										None applied	TRUSTED	<b>a</b>
2	BLACKLIST	-					1	10	(	×.		1	None applied	BLOCKED	1

5. Füllen Sie die Felder Name und Kommentar aus. Wählen Sie im Dropdown-Menü Policy (Richtlinien) die Option\$TRUSTED aus, und klicken Sie dann auf Submit (Senden) und Add Senders (Absender hinzufügen)

Name:	PHISHING_SIMULATION
Comment:	Allow 3rd Party Phishing Simulation emails
Policy:	TRUSTED
SBRS (Optional):	to Include SBRS Scores of "None" Recommended for suspected senders only.
External Threat Feeds (Optional): For IP lookups only	To add and configure Sources, go to Mail Policies > External Threat Feeds
DNS Lists (Optional): ⑦	(e.g. 'query.blacklist.example, query.blacklist2.example')
Connecting Host DNS Verification:	<ul> <li>Connecting host PTR record does not exist in DNS.</li> <li>Connecting host PTR record lookup fails due to temporary DNS failure.</li> <li>Connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A</li> </ul>

6. Geben Sie im ersten Feld die IP oder den Hostnamen ein, die Sie als Whitelist festlegen möchten. Ihr Phishing-Simulationspartner stellt Ihnen die Absender-IP-Informationen zur Verfügung.

Sender Type:	IP Addresses	Geolocation
Sender: 🕐	12.34.56.78	
	(IPv4 or IPv6)	
Comment:	Phishing Simulation Sender IP	

Wenn Sie alle Einträge hinzugefügt haben, klicken Sie auf die Schaltfläche *Senden*. Denken Sie daran, auf die Schaltfläche *Änderungen bestätigen* zu klicken, um Ihre Änderungen zu speichern.

#### Erstellen des Nachrichtenfilters

Nachdem die Absendergruppe erstellt wurde, um die Umgehung von Anti-Spam und Anti-Virus zuzulassen, ist ein Nachrichtenfilter erforderlich, um die anderen Sicherheitsmodule zu überspringen, die möglicherweise mit der Phishing-Kampagne/dem Phishing-Test übereinstimmen.

- 1. Herstellen einer Verbindung zur CLI der ESA
- 2. Führen Sie die Befehlsfilter aus.
- 3. Führen Sie den Befehl new aus, um einen neuen Nachrichtenfilter zu erstellen.
- 4. Kopieren Sie das folgende Filterbeispiel, und fügen Sie es ein. Bearbeiten Sie ggf. die tatsächlichen Namen der Absendergruppe:

```
skip_amp_graymail_vof_for_phishing_campaigns:
if(sendergroup == "PHISHING_SIMULATION")
{
    skip-ampcheck();
    skip-marketingcheck();
    skip-socialcheck();
    skip-bulkcheck();
    skip-vofcheck();
}
```

- 5. Kehren Sie zur Haupt-CLI-Eingabeaufforderung zurück, und drücken Sie die Eingabetaste.
- 6. Führen Sie *Commit aus*, um die Konfiguration zu speichern.

### Überprüfen

Verwenden Sie die Ressource eines Drittanbieters, um eine Phishing-Kampagne/einen Phishing-Test zu senden und die Ergebnisse in den Nachrichtenverfolgungsprotokollen zu überprüfen, um sicherzustellen, dass alle Engines übersprungen und die E-Mail zugestellt wurden.