Proteção do spoof usando a verificação do remetente

Índice

Introdução

Àrevelia Cisco envia por correio eletrónico a ferramenta de segurança (ESA) não impede a entrega de entrada das mensagens que são endereçadas “” do mesmo domínio que vai ao mesmo domínio. Isto permite que as mensagens sejam “falsificado” pelas empresas exteriores que legitimam o negócio com o cliente. Algumas empresas confiam na organização de 3ª parte para enviar o email em nome da empresa tal como cuidados médicos, das agências de viagens, etc.

Proteção do spoof usando a verificação do remetente

Configurar a política do fluxo de correio (MFP)

1. Na GUI: **Envie a política do > Add das políticas > das políticas do fluxo de correio…**
2. Crie um MFP novo usando um nome que seja relevante como SPOOF_ALLOW
3. Na seção da *verificação do remetente*, mude a configuração da *tabela da exceção da verificação do remetente do uso do* **padrão do uso a FORA**.
4. **Em políticas do correio > em políticas do fluxo de correio > em parâmetros da política padrão, ajuste a configuração da *tabela da exceção da verificação do remetente do uso a* sobre.**

Configurar o CHAPÉU

1. Na GUI: **Envie o grupo do remetente do > Add das políticas > da vista geral do CHAPÉU…**
2. Ajuste o nome em conformidade ao MFP criado mais cedo, isto é SPOOF_ALLOW.
3. Ajuste a ordem assim que está acima grupos do remetente WHITELIST e de LISTA NEGRA.
4. Atribua a política **SPOOF_ALLOW às** configurações de grupo deste remetente.
5. O clique **submete e adiciona remetentes…**
6. Adicionar o IP ou os domínios para todos os partidos externos que você quiser permitir ao spoof o domínio interno.

Configurar a tabela da exceção

1. Na GUI: **Envie políticas > exceção da verificação do remetente do > Add da tabela da exceção…**
2. Adicionar o domínio local à tabela da exceção da verificação do remetente

3. Ajuste o *comportamento* **para rejeitar**

Verificar

Neste momento, o correio que vem de *your.domain a* your.domainwould seja rejeitado a menos que o remetente for alistado no grupo SPOOF_ALLOW do remetente, porque estaria associado a um MFP que não use a tabela da exceção da verificação do remetente.

Um exemplo deste seria considerado terminando uma sessão de Telnet manual ao ouvinte:

```
$ telnet example.com 25
Trying 192.168.0.189...
Connected to example.com.
Escape character is '^]'.
220 example.com ESMTP
helo example.com
250 example.com
mail from: <test@example.com>
553 Envelope sender <test@example.com> rejected
```

A resposta de 553 S TP é um resultado da resposta direta da tabela da exceção como configurada no ESA das etapas acima.

Dos logs do correio, você pode ver que o endereço IP de Um ou Mais Servidores Cisco ICM NT de 192.168.0.9 não está no endereço IP válido para o grupo correto do remetente:

```
Wed Aug 5 21:16:51 2015 Info: New SMTP ICID 2692 interface Management (192.168.0.189) address
192.168.0.9 reverse dns host my.host.com verified no
Wed Aug 5 21:16:51 2015 Info: ICID 2692 RELAY SG RELAY_SG match 192.168.0.0/24 SBRS not enabled
Wed Aug 5 21:17:02 2015 Info: ICID 2692 Address: <test@example.com> sender rejected, envelope
sender matched domain exception
```

Um endereço IP de Um ou Mais Servidores Cisco ICM NT permitido que combina com o exemplo de configuração das etapas acima seria considerado como segue:

```
Wed Aug 5 21:38:19 2015 Info: New SMTP ICID 2694 interface Management (192.168.0.189) address
192.168.0.15 reverse dns host unknown verified no
Wed Aug 5 21:38:19 2015 Info: ICID 2694 ACCEPT SG SPOOF_ALLOW match 192.168.0.15 SBRS not
enabled
Wed Aug 5 21:38:29 2015 Info: Start MID 3877 ICID 2694
Wed Aug 5 21:38:29 2015 Info: MID 3877 ICID 2694 From: <test@example.com>
Wed Aug 5 21:38:36 2015 Info: MID 3877 ICID 2694 RID 0 To: <robert@example.com>
Wed Aug 5 21:38:50 2015 Info: MID 3877 Subject 'This is an allowed IP and email'
Wed Aug 5 21:38:50 2015 Info: MID 3877 ready 170 bytes from <test@example.com>
Wed Aug 5 21:38:50 2015 Info: MID 3877 matched all recipients for per-recipient policy DEFAULT
in the inbound table
Wed Aug 5 21:38:51 2015 Info: MID 3877 interim verdict using engine: CASE spam negative
Wed Aug 5 21:38:51 2015 Info: MID 3877 using engine: CASE spam negative
Wed Aug 5 21:38:51 2015 Info: MID 3877 interim AV verdict using Sophos CLEAN
Wed Aug 5 21:38:51 2015 Info: MID 3877 antivirus negative
Wed Aug 5 21:38:51 2015 Info: MID 3877 AMP file reputation verdict : CLEAN
Wed Aug 5 21:38:51 2015 Info: MID 3877 Outbreak Filters: verdict negative
Wed Aug 5 21:38:51 2015 Info: MID 3877 queued for delivery
Wed Aug 5 21:38:51 2015 Info: New SMTP DCID 354 interface 192.168.0.189 address 192.168.0.15
port 25
```

```
Wed Aug 5 21:38:51 2015 Info: Delivery start DCID 354 MID 3877 to RID [0]
Wed Aug 5 21:38:51 2015 Info: Message done DCID 354 MID 3877 to RID [0] [('X-IPAS-Result',
'A0GJMwA8usJV/w8AqMBbGQSEFRqFGKUygmUBkV2GMAKBcQEBAgEBAQOBB4QbKIEIhxuCQbxmoDcRAYNPAYE0AQSqSZB5gXA
BAQgCAYQjgT8DAgE'), ('X-IronPort-AV', 'E=Sophos;i="5.15,620,1432612800"; \r\n
d="scan\'";a="3877"')]
Wed Aug 5 21:38:51 2015 Info: MID 3877 RID [0] Response '2.0.0 Ok: queued as 1D74E1002A8'
Wed Aug 5 21:38:51 2015 Info: Message finished MID 3877 done
Wed Aug 5 21:38:56 2015 Info: DCID 354 close
```

Informações Relacionadas

- Grep ESA, S A, e WSA com o Regex para procurar logs
- Determinação da disposição da mensagem ESA
- Suporte Técnico e Documentação - Cisco Systems