

Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1241

(04/2008)

SERIE X: REDES DE DATOS, COMUNICACIONES DE
SISTEMAS ABIERTOS Y SEGURIDAD

Seguridad en el ciberespacio – Lucha contra el correo
basura

Marco técnico contra el correo basura

Recomendación UIT-T X.1241



RECOMENDACIONES UIT-T DE LA SERIE X
REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1241

Marco técnico contra el correo basura

Resumen

La Recomendación UIT-T X.1241 contiene el marco técnico contra el correo basura. Se describe una estructura recomendada de un dominio de procesamiento anticorreo basura y se definen las funciones de los principales módulos que lo integran. El principal objetivo del marco es establecer un mecanismo de intercambio de información sobre correo basura entre diversos servidores de correo electrónico. Los sistemas que se ajustan a este marco mejorarán la eficacia mediante la interconexión.

Orígenes

La Recomendación UIT-T X.1241 fue aprobada el 18 de abril de 2008 por la Comisión de Estudio 17 (2005-2008) del UIT-T por el procedimiento de la Resolución 1 de la AMNT.

Palabras clave

Anticorreo basura, correo electrónico, interconexión, correo basura, marco técnico.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT [ha recibido/no ha recibido] notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección <http://www.itu.int/ITU-T/ipr/>.

© UIT 2009

Reservados todos los derechos. Ninguna parte de esta publicación puede reproducirse por ningún procedimiento sin previa autorización escrita por parte de la UIT.

ÍNDICE

	Página
1 Alcance	1
2 Referencias	1
3 Definiciones.....	1
3.1 Términos definidos en otros documentos.....	1
3.2 Términos definidos en esta Recomendación	1
4 Abreviaturas y acrónimos	2
5 Convenios	2
6 Estructura general del sistema de procesamiento anticorreo basura	2
6.1 Estructura general.....	2
6.2 Modelo de referencia.....	4
7 Funciones del dominio de procesamiento anticorreo basura.....	5
7.1 Funciones del cliente de correo electrónico	5
7.2 Funciones del servidor de correo electrónico.....	5
7.3 Funciones de la entidad de procesamiento anticorreo basura	6
7.4 Funciones de la subentidad de procesamiento anticorreo basura.....	6
8 Identificación del correo basura.....	7
8.1 Características corrientes del correo basura	7
8.2 Reglas comunes para luchar contra el correo basura.....	8
9 Métodos de lucha contra el correo basura	9
9.1 Desactivación de la función "retransmisión abierta".....	9
9.2 Control de la autorización de entrega de correo-e.....	9
9.3 Técnicas de filtrado	9
9.4 Examen del rastreo	10
10 Interconexión entre dominios de procesamiento anticorreo basura	11
10.1 Interconexión entre entidades de procesamiento de nivel superior.....	11
10.2 Interconexión entre una entidad de procesamiento y una subentidad	11
10.3 Interconexión entre una subentidad de procesamiento y un servidor de correo electrónico	12
Bibliografía	13

Introducción

El desarrollo de las redes de telecomunicaciones basadas en el protocolo Internet (IP) ha llevado a que los usuarios intercambien un gran número de mensajes de correo electrónico. Al mismo tiempo, hay cada vez más mensajes de correo basura que se envían a los usuarios a través de dichas redes, lo que causa serios problemas.

El correo electrónico basura se ha convertido en una plaga que degrada la capacidad del servicio en las redes de telecomunicaciones IP. Los proveedores de servicio deben invertir grandes cantidades de dinero para contrarrestar los problemas causados por el correo basura, y los usuarios invierten mucho tiempo en eliminar estos mensajes.

Existen varias técnicas de detección, que detectan y eliminan los correos electrónicos basura. Sin embargo, los remitentes de tales correos son muy creativos a la hora de evitar la detección. Por ejemplo, pueden falsificar correos electrónicos normales y aleatorizar el contenido para evitar que los detecten los filtros de correo basura. Por consiguiente, es urgente establecer un marco técnico eficaz que solucione el problema del correo electrónico basura en su integridad.

Las soluciones contra el correo basura utilizan técnicas diferentes para contrarrestarlo. Estas tecnologías están en constante evolución, por lo que resulta muy difícil encontrar una descripción inmutable que abarque todos los detalles de las tecnologías anticorreo basura a largo plazo.

Así pues, es necesario establecer un marco abierto donde quepan las distintas soluciones. El marco debe ser compatible con todas las tecnologías anticorreo basura y no limitarse a un aspecto técnico concreto. A continuación se enumeran los requisitos del marco:

- Podrá estimar sistemáticamente si un correo electrónico es basura o no.
- Permitirá a distintos sistemas de servicio de correo electrónico compartir información contra el correo basura.
- Mejorará la veracidad de las herramientas anticorreo basura de los sistemas de servicio de correo electrónico.
- Garantizará que las entidades de distintos dominios administrativos intercambien información contra el correo basura.

Recomendación UIT-T X.1241

Marco técnico contra el correo basura

1 Alcance

Esta Recomendación contiene el marco técnico contra el correo basura. Se describe una estructura recomendada de un dominio de procesamiento anticorreo basura y se definen las funciones de los principales módulos que lo integran. El objetivo primero del marco es establecer un mecanismo de intercambio de información sobre correo basura entre diversos servidores de correo electrónico. Los sistemas que se ajustan a este marco, mejorarán la eficacia en toda la interconexión.

2 Referencias

Ninguna.

3 Definiciones

3.1 Términos definidos en otros documentos

En esta Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 campos encabezamiento [IETF RFC 2822]: Los campos encabezamiento tienen la misma estructura sintáctica general: un nombre de campo, seguido de una coma, seguido del cuerpo del campo.

3.1.2 objetos de correo [b-IETF RFC 2821]: El SMTP transporta un objeto de correo. El objeto de correo consta del sobre y su contenido.

3.2 Términos definidos en esta Recomendación

En esta Recomendación se definen los siguientes términos:

3.2.1 dominio de procesamiento anticorreo basura: Es un sistema independiente que contiene una entidad de procesamiento anticorreo basura, subentidades de procesamiento anticorreo basura, servidores de correo electrónico y clientes de correo electrónico.

3.2.2 entidad de procesamiento anticorreo basura: Una entidad de procesamiento anticorreo basura es el núcleo del dominio de procesamiento anticorreo basura. Recopila de las entidades de nivel inferior información sobre el correo basura con la que construye un sistema de reglas uniforme e integrado. Por último, el sistema de reglas debe presentarse a todas las entidades de nivel inferior.

3.2.3 subentidad de procesamiento anticorreo basura: La subentidad de procesamiento anticorreo basura está conectada a uno o más proveedores de servicio de correo electrónico. Recibe información de correo basura de los servidores de correo electrónico o de los equipos anticorreo basura y la remite a las entidades de nivel superior tras analizarla periódicamente. Recibe también periódicamente reglas actualizadas de las entidades de nivel superior y las distribuye a estas subentidades.

3.2.4 regla compuesta: Una regla compuesta está formada por dos o más reglas simples.

3.2.5 correo-e: Este término se utiliza principalmente para designar al correo electrónico transmitido por una red de telecomunicaciones.

3.2.6 correo-e basura: Este término se utiliza para describir las comunicaciones electrónicas no solicitadas enviadas por correo electrónico, que generalmente se envía con fines específicos.

3.2.7 regla: Una regla es un conjunto de condiciones y acciones básicas. Puede comprender diversos elementos, como comportamientos, filtros, etc.

3.2.8 correo-e muestra: Este término se emplea para designar el correo-e recibido de los servidores de correo electrónico ajustándose a determinadas reglas.

3.2.9 remitente de correo basura (*spammer*): Término que designa a la entidad o persona que crea y envía mensajes de correo-e basura.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas y acrónimos:

DNS	Sistema de nombres de dominio (<i>domain name system</i>)
Correo-e	Correo electrónico
ESMTP	Protocolo de transferencia de correo simple ampliado (<i>extended simple mail transfer protocol</i>)
FTP	Protocolo de transferencia de ficheros (<i>file transfer protocol</i>)
HTTP	Protocolo de transferencia de hipertexto (<i>hypertext transfer protocol</i>)
IMAP4	Protocolo de acceso de mensajes Internet, versión 4 (<i>Internet message access protocol version 4</i>)
IP	Protocolo Internet (<i>Internet protocol</i>)
POP3	Protocolo de oficina postal, versión 3 (<i>post office protocol version 3</i>)
RBL	Lista negra en tiempo real (<i>real-time blacklist</i>)
SASL	Autenticación simple y capa de seguridad (<i>simple authentication and security layer</i>)
SMTP	Protocolo de transferencia de correo simple (<i>simple mail transfer protocol</i>)
URL	Localizador uniforme de recursos (<i>uniform resource locator</i>)

5 Convenios

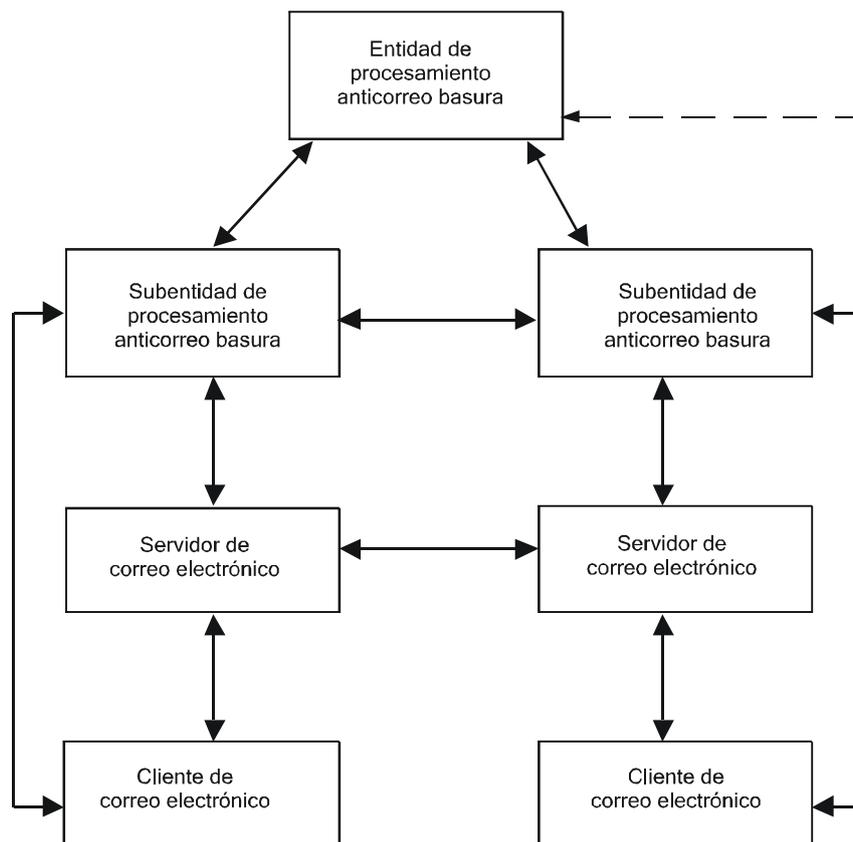
Ninguno.

6 Estructura general del sistema de procesamiento anticorreo basura

6.1 Estructura general

En la presente Recomendación se describen los componentes del marco, que comprende una entidad de procesamiento anticorreo basura, subentidades de procesamiento de correo basura y servidores y clientes de correo electrónico.

Estos componentes pueden comunicarse entre sí gracias a protocolos de mensajería bien conocidos. En esta cláusula se describen las características de estos componentes.



NOTA – La línea continua representa el trayecto de la información intercambiada entre los componentes del dominio de procesamiento anticorreo basura.

Figura 1 – Estructura general

En la figura 1, la entidad de procesamiento anticorreo basura recibe informes de las subentidades de procesamiento anticorreo basura y les comunica nuevas reglas.

Las subentidades de procesamiento anticorreo basura deben verificar la validez de las reglas que les transmite la entidad de procesamiento anticorreo basura y ajustarlas.

El cliente de correo electrónico es la entidad con la que los usuarios tratan directamente. El servidor de correo electrónico se encarga de la transmisión de los correos electrónicos por la red de telecomunicaciones IP.

El cliente de correo electrónico envía quejas a la subentidad de procesamiento anticorreo electrónico. En casos concretos, el cliente de correo electrónico puede quejarse directamente a la entidad de procesamiento anticorreo electrónico de nivel superior.

6.2 Modelo de referencia

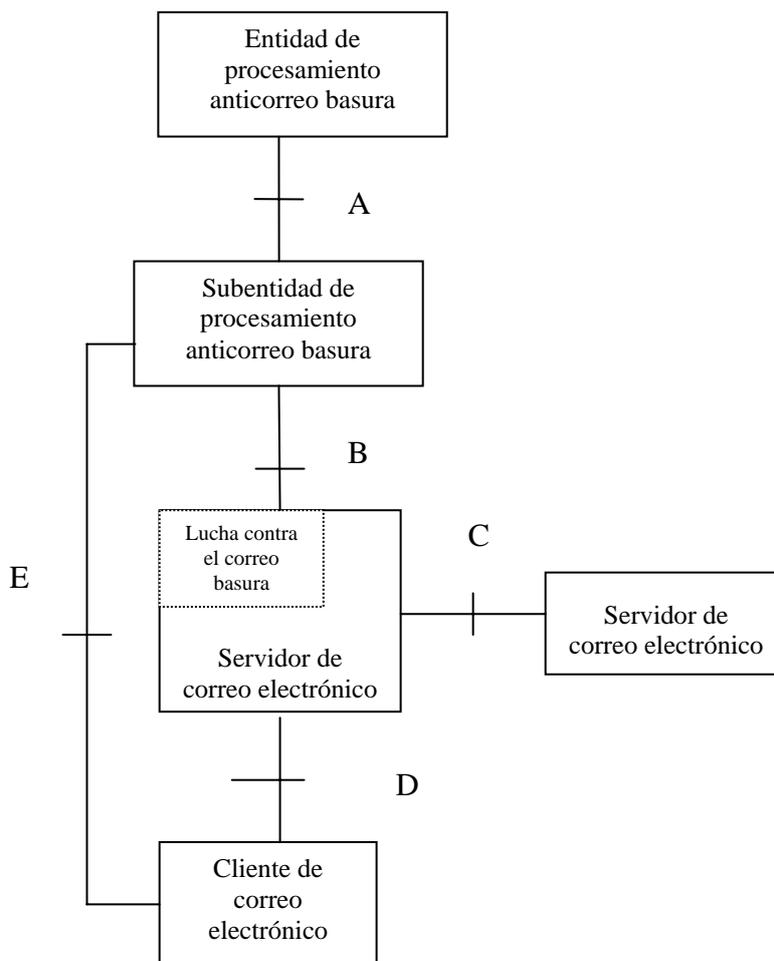


Figura 2 – Modelo de referencia

La interfaz A se sitúa entre la entidad de procesamiento anticorreo basura y la subentidad. Los informes de quejas y las reglas contra el correo basura se transmiten a través de la interfaz A. Las reglas pueden ser compuestas, como "IP de origen + URL". La interfaz A debe soportar los protocolos FTP y HTTP.

La interfaz B se sitúa entre la subentidad de procesamiento anticorreo basura y el servidor de correo electrónico. Se utiliza para transmitir los informes de quejas y las reglas. Del mismo modo, las reglas pueden ser compuestas, como "IP de origen + URL". La interfaz B debe soportar los protocolos FTP y HTTP. En casos concretos, el servidor de correo electrónico puede comunicarse directamente con la entidad de procesamiento anticorreo basura de nivel superior.

La interfaz C se sitúa entre los servidores de correo electrónico a través de los cuales los mensajes se transmiten utilizando el protocolo SMTP.

La interfaz D se sitúa entre el servidor de correo electrónico y el cliente de correo electrónico. Pueden utilizarse diversos protocolos para la transmisión de correos electrónicos, como POP3, IMAP4.

La interfaz E se sitúa entre el cliente de correo electrónico y la subentidad de procesamiento anticorreo basura. El cliente de correo electrónico puede enviar quejas a la subentidad de procesamiento de correo basura. En casos concretos, el cliente de correo electrónico puede enviar las quejas directamente a la entidad de procesamiento anticorreo basura de nivel superior. En esta interfaz pueden utilizarse software web en línea, telefónico, de correo-e y del cliente.

7 Funciones del dominio de procesamiento anticorreo basura

7.1 Funciones del cliente de correo electrónico

Las funciones del cliente de correo electrónico comprenden:

- Además de realizar las funciones generales de transmisión de correo-e, el cliente de correo electrónico posee un mecanismo que ayuda a los usuarios a enviar quejas de correo basura a la entidad de procesamiento anticorreo basura. Los destinatarios de los correos-e sólo han de determinar si un correo-e es correo basura de acuerdo con su contenido, título o direcciones. Por ejemplo, si los destinatarios no desean recibir publicidad, publicaciones electrónicas o propaganda, pueden enviar una queja relativa a tales correos-e a la entidad de procesamiento anticorreo basura utilizando el mecanismo del cliente de correo electrónico.
- El cliente de correo electrónico puede descargar las reglas de filtrado anticorreo basura automáticamente de la entidad de procesamiento anticorreo basura. Las reglas de filtrado se establecen en función de las quejas enviadas por los clientes de correo electrónico. Estas reglas pueden referirse al tamaño límite de un único correo-e, al número de correos-e que se envían durante un periodo dado de tiempo, palabras clave en el cuerpo principal de los correos-e, etc. Las reglas de filtrado se actualizan periódicamente en función de los informes de quejas. Están indexadas por nombre de usuario del buzón, dirección IP de salida y nombre de dominio.
- El cliente de correo electrónico puede reenviar el correo basura a la entidad de procesamiento anticorreo basura a fin de que se realice un análisis más detallado o se eliminen algunas reglas de filtrado al obtenerse falsos positivos. La entidad de procesamiento anticorreo electrónico puede actualizar las reglas de filtrado inmediatamente, de acuerdo con los requisitos o las quejas que le presente el cliente de correo electrónico.
- El cliente de correo electrónico puede filtrar directamente el correo basura. Normalmente, los destinatarios pueden conocer los resultados del filtrado a fin de evitar falsos positivos.

7.2 Funciones del servidor de correo electrónico

Las funciones del servidor de correo electrónico comprenden:

- Además de realizar las funciones generales de transmisión de correo-e, el servidor de correo electrónico ejecuta normalmente el intercambio de correo-e con otros servidores de correo electrónico, o el envío y recepción de correo-e entre clientes de correo electrónico. Al mismo tiempo, el servidor de correo-e debe prohibir la función retransmisión abierta para evitar que los remitentes de correo basura le obliguen a transmitir correo basura a otro servidor de correo electrónico.
- Todos los usuarios han de superar la verificación antes de poder enviar correos-e a través del servidor de correo electrónico. Cada sistema de correo-e puede utilizar distintos mecanismos de verificación. La verificación se realiza entre el servidor de correo electrónico y el cliente de correo electrónico.
- Todos los proveedores de servicio de correo electrónico deberían tener una lista negra de remitentes de correo basura, donde se consigne información (por ejemplo, nombre de anfitrión, nombre de dominio o dirección de correo-e) sobre los remitentes, para poder rechazar la recepción de correos-e procedentes de ellos.
- El servidor de correo electrónico puede devolver una instrucción verificar al origen, indicándola en la información del emisor del correo-e (como DNS, nombre de anfitrión, etc.). Si la instrucción verificar no confirma la autenticidad del origen, el servidor de correo electrónico rechazará el correo-e.

- Los remitentes de correo basura pueden utilizar algunas instrucciones del SMTP para adivinar la cuenta real del servidor de correo electrónico. El servidor de correo electrónico debe prohibir instrucciones como EXPN y VRFY.
- Algunos correos-e publicitarios o propagandísticos se envían sin información sobre el remitente. El servidor de correo electrónico debe añadir automáticamente un enlace HTTP al cuerpo del correo-e. Los usuarios pueden presentar las quejas que correspondan.
- El servidor de correo electrónico detecta el correo basura gracias a la tecnología anticorreo basura y remite informes al respecto a la subentidad de procesamiento anticorreo basura, desde la cual descarga las reglas de filtrado.
- Cuando se detecta un correo basura, el servidor de correo electrónico debe hacer una copia del correo basura original que incluya, por lo menos, el encabezamiento de origen y someterlo al filtrado.
- El servidor de correo electrónico ha de facilitar la información estadística y el registro cronológico de sistema del servidor de correo electrónico, del que se hacen periódicamente copias de seguridad, a la subentidad de procesamiento anticorreo basura.
- El servidor de correo electrónico devuelve diversos números de estado en función de cada regla.
- El servidor de correo electrónico puede limitar el volumen de tráfico que puede enviar un determinado usuario de correo-e.

7.3 Funciones de la entidad de procesamiento anticorreo basura

Las funciones de la entidad de procesamiento anticorreo basura comprenden:

- El intercambio de reglas de filtrado con otras entidades de procesamiento anticorreo basura. Pueden utilizarse varios protocolos, como FTP y HTTP, para transmitir la información.
- El almacenamiento de información original sobre correos basura de los usuarios y las subentidades de procesamiento anticorreo basura.
- La transmisión de reglas de filtrado a las subentidades de procesamiento anticorreo basura y la alerta a estas subentidades de correos-e peligrosos.
- La entidad de procesamiento anticorreo basura debe administrar y mantener las reglas de filtrado, que pueden obtenerse a través del sitio web para:
 - Recibir informes de los usuarios y las subentidades de procesamiento anticorreo basura.
 - La transmisión de información de autorización, incluida la de supervisión y gestión.

7.4 Funciones de la subentidad de procesamiento anticorreo basura

Las funciones de la subentidad de procesamiento anticorreo basura comprenden:

- La recepción de informes de quejas de los usuarios y de reglas de filtrado de la entidad de procesamiento anticorreo basura.
- El almacenamiento de información original sobre correos basura de los usuarios (al menos, su encabezamiento) y de otras entidades.
- La transmisión de reglas de filtrado a los servidores de correo electrónico o los clientes de correo electrónico y de alertas a los usuarios de correos-e peligrosos.
- El rastreo de la expansión del correo basura y la recopilación de información al respecto.
- La transmisión de informes sobre la expansión de los correos basura, y la información correspondiente, a las entidades de niveles superiores.

- La creación de nuevas reglas de filtrado a partir de la copia de los correos-e sospechosos, la verificación y modificación de reglas existentes, que pueden obtenerse a través del sitio web para:
 - Crear informes de correo basura de los usuarios y el servidor de correo electrónico.
 - Crear nuevas reglas de filtrado.

8 Identificación del correo basura

En esta cláusula se describen los criterios y características comunes del correo basura.

8.1 Características corrientes del correo basura

A continuación se enumeran algunas de las características corrientes del correo basura:

- Ocultación o falsificación de la verdadera dirección del remitente.
El contenido del campo "de" o "remitente" es inválido o nulo.
- Ocultación o falsificación del verdadero origen del correo-e
El "id de mensaje" del campo identificación es inválido o nulo.
- Remitente conocido de correo basura
En el campo "de" o "remitente" figura la dirección de un remitente de correo basura que está en lista negra.
- Falsificación de la información del destinatario
El contenido del campo destinatario ("a") o el campo destinatario con copia ("cc") es falso o guarda relación con el correo basura.
- Inclusión de palabras comunes utilizadas por los remitentes de correo basura
En el campo asunto ("asunto") o en el contenido del correo-e figuran palabras comúnmente utilizadas por los remitentes de correo basura.
- Falsificación de la información de reenvío
El contenido del campo reenvío, "reenviado de" o "reenviado por remitente", es falso.
- Falsificación de la información de rastreo
El campo rastreo tiene contenido irrelevante.
- Tamaño indebido
El tamaño de todo el correo-e, el campo encabezamiento o el contenido del correo-e es semejante al tamaño del campo encabezamiento y el contenido del correo-e de correos basura.
- Excesivos destinatarios
En un determinado campo hay demasiados destinatarios.
- Excesivos saltos de retransmisión
En el campo rastreo hay demasiados saltos.
- La dirección IP del remitente figura en determinados campos
En los campos "de" o "remitente" se incluye información relativa a los remitentes de correo basura confirmados.
- La dirección IP del servidor de correo electrónico figura en determinados campos
En el campo rastreo, "recibido", o en el campo reenvío "reenviado de" o "reenviado por remitente", se incluye información relativa a remitentes de correo basura confirmados.

- Nuevo correo basura

La entidad de procesamiento anticorreo basura puede resumir las características de un nuevo correo basura muestra y crear las correspondientes reglas de filtrado.

8.2 Reglas comunes para luchar contra el correo basura

Cada regla puede integrarse en una regla compuesta con distinta prioridad.

El servidor de correo electrónico puede aplicar reglas individuales y/o compuestas para luchar contra el correo basura.

8.2.1 Reglas fundamentales comunes

El servidor de correo electrónico puede fijar criterios en función de los siguientes factores:

- El campo origen ("de" o "remitente") está vacío o su contenido no es válido.
- El campo identificación ("id de mensaje") está vacío o su contenido no es válido.
- El campo origen ("de" o "remitente") contiene determinadas palabras clave que figuran en una lista negra.
- El campo destinatario ("a") o destinatario con copia ("cc") contiene palabras clave que figuran en una lista negra.
- El campo asunto ("asunto") o el contenido del correo-e contiene determinadas palabras clave.
- No puede encontrarse el verdadero origen en el campo reenvío ("reenviado de" y "reenviado por remitente") o en el contenido del campo rastreo.
- El tamaño de todo el correo-e, el campo encabezamiento o el contenido del correo-e es (aproximadamente) igual a un valor predeterminado.
- El número total de direcciones incluidas en el campo origen ("a", "cc" y "bcc") supera el límite fijado por el servidor de correo electrónico; o el número de veces que debe enviarse un determinado correo-e rebasa el límite autorizado por el servidor de correo electrónico.
- El número de rastros en el campo rastreo supera el límite fijado por el proveedor de servicio de correo electrónico o el administrador del dominio.
- El resultado de la operación DNS Reverse desde la información de "de" o "remitente" del campo origen está incluido en la lista negra especificada.
- El resultado de la operación DNS Reverse que debe figurar después de la información de "recibido" del campo rastreo, o del "reenviado de" o "reenviado por remitente" del campo reenvío está incluido en la lista negra especificada.
- Si el correo basura no se puede identificar con una única regla, se utilizará una regla compuesta.

8.2.2 Prioridad de los criterios

Se han de confirmar las prioridades de los criterios. Si un correo-e se ajusta a varias reglas (lo que se denomina conflicto de regla), se tratará en función de la regla con mayor prioridad. Si las reglas tienen idéntica prioridad, se aplicará la regla que finalmente se utilice de acuerdo con el principio de prioridad de conflicto. En la medida de lo posible han de evitarse los conflictos.

8.2.3 Conflictos en la detección de criterios

Esta función se utiliza para detectar conflictos entre los distintos criterios asignados. A continuación se describen las condiciones de conflicto más frecuentes:

- Ambas "condiciones de regla" contienen el mismo tipo de "reglas simples (reglas fundamentales)" de clase búsqueda de palabra clave (como "el asunto incluye XXX", "las

primeras 10 líneas descodificadas incluyen XXX", etc.), y las palabras clave de las dos "reglas simples" son las mismas, y una palabra clave incluye la otra.

- Ambas "condiciones de regla" contienen el mismo tipo de "reglas simples" de clase IP restringido (como "el IP del cliente es XXX", etc.), y los dos espacios IP determinados en las "reglas simples" son idénticos o tienen un punto en común.
- Ambas "condiciones de regla" contienen el mismo tipo de "reglas simples" de clase tamaño restringido y las condiciones de tamaño restringido se ajustan a la forma "el tamaño de XXX es el valor determinado" (puede ser "es superior a" o "es inferior a"), y los valores son idénticos. Por ejemplo, dos reglas pueden contener la misma regla simple: "el tamaño del texto del correo-e es 5 343 bytes".

9 Métodos de lucha contra el correo basura

Los principales métodos para luchar contra el correo basura incluyen la desactivación de la función "retransmisión abierta" del servidor de correo electrónico, el control de la autorización de entrega de correos-e y las técnicas de filtrado. El sistema anticorreo basura ha de soportar obligatoria o facultativamente los siguientes métodos.

9.1 Desactivación de la función "retransmisión abierta"

"Retransmisión abierta" significa que el servidor de correo electrónico retransmite todos los correos-e entrantes, independientemente de que los remitentes o destinatarios sean los usuarios estipulados. Por norma general, si el servidor de correo electrónico activa la función de retransmisión ilimitada, se considera que la retransmisión es abierta.

9.2 Control de la autorización de entrega de correo-e

Para evitar que usuarios no autorizados utilicen el servidor de correo electrónico:

- Los remitentes deben ser clientes legales del servidor.
- El servidor debe certificar las direcciones IP de los remitentes.
- El número de saltos del correo-e se limita para evitar la expansión de correo basura de forma exponencial.
- El servidor de correo electrónico puede verificar que el origen del correo-e es auténtico.

9.3 Técnicas de filtrado

La tecnología de filtrado puede dividirse en dos clases: filtrado de dirección IP y filtrado por análisis de texto.

9.3.1 Filtrado de dirección IP

El filtrado de dirección IP puede restringir la conexión al SMTP del sistema de correo-e. Sus principales atributos son la gama IP y los modos de restricción.

La gama IP comprende:

- La gama IP en tiempo real de la entidad de procesamiento anticorreo basura.
- La gama IP en tiempo real de las reglas de filtrado de otras organizaciones.
- La gama IP en tiempo real añadida por sí mismo.

Los modos de restricción son:

- Rechazo de conexión.
- Permiso de conexión incondicional.

- El número de veces que un IP de usuario se conecta al servidor de correo electrónico en un determinado periodo de tiempo debe estar limitado.

Si la dirección IP de un usuario pertenece a una gama de direcciones IP determinada, se aplicarán los modos de restricción.

9.3.2 Filtrado por análisis de texto

El servidor de correo electrónico puede fijar las reglas de filtrado o descargarlas de la entidad de procesamiento anticorreo basura. Bajo determinadas condiciones, los administradores pueden modificar las reglas de filtrado.

Si un correo-e se ajusta a una determinada regla, se clasificará en función del comportamiento correspondiente. Los comportamientos de las reglas de análisis de texto son:

- Rechazo: se devuelve un mensaje de rechazo al remitente tras la extracción de las características.
- Descarte: se da una respuesta normal a cada instrucción sin comportamiento alguno.
- Entrega: se realiza una entrega normal, ignorando el abandono tras optar por la entrega.
- Etiqueta: se añade una etiqueta específica al encabezamiento.
- Informe: se remiten al centro de informes las características extraídas del correo-e.
- Almacenamiento: se mantiene el correo-e intacto en la medida de lo posible y se remite una copia a la entidad de procesamiento anticorreo basura.

9.4 Examen del rastreo

En ocasiones resulta difícil detectar si un remitente es un cliente válido. Puesto que es imposible que el servidor que recibe el correo-e obtenga toda la información relativa al servidor que envía el correo-e, el servidor destinatario no puede certificar toda la información de los usuarios legales.

Los correos-e pueden dividirse en dos grupos: los que se pueden rastrear y los que no. A los correos-e rastreables se les aplican reglas de filtrado, si las alertas no resultan eficaces. Los correos-e no rastreables son difíciles de gestionar, pues normalmente utilizan un origen falso. La mayoría de los correos-e no rastreables son correos basura, por lo que el examen del rastreo es fundamental en la lucha contra el correo basura. Se recomienda seguir los siguientes pasos:

Primer paso: requisito

- La mayoría de los servidores destinatarios (el "MX" en el nombre de dominio) también son servidores remitentes de correo electrónico.
- La mayoría de servidores destinatarios y remitentes independientes tienen IP adyacentes.
- Otras computadoras con autorización para entregar correo-e tienen IP adyacentes a los servidores de correo electrónico "MX".
- Algunos servidores de correo electrónico pueden encontrarse utilizando la función DNS reverse, en cuyo caso el resultado de su aplicación ha de ser idéntico al que el usuario pretende.

Segundo paso: mecanismo de notificación de rastreo

Soportar la certificación en la red de telecomunicaciones IP:

- Confirmar que el campo correo-e del remitente está autorizado.
- Confirmar que el remitente es un usuario legal del campo correo-e.

Tercer paso: mecanismo de rastreo hacia el origen

- El rastreo del servicio y el examen constituyen una cadena hacia el origen.
- La cadena hacia el origen no se puede falsificar.

- Es fácil distinguir la parte falsa de la verdadera.

El sistema de rastreo puede investigar automáticamente la cadena hacia el origen.

10 Interconexión entre dominios de procesamiento anticorreo basura

Cuando los dominios de procesamiento anticorreo basura se conectan entre sí, lo pueden hacer de tres maneras: interconexión entre entidades de procesamiento de nivel superior, interconexión entre entidades de procesamiento y subentidades, interconexión entre un subentidades de procesamiento y servidores de correo electrónico. Cada tipo de interconexión ha de cumplir ciertos requisitos y puede darse en determinadas circunstancias.

10.1 Interconexión entre entidades de procesamiento de nivel superior

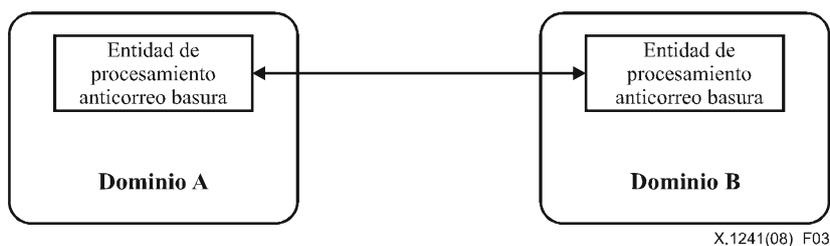


Figura 3 – Interconexión entre entidades de procesamiento de nivel superior

Se trata de una conexión bidireccional entre entidades de procesamiento de nivel superior. Las dos entidades sólo intercambian reglas. Si una entidad recibe información de la otra, aplicará determinados mecanismos y procedimientos para seleccionar reglas útiles a partir de la información recibida.

10.2 Interconexión entre una entidad de procesamiento y una subentidad

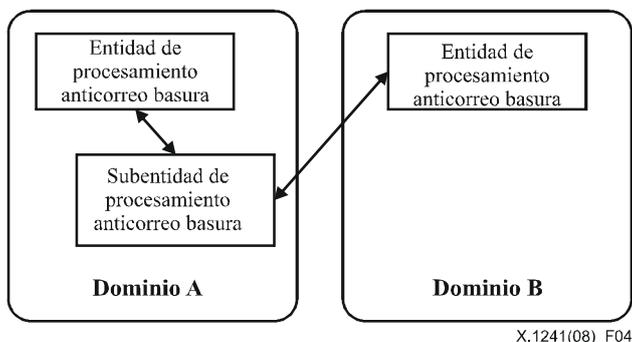


Figura 4 – Interconexión entre una entidad de procesamiento y una subentidad

Se trata de una conexión bidireccional entre una entidad de procesamiento y una subentidad. La subentidad debe descargar dos cuadros de reglas de filtrado desde las dos entidades de procesamiento. La subentidad crea reglas en función de correos-e sospechosos procedentes de los servidores anexos, y ha de comunicar las reglas a las dos entidades.

Se trata de un modo bastante seguro, pero se basa en una relación administrativa compleja entre la subentidad y las dos entidades, que puede causar problemas de escalabilidad. No es una interconexión global entre dominios.

10.3 Interconexión entre una subentidad de procesamiento y un servidor de correo electrónico

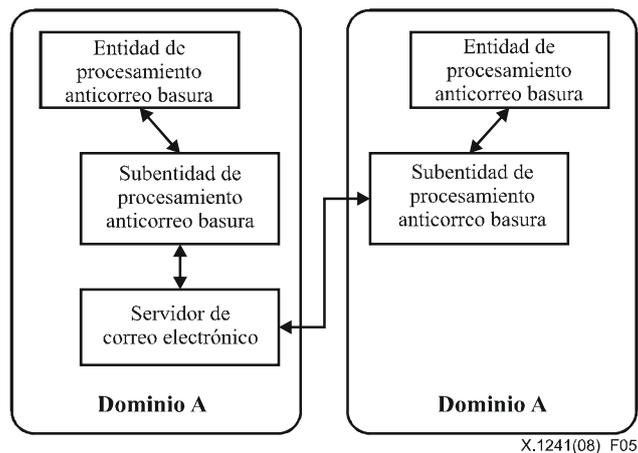


Figura 5 – Interconexión entre una subentidad de procesamiento y un servidor de correo electrónico

Se trata de una conexión bidireccional entre una subentidad de procesamiento y un servidor de correo electrónico. El servidor de correo electrónico descargará las reglas de filtrado de correo basura a partir de la subentidad y rendirá informes sobre los correos basura a la subentidad del otro dominio. La subentidad recibirá informes de correo basura del servidor de correo electrónico y comunicará sus propias reglas al servidor del otro dominio.

Se trata de una interconexión sencilla entre dominios, pero los servidores exteriores al dominio pueden atacar el dominio de procesamiento anticorreo basura, por lo que puede haber problemas de seguridad, además de problemas de escalabilidad. Por tanto, no se trata de una interconexión global entre dominios. El modo definido en la cláusula 10.1 es el de interconexión segura y recomendada.

Bibliografía

- [b-IETF RFC 1869] IETF RFC 1869 (1995), *SMTP Service Extensions*.
<<http://www.ietf.org/rfc/rfc1869.txt>>
- [b-IETF RFC 1939] IETF RFC 1939 (1996), *Post Office Protocol – Version 3*.
<<http://www.ietf.org/rfc/rfc1939.txt>>
- [b-IETF RFC 2060] IETF RFC 2060 (1996), *Internet Message Access Protocol – Version 4rev1*.
<<http://www.ietf.org/rfc/rfc2060.txt>>
- [b-IETF RFC 2222] IETF RFC 2222 (1997), *Simple Authentication and Security Layer (SASL)*.
<<http://www.ietf.org/rfc/rfc2222.txt>>
- [b-IETF RFC 2505] IETF RFC 2505 (1999), *Anti-Spam Recommendations for SMTP MTAs*.
<<http://www.ietf.org/rfc/rfc2505.txt>>
- [b-IETF RFC 2554] IETF RFC 2554 (1999), *SMTP Service Extension for Authentication*.
<<http://www.ietf.org/rfc/rfc2554.txt>>
- [b-IETF RFC 2821] IETF RFC 2821 (2001), *Simple Mail Transfer Protocol*.
<<http://www.ietf.org/rfc/rfc2821.txt>>
- [b-IETF RFC 2822] IETF RFC 2822 (2001), *Internet Message Format*.
<<http://www.ietf.org/rfc/rfc2822.txt>>

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Terminales y métodos de evaluación subjetivos y objetivos
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos, comunicaciones de sistemas abiertos y seguridad
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet y Redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación