

MANUAL DE IMPLEMENTACIÓN PROTOCOLOS DE DEFENSA SPF, DKIM, DMARC PARA SERVIDOR DE CORREOS EXCHANGE 2007/2010/2013/2016/2019



Universidad Nacional de Chimborazo
Realizado por: Alex Auquilla, Henry Espin
Riobamba- Ecuador
2018-2019

CONTENIDO

1. Introducción

La información es un activo de alta importancia en una entidad para su desarrollo continuo de la misión y el cumplimiento del objetivo de la misma, lo cual genera la necesidad de implementar mecanismos que permitan proteger la confidencialidad, integridad y disponibilidad en todo el ciclo de vida de la información.

La seguridad de la información ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes ha traído consigo la aparición de nuevas amenazas. Estos riesgos que se enfrentan han llevado a que se implemente mecanismos que se orientan a evitar intrusiones de atacantes externos lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la misma institución, los mecanismos de defensa son definidos partiendo de un ataque denominado smtp spoofing.

La Universidad Nacional de Chimborazo no es invulnerable a este tipo de ataques, debido a este motivo se analizó y se previno las amenazas en la seguridad de la red, por ende, con los resultados obtenidos en el ambiente simulado en donde se realizó pruebas se obtuvo un resultado muy aceptable en la mitigación de ataques SMTP Spoofing. Por lo cual, para manejar este tipo de situaciones se realizó esta guía de usuario en el que se muestra las configuraciones recomendadas en la implementación de SPF, DKIM y DMARC para mitigar los ataques mencionados.

2. Requisitos para la instalación de Exchange-Servidor de correos 2007/2010/2013/2016/2019

2.1. ¿Qué se necesita saber antes de la instalación?

- Comprobar que el servicio de Active Directory y sus complementos están correctamente instalados (Comprobar en el Administrador de Servidores).
- Compruebe que el equipo se haya asociado al dominio Active Directory interno.
- Comprobar si el sistema operativo está instalado las actualizaciones más recientes (comprobar en Windows Update).

2.2. Requisitos previos de software

- .NET Framework 4.7.2 o posterior (revizar en la página oficial de Microsoft)
- Instalar el paquete Redistributable de Visual C++ para Visual Studio 2012
- Instalar el complemento Unified Communications Managed API 4.0.
- Tener instalado en el cliente Outlook 2007/2010/2013/2016/2019.

2.3. Requisitos previos de conocimientos en parámetros SPF

SPF (Sender Policy Framework) es un método usado para impedir la falsificación de la dirección de un remitente, es decir, el uso de direcciones falsas. Este permite al servidor de correo verificar que los correos procedentes de un dominio proceden de un host autorizado por el administrador de dicho dominio.

Activación o desactivación de SPF en el servidor

Cuando activa SPF para comprobar los correos entrantes, el servidor de correo efectúa una búsqueda DNS en el host del remitente para localizar algún registro DNS relacionado con SPF. Pueden definirse los siguientes grupos de reglas:

Reglas locales. - Reglas usadas por el filtro antispam antes de que el servidor de correo inicie la comprobación SPF.

Nota: estas reglas se concatenan con las reglas especificadas en el registro DNS relacionado con SPF o el remitente. Por ejemplo, si el remitente tiene la siguiente directiva SPF: **example.com. txt v=spf1 +a +mx -all** y la regla local es **a:ejemplo.com**, la directiva resultante será **example.com. txt v=spf1 +a +mx +a:ejemplo.com -all**.

Reglas de conjetura - Reglas aplicadas a los dominios que no publican registros SPF ejemplo.com. TXT v=spf1 +a +mx +a:ejemplo.com -all

Tabla 1. Parámetros SPF

Parte	Descripción
v=spf1	El dominio usa SPF de la versión 1.
+a	Todos los hosts de los registros "A" pueden enviar correos.
+mx	Todos los hosts de los registros "MX" pueden enviar correos.
+a:ejemplo.com	El dominio <i>ejemplo.com</i> puede enviar correos.
-all	Todos los demás dominios no pueden enviar correos.

2.4. Requisitos previos de conocimientos en parámetros DKIM

DKIM (DomainKeys Identified Mail) es un método usado para asociar la identidad de un nombre de dominio con un correo saliente. Asimismo, también sirve para validar la identidad de un nombre de dominio asociado con un correo entrante mediante autenticación criptográfica.

Activación o desactivación de DKIM en el servidor

Para activar la funcionalidad DKIM en su servidor, vaya a Herramientas y configuración -> Configuración del servidor de correo (en el grupo Correo) y desplácese a la sección Protección antispam DKIM. Las siguientes opciones le permiten gestionar DKIM en su servidor:

- **Permitir firmar correo saliente.** Esta opción permite a los clientes activar la firma con DKIM de los correos salientes por dominios. Tenga en cuenta que esta opción no activa la firma de todos los correos salientes de forma automática. Para poder usar DKIM, los usuarios deben activarlo para los dominios individuales.
- **Comprobar correo entrante.** Esta opción activa el análisis de todos los correos entrantes por parte de DKIM. Se analizan todos los correos y, de experimentarse algún error durante el análisis, los correos pertinentes se marcan con un encabezado especial.

Tenga en cuenta que cada una de estas opciones puede seleccionarse de forma independiente. Puede optar por habilitar la firma de correo saliente, comprobar el correo entrante o ambas.

Una vez activado DKIM para un dominio, añada los siguientes dos registros a la zona DNS del dominio:

- **default._domainkey.<ejemplo.com>** - contiene la parte pública de la clave generada.
- **_domainkey.<ejemplo.com>** - contiene la directiva DKIM.

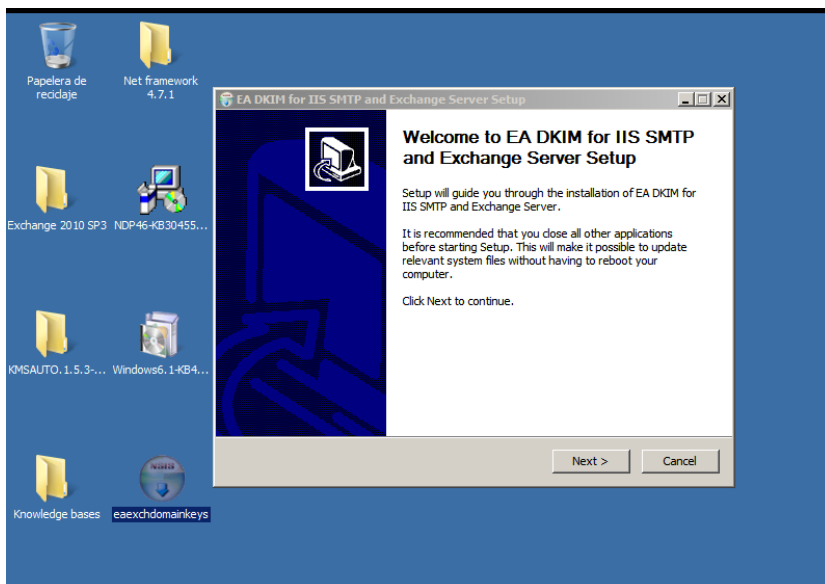
2.5. Requisitos previos en conocimiento de las políticas DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) es una tecnología que permite ampliar las capacidades de los métodos SPF y DKIM. La directiva DMARC define la forma en la que el receptor debería tratar los correos en función de los resultados de la comprobación DKIM y SPF.

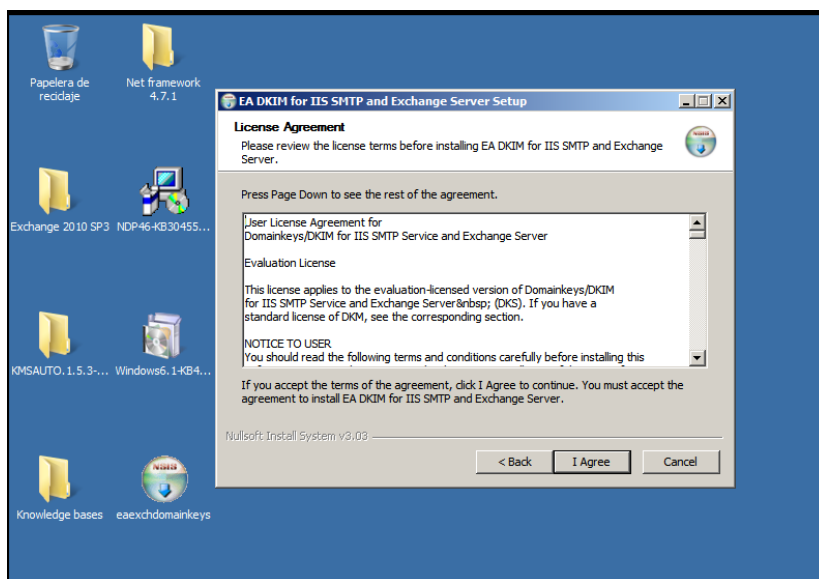
3. Implementación de mecanismos de defensa en servidor de correos Exchange.

3.1. Implementación de DKIM en servidor Exchange

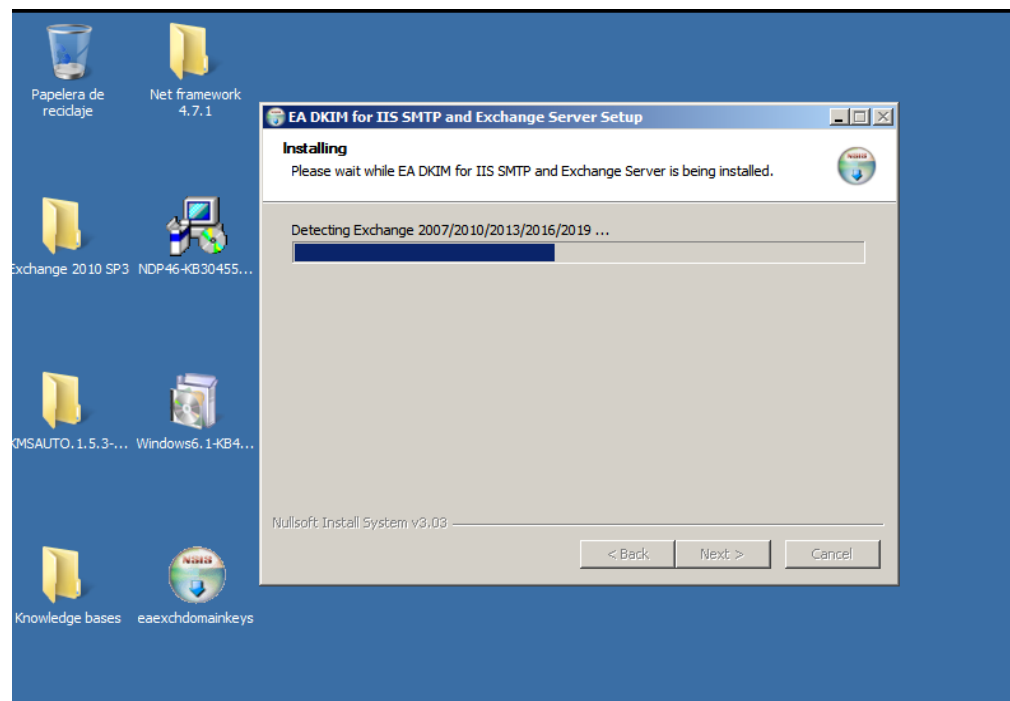
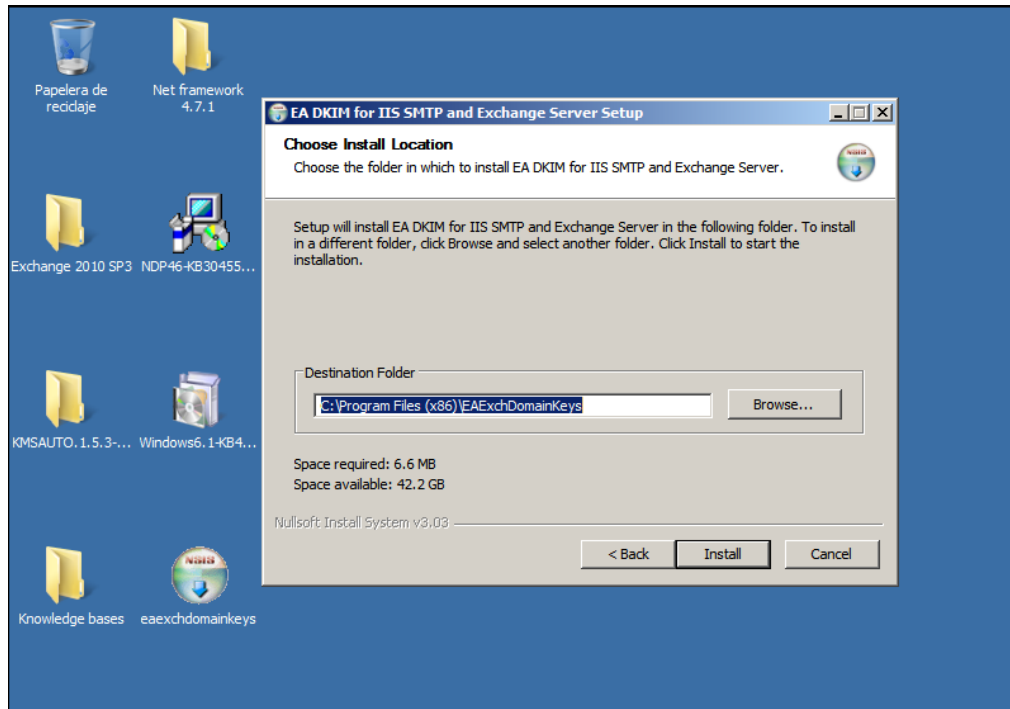
Para la instalación del dkim se procede a descargar el instalador desde el siguiente enlace: <https://www.emailarchitect.net/webapp/download/eaexchdomainkeys.exe>. Una vez descargado se procede a abrirlo. Después de ejecutarlo click en siguiente.



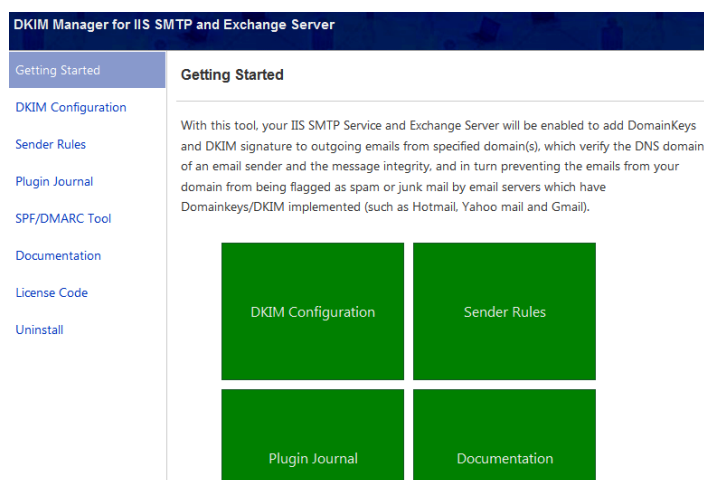
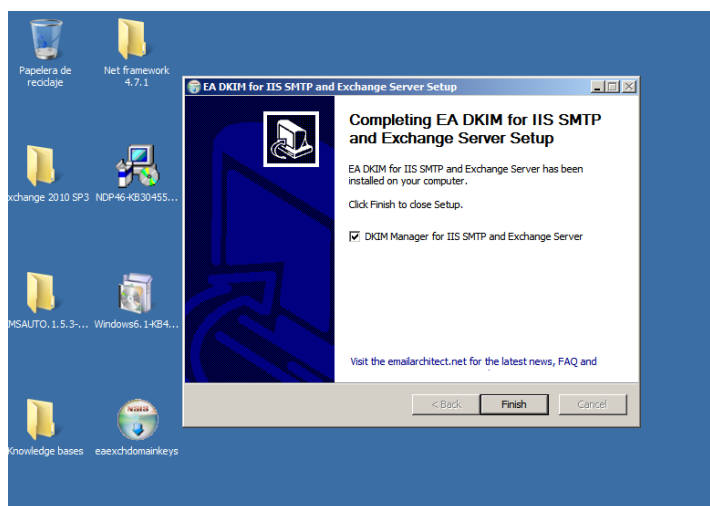
Se mostrará la siguiente pantalla en la cual se dará click en “I agree” para continuar con la instalación.



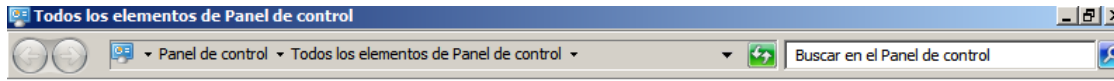
En la siguiente ventana, clic en “Install” sin modificar la ubicación de la instalación y esperamos que la instalación se cargue.



Para continuar dar clic en “Finish” para finalizar con la instalación de DKIM y se mostrará la siguiente ventana.

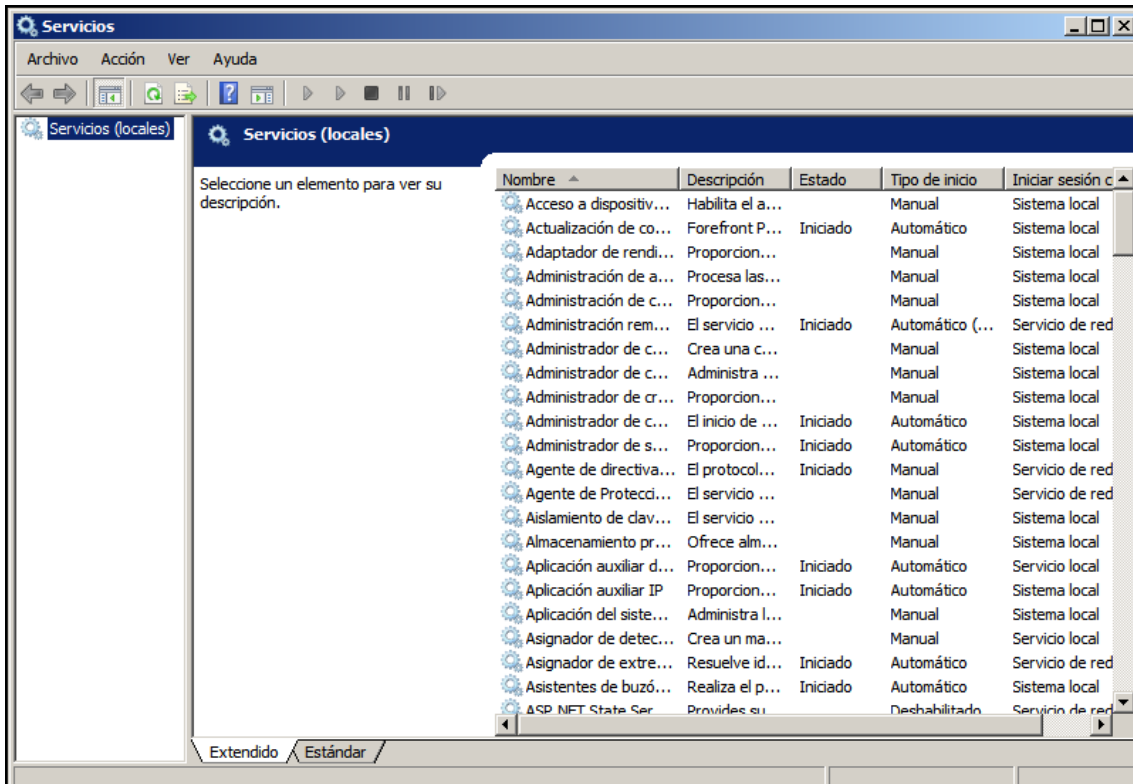


Una vez completada la instalación marcar “Servicio de transporte de Microsoft Exchange” y “Servicio de envío de correo de Microsoft Exchange” ubicándose en panel de control -> administrar servicios y verifique si esos servicios se están ejecutando, si esos servicios no se están ejecutando, inícielo.



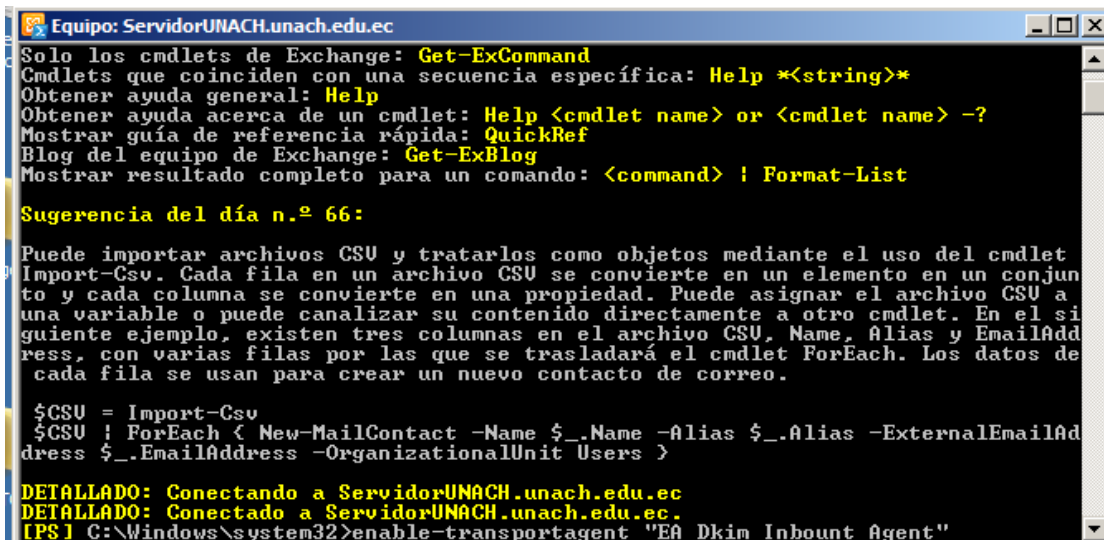
Ajustar la configuración del equipo

Ver por: Iconos grandes



En la siguiente ventana se muestra como desde la Shell de Exchange se habilita el agente de transporte entrante DKIM pues, el complemento DKIM sólo habilita el agente saliente al finalizar la instalación, realizarlo manualmente.

Comando: enable-transportagent "EA Dkim Inbound Agent"



```
Equipo: ServidorUNACH.unach.edu.ec
Solo los cmdlets de Exchange: Get-ExchangeCommand
Cmdlets que coinciden con una secuencia específica: Help *<string>*
Obtener ayuda general: Help
Obtener ayuda acerca de un cmdlet: Help <cmdlet name> or <cmdlet name> -?
Mostrar guía de referencia rápida: QuickRef
Blog del equipo de Exchange: Get-ExBlog
Mostrar resultado completo para un comando: <command> ! Format-List

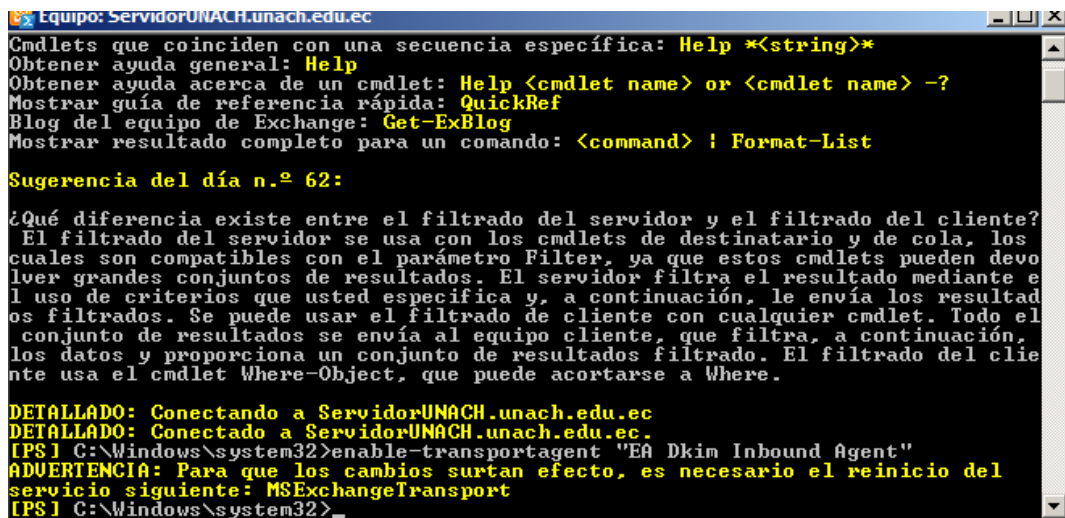
Sugerencia del día n.º 66:

Puede importar archivos CSV y tratarlos como objetos mediante el uso del cmdlet
Import-Csv. Cada fila en un archivo CSV se convierte en un elemento en un conjun
to y cada columna se convierte en una propiedad. Puede asignar el archivo CSV a
una variable o puede canalizar su contenido directamente a otro cmdlet. En el si
guiente ejemplo, existen tres columnas en el archivo CSV, Name, Alias y EmailAd
ress, con varias filas por las que se trasladará el cmdlet ForEach. Los datos de
cada fila se usan para crear un nuevo contacto de correo.

$CSV = Import-Csv
$CSV ! ForEach < New-MailContact -Name $_.Name -Alias $_.Alias -ExternalEmailAd
dress $_.EmailAddress -OrganizationalUnit Users >

DETALLADO: Conectando a ServidorUNACH.unach.edu.ec
DETALLADO: Conectado a ServidorUNACH.unach.edu.ec.
[PS] C:\Windows\system32>enable-transportagent "EA Dkim Inbound Agent"
```

Como se muestra en la ventana siguiente notifica el sistema que es necesario reiniciar el servicio.



```
Equipo: ServidorUNACH.unach.edu.ec
Cmdlets que coinciden con una secuencia específica: Help *<string>*
Obtener ayuda general: Help
Obtener ayuda acerca de un cmdlet: Help <cmdlet name> or <cmdlet name> -?
Mostrar guía de referencia rápida: QuickRef
Blog del equipo de Exchange: Get-ExBlog
Mostrar resultado completo para un comando: <command> ! Format-List

Sugerencia del día n.º 62:

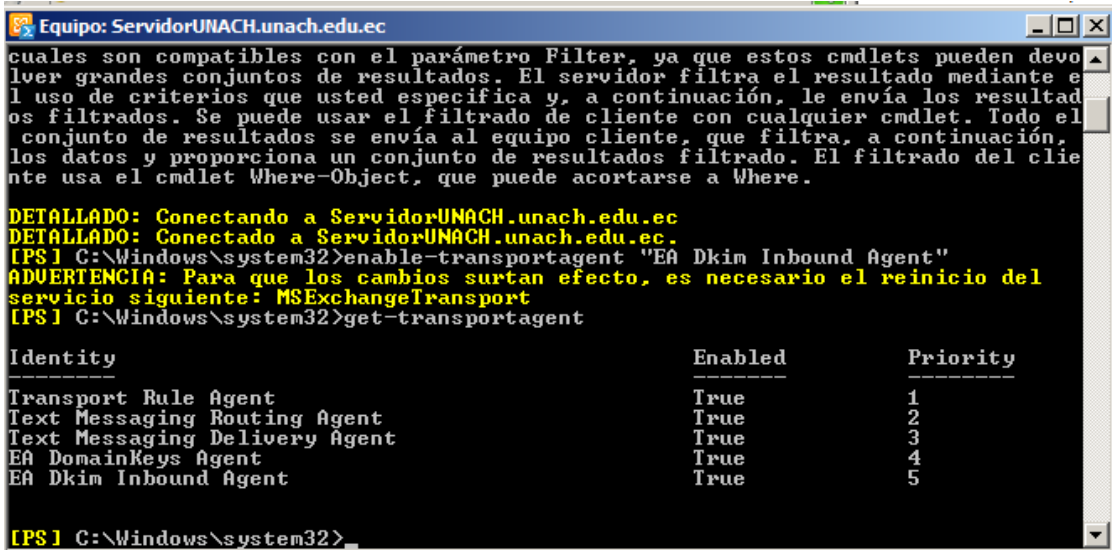
¿Qué diferencia existe entre el filtrado del servidor y el filtrado del cliente?
El filtrado del servidor se usa con los cmdlets de destinatario y de cola, los
cuales son compatibles con el parámetro Filter, ya que estos cmdlets pueden devo
lver grandes conjuntos de resultados. El servidor filtra el resultado mediante e
l uso de criterios que usted especifica y, a continuación, le envía los resultad
os filtrados. Se puede usar el filtrado de cliente con cualquier cmdlet. Todo el
conjunto de resultados se envía al equipo cliente, que filtra, a continuación,
los datos y proporciona un conjunto de resultados filtrado. El filtrado del clie
nte usa el cmdlet Where-Object, que puede acortarse a Where.

DETALLADO: Conectando a ServidorUNACH.unach.edu.ec
DETALLADO: Conectado a ServidorUNACH.unach.edu.ec.
[PS] C:\Windows\system32>enable-transportagent "EA Dkim Inbound Agent"
ADVERTENCIA: Para que los cambios surtan efecto, es necesario el reinicio del
servicio siguiente: MExchangeTransport
[PS] C:\Windows\system32>
```

Verificar que el servicio se añadió y se procede a reiniciar con los comandos descritos a continuación:

Comandos: get-transportagent

Restart-Service "MSExchangeTransport"

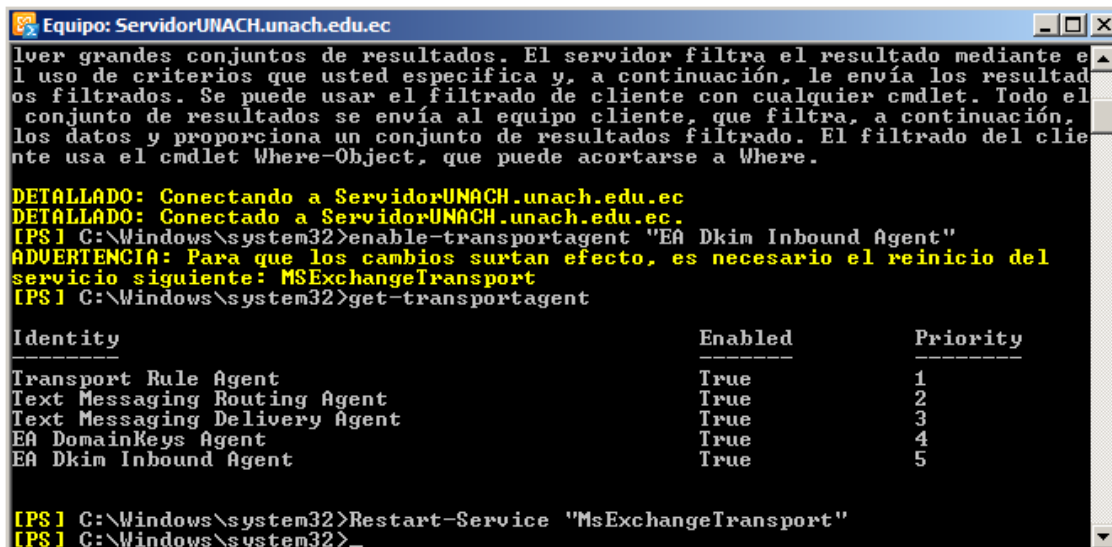


```
Equipo: ServidorUNACH.unach.edu.ec
cuales son compatibles con el parámetro Filter, ya que estos cmdlets pueden devolver grandes conjuntos de resultados. El servidor filtra el resultado mediante el uso de criterios que usted especifica y, a continuación, le envía los resultados filtrados. Se puede usar el filtrado de cliente con cualquier cmdlet. Todo el conjunto de resultados se envía al equipo cliente, que filtra, a continuación, los datos y proporciona un conjunto de resultados filtrado. El filtrado del cliente usa el cmdlet Where-Object, que puede acortarse a Where.

DETALLADO: Conectando a ServidorUNACH.unach.edu.ec
DETALLADO: Conectado a ServidorUNACH.unach.edu.ec.
[PS] C:\Windows\system32>enable-transportagent "EA Dkim Inbound Agent"
ADVERTENCIA: Para que los cambios surtan efecto, es necesario el reinicio del servicio siguiente: MSExchangeTransport
[PS] C:\Windows\system32>get-transportagent

Identity                               Enabled  Priority
-----                               -
Transport Rule Agent                   True     1
Text Messaging Routing Agent            True     2
Text Messaging Delivery Agent           True     3
EA DomainKeys Agent                     True     4
EA Dkim Inbound Agent                   True     5

[PS] C:\Windows\system32>
```



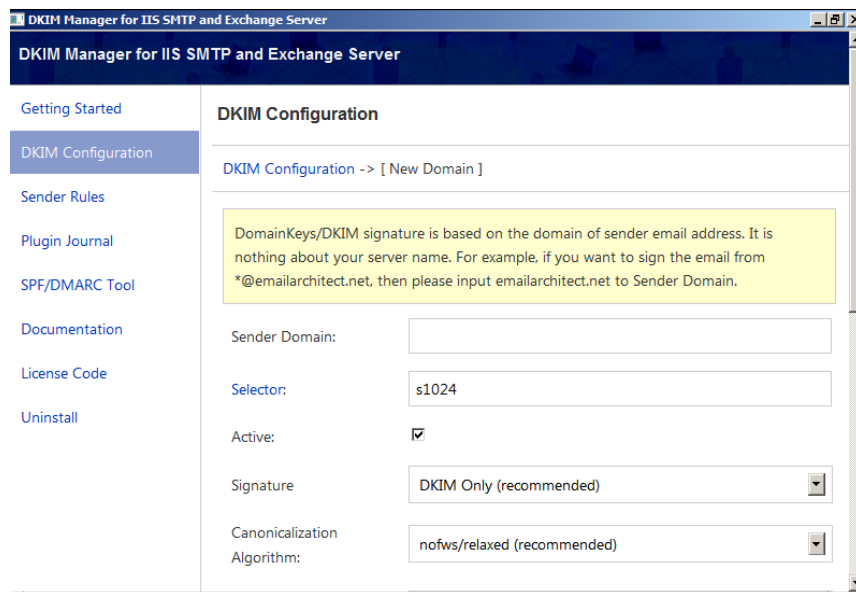
```
Equipo: ServidorUNACH.unach.edu.ec
lver grandes conjuntos de resultados. El servidor filtra el resultado mediante el uso de criterios que usted especifica y, a continuación, le envía los resultados filtrados. Se puede usar el filtrado de cliente con cualquier cmdlet. Todo el conjunto de resultados se envía al equipo cliente, que filtra, a continuación, los datos y proporciona un conjunto de resultados filtrado. El filtrado del cliente usa el cmdlet Where-Object, que puede acortarse a Where.

DETALLADO: Conectando a ServidorUNACH.unach.edu.ec
DETALLADO: Conectado a ServidorUNACH.unach.edu.ec.
[PS] C:\Windows\system32>enable-transportagent "EA Dkim Inbound Agent"
ADVERTENCIA: Para que los cambios surtan efecto, es necesario el reinicio del servicio siguiente: MSExchangeTransport
[PS] C:\Windows\system32>get-transportagent

Identity                               Enabled  Priority
-----                               -
Transport Rule Agent                   True     1
Text Messaging Routing Agent            True     2
Text Messaging Delivery Agent           True     3
EA DomainKeys Agent                     True     4
EA Dkim Inbound Agent                   True     5

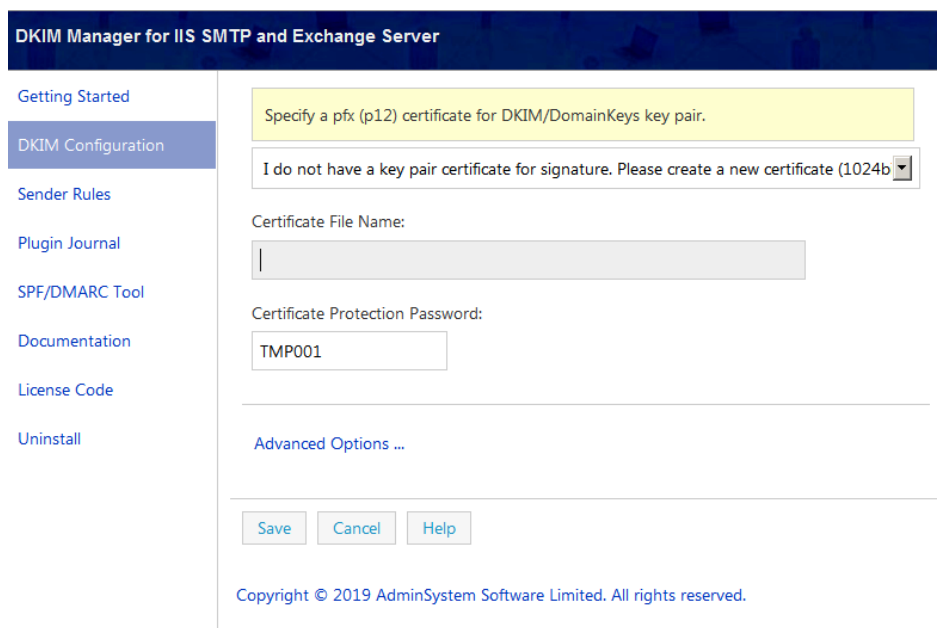
[PS] C:\Windows\system32>Restart-Service "MsExchangeTransport"
[PS] C:\Windows\system32>
```

Ahora para configurar el DKIM haga clic en “DKIM Cofiguration” y crear una nueva firma DKIM de dominio. La firma DKIM se basa en el dominio de la dirección de correo electrónico del remitente. No es nada sobre el nombre del servidor.

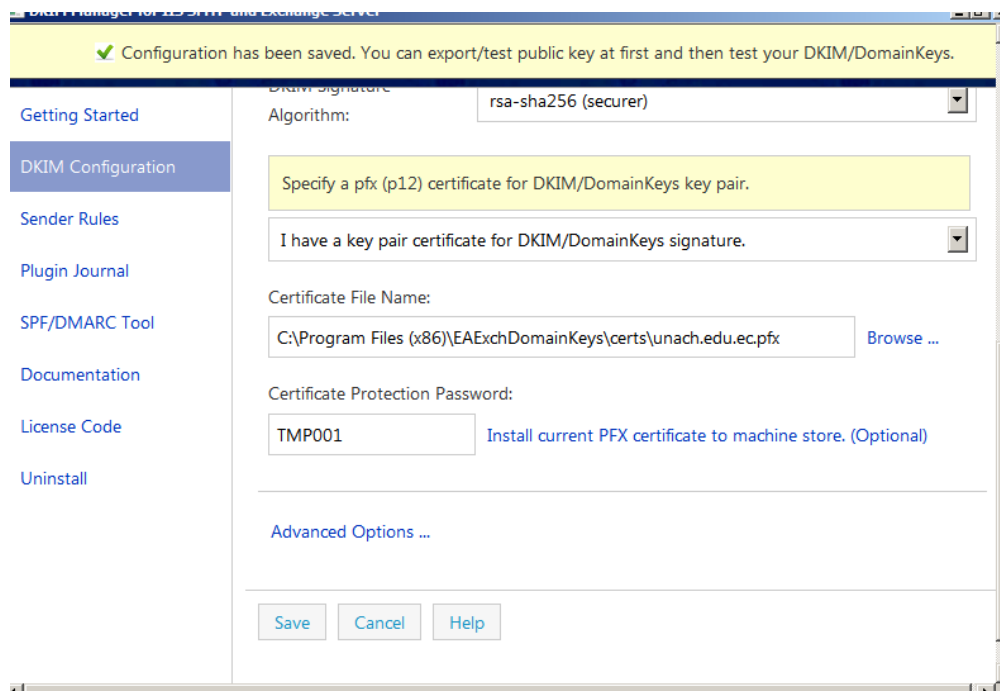


The screenshot shows the 'DKIM Manager for IIS SMTP and Exchange Server' application. The left sidebar contains navigation links: Getting Started, DKIM Configuration (selected), Sender Rules, Plugin Journal, SPF/DMARC Tool, Documentation, License Code, and Uninstall. The main content area is titled 'DKIM Configuration' and shows 'DKIM Configuration -> [New Domain]'. A yellow warning box states: 'DomainKeys/DKIM signature is based on the domain of sender email address. It is nothing about your server name. For example, if you want to sign the email from *@emailarchitect.net, then please input emailarchitect.net to Sender Domain.' Below this, the configuration fields are: Sender Domain (empty), Selector (s1024), Active (checked), Signature (DKIM Only (recommended)), and Canonicalization Algorithm (nofws/relaxed (recommended)).

Simplemente ingrese su dominio, use la configuración predeterminada para otros parámetros, finalmente haga clic en "Guardar" para crear su firma DKIM. En el caso que no tener debe usar el certificado emitido por autoridades de terceros, se recomienda utilizar el administrador DKIM para generar el certificado automáticamente.



The screenshot shows the 'DKIM Manager for IIS SMTP and Exchange Server' application. The left sidebar is the same as in the previous screenshot. The main content area is titled 'DKIM Configuration' and shows a yellow warning box: 'Specify a pfx (p12) certificate for DKIM/DomainKeys key pair.' Below this, a dropdown menu is set to 'I do not have a key pair certificate for signature. Please create a new certificate (1024b)'. The fields are: Certificate File Name (empty), Certificate Protection Password (TMP001), and an 'Advanced Options ...' link. At the bottom, there are 'Save', 'Cancel', and 'Help' buttons. The footer text reads: 'Copyright © 2019 AdminSystem Software Limited. All rights reserved.'



Como se muestra a continuación se ha creado la firma DKIM de dominio para el servidor. En este ejemplo el dominio es: unach.edu.ec

DKIM Configuration

[New](#) | [Edit](#) | [Delete](#) - Total 1 Domain(s)

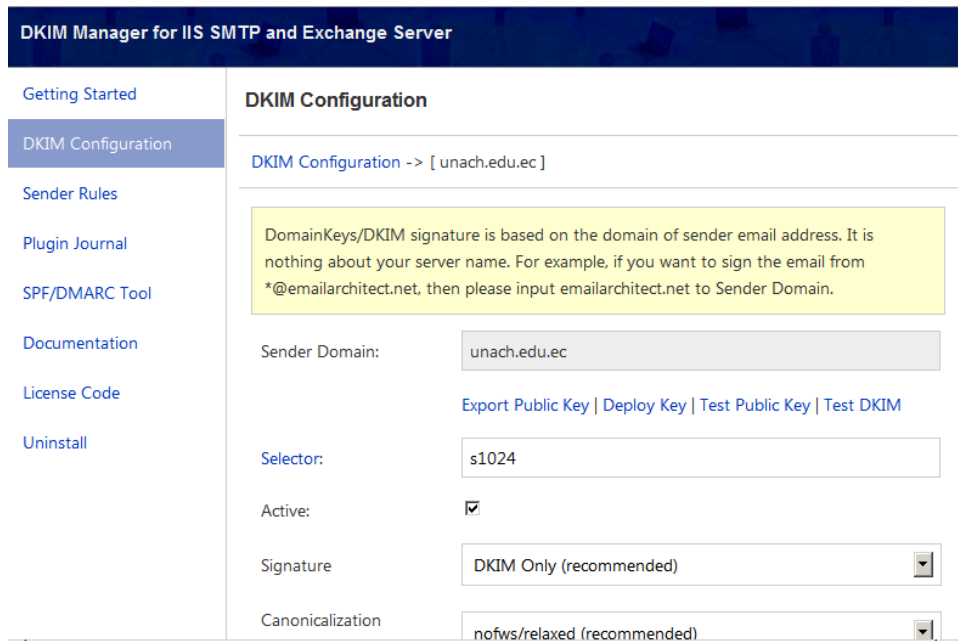
Filter: ALL - ALL - A - B - C - D - E - F - G - H - I - J - K - L - M - N - O - P - Q - R - S - T - U - V - W - X - Y - Z

<input type="checkbox"/>	Domain	Active
<input type="checkbox"/>	unach.edu.ec	✓

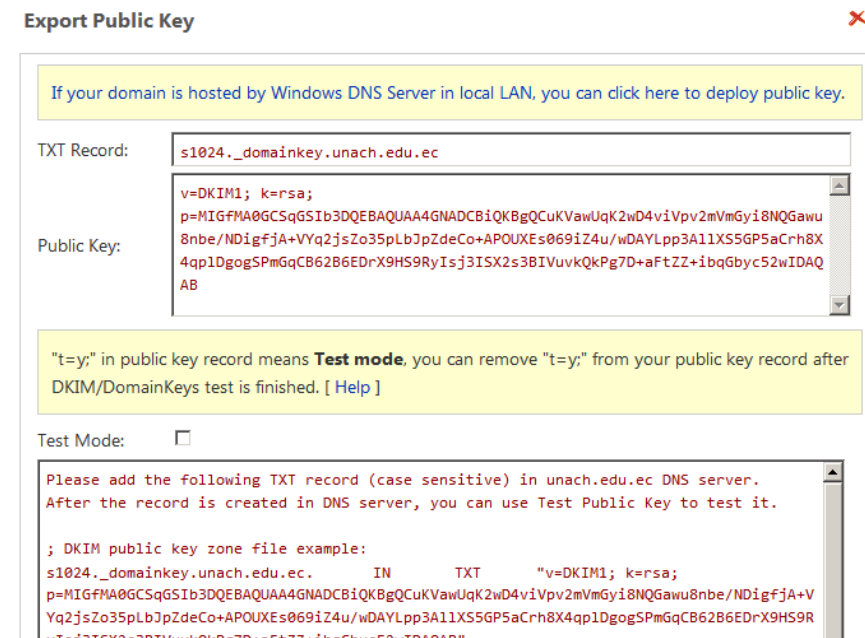
[New](#) | [Edit](#) | [Delete](#)

Copyright © 2019 AdminSystem Software Limited. All rights reserved.

Ahora el sistema de correo del destinatario debe consultar la clave pública para verificar la firma DKIM. Por lo tanto, necesitamos implementar la clave pública DKIM en el servidor DNS del dominio, luego el sistema del destinatario puede consultarla mediante el servidor DNS. Ahora volver al administrador de DKIM, seleccionar su dominio y clic en "Exportar clave pública":

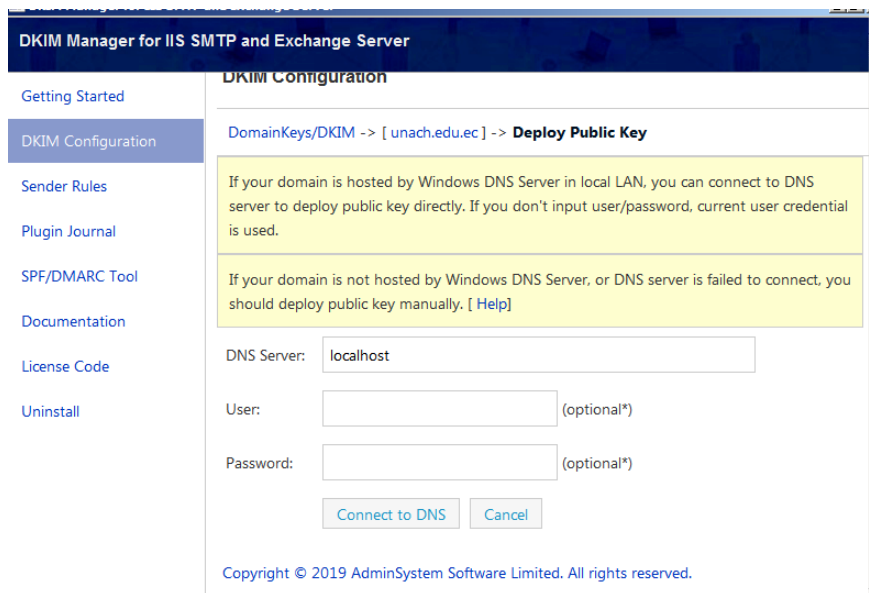


Aparecerá una ventana que mostrará una clave pública y un registro TXT para la implementación en su servidor DNS.

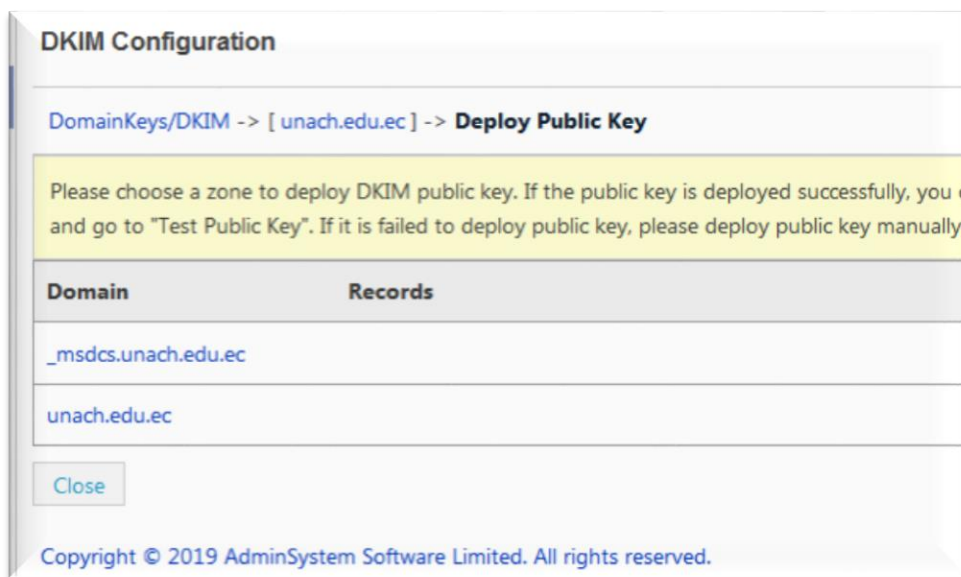


Si su dominio está alojado en el servidor DNS de Windows en la LAN local, después de agregar un dominio en DKIM Plugin Manager, puede seleccionar el dominio y hacer clic en

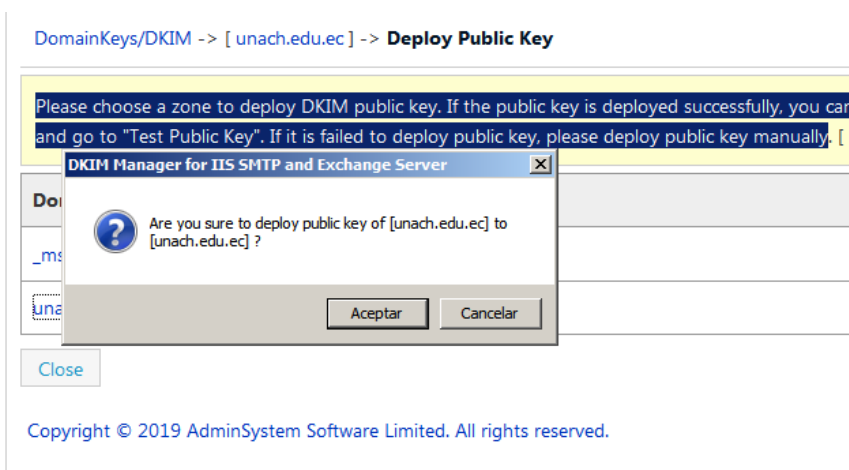
"Implementar clave", ingresar su dirección de servidor DNS y elegir la zona DNS, la clave pública se implementará en el servidor DNS automáticamente.



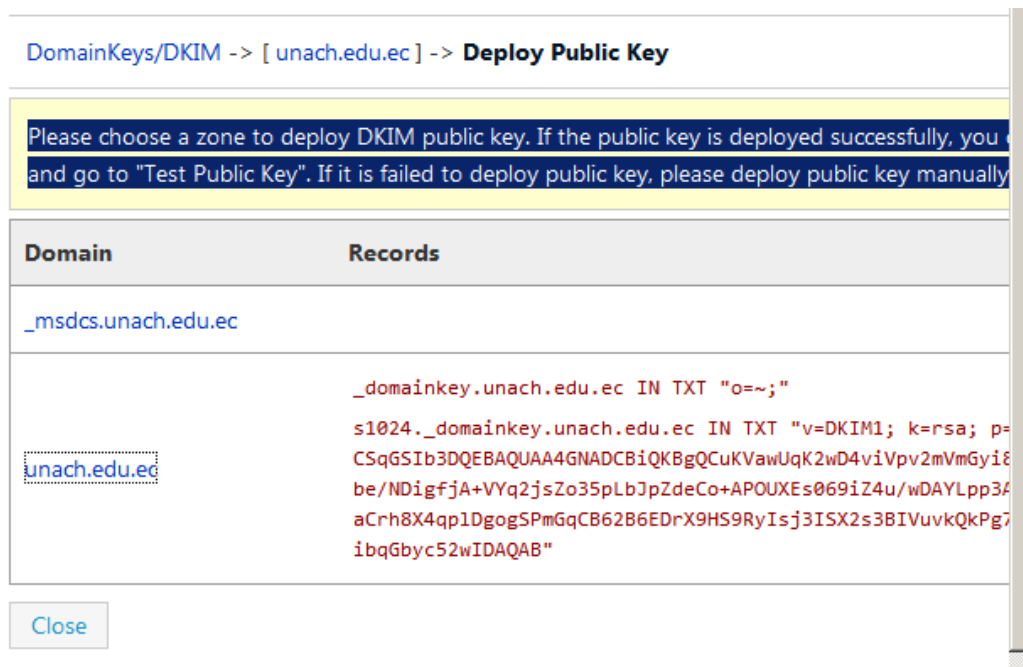
En la ventana siguiente se puede observar que se la clave pública se ha añadió satisfactoriamente.



Abrir la clave publica y damos en aceptar en el cuadro de dialogo que aparecerá.



Después de realizada la implementación de la clave pública, verificarsi esta se añadió a nuestro dominio.



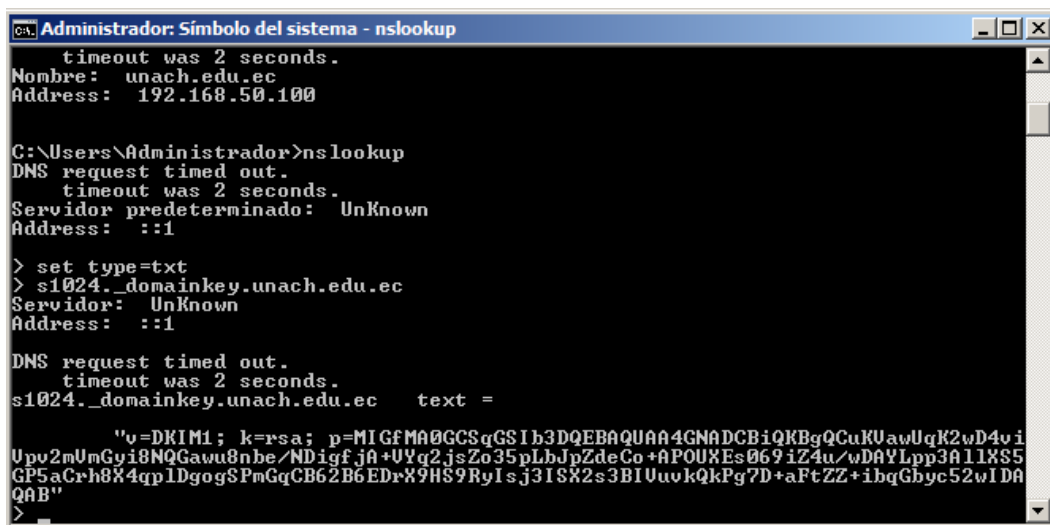
3.1. Comprobación de implementación DKIM

Después de añadir la clave pública procedemos a probarla con a través del cmd.

Comandos: nslookup

set type=txt

s1024._domainkey.sudominio



```
Administrador: Símbolo del sistema - nslookup
timeout was 2 seconds.
Nombre: unach.edu.ec
Address: 192.168.50.100

C:\Users\Administrador>nslookup
DNS request timed out.
timeout was 2 seconds.
Servidor predeterminado: UnKnown
Address: ::1

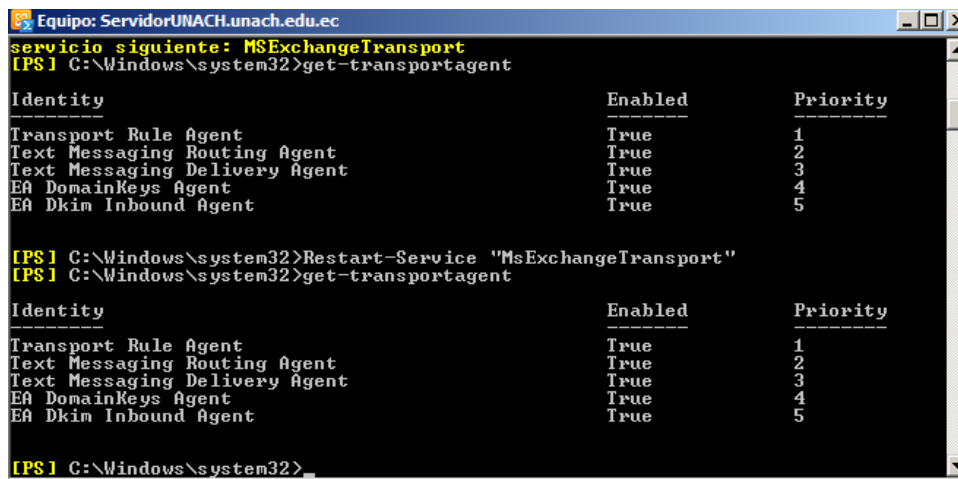
> set type=txt
> s1024._domainkey.unach.edu.ec
Servidor: UnKnown
Address: ::1

DNS request timed out.
timeout was 2 seconds.
s1024._domainkey.unach.edu.ec text =

"v=DKIM1; k=rsa; p=MI GfMA0GCSqGS l b3DQEBaQUAA4GNADCBi QKBgQCuKU awUqK2wD4v i
Uvu2mUmGyi8NQGawu8nbe /ND igf jA +U Yq2 js Zo35 pLbJpZde Co +A POU XEs069 iZ4u /wDAY Lpp3A l l X S5
GP5a Cr h8 X 4 q p l D g o g S P m G q C B 6 2 B 6 E D r X 9 H S 9 R y I s j 3 I S X 2 s 3 B I U u v k Q k P g 7 D + a F t Z Z + i b q G b y c 5 2 w I D A
Q A B"
```

Verificar la instalación del agente de transporte de Exchange, esto lo haremos a través de la shell de administración de Exchange.

Comando: get-transportagent



```
Equipo: ServidorUNACH.unach.edu.ec
servicio siguiente: MsExchangeTransport
[PS] C:\Windows\system32>get-transportagent

Identity                               Enabled      Priority
-----                               -
Transport Rule Agent                   True         1
Text Messaging Routing Agent           True         2
Text Messaging Delivery Agent          True         3
EA DomainKeys Agent                    True         4
EA Dkim Inbound Agent                  True         5

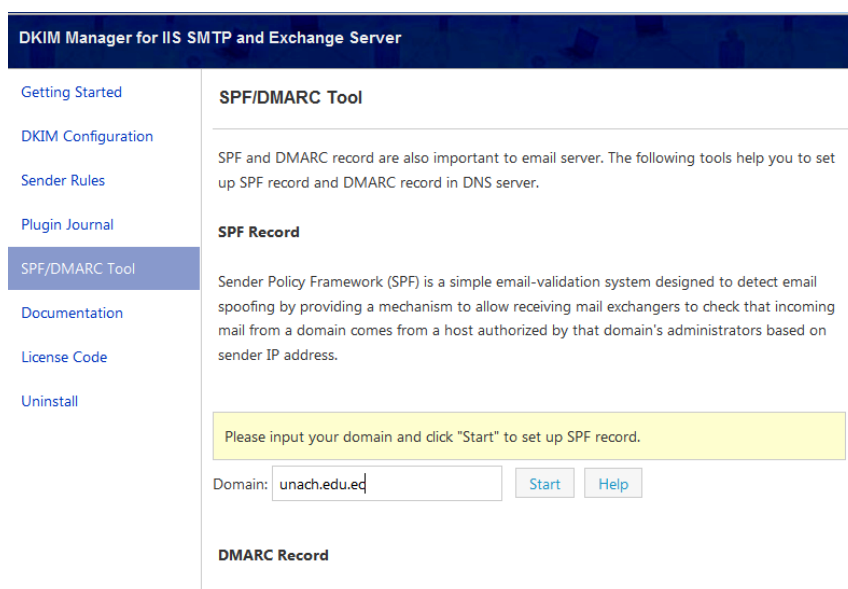
[PS] C:\Windows\system32>Restart-Service "MsExchangeTransport"
[PS] C:\Windows\system32>get-transportagent

Identity                               Enabled      Priority
-----                               -
Transport Rule Agent                   True         1
Text Messaging Routing Agent           True         2
Text Messaging Delivery Agent          True         3
EA DomainKeys Agent                    True         4
EA Dkim Inbound Agent                  True         5

[PS] C:\Windows\system32>
```

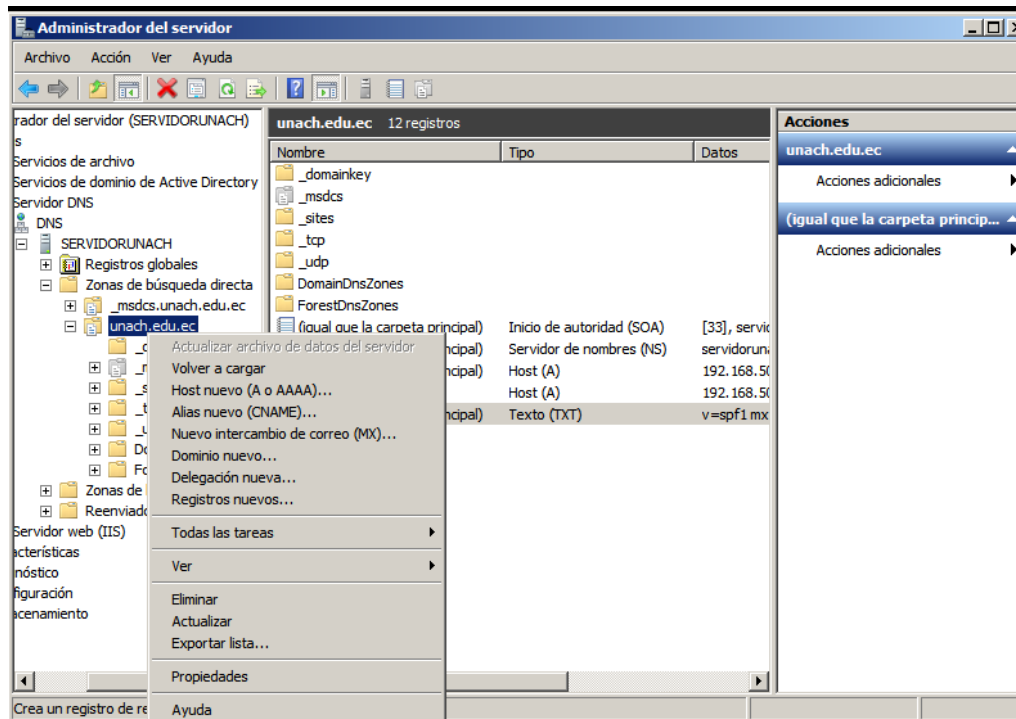
3.2. Implementación SPF

Para continuar con la configuración del SPF se deberá abrir DKIM Manager después se dirige a la opción SPF / DMARC Tool" continuando con "SPF" estado en esta opción se ingresa el dominio y hacer clic en "Inicio"

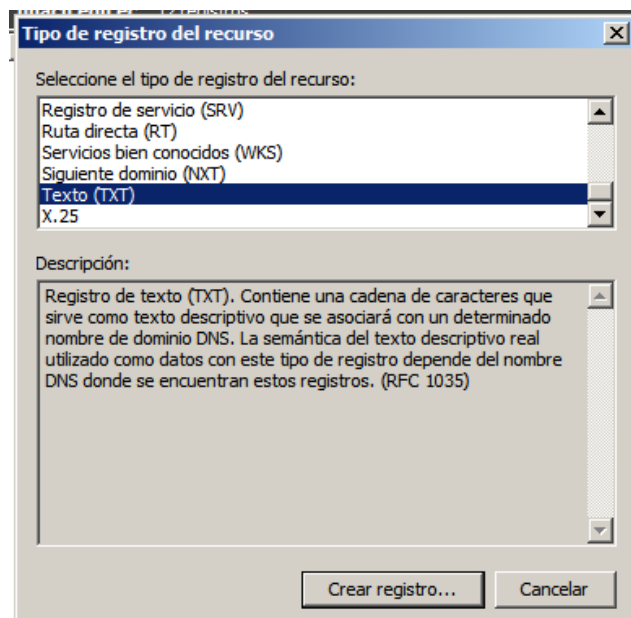


Nota: si nuestro servidor está conectado a Internet el sistema lo implementará automáticamente, caso contrario se lo debe realizar manualmente. Se recomienda implementar manualmente de acuerdo a las necesidades de cada administrador de servidor de correos.

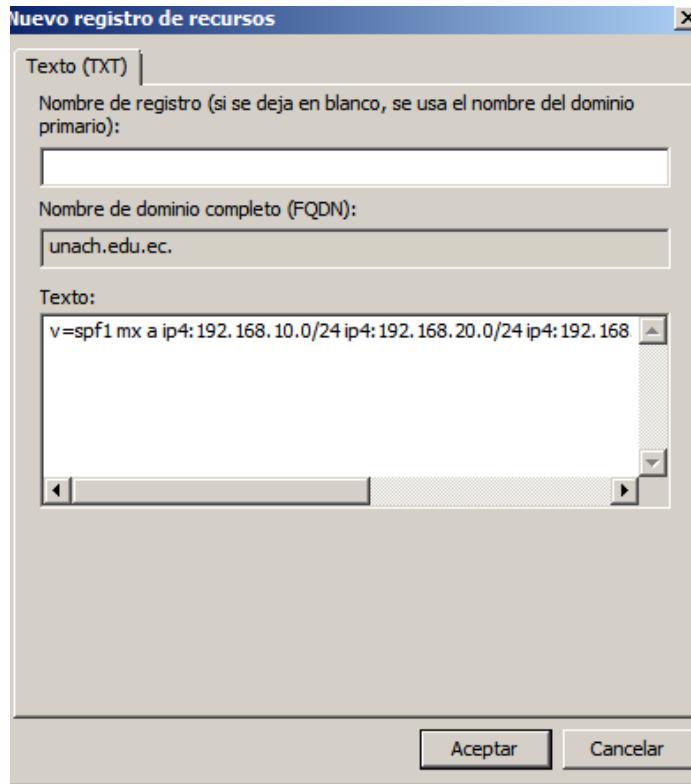
Abrir el servidor DNS -> seleccionar el dominio al que desea agregar un registro SPF, dar clic con el botón derecho en la lista de registros y seleccione "registros nuevos" en el menú de opciones.



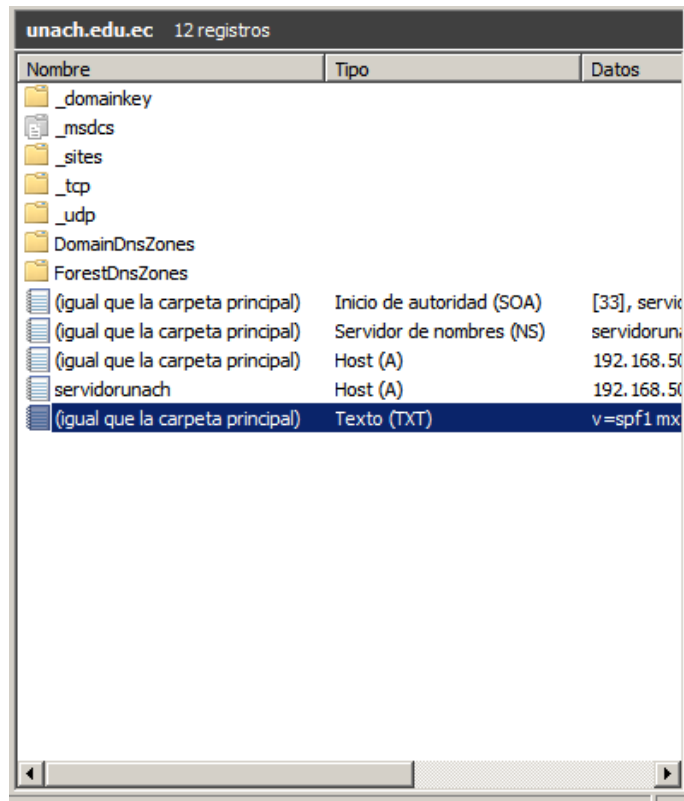
Seleccione el tipo de registro de texto (TXT) y clic en el botón "Crear registro".



Copie el valor (v = spf1) del valor de registro y péguelo en el cuadro de texto "texto" y no ingrese nada en "Nombre de registro". Clic en el botón Aceptar.



Como se puede observar el registro se ha creado satisfactoriamente.

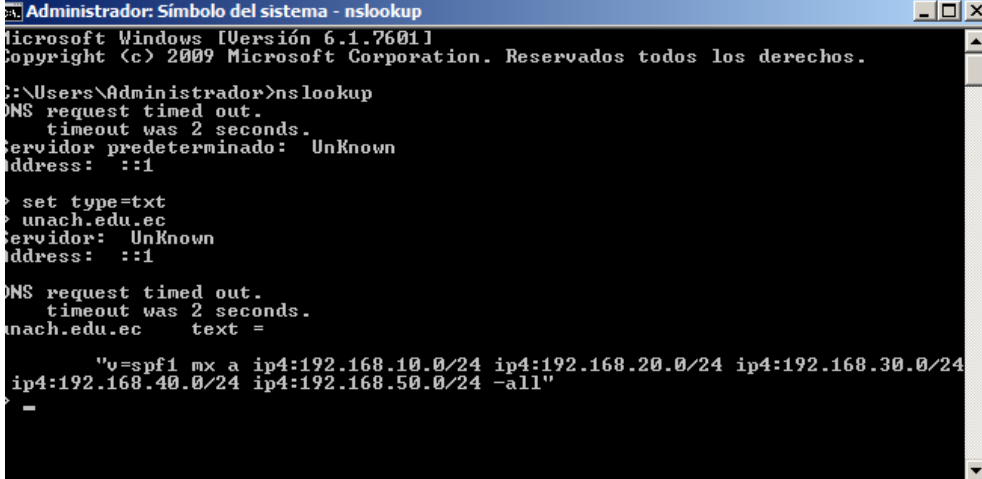


3.2.1. Comprobación de implementación SPF

Después de añadir el registro procedemos a comprobar a través del cmd.

Comandos: nslookup

sudominio



```
Administrador: Símbolo del sistema - nslookup
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\Administrador>nslookup
DNS request timed out.
  timeout was 2 seconds.
Servidor predeterminado: UnKnown
Address: ::1

> set type=txt
type=txt
> unach.edu.ec
Servidor: UnKnown
Address: ::1

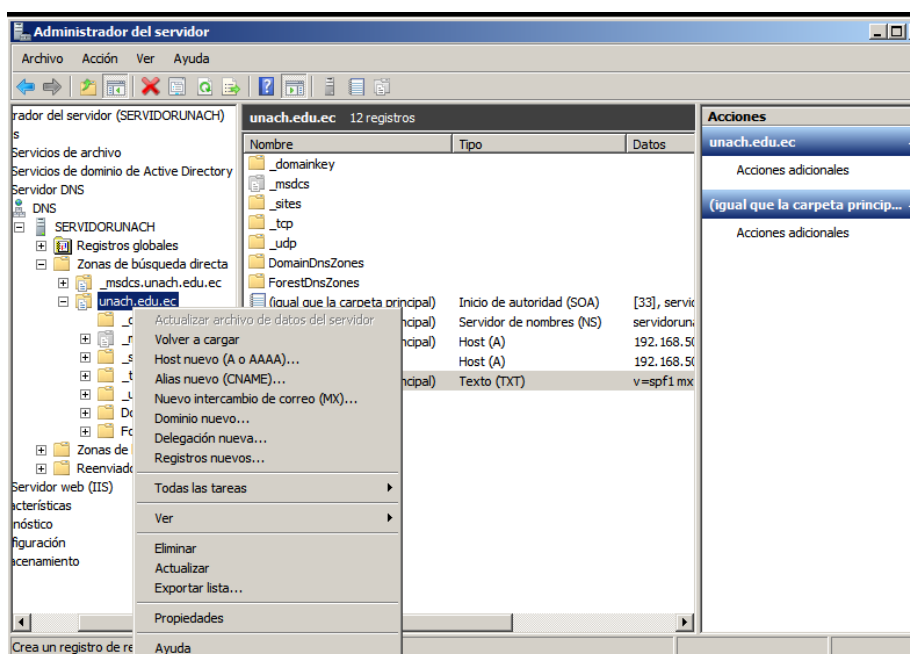
DNS request timed out.
  timeout was 2 seconds.
unach.edu.ec    text =

        "v=spf1 mx a ip4:192.168.10.0/24 ip4:192.168.20.0/24 ip4:192.168.30.0/24
ip4:192.168.40.0/24 ip4:192.168.50.0/24 -all"
>
```

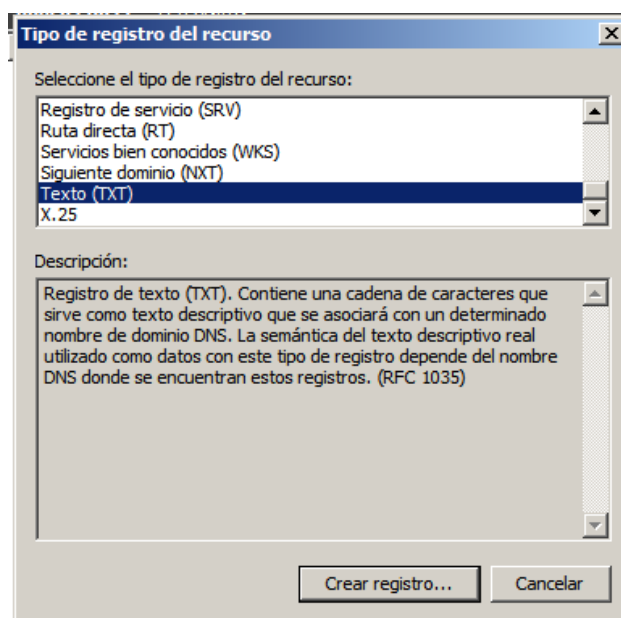
Se observa en la imagen anterior que con satisfacción el registro SPF se ha implementado, ya que automáticamente lo reconoce.

3.3. Implementación DMARC

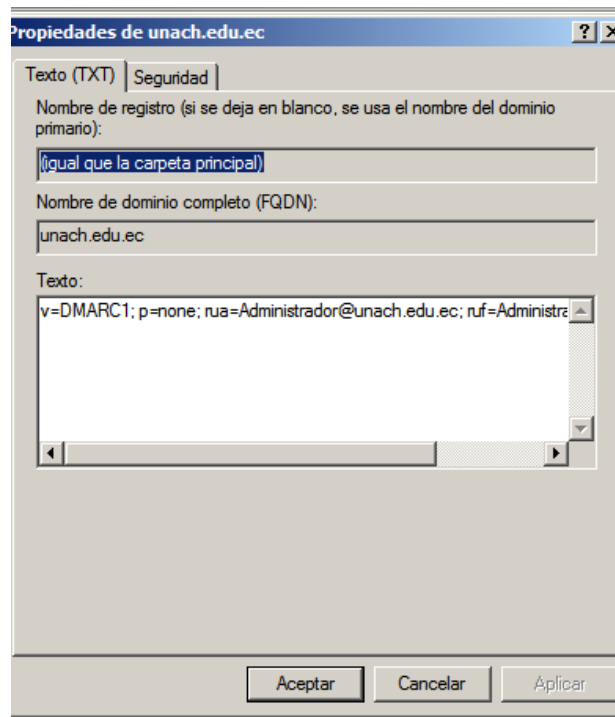
Seleccionar y abrir en el servidor DNS y el dominio en el que se desea agregar un registro DMARC. Clic con el botón derecho en la lista de registros y seleccione "registros nuevos." en el menú de opciones.



Seleccione el tipo de registro de texto (TXT) y haga clic en el botón "Crear registro".

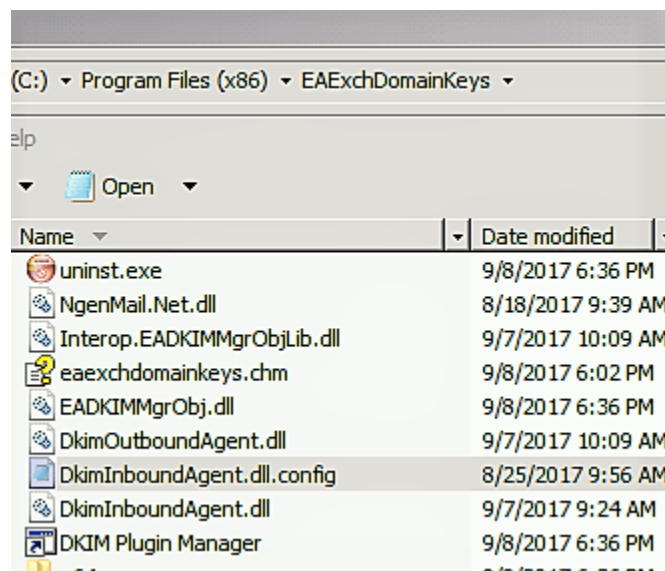


Copie el valor (v = DMARC1) del Valor de registro y péguelo en el cuadro de texto "Texto" e ingrese "_dmarc" en Nombre de registro. Clic en el botón "Aceptar".



3.3.1. Comprobación de los mecanismos de defensa aplicando las políticas DMARC

Para la comprobación de la correcta implementación de las políticas DMARC, independientemente de cómo se haya implementado ya sea con la herramienta o manualmente. Se procede a ir al directorio raíz de instalación de EAExchDomainKeys por defecto está en:



C:\Archivos de Programa(x86)\EAExchDomainKeys.

Una vez en este directorio, abrir el archivo “*DkimInboundAgent.dll.config*” con un editor de texto. A continuación, se puede observar el contenido predeterminado del archivo de configuración:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
<configSections>
  <section name="spfResultToReject" type="System.Configuration.AppSettingsSection,
System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
  <section name="ignoredGatewayIPAddressesForSpfCheck"
type="System.Configuration.AppSettingsSection, System.Configuration, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
  <section name="ignoredGatewayNameForSpfCheck"
type="System.Configuration.AppSettingsSection, System.Configuration, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
  <section name="ignoreSpfResultDomains" type="System.Configuration.AppSettingsSection,
System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />

  <section name="dkimResultToReject" type="System.Configuration.AppSettingsSection,
System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
  <section name="ignoreBodyHashErrorDomains"
type="System.Configuration.AppSettingsSection, System.Configuration, Version=4.0.0.0,
Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
  <section name="ignoreDkimResultDomains" type="System.Configuration.AppSettingsSection,
System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />

  <section name="dmarcResultToReject" type="System.Configuration.AppSettingsSection,
System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
  <section name="ignoreDmarcResultDomains" type="System.Configuration.AppSettingsSection,
System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />

  <section name="blockedIPAddresses" type="System.Configuration.AppSettingsSection,
System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
  <section name="blockedSenderOrHeloDomain" type="System.Configuration.AppSettingsSection,
System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />

  <section name="trustedIPAddresses" type="System.Configuration.AppSettingsSection,
System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
  <section name="trustedSenderOrDomain" type="System.Configuration.AppSettingsSection,
System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" />
</configSections>

<spfResultToReject>
  <!--
  <add key="fail" value="550 5.7.1 your message from [%source_ip%] is against our SPF
policy (fail)" />
  <add key="softfail" value="550 5.7.1 your message from [%source_ip%] is against our SPF
policy (softfail)" />
  <add key="none" value="550 5.7.1 your message from [%source_ip%] is against our SPF
policy (none)" />
  <add key="neutral" value="550 5.7.1 your message from [%source_ip%] is against our SPF
policy (neutral)" />
  <add key="temperror" value="451 4.4.3 your message from [%source_ip%] encountered a
temporal error with SPF verification (temperror)" />
  <add key="permerror" value="550 5.7.1 your message from [%source_ip%] encountered a
permanent error with SPF verification (permerror)" />
  -->
</spfResultToReject>
```



```
-->
</spfResultToReject>

<!--
  ignoredGatewayIPAddressesForSpfCheck:

  If your Exchange server is behind of a gateway/MTA,
  the SPF check will be incorrect due to original IP address is hidden by gateway or MTA.

  You can add your gateway/MTA IP address to skip the gateway IP/domain to detect original
  IP address/helo domain from message headers.

  CIDR syntax is supported in IP address.
-->
<ignoredGatewayIPAddressesForSpfCheck>
  <!--
  <add key="192.168.0.8" value="ignore"/>
  -->
</ignoredGatewayIPAddressesForSpfCheck>

<!--
  ignoredGatewayNameForSpfCheck:

  If your Exchange server is behind of a gateway/MTA,
  the SPF check will be incorrect due to original IP address/helo domain is hidden by
  gateway or MTA.

  You can add your gateway/MTA name to skip the gateway IP/domain to detect original IP
  address/helo domain from message headers.

  You can use regular expression like this "/^emailarchitect\.(net|com)$/"

  "/^emailarchitect\.(net|com)$/" matches "emailarchitect.net" and "emailarchitect.com"

  "/.?emailarchitect\.net$/" matches "*.emailarchitect.net" and "emailarchitect.net"
-->
<ignoredGatewayNameForSpfCheck>
  <!--
  <add key="dispatch.gateway.net" value="ignore"/>
  -->
</ignoredGatewayNameForSpfCheck>

<!--
  ignoreSpfResultDomains does not take effect to the following domains even the result
  matches spfResultToReject

  You can use regular expression like this "/^emailarchitect\.(net|com)$/"

  "/^emailarchitect\.(net|com)$/" matches "emailarchitect.net" and "emailarchitect.com"

  "/.?emailarchitect\.net$/" matches "*.emailarchitect.net" and "emailarchitect.net"
-->
<ignoreSpfResultDomains>
  <!--
  <add key="emailarchitect.net" value="ignore"/>
  -->
</ignoreSpfResultDomains>

<dkimResultToReject>
```

```
<!--
  <add key="fail" value="550 5.7.1 your message from [%header_from%] is against our DKIM
policy (fail)" />
  <add key="none" value="550 5.7.1 your message from [%header_from%] is against our DKIM
policy (none)" />
  <add key="neutral" value="550 5.7.1 your message from [%header_from%] is against our
DKIM policy (neutral)" />
  <add key="temperror" value="451 4.4.3 your message from [%header_from%] encountered a
temporal error with DKIM verification (temperror)" />
  <add key="permerror" value="550 5.7.1 your message from [%header_from%] encountered a
permanent error with DKIM verification (permerror)" />
-->
</dkimResultToReject>
```

```
<!--
  ignoreBodyHashErrorDomains:

  If the sender or signer domain is in the ignoreBodyHashErrorDomains list, body hash
error with DKIM verification is ignored, only the signature is verified.

  Office 365 default DKIM signature has a common body hash error problem, so you can add
./.?onmicrosoft.com$/ to bypass body hash check for office 365.

  you can use regular expression like this "/^emailarchitect\.(net|com)$/"

  "/^emailarchitect\.(net|com)$/" matches "emailarchitect.net" and "emailarchitect.com"

  "/.?emailarchitect\.net$/" matches "*.emailarchitect.net" and "emailarchitect.net"
-->
```

```
<ignoreBodyHashErrorDomains>
<!--
  <add key="/.?onmicrosoft.com$/" value="ignore"/>
-->
</ignoreBodyHashErrorDomains>
```

```
<!--
  ignoreDkimResultDomains does not take effect to the following domains even the result
matches dkimResultToReject

  You can use regular expression like this "/^emailarchitect\.(net|com)$/"

  "/^emailarchitect\.(net|com)$/" matches "emailarchitect.net" and "emailarchitect.com"

  "/.?emailarchitect\.net$/" matches "*.emailarchitect.net" and "emailarchitect.net"
-->
```

```
<ignoreDkimResultDomains>
<!--
  <add key="emailarchitect.net" value="ignore"/>
-->
</ignoreDkimResultDomains>
```

```
<dmARCResultToReject>
<!--
  <add key="fail" value="550 5.7.1 your message from [%header_from%] is against our DMARC
policy (fail)" />
  <add key="none" value="550 5.7.1 your message from [%header_from%] is against our DMARC
policy (none)" />
  <add key="temperror" value="451 4.4.3 your message from [%header_from%] encountered a
temporal error with DMARC verification (temperror)" />
-->
```

```
    <add key="permerror" value="550 5.7.1 your message from [%header_from%] encountered a
    permanent error with DMARC verification (permerror)" />
    -->
</dmarcResultToReject>
```

```
<!--
    ignoreDmarcResultDomains does not take effect to the following domains even the result
    matches dmarcResultToReject
```

```
    you can use regular expression like this "/^emailarchitect\.(net|com)$/"
```

```
    "/^emailarchitect\.(net|com)$/" matches "emailarchitect.net" and "emailarchitect.com"
```

```
    "/.?emailarchitect\.net$/" matches "*.emailarchitect.net" and "emailarchitect.net"
```

```
    -->
```

```
<ignoreDmarcResultDomains>
```

```
<!--
```

```
    <add key="emailarchitect.net" value="ignore"/>
```

```
    -->
```

```
</ignoreDmarcResultDomains>
```

```
<!--
```

```
bLockedIPAddresses:
```

```
The email from the following IP address(es) will be rejected directly regardless of SPF/DKIM
result.
```

```
CIDR syntax is supported in IP address.
```

```
    -->
```

```
<blockedIPAddresses>
```

```
<!--
```

```
    <add key="127.0.0.2" value="550 5.7.1 your message from [%source_ip%] is in our black
    list." />
```

```
    <add key="192.168.0.0/24" value="550 5.7.1 your message from [%source_ip%] is in our
    black list." />
```

```
    -->
```

```
</blockedIPAddresses>
```

```
<!--
```

```
bLockedSenderOrHeLoDomain
```

```
The email from (SMTP MAIL FROM or HELO DOMAIN) the following address(es)/domain(s) will be
rejected directly regardless of SPF/DKIM result.
```

```
    -->
```

```
<blockedSenderOrHeLoDomain>
```

```
<!--
```

```
    You can use regular expression like this: "/^(support/sales)@emailarchitect\.net$/"
```

```
    "/^(support/sales)@emailarchitect\.net$/" matches "support@emailarchitect.net" and
    "sales@emailarchitect.net".
```

```
    "/^[^@]+@emailarchitect\.net$/" matches "*@emailarchitect.net"
```

```
    -->
```

```
<!--
```

```
    <add key="faked-emailarchitect.net" value="550 5.7.1 your message from
    [%bLocked_domainOrAddress%] is in our black list." />
```

```
    <add key="spoof@faked-emailarchitect.net" value="550 5.7.1 your message from
    [%bLocked_domainOrAddress%] is in our black list." />
```

```
    -->
```

```
</blockedSenderOrHeLoDomain>
```

```

<!--
trustedIPAddresses:

The email from the following IP address(es) will be accepted directly regardless of SPF/DKIM
result.
CIDR syntax is supported in IP address.
-->
<trustedIPAddresses>
  <add key="127.0.0.1" value="pass"/>
  <add key="::1" value="pass"/>
  <!--
  <add key="192.168.0.0/24" value="pass"/>
  -->
</trustedIPAddresses>

<!--
trustedSenderOrDomain:

The email from (rfc822.header.from) the following address(es)/domain(s) will be accepted
directly regardless of SPF/DKIM result.
-->
<trustedSenderOrDomain>
  <!--
    You can use regular expression like this: "/^(support/sales)@emailarchitect\.net$/"

    "/^(support/sales)@emailarchitect\.net$/" matches "support@emailarchitect.net" and
    "sales@emailarchitect.net".

    "/^[^@]+@emailarchitect\.net$/" matches "*@emailarchitect.net"
  -->
  <!--
  <add key="support@emailarchitect.net" value="pass"/>
  <add key="emailarchitect.net" value="pass"/>
  -->
</trustedSenderOrDomain>

<appSettings>
  <add key ="LogLevel" value="OnlyError"/>
  <!-- <add key ="LogLevel" value="FullDebug"/> -->
  <add key ="trackingSender" value="*"/>
  <add key ="trackingSourceIP" value="*"/>
  <add key ="useLastExternalIPAddress" value="false"/>
  <!-- System default DNS server is used by default, you don't have to set this value
manually
  If you want to use specified DNS server address, you must input DNS server IP address.
  For example, you can use 8.8.8.8 (Google Public DNS Server) as the DNS server address.
-->
  <add key ="dnsServerAddress" value=""/>
</appSettings>
</configuration>

```

En el que se debe modificar el agente de transporte entrante, cambiar la siguiente línea:

```
<add key="LogLevel" value="OnlyError"/>
```

por:

```
<add key="LogLevel" value="FullDebug"/>
```

Rechazar correos electrónicos basado en DKIM / SPF / DMARC en el servicio SMTP

Aunque se puede usar los resultados de autenticación para filtrar el correo electrónico a la carpeta de correo no deseado, este consume recursos y almacenamiento del servidor. Por lo tanto, la mejor manera es rechazar el correo electrónico en el servicio SMTP directamente en función de los resultados de autenticación.

- Para rechazar el correo electrónico contra la política de SPF, puede cambiar la sección: spfResultToReject.
- Para rechazar el correo electrónico en contra de la política DKIM, puede cambiar la sección dkimResultToReject.
- Para rechazar el correo electrónico contra la política de DMARC, puede cambiar la sección: dmarcResultToReject.

A continuación, se observará la configuración predeterminada para rechazar correos en configuración de bajo nivel:

```
<spfResultToReject>
  <add key="fail" value="550 5.7.1 your message from [%source_ip%] is against our SPF
policy (fail)" />
  <add key="softfail" value="550 5.7.1 your message from [%source_ip%] is against our SPF
policy (softfail)" />
</spfResultToReject>

<dkimResultToReject>
  <add key="fail" value="550 5.7.1 your message from [%header_from%] is against our DKIM
policy (fail)" />
</dkimResultToReject>

<dmarcResultToReject>
  <add key="fail" value="550 5.7.1 your message from [%header_from%] is against our DMARC
policy (fail)" />
</dmarcResultToReject>
```

Configuración de nivel medio:

```
<spfResultToReject>
  <add key="fail" value="550 5.7.1 your message from [%source_ip%] is against our SPF
policy (fail)" />
  <add key="softfail" value="550 5.7.1 your message from [%source_ip%] is against our SPF
policy (softfail)" />
  <add key="none" value="550 5.7.1 your message from [%source_ip%] is against our SPF
policy (none)" />
  <add key="neutral" value="550 5.7.1 your message from [%source_ip%] is against our SPF
policy (neutral)" />
  <add key="temperror" value="451 4.4.3 your message from [%source_ip%] encountered a
temporal error with SPF verification (temperror)" />
  <add key="permerror" value="550 5.7.1 your message from [%source_ip%] encountered a
permanent error with SPF verification (permerror)" />
</spfResultToReject>

<dkimResultToReject>
  <add key="fail" value="550 5.7.1 your message from [%header_from%] is against our DKIM
policy (fail)" />
</dkimResultToReject>

<dmARCResultToReject>
  <add key="fail" value="550 5.7.1 your message from [%header_from%] is against our DMARC
policy (fail)" />
</dmARCResultToReject>
```

A continuación, se observa la configuración recomendada para el nivel más alto, ya que hay muchos servidores SMTP que no implementan la firma DKIM o el registro DMARC, esta configuración no se recomienda, ya que rechaza todos los correos electrónicos sin "spf = pass" y "dkim = pass" en el servicio SMTP.

```
<spfResultToReject>
  <add key="fail" value="550 5.7.1 your message from [%source_ip%] is against our SPF
policy (fail)" />
  <add key="softfail" value="550 5.7.1 your message from [%source_ip%] is against our SPF
policy (softfail)" />
  <add key="none" value="550 5.7.1 your message from [%source_ip%] is against our SPF
policy (none)" />
  <add key="neutral" value="550 5.7.1 your message from [%source_ip%] is against our SPF
policy (neutral)" />
  <add key="temperror" value="451 4.4.3 your message from [%source_ip%] encountered a
temporal error with SPF verification (temperror)" />
  <add key="permerror" value="550 5.7.1 your message from [%source_ip%] encountered a
permanent error with SPF verification (permerror)" />
</spfResultToReject>

<dkimResultToReject>
  <add key="fail" value="550 5.7.1 your message from [%header_from%] is against our DKIM
policy (fail)" />
  <add key="none" value="550 5.7.1 your message from [%header_from%] is against our DKIM
policy (none)" />
  <add key="neutral" value="550 5.7.1 your message from [%header_from%] is against our
DKIM policy (neutral)" />
  <add key="temperror" value="451 4.4.3 your message from [%header_from%] encountered a
temporal error with DKIM verification (temperror)" />
```

```

    <add key="permerror" value="550 5.7.1 your message from [%header_from%] encountered a
    permanent error with SPF verification (permerror)" />
</dkimResultToReject>

<dmARCResultToReject>
    <add key="fail" value="550 5.7.1 your message from [%header_from%] is against our DMARC
    policy (fail)" />
    <add key="none" value="550 5.7.1 your message from [%header_from%] is against our DMARC
    policy (none)" />
    <add key="temperror" value="451 4.4.3 your message from [%header_from%] encountered a
    temporal error with DMARC verification (temperror)" />
    <add key="permerror" value="550 5.7.1 your message from [%header_from%] encountered a
    permanent error with DMARC verification (permerror)" />
</dmARCResultToReject>

```

También se puede configurar en manera de direcciones IP de confianza en el que se puede agregar direcciones IP a la sección: trustedIPAddresses, el agente de DKIM / SPF entrante no verificará el correo electrónico de esas direcciones IP. Es compatible con una sola dirección IP o sintaxis CIDR.

Por ejemplo:

```

<trustedIPAddresses>
    <add key="127.0.0.1" value="pass"/>
    <add key="192.168.0.0/24" value="pass"/>
</trustedIPAddresses>

```

Otra manera de configurar es mediante remitente o dominio de confianza en el que se puede agregar direcciones o dominios de remitentes a la sección trustedSenderOrDomain, el agente de DKIM / SPF entrante no revisará el correo electrónico de esos remitentes o dominios.

Por ejemplo:

```

<trustedSenderOrDomain>
  <!--
    You can use regular expression like this: "/^(support/sales)@emailarchitect\.net$/"

    "/^(support/sales)@emailarchitect\.net$/" matches "support@emailarchitect.net" and
    "sales@emailarchitect.net".

    "/^[^@]+@emailarchitect\.net$/" matches "*@emailarchitect.net"
  -->
  <add key="support@emailarchitect.net" value="pass"/>
  <add key="emailarchitect.net" value="pass"/>
</trustedSenderOrDomain>

```

En la configuración el administrador de servidores puede bloquear direcciones mediante IP en el que puede agregar direcciones IP a la sección: blockedIPAddresses, el agente de DKIM / SPF entrante rechazará el correo electrónico de esas direcciones directamente, independientemente del resultado de SPF / DKIM. Es compatible con una sola dirección IP o sintaxis CIDR.

```
<blockedIPAddresses>  
  <add key="127.0.0.2" value="550 5.7.1 your message from [%source_ip%] is in our black  
list." />  
</blockedIPAddresses>
```