

INSTRUCTIVO DE CONFIGURACIÓN

Clearswift Secure Email Gateway 4.x

PREPARADO POR:

Pablo Schivo – Analista en Seguridad Informática

pschivo@ransecurity.com

RAN Security

Buenos Aires, 2019

ARGENTINA

Rivadavia 877 Piso 5°
(C1002AAG) · CABA · Argentina
tel/fax (+54 11) 5353 9999

CHILE

San Sebastián 2812 Oficina 312
Las Condes · Santiago de Chile · Chile
tel/fax (+56 2) 3223 9532

PERÚ

Los Zorzales 160 Piso 3°
San Isidro · Lima · Perú
tel/fax (+51 1) 712 4764

● www.ransecurity.com
expertos@ransecurity.com
LINKEDIN /RANSecurity
TWITTER @RANSecurityv

INSTRUCTIVO DE CONFIGURACIÓN

Clearswift Secure Email Gateway 4.x

Contenido

- Resumen ejecutivo2
- Introducción 2-3
- Descripción de tareas a realizar..... 3-3
- Recomendaciones y observaciones.....7

Resumen ejecutivo

Solución gestionada	Versión
Secure Email Gateway	4.x

El presente instructivo tiene como objetivo la creación y configuración de reglas contra EMOTET para Clearswift Secure Email Gateway 4.x.

Introducción

EMOTET es un troyano polimórfico que es distribuido mediante campañas masivas de SPAM/Phishing y usualmente se camufla como un e-mail legítimo con adjuntos Word y/o PDF simulando ser una factura, notificación de pago, etc.

Para poder frenar este tipo de ataques, necesitamos entender qué información necesitamos obtener del **Header** de los mensajes. A continuación, veremos el header de una muestra del troyano en cuestión.

Así luce una muestra de EMOTET:



ARGENTINA
 Rivadavia 877 Piso 5°
 (C1002AAG) · CABA · Argentina
 tel/fax (+54 11) 5353 9999

CHILE
 San Sebastián 2812 Oficina 312
 Las Condes · Santiago de Chile · Chile
 tel/fax (+56 2) 3223 9532

PERÚ
 Los Zorzales 160 Piso 3°
 San Isidro · Lima · Perú
 tel/fax (+51 1) 712 4764

● www.ransecurity.com
expertos@ransecurity.com
 LINKEDIN /RANSecurity
 TWITTER @RANSecurityv

Así luce el **Header** de la muestra anterior:

```
Received: from Servidor interno de correo de la víctima
with Microsoft SMTP Server id 14.3.408.0; Mon, 28 Jan 2019
13:58:30 -0300 Dominio no deseado IP no deseada
Received: from valappottukal.b4blaze.in (unknown [209.126.106.55]) by
Servidor interno de correo (MTA) with ESMTF id 43pGLd1BMzwpJT for
Casilla de la víctima ; Mon, 28 Jan 2019 14:08:57 -0300 (-03)
Received: by [condor1211.startdedicated.com] (Postfix, from userid 10016) id
CF00220A5395F; Mon, 28 Jan 2019 22:26:47 +0530 (IST)
From: Netflix <Verificar-netflix.com.ar@valappottukal.b4blaze.in> ID falsa del atacante
To: Casilla de la víctima
Subject: CUENTA SUSPENDIDA
Thread-Topic: CUENTA SUSPENDIDA
Thread-Index: AQHÜtyqy+EP6T3ZBe0KUXZ/DWuhMCA==
Date: Mon, 28 Jan 2019 16:56:47 +0000 Dominio no deseado
Message-ID: <20190128165647.CF00220A5395F@condor1211.startdedicated.com>
Content-Language: es-AR
X-MS-Exchange-Organization-AuthSource: MX de la víctima
X-MS-Has-Attach:
X-MS-TNEF-Correlator: IP no deseada
x-msw-jemd-lastmta: 209.126.106.55
x-msw-jemd-refid: Dominio no deseado IP no deseada
[2]6xqtxq4tefjxxhantt5jqwc9e.y-lbl8.mailshell.net-223.238.255.100; CacheIP:none, Bayesi
bulk, SPF:fn,MSBL:0, DNSBL:neutral, Custom_rules:0:0:0, LFtime:190, LUA_SUMMARY:none; newsl
Content-Type: multipart/alternative;
boundary="_000_20190128165647CF00220A5395Fcondor1211startdedicatedcom_"
MIME-Version: 1.0
```

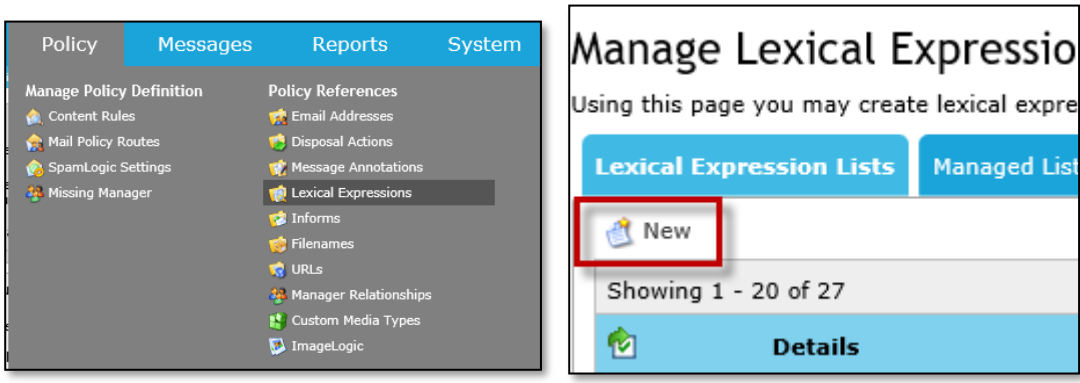
Nuestro objetivo es bloquear **todos los dominios y las IP que provienen de fuentes no confiables** luego de haber analizado el Header.

Nota: si usted no está seguro de lo que tiene que bloquear, por favor contactarse con el Soporte de RAN Security para su asistencia.

Descripción de las tareas a realizar

Usaremos a continuación como ejemplo los datos que obtuvimos del Header anteriormente analizado.

- 1) En primer lugar vamos a ingresar a la consola web del SEG con nuestras credenciales de administrador.
- 2) Vamos a proceder a crear un diccionario o **Lexical Expressions** para poder detectar patrones en el Header del correo.



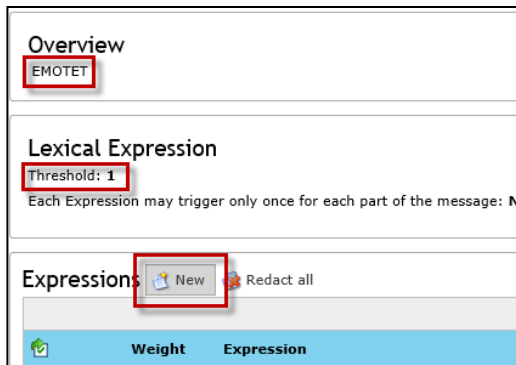
ARGENTINA
Rivadavia 877 Piso 5°
(C1002AAG) · CABA · Argentina
tel/fax (+54 11) 5353 9999

CHILE
San Sebastián 2812 Oficina 312
Las Condes · Santiago de Chile · Chile
tel/fax (+56 2) 3223 9532

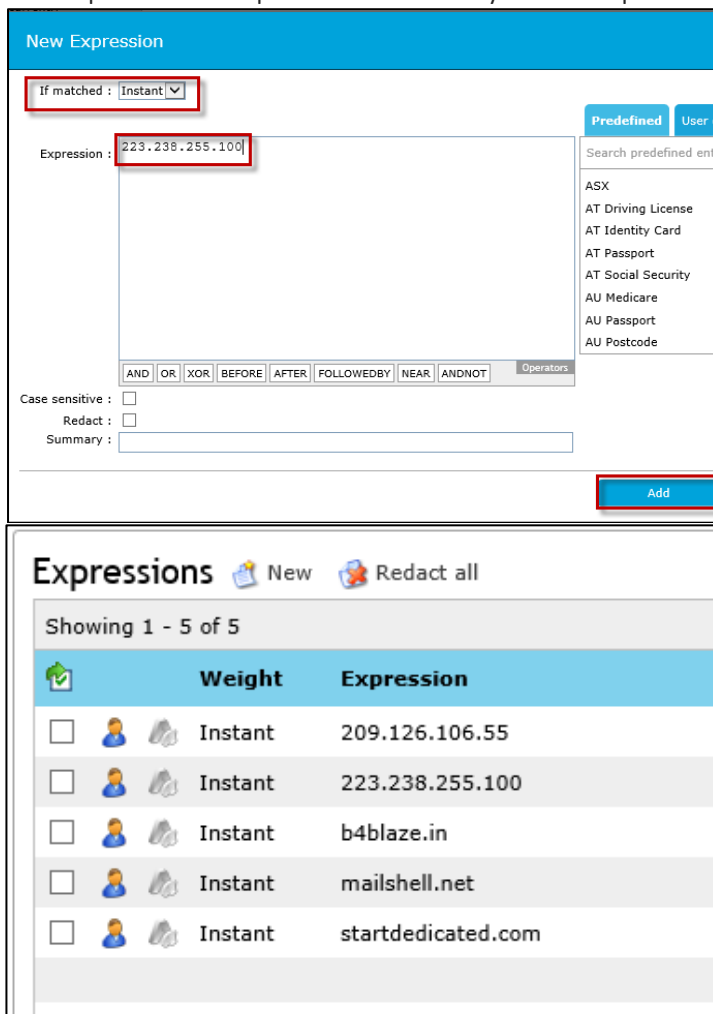
PERÚ
Los Zorzales 160 Piso 3°
San Isidro · Lima · Perú
tel/fax (+51 1) 712 4764

● www.ransecurity.com
expertos@ransecurity.com
[LINKEDIN /RANSecurity](https://www.linkedin.com/company/RANSecurity)
[TWITTER @RANSecurity](https://twitter.com/RANSecurity)

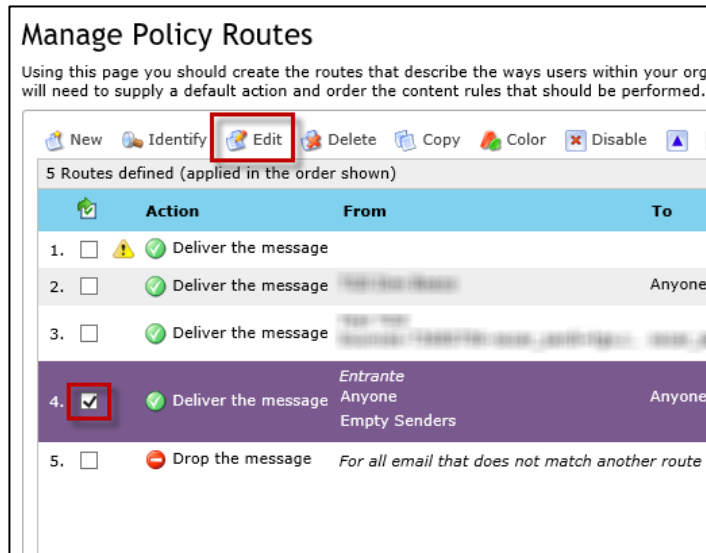
- 3) En **Overview** escribiremos el nombre de nuestro diccionario. En este caso, **EMOTET**, clickeamos **Save**. Luego cambiaremos el valor de **Threshold** a **1** (clickeamos **Save**), y luego clickeamos en **New**.



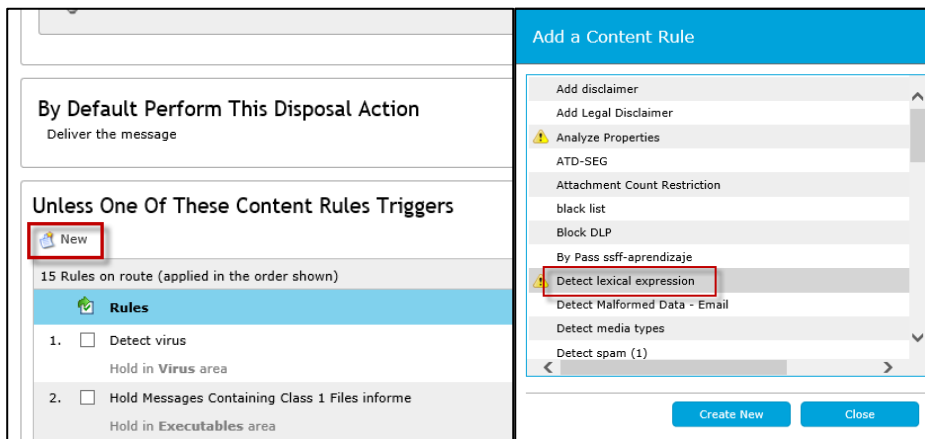
- 4) Cambiamos **If matched** a **Instant**. Cargamos el primer valor que es la IP de donde se originó el mensaje y clickeamos en **Add**. Repetiremos este paso con todas las IP y Dominios que deseamos bloquear.



- 5) Nos dirigimos a **Policy** → **Mail Policy Routes**. Seleccionamos nuestra regla principal de **Correo entrante** y la editamos.

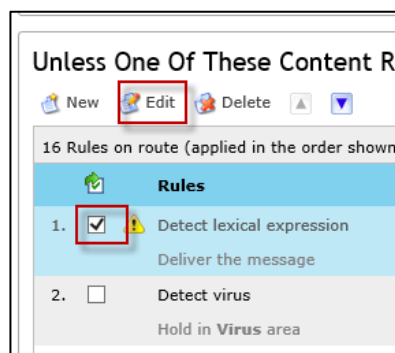


- 6) Agregamos una nueva **Content Rule** en la parte inferior de la política del tipo **Detect Lexical Expression**. Luego clickeamos en **Close**.



5

- 7) Movemos nuestra nueva Content Rule a la posición 1 y la editamos.



ARGENTINA

Rivadavia 877 Piso 5°
(C1002AAG) · CABA · Argentina
tel/fax (+54 11) 5353 9999

CHILE

San Sebastián 2812 Oficina 312
Las Condes · Santiago de Chile · Chile
tel/fax (+56 2) 3223 9532

PERÚ

Los Zorzales 160 Piso 3°
San Isidro · Lima · Perú
tel/fax (+51 1) 712 4764

● www.ransecurity.com
expertos@ransecurity.com
LINKEDIN /RANSecurity
TWITTER @RANSecurity

- 8) Nombramos a nuestra regla como **Detección EMOTET**. Configuramos la Content Rule como figura en la imagen a continuación, agregando los valores de **Header** que figuran en la misma y luego clickeamos **Save**.


Using the expression list and trigger conditions below :

Expression list :

Trigger :

Scan the following parts of the message :

- Content - the message body.
- Content - the attachments matching the conditions in the other clauses.
- The subject line.
- Specific message header(s)
 - envelope-from
 - From
 - Message-ID
 - Received
 - X-ATD-FILEVERDICTS
 - X-ATD-VERDICT
 - x-msw-jemd-lastmta
 - x-msw-jemd-refid
 - x-rcis

 **Note that when scanning content you must select at least one of Scan body, Scan header and footer, Scan properties and Scan comments.**

Document options (for content) :

- Scan body
- Scan header and footer
- Scan properties
- Scan comments
- Scan embedded script

6

- 9) En la sección **What To Do?** → **Disposal Action** vamos a elegir **Hold in Phishing** área. Clickeamos **Save**.

And Size Restriction Of

No size restriction will be applied to this content rule.

And Scan text extracted from images (OCR)

Text extracted from images will not be scanned

What To Do?

If the conditions in the **'What to Look For?'** panel are met then the actions defined in this panel will be performed.

Disposal Action

and also

What Else To Do?

- No additional actions

ARGENTINA

Rivadavia 877 Piso 5°
(C1002AAG) · CABA · Argentina
tel/fax (+54 11) 5353 9999

CHILE

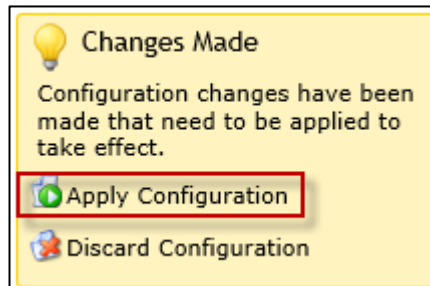
San Sebastián 2812 Oficina 312
Las Condes · Santiago de Chile · Chile
tel/fax (+56 2) 3223 9532

PERÚ

Los Zorzales 160 Piso 3°
San Isidro · Lima · Perú
tel/fax (+51 1) 712 4764

• www.ransecurity.com
expertos@ransecurity.com
LINKEDIN /RANSecurity
TWITTER @RANSecuritytv

10) Aplicamos los cambios efectuados.



Recomendaciones y observaciones

- Se recomienda que el Administrador de la plataforma Anti-Spam verifique en los próximos días la cuarentena de **Phising** para descartar que no haya falsos positivos.

7



www.ransecurity.com

[/RANsecurity](https://www.linkedin.com/company/RANsecurity)

[@RANsecurity](https://twitter.com/RANsecurity)

SobreRANsecurity®. | Somos una empresa líder en Seguridad Informática establecida en Argentina desde 1991, y con operaciones en Chile, Perú y Uruguay, ofreciendo soluciones de seguridad informática de primera calidad en las áreas de:

- Protección endpoint de próxima generación
- Firewall de próxima generación (NGFW)
- Control de acceso a la red (NAC)
- Seguridad y cumplimiento para entornos virtuales
- Protección y Antivirus para servidores y estaciones de trabajo
- Gestión y protección de dispositivos móviles
- Protección de e-mail y web
- Correlación de eventos (SIEM)
- Gestión de Vulnerabilidades
- Control de cambios para servidores y puntos de venta
- Gestión de licencias de software y control de activos tecnológicos
- Gestión de permisos privilegiados, entre otros.

Somos el VAR más importante de McAfee (Intel Security) en la región y socio estratégicos de: •ForeScout •Forcepoint, •Cylance •Tripwire •Varonis, •Blackberry •Proofpoint, también desarrolla la solución de gestión de activos de IT y soporte técnico con su marca fixIQ®.

Adicionalmente contamos con un área especializada de servicios llamada servicios expertos®, que ofrece servicios de: •Centro de Operaciones de Seguridad (SOC) •Implementación, actualizaciones y migraciones de soluciones de seguridad informática •Gestión de infraestructura informática •Administración remota y en sitio •Auditoría •Análisis GAP •Outsourcing •Co-Sourcing, y •Capacitaciones. Contamos con un plantel de expertos certificados con experiencia en entornos heterogéneos, distribuidos y envergaduras diversas.

Más de 500 empresas avalan nuestros servicios. Para mayor información, visita: www.ransecurity.com

ARGENTINA

Rivadavia 877 Piso 5°
(C1002AAG) · CABA · Argentina
tel/fax (+54 11) 5353 9999

CHILE

San Sebastián 2812 Oficina 312
Las Condes · Santiago de Chile · Chile
tel/fax (+56 2) 3223 9532

PERÚ

Los Zorzales 160 Piso 3°
San Isidro · Lima · Perú
tel/fax (+51 1) 712 4764

• www.ransecurity.com
expertos@ransecurity.com
LINKEDIN /RANSecurity
TWITTER @RANSecurityv