E-mailspoofing detecteren en voorkomen

Inhoud

Inleiding

Dit document beschrijft hoe u e-mailspoofing kunt detecteren en voorkomen bij gebruik van Cisco Secure Email.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan.

- Cisco beveiligde e-mail

Gebruikte componenten

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.

Over dit document

Dit document is bedoeld voor Cisco-klanten, Cisco Channel Partners en Cisco-engineers die beveiligde e-mail van Cisco implementeren. Dit document omvat:

- Wat is e-mailspoofing?
- E-mail spoofing defence-werkstroom
- Wat kun je nog meer doen met het voorkomen van spoofing?

Wat is e-mailspoofing

E-mail Spoofing is e-mail header vervalsing waar het bericht lijkt te zijn voortgekomen uit iemand of ergens anders dan de werkelijke bron. E-mail Spoofing wordt gebruikt in phishing en spam campagnes omdat mensen waarschijnlijk een e-mail te openen wanneer zij denken dat een legitieme, betrouwbare bron het heeft verzonden. Raadpleeg voor meer informatie over spoofing Wat is e-mailspoofing en hoe u het kunt detecteren.

E-mail spoofing valt in deze categorieën:

Categorie	Beschrijving	Hoofddoel
Direct Domain Spoofing	Imiteren van een soortgelijk domein in de Envelope From als het domein van de ontvanger.	Werknemers
Naambedrog weergeven	De Van kopbal toont een wettige afzender met een uitvoerende naam van een organisatie. Ze staan ook bekend als Business Email Compromis (BEC).	Werknemers
Merknaam imitatie	De From-header toont een legitieme afzender met de merknaam van een bekende organisatie.	Klanten / partners
Op Phish URL gebaseerde aanval	Een e-mail met een URL die probeert gevoelige gegevens te stelen of informatie in te loggen van het slachtoffer. Een nep-e-mail van een bank die je vraagt om op een link te klikken en je accountgegevens te verifiëren is een voorbeeld van een phishing URL-gebaseerde aanval.	Werknemers/partners
Neef- of dubbelganger-domeinaanval	De envelop van of van kopbalwaarde toont een gelijkaardig afzenderadres dat echte nadoet om het Kader van het Beleid van de Afzender (SPF), Domeinsleutels te omzeilen Identificeerde Post (DKIM),	Werknemers/partners

	en Domeingebaseerde de Verificatie van het Bericht, Rapportage en Conformiteit (DMARC) inspecties te mijden.	
Account overnemen / Gecomprimeerde account	Verkrijg onbevoegde toegang tot een echt e-mailaccount dat toebehoort aan iemand, en verstuur vervolgens e-mails naar andere slachtoffers als de legitieme e-mailaccounteigenaar.	Iedereen

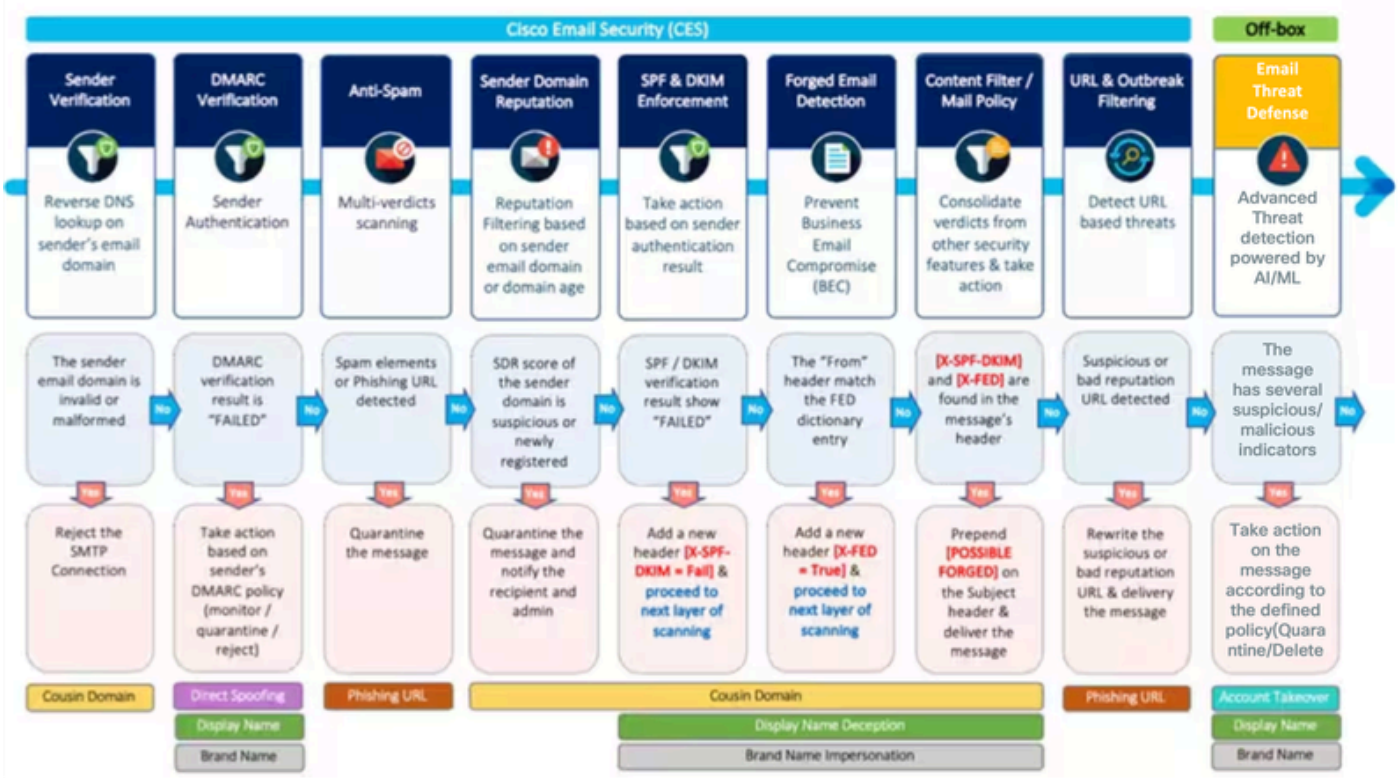
De eerste categorie heeft betrekking op misbruik van de domeinnaam van de eigenaar in de Envelope From-waarde in de internetheader van een e-mail. Cisco Secure Email kan deze aanval herstellen met DNS-verificatie (Domain Name Server) van de afzender, zodat alleen legitieme afzenders worden toegestaan. Het zelfde resultaat kan globaal worden bereikt met behulp van DMARC, DKIM, en SPF verificatie.

Echter, de andere categorieën schenden slechts gedeeltelijk het domein gedeelte van het e-mailadres van de afzender. Daarom is het niet gemakkelijk om te worden afgeschrokken wanneer u DNS tekstrecords of alleen afzenderverificatie gebruikt. Idealiter zou het best zijn om bepaalde beveiligde e-mailfuncties van Cisco en Cisco Secure Email Threat Defense (ETD) te combineren om dergelijke geavanceerde bedreigingen te bestrijden. Zoals u weet, kunnen Cisco Secure Email Management en de configuratie van functies van organisatie tot organisatie verschillen en kan een onjuiste toepassing leiden tot een hoge incidentie van fout-positieven. Om inzicht te krijgen in de bedrijfsbehoeften van de organisatie en de kenmerken op maat te maken is daarom essentieel.

E-mail spoofing defence-werkstroom

De beveiligingsfuncties die betrekking hebben op de beste praktijken voor bewaking, waarschuwingen en afdwingen van aanvallen door spoofing worden in het diagram weergegeven (afbeelding 1). De details van elke functie worden in dit document weergegeven. De beste praktijk is een diepgaande defensie benadering om e-mail spoofing te ontdekken. Aanvallen kunnen hun methoden tegen een organisatie in de loop der tijd wijzigen, zodat een beheerder alle wijzigingen moet controleren en de juiste waarschuwingen en handhaving moet controleren.

Afbeelding 1. Cisco Secure Email Spoof Defense-pijpleiding

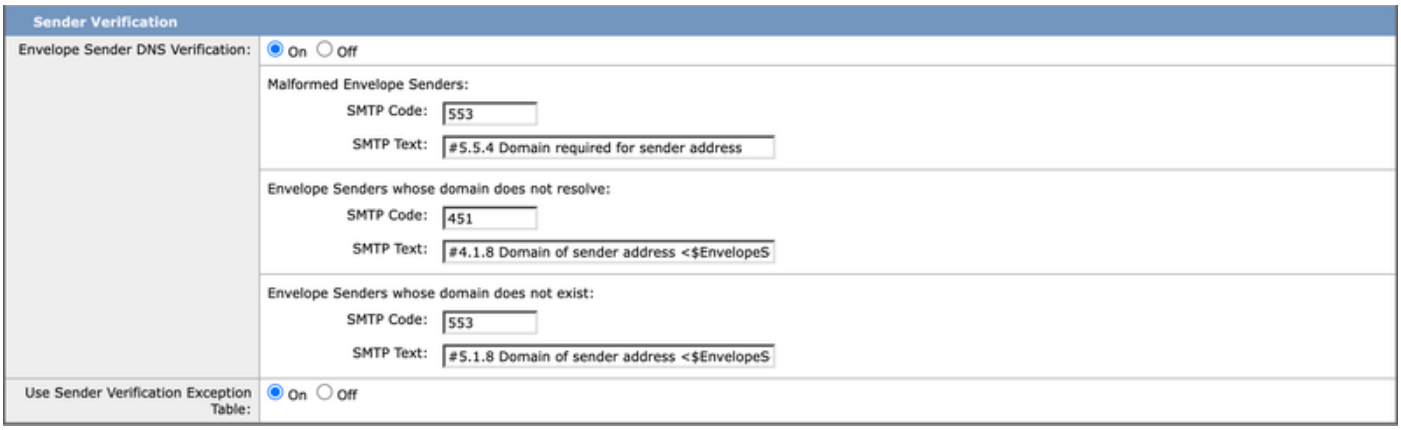


Layer 1: Geldigheidscontrole op het domein van de afzender

Sender Verification is een eenvoudiger manier om e-mails te voorkomen die worden verzonden vanuit een nep-e-mailadres, zoals neef-domeinspoofing (c1sc0.com is bijvoorbeeld de imposter van cisco.com). Cisco Secure Email maakt een MX-record query voor het domein van het e-mailadres van de afzender en voert een A-record lookup uit op het MX-record tijdens het SMTP-gesprek. Als de DNS-query NXDOMAIN retourneert, kan het domein als niet-bestaand behandelen. Het is een veel gebruikte techniek voor aanvallers om de informatie van de envelopzender te vervalsen, zodat de e-mail van een niet-geverifieerde afzender wordt geaccepteerd en verder verwerkt. Cisco Secure Email kan alle inkomende berichten weigeren die niet voldoen aan de verificatiecontrole die deze functie gebruikt, tenzij het domein of IP-adres van de afzender is toegevoegd aan de tabel met uitzonderingen.

Best Practice: het instellen van Cisco Secure Email om het SMTP-gesprek af te wijzen als het e-maildomein van het veld van de envelopverzender ongeldig is. Laat alleen legitieme afzenders toe door het poststroombeleid, de verificatie van de afzender en de uitzonderingstabel te configureren (optioneel). Ga voor meer informatie naar Spoof Protection met Sender Verification.

Afbeelding 2. Sectie Verificatie afzender in standaard mailstroombeleid



Layer 2: Controleer de status van de header met DMARC

DMARC verificatie is een veel krachtiger functie om te vechten tegen Direct Domain Spoofing, en omvat ook Display Name en Brand Impersonation aanvallen. DMARC verbindt geverifieerde informatie met SPF of DKIM (het verzenden van domeinbron of handtekening) met wat aan de eindontvanger in van kopbal wordt voorgesteld en controleert dat SPF en de herkenningstekens DKIM aan VAN kopbalherkenningsteken worden gericht.

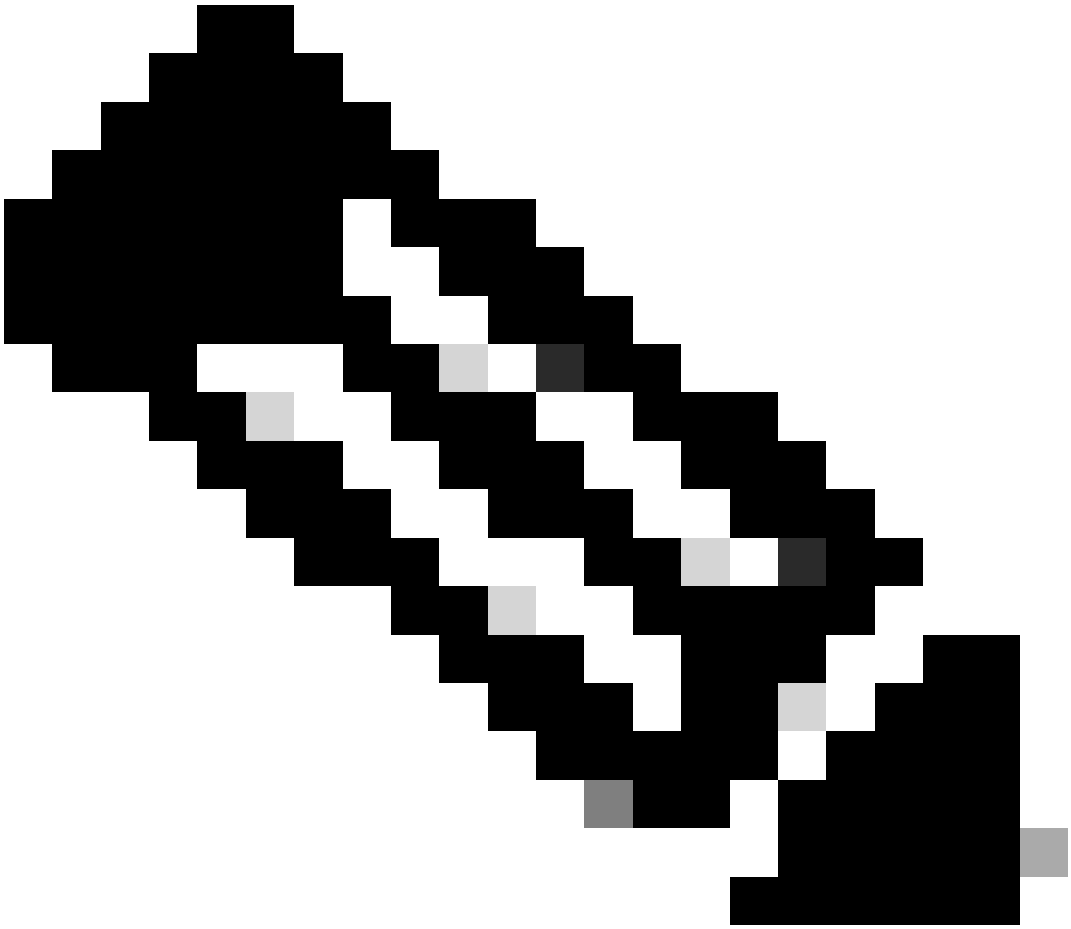
Om DMARC-verificatie te kunnen doorstaan, moet een inkomende e-mail minstens één van deze authenticatiemechanismen doorstaan. Daarnaast kan de beheerder via Cisco Secure Email ook een DMARC-verificatieprofiel definiëren om het DMARC-beleid van de domeineigenaar te negeren en geaggregeerde (RUA) en mislukking/forensische (RUF) rapporten naar de domeineigenaren te sturen. Dit helpt om hun authenticatie implementaties in ruil te versterken.

Best Practice: Bewerk het standaard DMARC profiel dat de DMARC beleidsacties gebruikt die de afzender adviseert. Bovendien moeten de globale instellingen van de DMARC-verificatie worden bewerkt om een correcte rapportage mogelijk te maken. Zodra het profiel op de juiste manier is geconfigureerd, moet de DMARC-verificatieservice zijn ingeschakeld in het standaardbeleid voor Mail Flow Policies.

Afbeelding 3. DMARC-verificatieprofiel

Create DMARC Verification Profile

Profile Name:	DEFAULT
Message Action when the Policy in DMARC Record is Reject:	○ No Action ○ Quarantine to: ACCOUNT_TAKEOVER (centralized) ◉ Reject SMTP Code: 550 SMTP Response: #5.7.1 DMARC unauthenticated mai
Message Action when the Policy in DMARC Record is Quarantine:	○ No Action ◉ Quarantine to: Policy (centralized)
Message Action for Temporary Failure:	◉ Accept ○ Reject SMTP Code: 451 SMTP Response: #4.7.1 Unable to perform DMARC v
Message Action for Permanent Failure:	○ Accept ◉ Reject SMTP Code: 550 SMTP Response: #5.7.1 DMARC verification failed.



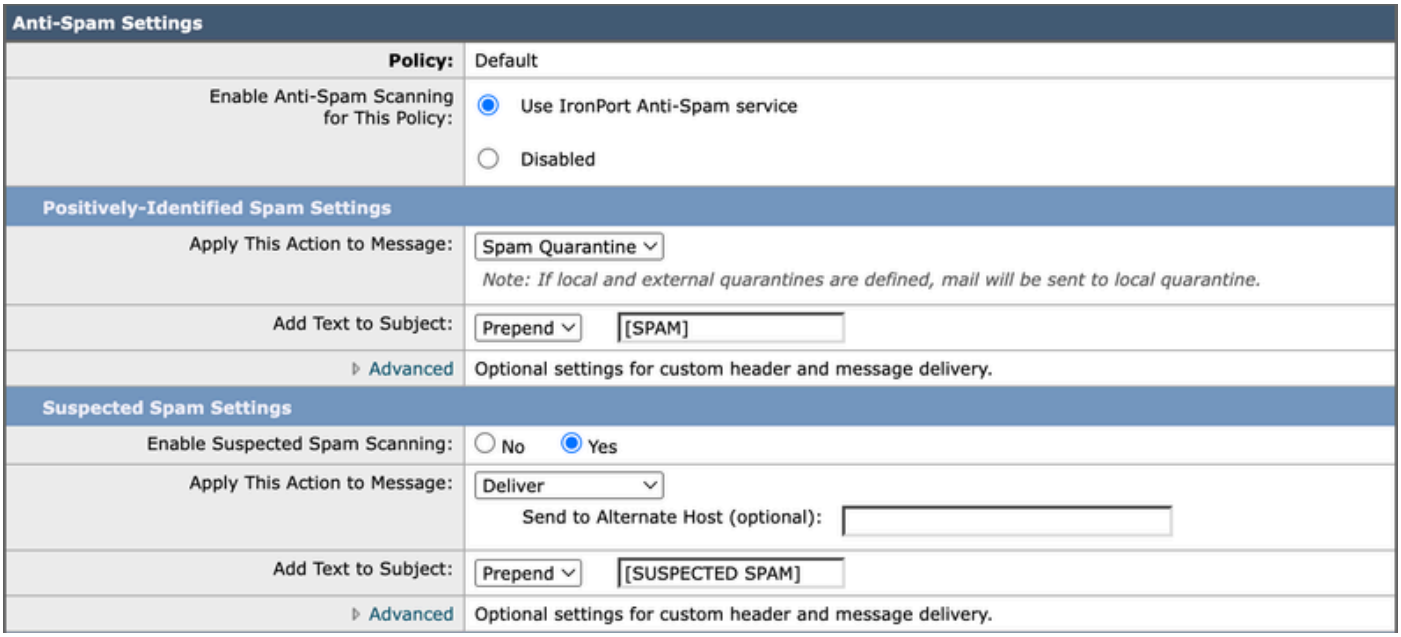
Opmerking: DMARC moet worden geïmplementeerd door de eigenaar van het domein te verzenden in combinatie met een domeinbewakingstool, zoals Cisco Domain Protection. Wanneer DMARC-handhaving in Cisco Secure Email op de juiste manier wordt geïmplementeerd, helpt het programma bescherming te bieden tegen phishing-e-mails die naar werknemers worden gestuurd door onbevoegde afzenders of domeinen. Ga voor meer informatie over Cisco Domain Protection naar deze link: Cisco Secure Email Domain Protection At-A-Glance.

Layer 3: Voorkomen dat spammers gespoofde e-mails verzenden

Spoofingaanvallen kunnen een andere veel voorkomende vorm van een spamcampagne zijn. Om frauduleuze e-mails met spam/phishing-elementen effectief te kunnen identificeren en blokkeren, is het daarom van essentieel belang antispambescherming in te stellen. Anti-spam, in combinatie met andere best practice-acties die grondig worden beschreven in dit document, biedt de beste resultaten zonder verlies van legitieme e-mails.

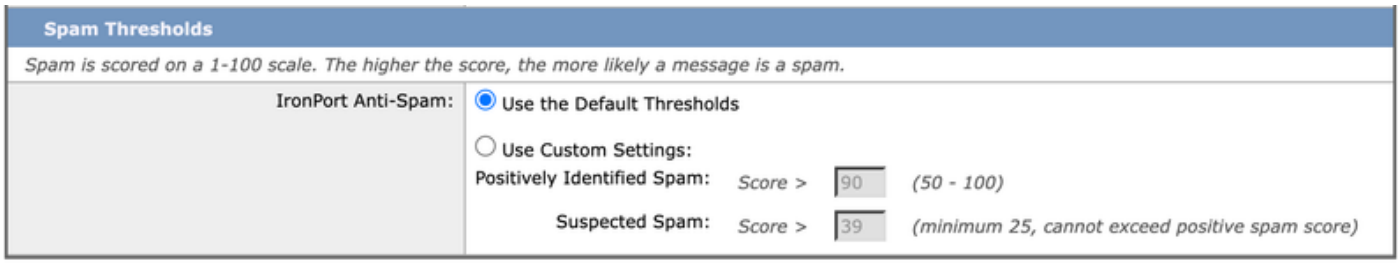
Best Practice: Schakel anti-spam scannen in het standaard mail beleid in en stel quarantaine actie in om spam instellingen positief te identificeren. Vergroot de minimale scangrootte voor spamberichten naar minimaal 2M wereldwijd.

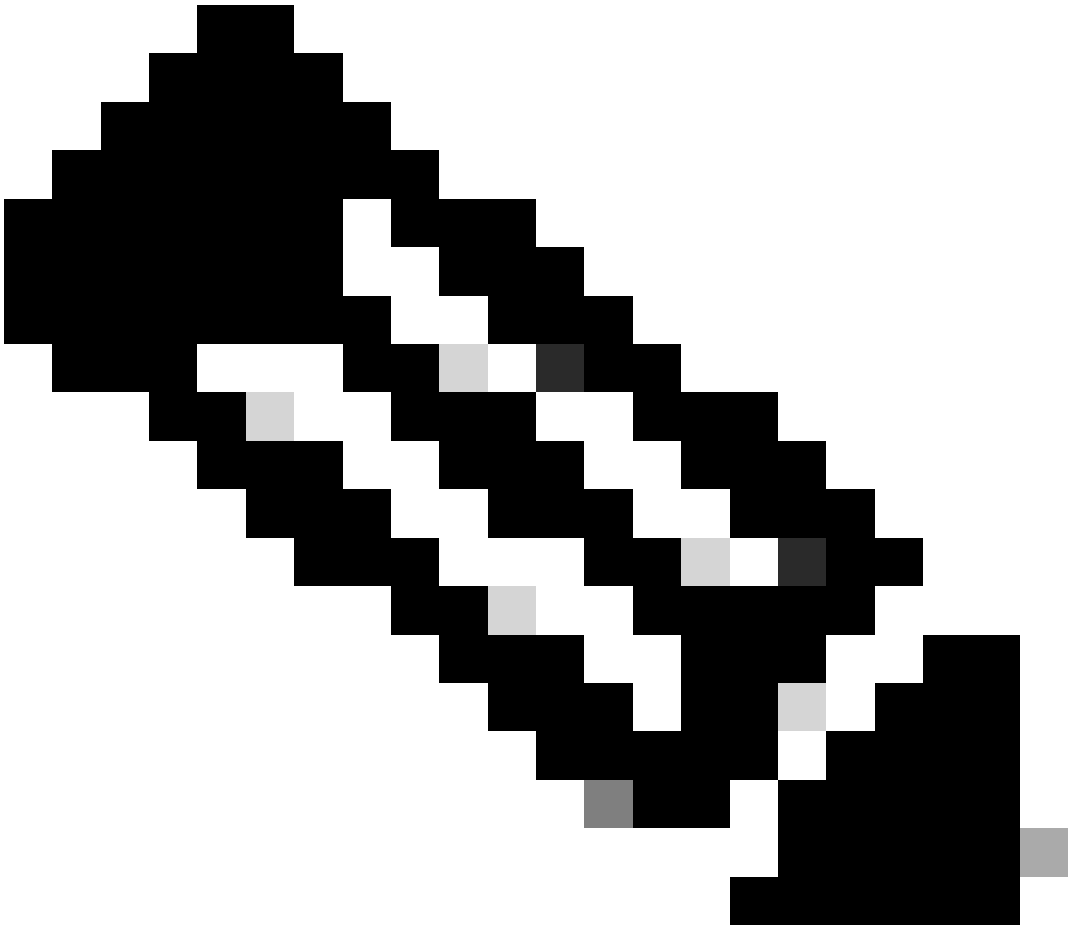
Afbeelding 4. Anti-Spam-instelling in standaard-mailbeleid



De drempelwaarde voor spam kan worden aangepast voor positieve en verdachte spam om de gevoeligheid (afbeelding 5) te verhogen of te verlagen; Cisco ontmoedigt de beheerder echter om dit te doen en de standaarddrempels alleen als basislijn te gebruiken, tenzij Cisco anders heeft verteld.

Afbeelding 5. Antispamdrempels in standaard mailbeleid instellen





Opmerking: Cisco Secure Email biedt een add-on Intelligent Multi-Scan (IMS)-engine die verschillende combinaties biedt van de anti-spamengine om de spampakketsnelheden te verhogen (meest agressieve vangstsnelheid).

Layer 4: Vaststellen van kwaadaardige afzenders via Email Domain

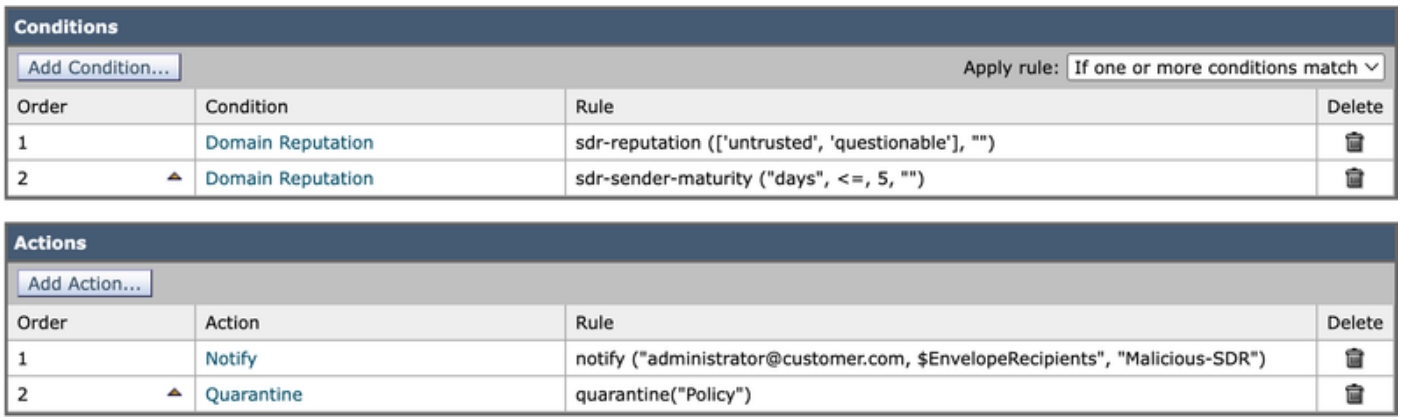
Cisco Talos Sender Domain Reputation (SDR) is een cloudservice die een reputatieoordeel geeft voor e-mailberichten op basis van de domeinen in de e-mailenvelop en header. De op het domein gebaseerde reputatieanalyse maakt een hogere spam catch rate mogelijk door verder te kijken dan de reputatie van gedeelde IP-adressen, hosting of infrastructuuraanbieders. In plaats

daarvan, leidt het vonnissen af die op eigenschappen worden gebaseerd die met volledig - gekwalificeerde domeinnamen (FQDNs) worden geassocieerd en andere afzenderinformatie in het Eenvoudige het gesprek en de berichtkopballen van het Protocol van de Overdracht van de Post (SMTP).

Afzender Looptijd is een essentieel kenmerk om de reputatie van de afzender vast te stellen. De Looptijd van de afzender wordt automatisch gegenereerd voor spamclassificatie op basis van meerdere informatiebronnen, en kan verschillen van de op Whois gebaseerde domeinleeftijd. De vervaltijd van de afzender is ingesteld op een limiet van 30 dagen, en boven deze limiet wordt een domein als volwassen beschouwd als een e-mailafzender, en worden geen verdere details verstrekt.

Best Practice: Maak een inkomende content filter die het verzendende domein vastlegt waarin de SDR reputatie verdict valt onder ofwel Onbetrouwbaar/twijfelachtig of de Afzender looptijd is minder dan of gelijk aan 5 dagen. De aanbevolen actie is om het bericht in quarantaine te plaatsen en de e-mail security beheerder en de oorspronkelijke ontvanger op de hoogte te stellen. Raadpleeg de Cisco-video op Cisco Email Security Update (versie 12.0) voor meer informatie over het configureren van SDR: Sender Domain Reputation (SDR)

Afbeelding 6. Content Filter voor SDR reputatie en Domeinleeftijd met Waarschuwingen en Quarantaine acties.

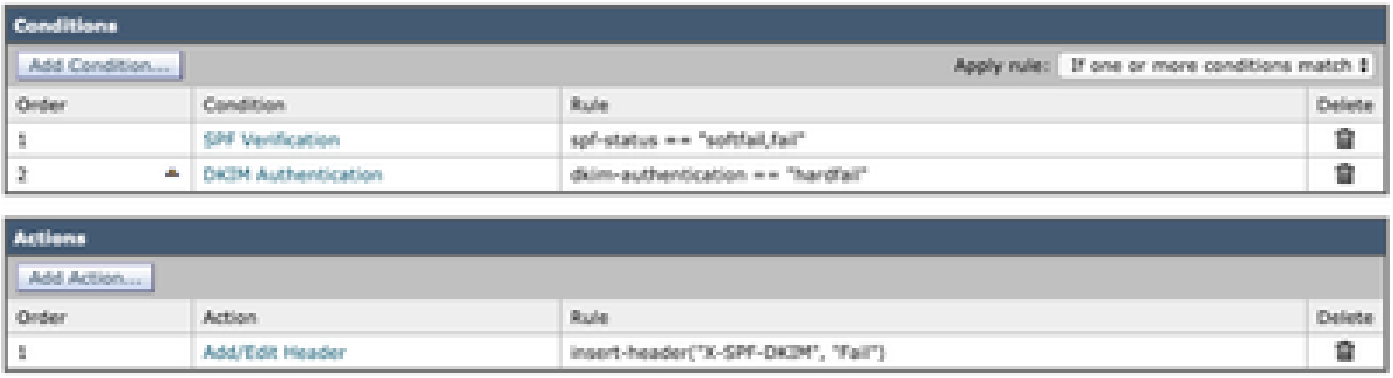


Layer 5: Verlaag het aantal valse positieve punten met SPF- of DKIM-verificatieresultaten

Het is noodzakelijk om SPF- of DKIM-verificatie (beide of een van beide) af te dwingen om meerdere lagen parodie-e-maildetectie te bouwen voor de meeste aanvalstypes. In plaats van een definitieve actie te ondernemen (zoals beëindigen of quarantaine), raadt Cisco aan een nieuwe header toe te voegen zoals [X-SPF-DKIM] op het bericht dat niet voldoet aan de SPF- of DKIM-verificatie en het resultaat samen te werken met de functie Vaste e-maildetectie (FED), die later wordt afgedekt, ten gunste van een verbeterd pakketpercentage van spoofing-e-mails.

Best Practice: Maak een inhoudsfilter dat SPF- of DKIM-verificatieresultaten inspecteert van elk inkomend bericht dat door eerdere inspecties is doorgegeven. Voeg een nieuwe X-header (bijvoorbeeld X-SPF-DKIM=Fail) toe op het bericht dat niet voldoet aan de SPF- of DKIM-verificatie en levert aan de volgende scanlaag - Forged Email Detection (FED).

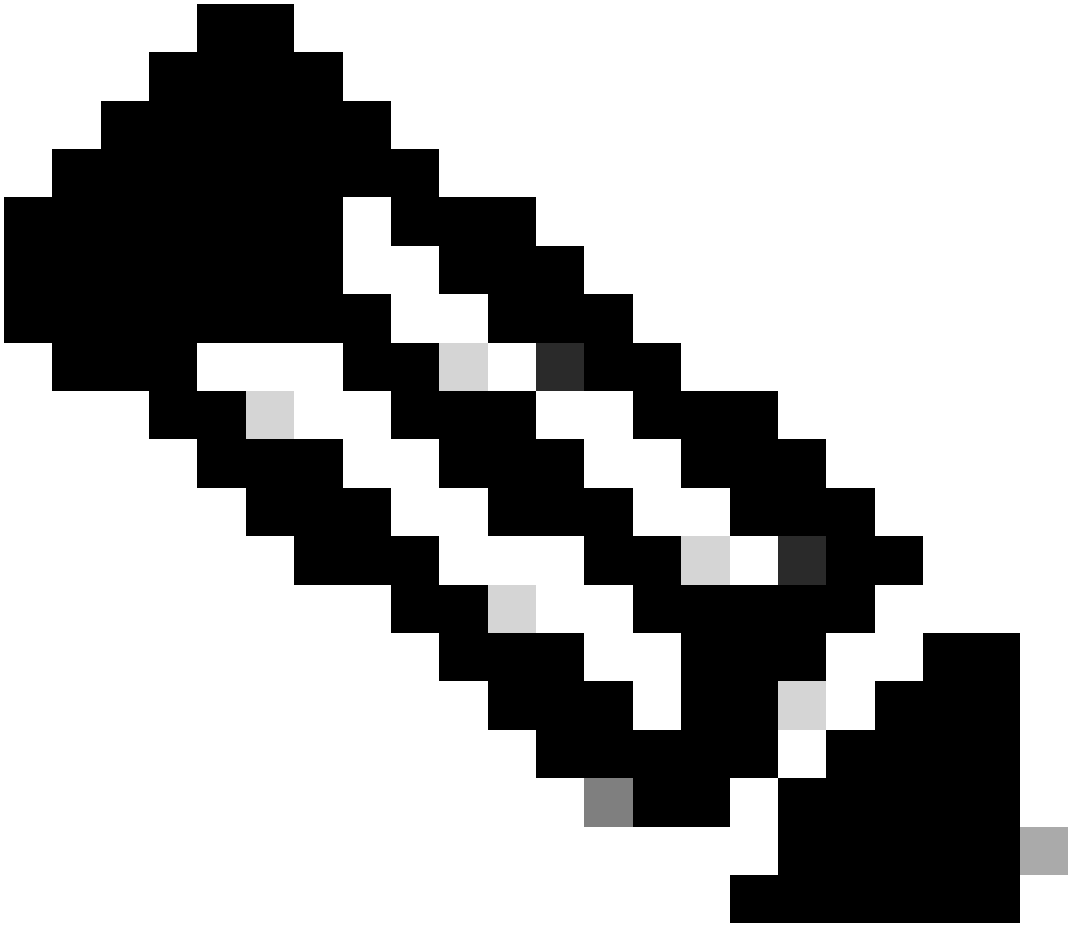
Afbeelding 7. Content Filter dat berichten met mislukte SPF- of DKIM-resultaten inspecteert



Layer 6: Detecteer berichten met mogelijk vervalste afzendernaam

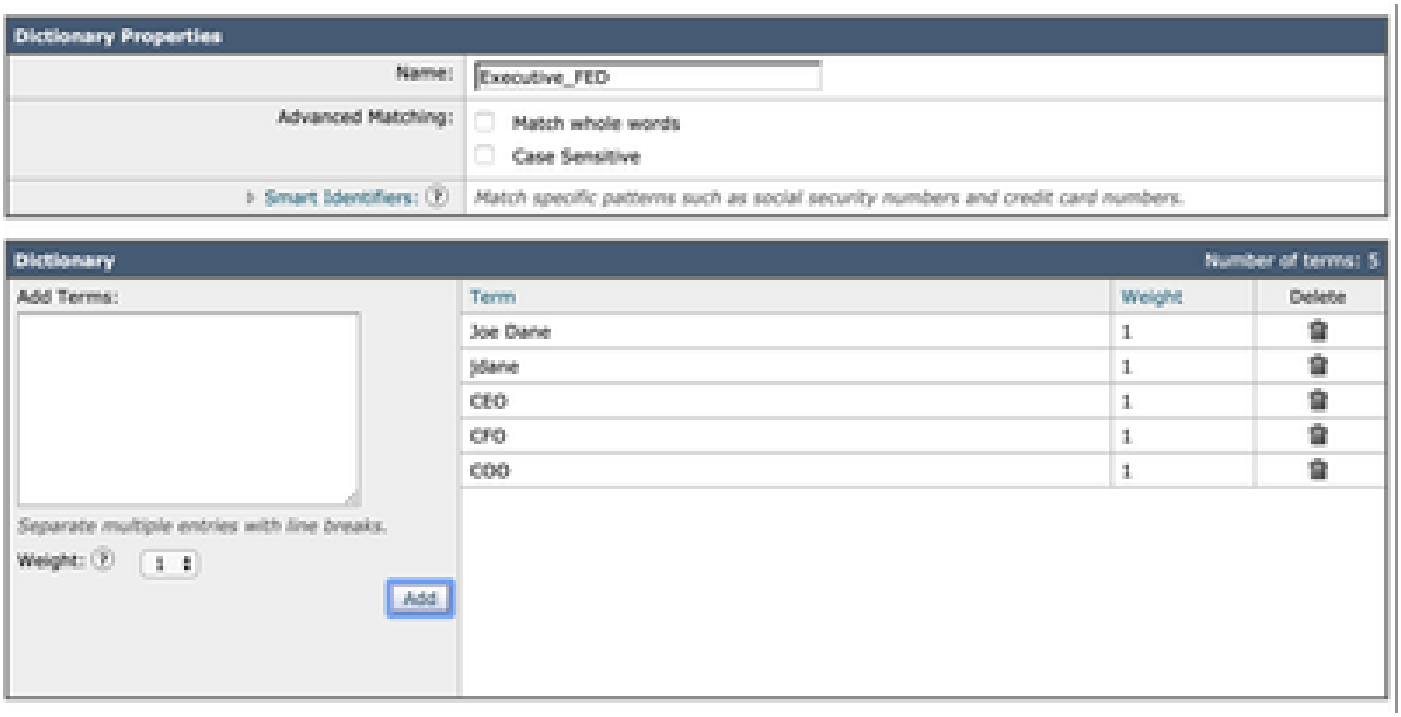
Het aanvullen van SPF-, DKIM- en DMARC-verificaties is de zoveelste cruciale verdedigingslinie tegen e-mailspoofing. De FED is ideaal om nepaanvallen tegen te gaan die de Van-waarde in het berichtlichaam misbruiken. Gezien het feit dat u de uitvoerende namen binnen de organisatie al kent, kunt u een woordenboek met deze namen maken en dat woordenboek vervolgens in inhoudsfilters met de FED-conditie verwijzen. Verder kunt u, naast de uitvoerende namen, een woordenboek van neef- of lookalike-domeinen maken op basis van uw domein door gebruik te maken van DNSTWIST (DNSTWIT) om te matchen tegen lookalike domeinspoofing.

Best Practice: Identificeer de gebruikers in uw organisatie van wie de berichten waarschijnlijk worden vervalst. Maak een aangepast woordenboek dat verantwoording aflegt voor managers. Voor elke uitvoerende naam moet het woordenboek de gebruikersnaam en alle mogelijke gebruikersnamen als termen bevatten (afbeelding 8). Wanneer het woordenboek is voltooid, gebruikt u de optie Vervalste e-maildetectie in het inhoudsfilter om de waarde Van van inkomende berichten af te stemmen op deze woordenboekvermeldingen.



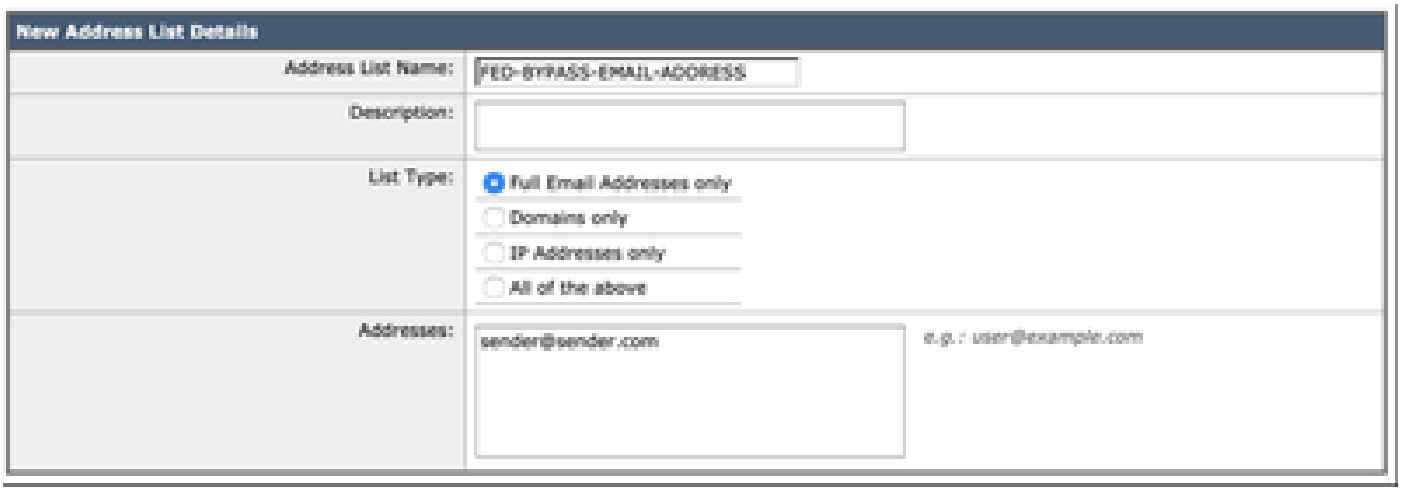
Opmerking: Aangezien de meeste domeinen niet zijn geregistreerd permutaties, DNS-sender verificatie beschermt tegen hen. Als u ervoor kiest om woordenboekvermeldingen te gebruiken, let dan alleen op de geregistreerde domeinen en zorg ervoor dat u niet meer dan 500-600 vermeldingen per woordenboek gebruikt.

Afbeelding 8. Aangepaste map voor vervalste e-maildetectie



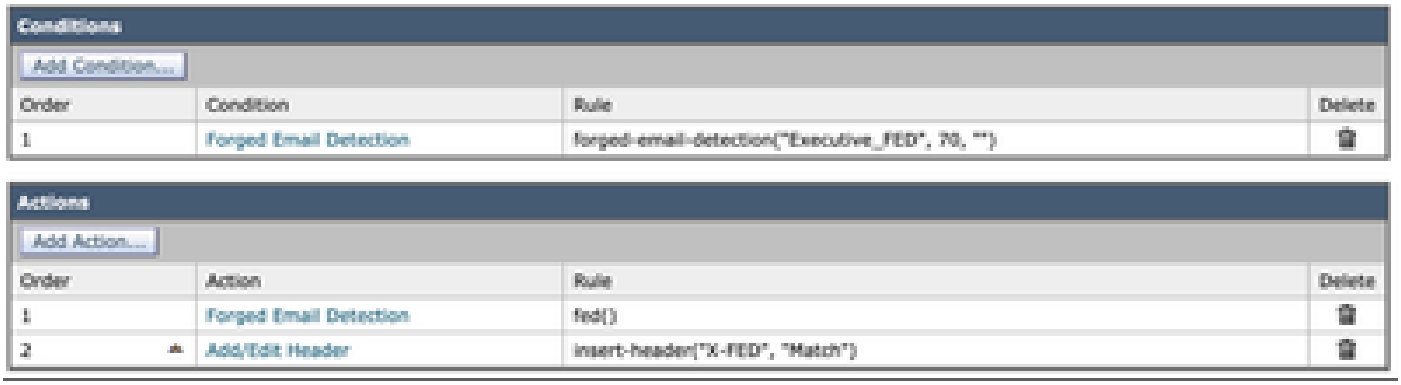
Het is optioneel om een uitzonderingsvoorwaarde toe te voegen voor uw e-maildomein in de Envelope Send om de FED-inspectie te omzeilen. Er kan ook een aangepaste adreslijst worden gemaakt om de FED-inspectie te omzeilen naar een lijst van e-mailadressen die in de Fromheader worden weergegeven (afbeelding 9).

Afbeelding 9. Een adreslijst maken om de FED-inspectie te omzeilen



Pas de merkgebonden actie van de Vervalste E-mail Detectie toe om van waarde te ontdoen van en het daadwerkelijke adres van de envelopafzender e-mail in bericht inbox te herzien. Voeg vervolgens, in plaats van een definitieve actie toe, een nieuwe X-header (bijvoorbeeld X-FED=Match) toe op het bericht dat overeenkomt met de voorwaarde en blijf het bericht leveren op de volgende inspectielaag (Afbeelding 10).

Afbeelding 10. Aanbevolen contentfilter-instelling voor FED

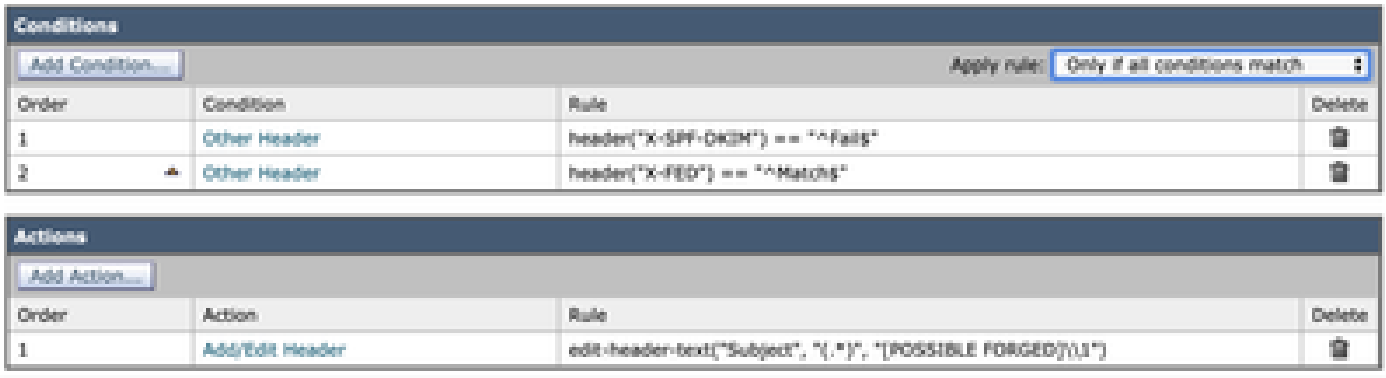


Layer 7: Positive Identified Spoofing Email

Het identificeren van een echte spoofingcampagne is effectiever door het verwijzen naar andere uitspraken van verschillende beveiligingsfuncties in de pijpleiding, zoals de X-header informatie geproduceerd door SPF/DKIM Enforcemen en FE. Beheerders kunnen bijvoorbeeld een inhoudsfilter aanmaken om berichten te identificeren die zijn toegevoegd met zowel nieuwe X-headers als gevolg van mislukte SPF/DKIM verificatieresultaten (X-SPF-DKIM=Fail) en die Van header overeenkomt met de FED woordenboekvermeldingen (X-FED=Match).

De aanbevolen actie kan zijn om het bericht in quarantaine te plaatsen en de ontvanger hiervan op de hoogte te stellen, of door te gaan met het leveren van het oorspronkelijke bericht, maar met het voorlezen van [MOGELIJKE VERVALSTE] woorden aan de onderwerpregel als een waarschuwing aan de ontvanger, zoals afgebeeld (afbeelding 11).

Afbeelding 11. Alle X-headers combineren tot een enkele (finale) regel

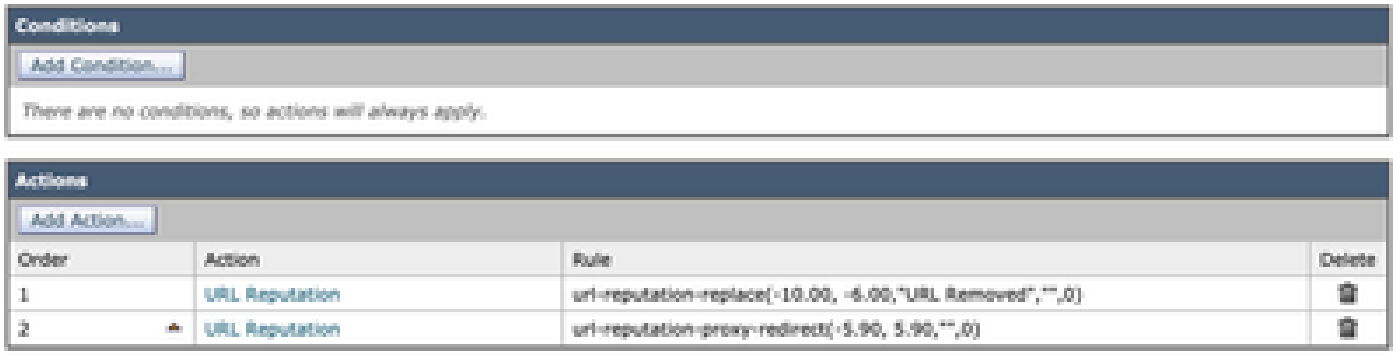


Layer 8: Bescherming tegen phishing-URL's

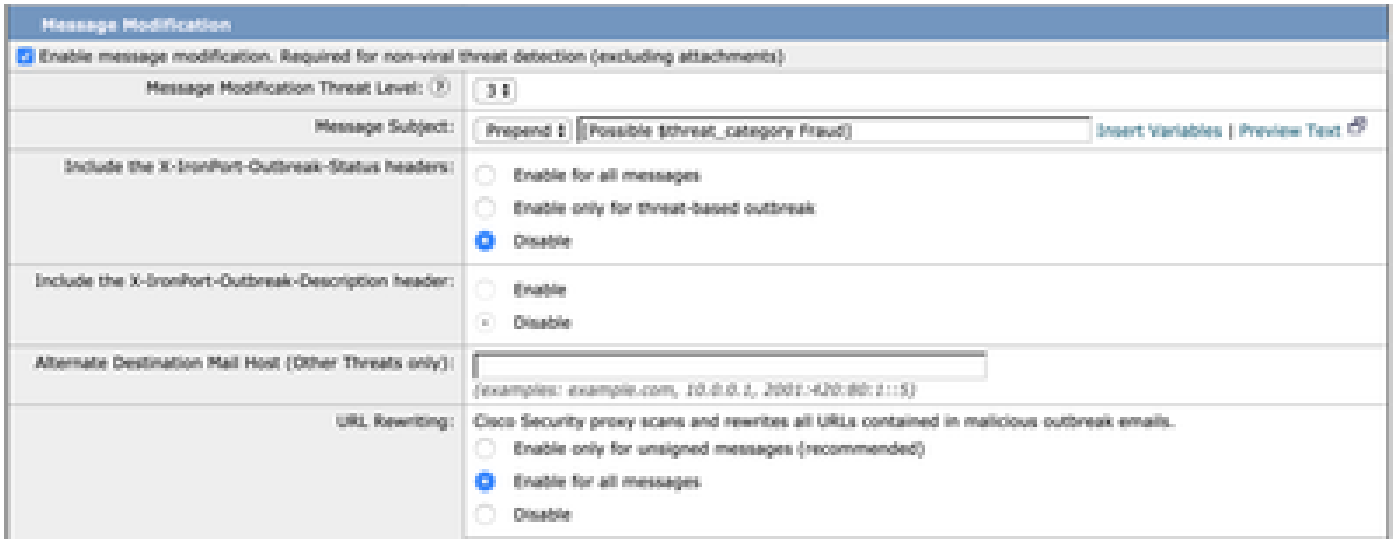
Bescherming tegen phishing-links is opgenomen in de URL en uitbraakfiltering in het beveiligde e-mailadres van Cisco. Blended bedreigingen combineren spoofing en phishing berichten om meer legitiem te kijken naar het doel. Het inschakelen van uitbraakfiltering is cruciaal om dergelijke bedreigingen in real-time te helpen detecteren, analyseren en stoppen. Het is de moeite waard om te weten dat URL reputatie wordt beoordeeld binnen de Anti-Spam-motor, en kan worden gebruikt als deel van de beslissing voor spamdetectie. Als de Anti-Spam motor niet het bericht met URL als Spam tegenhoudt, wordt het beoordeeld door URL en Uitbarstingsfiltering in het laatstgenoemde deel van de veiligheidspijpleiding.

Aanbeveling: maak een content filter regel die een URL blokkeert met een kwaadaardige reputatiescore en leidt de URL met een neutrale reputatiescore om naar Cisco Security Proxy (afbeelding 12). Schakel Threat Outbreak Filters in door Berichtwijziging in te schakelen. Met URL Rewrite kunnen verdachte URL's worden geanalyseerd door Cisco Security Proxy (afbeelding 13). Ga voor meer informatie naar: URL-filtering configureren voor beveiligde e-mailgateway en cloudgateway

Afbeelding 12. Content Filter voor URL-reputaties



Afbeelding 13. URL-herschrijven bij uitbraakfiltering inschakelen



Layer 9: Augment-detectiemogelijkheid met Cisco Secure Email Threat Defence (ETD)

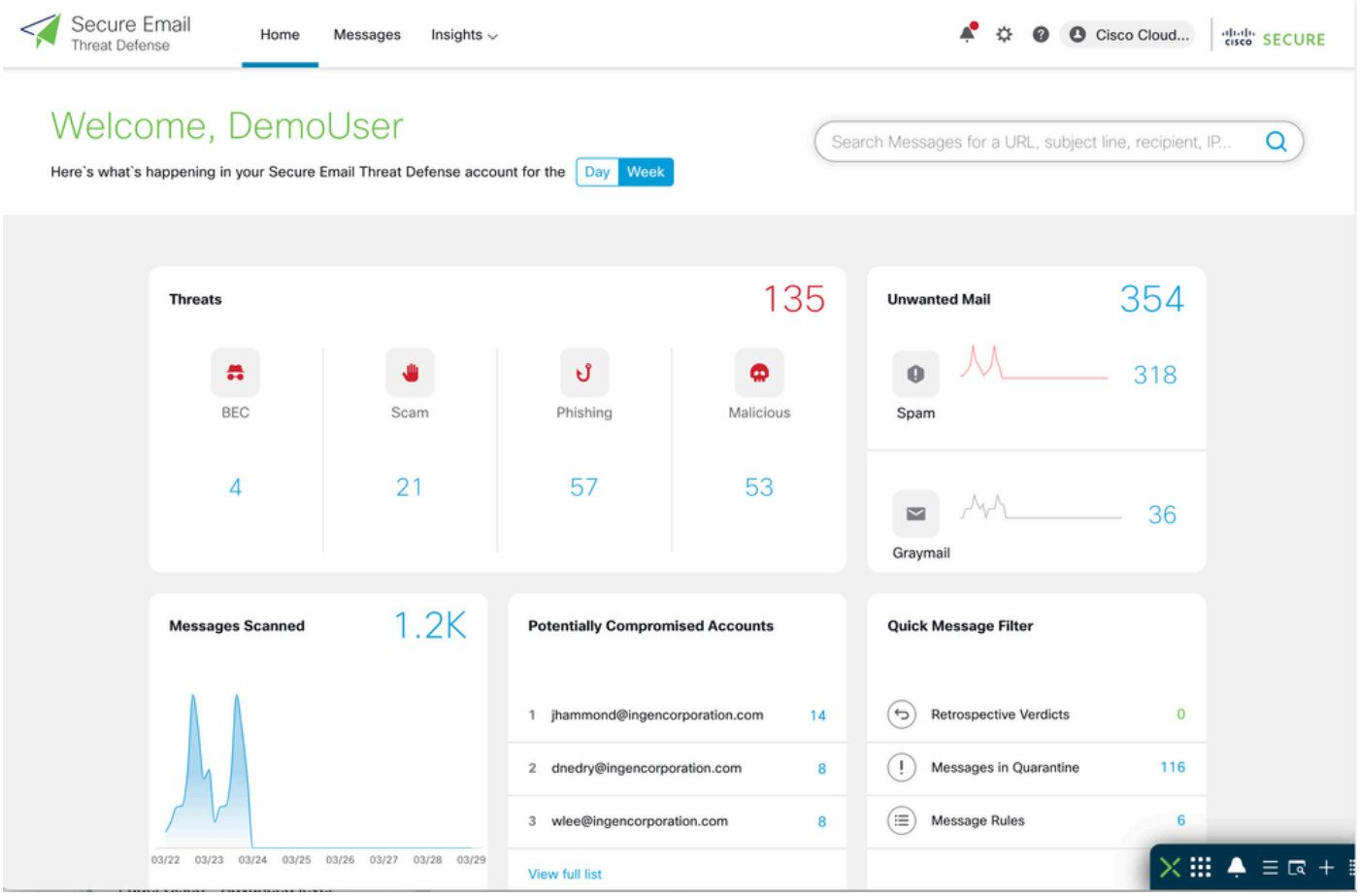
Cisco biedt E-mail Threat Defense, een cloud-native oplossing waarbij gebruik wordt gemaakt van superieure bedreigingsinformatie van Cisco Talos. Het heeft een API-enabled architectuur voor snellere reactietijden, volledige e-mailzichtbaarheid, inclusief interne e-mails, een gesprek weergave voor betere contextuele informatie, en tools voor automatische of handmatige herstel van bedreigingen die in Microsoft 365 mailboxen liggen. Bezoek het Cisco Secure Email Threat Defense-gegevensblad voor meer informatie.

Cisco Secure Email Threat Defense bestrijdt phishing met behulp van verificatie van afzenders en BEC-detectiemogelijkheden. Het integreert machine learning en Artificial Intelligence machines die lokale identiteit en relatie modellering combineren met real-time gedragsanalyse om te

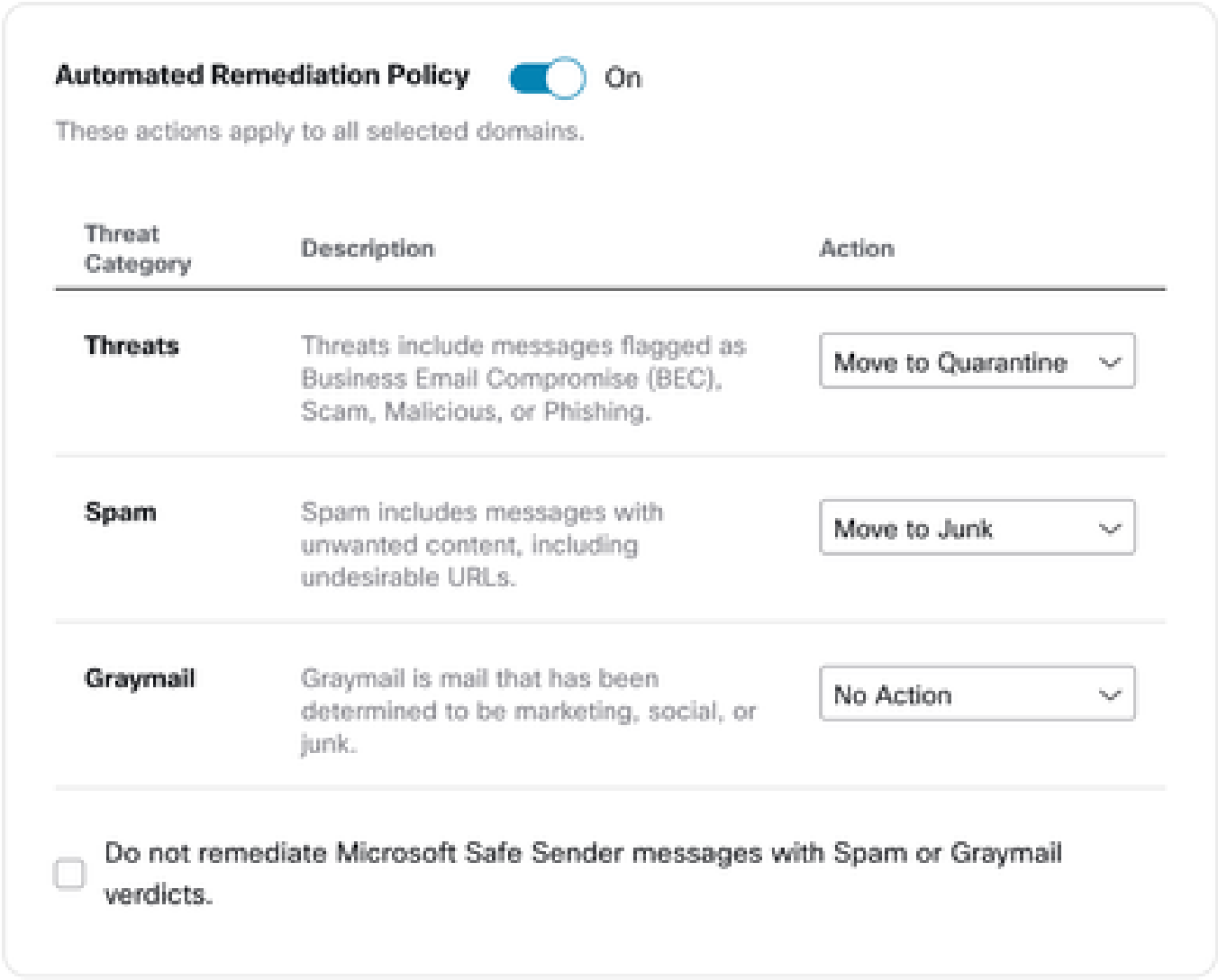
beschermen tegen op identiteitsbedrog gebaseerde bedreigingen. Het modelleert vertrouwd e-mailgedrag binnen organisaties en tussen individuen. E-mail Threat Defence biedt onder andere de volgende voordelen:

- Ontdek bekende, opkomende en gerichte bedreigingen met geavanceerde mogelijkheden voor bedreigingsdetectie.
- Identificeer kwaadaardige technieken en verkrijg context voor specifieke bedrijfsrisico's.
- Snel op zoek naar gevaarlijke bedreigingen en herstel ze in real-time.
- Gebruik doorzoekbare bedreigingstelemetrie om bedreigingen te categoriseren en te begrijpen welke delen van uw organisatie het meest kwetsbaar zijn voor aanvallen.

Afbeelding 14. Cisco Secure Email Threat Defense biedt informatie over de manier waarop uw organisatie wordt ondersteund.



Afbeelding 15. Met de instelling Cisco Email Threat Defense Policy wordt automatisch bepaald of het bericht overeenkomt met de geselecteerde bedreigingscategorie



Wat kunt u nog meer doen met het voorkomen van spoofing?

Vele spoofs kunnen worden verholpen met een paar eenvoudige voorzorgsmaatregelen die omvatten, maar niet beperkt tot deze:

- De grens staat vermelde domeinen in de Lijst van de Toegang van de Gastheer (HAT) aan zeer weinig kernpartners toe.
- Volg en update leden continu in de SPOOF_ENABLE afzendergroep als u er een hebt gemaakt en gebruik de instructies die worden gegeven in de best practices link.
- Schakel de grijsmaildetectie in en plaats ze ook in de spamquarantaine.

Maar het belangrijkste van alles, laat SPF, DKIM, en DMARC toe en voer hen geschikt uit. De richtlijnen voor het publiceren van SPF-, DKIM- en DMARC-records vallen echter buiten het bereik van dit document. Voor dat, verwijs naar dit Witboek: E-mail de Beste praktijken van de Verificatie: De Optimale Manieren om SPF, DKIM, en DMARC op te stellen.

Begrijp de uitdaging van het herstellen van e-mailaanvallen zoals de spoofing campagnes hier besproken. Als u vragen hebt over het implementeren van deze best practices, neemt u contact op met Cisco Technical Support en opent u een case. U kunt ook contact opnemen met uw Cisco-

accountteam voor een oplossing en ontwerpadvies. Raadpleeg de Cisco Secure Email website voor meer informatie over Cisco Secure Email.

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.