Blokkeer URL's in e-mails op basis van TLD in beveiligde e-mail

Inhoud

Inleiding

Dit document beschrijft hoe u URL's in Cisco Secure Email kunt blokkeren op basis van specifieke topleveldomeinen (TLD's).

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Secure E-mail.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Het blokkeren van URL's op basis van specifieke top-level domeinen (TLD's) kan een effectieve manier zijn om uw e-mailsysteem te beschermen tegen mogelijke bedreigingen. Cisco Email Security Gateway (CES/ESA) analyseert de reputatie van URL's en voert deze uit op basis van verschillende criteria.

Als uw bedrijfsbeleid echter vereist dat bepaalde TLD's worden geblokkeerd, wordt in deze procedure uitgelegd hoe u dit kunt bereiken met behulp van filters en woordenboeken in uw e-mailsysteem.

Stap 1. Een filter maken

Om een gehele TLD te blokkeren, moet u eerst een inhoudsfilter in uw e-mailsysteem maken. Dit filter identificeert en blokkeert URL's die de TLD's bevatten die u wilt beperken. U kunt dit proces verbeteren door woordenboeken te gebruiken om lijsten van TLD's te beheren en relevante reguliere expressies op te nemen. Door deze reguliere expressies aan een woordenboek toe te voegen, kunt u uw filtercriteria efficiënt beheren en toepassen.

Stap 2. Gebruik normale expressies

Reguliere expressies (regex) zijn een krachtig hulpmiddel om specifieke patronen in URL's te identificeren.

Om URL's op basis van TLD's effectief te blokkeren, kunt u deze reguliere expressies aan een woordenboek toevoegen. Deze benadering maakt eenvoudig beheer en updates van uw filtercriteria mogelijk:

1. Reguliere expressie voor het blokkeren van URL’s beginnend met http of https, inclusief ondersteuning voor Punycode domeinen:

```
(?i)https?:\/\/((xn--\w+\.)|(\w+\.))+(zip|mov)
```

2. Normale expressie voor het blokkeren van URL's met een e-mailformaat, ook met Punycode:

```
(?i)https?:\/\/.*@((xn--\w+\.)|(\w+\.))+(zip|mov)
```

Door deze reguliere expressies aan een woordenboek toe te voegen, kunt u het proces voor het filteren van URL's stroomlijnen, zodat uw e-mailsysteem de opgegeven TLD's efficiënt blokkeert.

Dictionary Properties

Name: URL_TLD

Advanced Matching:
- [ ] Match whole words
- [ ] Case Sensitive

▸ Smart Identifiers: *Match specific patterns such as social security numbers and credit card numbers.*

Dictionary Number of terms: 2

Add Terms:

Separate multiple entries with line breaks.

Weight: 1

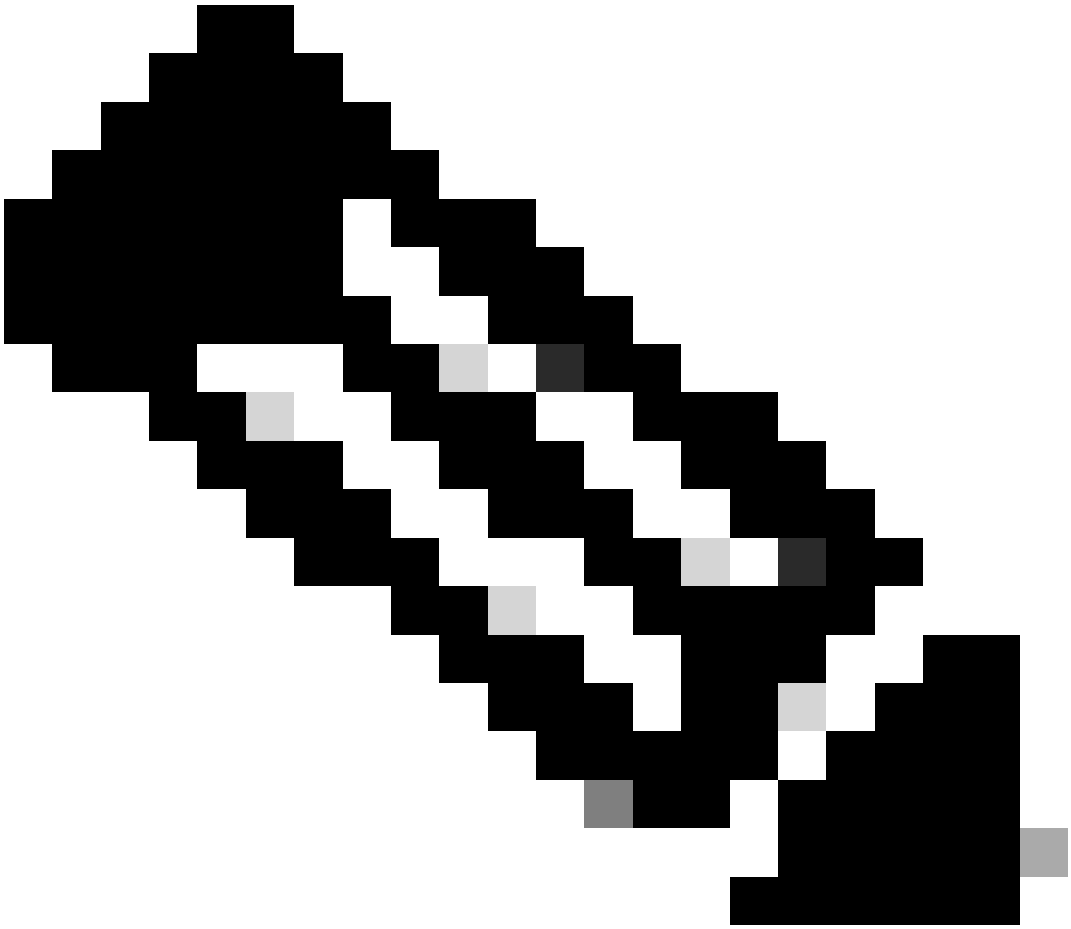
Add

Displaying 1 - 2 of 2 items
Page 1 of 1

<< Previous 1 Next >> 10

Term	Weight	Delete
https?:\/\/((xn--\w+\.)|(\w+\.))+(zip|mov)	1	
https?:\/\/.*@((xn--\w+\.)|(\w+\.))+(zip|mov)	1	

Cancel Submit



Opmerking: Als u Unicode-tekens zoals U+2215 (⁄) en U+2044 (/) in overweging moet nemen, kunnen extra aanpassingen aan uw reguliere expressie nodig zijn.

Stap 3. Test in monitormodus

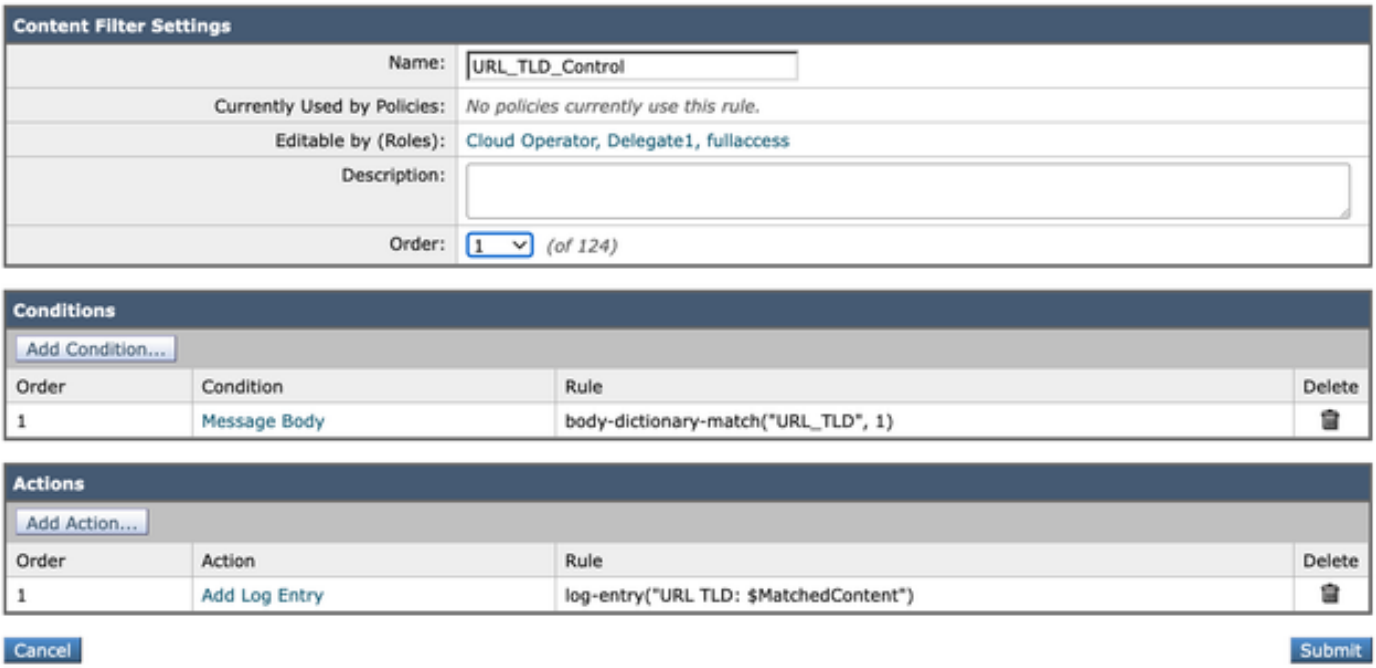
Alvorens deze filters in een productiemilieu uit te voeren, is het raadzaam om hen in monitorwijze te gebruiken. Deze aanpak stelt u in staat om de effectiviteit van uw filters te beoordelen zonder onmiddellijk e-mails te blokkeren, waardoor onbedoelde verstoringen van uw e-mailsysteem worden voorkomen.

In monitormodus, het systeem logt instanties waar URL's overeenkomen met uw gespecificeerde criteria, zodat u de resultaten kunt observeren en de nodige aanpassingen te maken. Om dit te vergemakkelijken, kunt u een actie van de logboekingang vormen die relevante informatie over aangepaste URLs vangt. U kunt bijvoorbeeld deze actie voor logboekinvoer gebruiken:

```
log-entry("URL TLD: $MatchedContent")
```

Deze actie registreert de specifieke inhoud die aansloot bij uw filtercriteria, en geeft waardevolle inzichten in de URL's die zouden worden geblokkeerd als de filter actief was. Door deze logboeken te bekijken, kunt u uw reguliere expressies en woordenboekvermeldingen verfijnen om er zeker van te zijn dat ze de bedoelde URL's nauwkeurig vastleggen zonder dat dit gevolgen heeft voor legitieme e-mails.

Bovendien kunt u door de logbestanden over een bepaalde periode te bewaken de impact van uw filters op de prestaties evalueren en indien nodig optimalisaties uitvoeren. Als u er zeker van bent dat de filters naar behoren functioneren, kunt u overschakelen van monitor naar actieve blokkeringsmodus:



Prestatieoverwegingen

Uitgebreid gebruik van reguliere expressies kan invloed hebben op de prestaties van uw e-mailsysteem. Daarom is het essentieel om te testen en te optimaliseren wanneer dat nodig is.

Conclusie

Het blokkeren van URL's op basis van specifieke TLD's kan de beveiliging van uw e-mailsysteem verbeteren. Vooral nieuwe TLD's die door Google worden geïntroduceerd, zoals .zip en .mov, hebben beveiligingsproblemen veroorzaakt door hun gelijkenis met populaire bestandsextensies. Door uw filters zorgvuldig te testen en de invloed op de prestaties te overwegen, blijft u een efficiënt en veilig systeem behouden.

Google Registry kondigde acht nieuwe TLD's aan: .dad, .phd, .prof, .esq, .foo, .zip, .mov en .nexus. .zip en .mov hebben echter extra de aandacht getrokken vanwege hun gelijkenis met veel gebruikte bestandsextensies, waardoor het cruciaal is om deze in uw beveiligingsmaatregelen aan te pakken.

Voor meer inzichten in de veiligheidsimplicaties van de .zip TLD, kunt u verwijzen naar de Talos Intelligence blog post: Informatie over ZIP-TLD lekt. Deze bron biedt een extra kader voor de potentiële risico's die aan deze TLD's zijn verbonden en onderstreept het belang van de implementatie van passende filterstrategieën.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.