

Habilitación y mejores prácticas del Filtrado de URL ESA

Contenido

[Introducción](#)

[Antecedentes](#)

[Filtrado de URL del permiso](#)

[Cree las acciones del Filtrado de URL](#)

[Contente los filtros para los URL limpios](#)

[Contente los filtros para los URL neutrales o sospechados](#)

[Contente los filtros para los URL malévolos](#)

[Señale los URL Uncategorized y clasificados equivocadamente](#)

[Los URL malévolos y los mensajes del marketing no son cogidos por los filtros del Anti-Spam o del brote](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo habilitar el Filtrado de URL en el dispositivo de seguridad del correo electrónico de Cisco (ESA) y las mejores prácticas para su uso.

Antecedentes

Cuando usted habilita el Filtrado de URL en el ESA, usted debe también habilitar las otras funciones, dependientes sobre sus funciones deseadas. Aquí están algunas características típicas que se habilitan junto al Filtrado de URL:

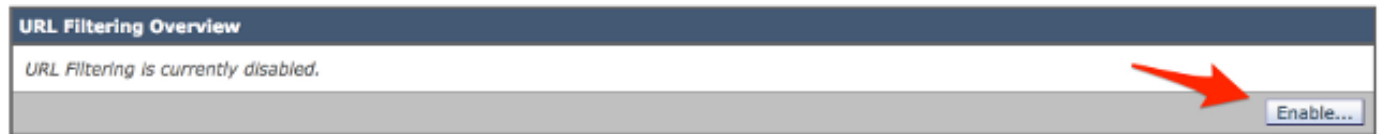
- Para la protección mejorada contra el Spam, la característica de la exploración del Anti-Spam se debe habilitar global de acuerdo con la directiva aplicable del correo. Ésta puede ser el Anti-Spam de Cisco IronPort (IPA) o la característica inteligente de la Multi-exploración de Cisco (IMS).
- Para la protección mejorada contra el malware, la característica de los filtros del brote o de los filtros del brote de virus (VOF) se debe habilitar global de acuerdo con la directiva aplicable del correo.
- Para las acciones basadas en la reputación URL, o para aplicar las directivas aceptables del uso con el uso de los filtros del mensaje y del contenido, usted debe habilitar VOF global.

Filtrado de URL del permiso

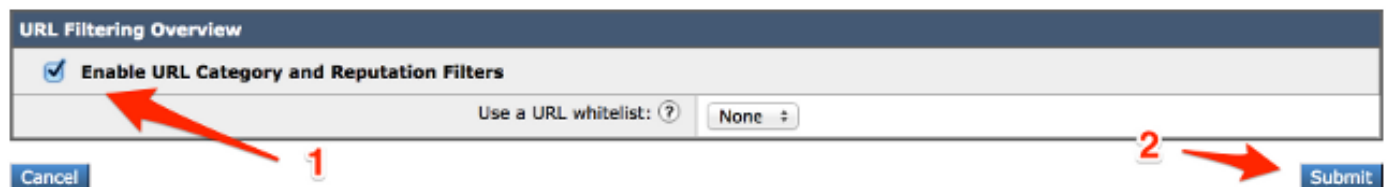
Para implementar el Filtrado de URL en el ESA, usted debe primero habilitar la característica. Hay dos métodos distintos que usted puede utilizar para habilitar esta característica: Con el uso del GUI o del CLI.

Para habilitar el Filtrado de URL con el uso del GUI, navegue a los **Servicios de seguridad > al Filtrado de URL > al permiso:**

URL Filtering



URL Filtering



Para habilitar el Filtrado de URL con el uso del CLI, ingrese el comando del **websecurityconfig**:

```
myesa.local> websecurityconfig
Enable URL Filtering? [N]> y
```

Es importante observar que usted debe también habilitar el registro URL dentro del VOF. Ésta es una característica CLI-solamente que se debe habilitar como se muestra aquí:

```
myesa.local> outbreakconfig
```

```
Outbreak Filters: Enabled
```

```
Choose the operation you want to perform:
```

- SETUP - Change Outbreak Filters settings.
- CLUSTERSET - Set how the Outbreak Filters are configured in a cluster.
- CLUSTERSHOW - Display how the Outbreak Filters are configured in a cluster.

```
[ ]> setup
```

```
Outbreak Filters: Enabled
```

```
Would you like to use Outbreak Filters? [Y]>
```

```
Outbreak Filters enabled.
```

```
Outbreak Filter alerts are sent when outbreak rules cross the threshold (go above or back down below), meaning that new messages of certain types could be quarantined or will no longer be quarantined, respectively.
```

```
Would you like to receive Outbreak Filter alerts? [N]>
```

```
What is the largest size message Outbreak Filters should scan?
[2097152]>
```

```
Do you want to use adaptive rules to compute the threat level of messages? [Y]>
```

```
Logging of URLs is currently disabled.
```

```
Do you wish to enable logging of URL's? [N]> y
```

```
Logging of URLs has been enabled.
```

```
The Outbreak Filters feature is now globally enabled on the system. You must use the 'policyconfig' command in the CLI or the Email Security Manager in the GUI to enable Outbreak Filters for the desired Incoming and Outgoing Mail Policies.
```

Nota: Asegúrese de que usted **confíe cualquiera y todos los** cambios a su configuración antes de que usted proceda del GUI o del CLI en su ESA.

Cree las acciones del Filtrado de URL

Cuando usted habilita el Filtrado de URL solamente, no toma medidas contra los mensajes que pudieron contener los URL vivos y válidos.

Los URL incluidos en los mensajes entrantes y salientes (con la exclusión de las conexiones) se evalúan. Cualquier Cadena válida para un URL se evalúa, para incluir las cadenas con estos componentes:

- HTTP, HTTPS, o WWW
- Dominio o IP Addresses
- Números del puerto precedidos por los dos puntos (:)
- Mayúscula o letras minúsculas

Cuando el sistema evalúa los URL para determinar si un mensaje es Spam, en caso necesario para la Administración de la carga, da prioridad y defiende a los mensajes entrantes sobre los mensajes de salida.

Para analizar rápidamente los URL y tomar medidas, usted puede crear un filtro contenido de modo que *si el* mensaje tiene un URL válido, *después la* acción es aplicada. Del GUI, navegue para enviar las directivas > filtro contenido entrante de los filtros > Add.

Contente los filtros para los URL limpios

Este ejemplo muestra una exploración para los URL limpios con la implementación de este filtro contenido entrante:

Content Filter Settings			
Name:	<input type="text" value="CLEAN_URL"/>		
Currently Used by Policies:	Default Policy		
Description:	<input type="text"/>		
Order:	2 (of 15)		

Conditions			
<input type="button" value="Add Condition..."/>			
Order	Condition	Rule	Delete
1	URL Reputation	url-reputation(6.00, 10.00, "")	<input type="button" value="Delete"/>

Actions			
<input type="button" value="Add Action..."/>			
Order	Action	Rule	Delete
1	Add Log Entry	log-entry("====> CLEAN URL! <====")	<input type="button" value="Delete"/>

Con este filtro en el lugar, el sistema busca para un URL con una reputación *limpia* (6.00 a 10.00) y agrega simplemente una entrada de registro al correo abre una sesión la orden para accionar y para registrar la calificación en Internet de la reputación (WBRS). Esta entrada de registro también ayuda a identificar el proceso se acciona que. Aquí está un ejemplo de los registros del

correo:

```
Wed Nov 5 21:11:10 2014 Info: Start MID 182 ICID 602
Wed Nov 5 21:11:10 2014 Info: MID 182 ICID 602 From: <bad_user@that.domain.net>
Wed Nov 5 21:11:10 2014 Info: MID 182 ICID 602 RID 0 To: <joe.user@goodmailguys.com>
Wed Nov 5 21:11:10 2014 Info: MID 182 Message-ID
'<D08042EA.24BA4%bad_user@that.domain.net>'
Wed Nov 5 21:11:10 2014 Info: MID 182 Subject 'Starting at the start!'
Wed Nov 5 21:11:10 2014 Info: MID 182 ready 2798 bytes from
<bad_user@that.domain.net>
Wed Nov 5 21:11:10 2014 Info: MID 182 matched all recipients for per-recipient policy
DEFAULT in the inbound table
Wed Nov 5 21:11:11 2014 Info: MID 182 interim AV verdict using Sophos CLEAN
Wed Nov 5 21:11:11 2014 Info: MID 182 antivirus negative
Wed Nov 5 21:11:11 2014 Info: MID 182 URL http:// www .yahoo.com has reputation 8.39
matched url-reputation-rule
Wed Nov 5 21:11:11 2014 Info: MID 182 Custom Log Entry: <===> CLEAN URL! <===>
Wed Nov 5 21:11:11 2014 Info: MID 182 Outbreak Filters: verdict negative
Wed Nov 5 21:11:11 2014 Info: MID 182 queued for delivery
Wed Nov 5 21:11:11 2014 Info: New SMTP DCID 23 interface 192.168.0.199 address
192.168.0.200 port 25
Wed Nov 5 21:11:11 2014 Info: Delivery start DCID 23 MID 182 to RID [0]
Wed Nov 5 21:11:11 2014 Info: Message done DCID 23 MID 182 to RID [0] [('X-IronPort-AV',
'E=Sophos;i="5.07,323,1413259200"; \r\n d="scan\'208,217";a="182"'), ('x-ironport-av',
'E=Sophos;i="5.07,323,1413244800"; \r\n d="scan\'208,217";a="93839309"')]
Wed Nov 5 21:11:11 2014 Info: MID 182 RID [0] Response '2.0.0 Ok: queued as 7BAF5801C2'
Wed Nov 5 21:11:11 2014 Info: Message finished MID 182 done
Wed Nov 5 21:11:16 2014 Info: ICID 602 close
Wed Nov 5 21:11:16 2014 Info: DCID 23 close
```

Nota: El URL que se integra en el ejemplo anterior tiene los espacios adicionales incluidos en el cuerpo URL, así que lo no dispara ningunas exploraciones de la red o detección del proxy.

Tal y como se muestra en del ejemplo, **Yahoo.com** se juzga **LIMPIO** y se da una calificación de **8.39**, se observa en los registros del correo, y se entrega al usuario final.

Filtros contenidos para los URL neutrales o sospechados

Nota: En [AsyncOS 9.7 para la Seguridad del correo electrónico](#) y posterior, los URL que antes fueron etiquetados “sospechosos” ahora se etiquetan “neutral.” Solamente el etiquetado ha cambiado; la lógica subyacente y el proceso no han cambiado.

Este ejemplo muestra una exploración para neutral/el sospechoso URL con la implementación de este filtro contenido entrante:

Content Filter Settings	
Name:	SUSPECT_URL
Currently Used by Policies:	Default Policy
Editable by (Roles):	No roles selected
Description:	
Order:	4 (of 5)

Conditions			
Add Condition...			
Order	Condition	Rule	Delete
1	URL Reputation	url-reputation(-5.90, -3.10, "")	

Actions			
Add Action...			
Order	Action	Rule	Delete
1	Add Log Entry	log-entry("<====> SUSPECT URL! <====>")	
2	Add/Edit Header	edit-header-text("Subject", "(.*)", "[SUSPECT URL!]\1")	

Con este filtro en el lugar, el sistema busca para un URL con un *neutral*, o el *sospechoso*, la reputación (-5.90 a -3.1) y agrega una entrada de registro a los registros del correo. Este ejemplo muestra un tema modificado para prepend el "[SUSPECT URL!>". Aquí está un ejemplo de los registros del correo:

```
Wed Nov 5 21:22:23 2014 Info: Start MID 185 ICID 605
Wed Nov 5 21:22:23 2014 Info: MID 185 ICID 605 From: <bad_user@that.domain.net>
Wed Nov 5 21:22:23 2014 Info: MID 185 ICID 605 RID 0 To: <joe.user@goodmailguys.com>
Wed Nov 5 21:22:23 2014 Info: MID 185 Message-ID
'<D0804586.24BAE%bad_user@that.domain.net>'
Wed Nov 5 21:22:23 2014 Info: MID 185 Subject 'Middle of the road?'
Wed Nov 5 21:22:23 2014 Info: MID 185 ready 4598 bytes from
<bad_user@that.domain.net>
Wed Nov 5 21:22:23 2014 Info: MID 185 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Wed Nov 5 21:22:24 2014 Info: MID 185 interim AV verdict using Sophos CLEAN
Wed Nov 5 21:22:24 2014 Info: MID 185 antivirus negative
Wed Nov 5 21:22:24 2014 Info: MID 185 URL https:// www.udemy.com/official-udemy-
instructor-course/?refcode=slfgiacoitvbfgl7tawqoxwqrdqcerbhublflhsmfilcfkulte5x
ofictyrmwfcfxcvfgdkobgbcjv4bxcqbfmzcrmamwauxcuydtksayhpovebpvmdllxgxsu5vx8wzkj
hiwazhg5m&utm_campaign=email&utm_source=sendgrid.com&utm_medium=email has
reputation -5.08 matched url-reputation-rule
Wed Nov 5 21:22:24 2014 Info: MID 185 Custom Log Entry: <====> SUSPECT URL! <====>
Wed Nov 5 21:22:24 2014 Info: MID 185 Outbreak Filters: verdict negative
Wed Nov 5 21:22:24 2014 Info: MID 185 queued for delivery
Wed Nov 5 21:22:24 2014 Info: New SMTP DCID 26 interface 192.168.0.199 address
192.168.0.200 port 25
Wed Nov 5 21:22:24 2014 Info: Delivery start DCID 26 MID 185 to RID [0]
Wed Nov 5 21:22:24 2014 Info: Message done DCID 26 MID 185 to RID [0]
[('X-IronPort-AV', 'E=Sophos;i="5.07,323,1413259200"; \r\n d="scan\'208,217";a="185"'),
('x-ironport-av', 'E=Sophos;i="5.07,323,1413244800"; \r\n d="scan\
'208,217";a="93843786"')]
Wed Nov 5 21:22:24 2014 Info: MID 185 RID [0] Response '2.0.0 Ok: queued as 0F8F9801C2'
Wed Nov 5 21:22:24 2014 Info: Message finished MID 185 done
```

Nota: El URL que se integra en el ejemplo anterior tiene los espacios adicionales incluidos en el cuerpo URL, así que lo no dispara ningunas exploraciones de la red o detección del proxy.

El link de Udemty en el ejemplo anterior no aparece limpio, y es **SOSPECHOSO** anotado en - **5.08**. Tal y como se muestra en de la entrada de registros del correo, este mensaje se permite ser entregado al usuario final.

Filtros contenidos para los URL malévolos

Este ejemplo muestra una exploración para los URL malévolos con la implementación de este filtro contenido entrante:

Content Filter Settings

Name:	<input type="text" value="MALICIOUS_URL"/>
Currently Used by Policies:	Default Policy
Description:	<input type="text" value="Log mail_logs, Defang, and Quarantine message with a poor reputation."/>
Order:	4 (of 15)

Conditions

Order	Condition	Rule	Delete
1	URL Reputation	url-reputation(-10.00, -6.00, "")	

Actions

Order	Action	Rule	Delete
1	Add Log Entry	log-entry("<====> MALICIOUS URL! <====>")	
2	URL Reputation	url-reputation-defang(-10.00, -6.00, "", 0)	
3	Quarantine	quarantine("URL Filtering Quarantine")	

Con este filtro en el lugar, los análisis del sistema para un URL con una reputación *malévola* (-10.00 a -6.00), agregan una entrada de registro a los registros del correo, utilizan la acción del *defang* para hacer el link unclickable, y colocan esto en una cuarentena del Filtrado de URL. Aquí está un ejemplo de los registros del correo:

```

Wed Nov 5 21:27:18 2014 Info: Start MID 186 ICID 606
Wed Nov 5 21:27:18 2014 Info: MID 186 ICID 606 From: <bad_user@that.domain.net>
Wed Nov 5 21:27:18 2014 Info: MID 186 ICID 606 RID 0 To: <joe.user@goodmailguys.com>
Wed Nov 5 21:27:18 2014 Info: MID 186 Message-ID
'<COL128-W95DE5520A96FD9D69FAC2D9D840@phx.gbl>'
Wed Nov 5 21:27:18 2014 Info: MID 186 Subject 'URL Filter test malicious'
Wed Nov 5 21:27:18 2014 Info: MID 186 ready 2230 bytes from
<bad_user@that.domain.net>
Wed Nov 5 21:27:18 2014 Info: MID 186 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Wed Nov 5 21:27:18 2014 Info: ICID 606 close
Wed Nov 5 21:27:19 2014 Info: MID 186 interim verdict using engine: CASE spam positive
Wed Nov 5 21:27:19 2014 Info: MID 186 using engine: CASE spam positive
Wed Nov 5 21:27:19 2014 Info: ISQ: Tagging MID 186 for quarantine
Wed Nov 5 21:27:19 2014 Info: MID 186 interim AV verdict using Sophos CLEAN
Wed Nov 5 21:27:19 2014 Info: MID 186 antivirus negative
Wed Nov 5 21:27:19 2014 Info: MID 186 URL http:// peekquick .com /sdeu/cr.sedin/sdac/
denc.php has reputation -6.77 matched url-reputation-rule
Wed Nov 5 21:27:19 2014 Info: MID 186 Custom Log Entry: <====> MALICIOUS URL! <====>
Wed Nov 5 21:27:19 2014 Info: MID 186 URL http:// peekquick .com/sdeu/cr.sedin/sdac/
denc.php has reputation -6.77 matched url-reputation-defang-action
Wed Nov 5 21:27:19 2014 Info: MID 186 URL http:// peekquick .com /sdeu/cr.sedin/sdac/
denc.php has reputation -6.77 matched url-reputation-defang-action
Wed Nov 5 21:27:19 2014 Info: MID 186 rewritten to MID 187 by

```

```
url-reputation-defang-action filter '__MALICIOUS_URL__'
Wed Nov 5 21:27:19 2014 Info: Message finished MID 186 done
Wed Nov 5 21:27:19 2014 Info: MID 187 Outbreak Filters: verdict positive
Wed Nov 5 21:27:19 2014 Info: MID 187 Threat Level=5 Category=Phish Type=Phish
Wed Nov 5 21:27:19 2014 Info: MID 187 rewritten URL u'http:// peekquick .com
/sdeu/cr.sedin/sdac/denc.php-Robert'
Wed Nov 5 21:27:19 2014 Info: MID 187 rewritten to MID 188 by url-threat-protection
filter 'Threat Protection'
Wed Nov 5 21:27:19 2014 Info: Message finished MID 187 done
Wed Nov 5 21:27:19 2014 Info: MID 188 Virus Threat Level=5
Wed Nov 5 21:27:19 2014 Info: MID 188 quarantined to "Outbreak"
(Outbreak rule:Phish: Phish)
Wed Nov 5 21:27:19 2014 Info: MID 188 quarantined to "URL Filtering Quarantine"
(content filter:__MALICIOUS_URL__)
Wed Nov 5 21:28:20 2014 Info: SDS_CLIENT: Generated URL scanner configuration
Wed Nov 5 21:28:21 2014 Info: SDS_CLIENT: URL scanner enabled=1
Wed Nov 5 21:28:21 2014 Info: SDS_CLIENT: Generated URL scanner configuration
Wed Nov 5 21:28:21 2014 Info: SDS_CLIENT: URL scanner enabled=1
```

Nota: El URL que se integra en el ejemplo anterior tiene los espacios adicionales incluidos en el cuerpo URL, así que lo no dispara ningunas exploraciones de la red o detección del proxy.

Este URL para **peekquick.com** es **MALÉVOLO** y anotado en **-6.77**. Una entrada se hace en los registros del correo, donde usted puede ver todos los procesos en la acción. El filtro URL detectó el URL malévolo, defanged, y quarantined lo. El VOF también lo anotó positivo basado en su conjunto de la regla, y con tal que los detalles que esto era un Phish relacionado.

Si VOF no se habilita, el mismo mensaje se procesa a través, pero las exploraciones URL no se actúan sobre sin la capacidad agregada de VOF de conducir las exploraciones y la acción. Sin embargo, en este ejemplo el motor antispam de Cisco analiza (CASO) y se juzga al cuerpo del mensaje como Spam-positivo:

```
Wed Nov 5 21:40:49 2014 Info: Start MID 194 ICID 612
Wed Nov 5 21:40:49 2014 Info: MID 194 ICID 612 From: <bad_user@that.domain.net>
Wed Nov 5 21:40:49 2014 Info: MID 194 ICID 612 RID 0 To: <joe.user@goodmailguys.com>
Wed Nov 5 21:40:49 2014 Info: MID 194 Message-ID
'<COL128-W145FD8B772C824CEF33F859D840@phx.gbl>'
Wed Nov 5 21:40:49 2014 Info: MID 194 Subject 'URL Filter test malicious'
Wed Nov 5 21:40:49 2014 Info: MID 194 ready 2230 bytes from <bad_user@that.domain.net>
Wed Nov 5 21:40:49 2014 Info: MID 194 matched all recipients for per-recipient policy
DEFAULT in the inbound table
Wed Nov 5 21:40:50 2014 Info: ICID 612 close
Wed Nov 5 21:40:50 2014 Info: MID 194 interim verdict using engine: CASE spam positive
Wed Nov 5 21:40:50 2014 Info: MID 194 using engine: CASE spam positive
Wed Nov 5 21:40:50 2014 Info: ISQ: Tagging MID 194 for quarantine
Wed Nov 5 21:40:50 2014 Info: MID 194 interim AV verdict using Sophos CLEAN
Wed Nov 5 21:40:50 2014 Info: MID 194 antivirus negative
Wed Nov 5 21:40:50 2014 Info: MID 194 queued for delivery
Wed Nov 5 21:40:52 2014 Info: RPC Delivery start RCID 20 MID 194 to local IronPort
Spam Quarantine
Wed Nov 5 21:40:52 2014 Info: ISQ: Quarantined MID 194
Wed Nov 5 21:40:52 2014 Info: RPC Message done RCID 20 MID 194
Wed Nov 5 21:40:52 2014 Info: Message finished MID 194 done
```

Esta detección vía el CASO solamente no ocurre siempre. Hay las épocas en que las reglas del CASO y IPA pudieron contener esa coincidencia contra un ciertos remitente, dominio, o contenidos del mensaje para detectar esta amenaza solamente.

Señale los URL Uncategorized y clasificados equivocadamente

A veces, un URL no se pudo clasificar todavía, o puede ser que miscategorized. Para señalar los URL que miscategorized, y los URL que no se categorizan sino deben ser, visite la página de las [peticiones de la clasificación de Cisco URL](#).

Usted puede ser que también desee de marcar el estatus de los URL sometidos. Para hacer esto, haga clic el **estatus** en la lengüeta sometida URL de esta página.

Los URL malévolos y los mensajes del márketing no son cogidos por los filtros del Anti-Spam o del brote

Esto puede ocurrir porque la reputación y la categoría del Web site son solamente dos criterios entre muchos que los filtros del anti-Spam y del brote utilicen para determinar sus veredictos. Para aumentar la sensibilidad de estos filtros, baje los umbrales que se requieren para tomar medidas, tales como reescritura o reemplazo de los URL por el texto, o quarantining o mensajes de caída.

Alternativamente, usted puede crear los filtros del contenido o del mensaje basados en la calificación de la reputación URL.

Información Relacionada

- [Dispositivo de seguridad del correo electrónico de Cisco - Guías del usuario final](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)