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 official de Microsoft)
- Instalar el paquete Redistributable de Visual C++ apra 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, añade 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: <u>https://www.emailarchitect.net/webapp/download/eaexchdomainkeys.exe</u>. 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.



Danalara da	Net framework		
reciclaje	4.7.1	😽 EA DKIM for IIS SMTP and Exchange Server Setup	
	_	Installing Please wait while EA DKIM for IIS SMTP and Exchange Server is being installed.	
Exchange 2010 SP3	И Р 46-КВ 30 455	Detecting Exchange 2007/2010/2013/2016/2019	
	a		
(MSAUTO.1.5.3)	Windows6.1-KB4		
		Nullsoft Install System v3.03	
		< Back Next >	Cancel
Knowledge bases	eaexchdomainkeys		

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.



🖏 Servicios						<u>- 0 ×</u>
Archivo Acción Ver	Ayuda					
) 📝 📷 🛛 🖉 🖬 🖬 🚺					
🤹 Servicios (locales)	🔅 Servicios (locales)					
	Seleccione un elemento para ver su	Nombre 🔺	Descripción	Estado	Tipo de inicio	Iniciar sesión c 🔺
	descripción.	Acceso a dispositiv	Habilita el a		Manual	Sistema local
		Actualización de co	Forefront P	Iniciado	Automático	Sistema local
		Adaptador de rendi	Proporcion		Manual	Sistema local
		🔍 Administración de a	Procesa las		Manual	Sistema local
		🔍 Administración de c	Proporcion		Manual	Sistema local
		🎑 Administración rem	El servicio	Iniciado	Automático (Servicio de red
		🎑 Administrador de c	Crea una c		Manual	Sistema local
		🎑 Administrador de c	Administra		Manual	Sistema local
		🎑 Administrador de cr	Proporcion		Manual	Sistema local
		🔍 Administrador de c	El inicio de	Iniciado	Automático	Sistema local
		🎑 Administrador de s	Proporcion	Iniciado	Automático	Sistema local
		🎑 Agente de directiva	El protocol	Iniciado	Manual	Servicio de red
		🎑 Agente de Protecci	El servicio		Manual	Servicio de red
		🔍 Aislamiento de clav	El servicio		Manual	Sistema local
		🔍 Almacenamiento pr	Ofrece alm		Manual	Sistema local
		🔍 Aplicación auxiliar d	Proporcion	Iniciado	Automático	Servicio local
		🔍 Aplicación auxiliar IP	Proporcion	Iniciado	Automático	Sistema local
		Aplicación del siste	Administra I		Manual	Sistema local
		Asignador de detec	Crea un ma		Manual	Servicio local
		🔍 Asignador de extre	Resuelve id	Iniciado	Automático	Servicio de red
		🔍 Asistentes de buzó	Realiza el p	Iniciado	Automático	Sistema local
		O ASP NET State Ser ▲	Provides su		Deshabilitado	Servicio de red
	Extendido Estándar					
·	,,					

En la siguiente ventana se muetra 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	_ 🗆 🗵
c	Solo los cmdlets de Exchange: Get-ExCommand 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</cmdlet></cmdlet></string>	
	Sugerencia del día n.º 66:	
,	Puede importar archivos CSU y tratarlos como objetos mediante el uso del cmu Import-Csv. Cada fila en un archivo CSU se convierte en un elemento en un cr to y cada columna se convierte en una propiedad. Puede asignar el archivo C una variable o puede canalizar su contenido directamente a otro cmdlet. En guiente ejemplo, existen tres columnas en el archivo CSU, Name, Alias y Ema ress, con varias filas por las que se trasladará el cmdlet ForEach. Los dat cada fila se usan para crear un nuevo contacto de correo.	llet onjun SV a el si ilAdd os de
	\$CSU = Import-Csu \$CSU ForEach < New-MailContact -Name \$Name -Alias \$Alias -ExternalEm dress \$EmailAddress -OrganizationalUnit Users >	ailAd
1	DETALLADO: Conectando a ServidorUNACH.unach.edu.ec DETALLADO: Conectado a ServidorUNACH.unach.edu.ec. IPS] C:\Windows\system32>enable-transportagent "EA Dkim Inbount 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: <mark>Help ×(string)×</mark> Obtener ayuda general: <mark>Help</mark>	
Untener ayuda acerca de un cmalet: Help \cmalet name> or \cmalet name> -{ Mostrar guía de referencia rápida: QuickRef Blog del eguino de Exchange: Get=FxBlog	
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 clien El filtrado del servidor se usa con los cmdlets de destinatario y de cola, l cuales son compatibles con el parámetro Filter, ya que estos cmdlets pueden d lver grandes conjuntos de resultados. El servidor filtra el resultado mediant l uso de criterios que usted específica y, a continuación, le envía los resul os filtrados. Se puede usar el filtrado de cliente con cualquier cmdlet. Todo conjunto de resultados se envía al equipo cliente, que filtra, a continuació los datos y proporciona un conjunto de resultados filtrados. El filtrado del c nte usa el cmdlet Where-Object, que puede acortarse a Where.	te? os evo tad el n, lie
DETALLADO: Conectando a ServidorUNACH.unach.edu.ec DETALLADO: Conectado a ServidorUNACH.unach.edu.ec. LPS1 C:\Windows\system32>enable-transportagent "EA Dkim Inbound Agent" ADVERTENCIA: Para que los cambios surtan efecto, es necesario el reinicio del servicio siguiente: MSExchangeTransport LPS1 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, lver grandes conjuntos de resultados. El servido l uso de criterios que usted especifica y, a con os filtrados. Se puede usar el filtrado de clien conjunto de resultados se envía al equipo clien los datos y proporciona un conjunto de resultado nte usa el cmdlet Where-Object, que puede acorta DETALLADO: Conectando a ServidorUNACH.unach.edu. DETALLADO: Conectado a ServidorUNACH.unach.edu. DETALLADO: Conectado a ServidorUNACH.unach.edu. ELSI C:\Windows\system32>enable-transportagent " ADUERTENCIA: Para que los cambios surtan efecto, servicio siguiente: MSExchangeTransport [PSI C:\Windows\system32>get-transportagent	ya que estos cr r filtra el res tinuación, le d te con cualqui te, que filtra s filtrado. El rse a Where. ec c. EA Dkim Inbound es necesario d	mdlets pueden dew sultado mediante envia los resulta er cmdlet. Todo (, a continuación filtrado del cl d Agent" el reinicio del	vo 🔺 e ad e l
Identity	Enabled	Priority	
Transport Rule Agent Text Messaging Routing Agent Text Messaging Delivery Agent EA DomainKeys Agent EA Dkim Inbound Agent	True True True True True	1 2 3 4 5	
[PS] C:\Windows\system32>_			

🚱 Equipo: ServidorUNACH.unach.edu.ec		
lver grandes conjuntos de resultados. El ser l uso de criterios que usted especifica y, a os filtrados. Se puede usar el filtrado de c conjunto de resultados se envía al equipo o los datos y proporciona un conjunto de resul nte usa el cmdlet Where-Object, que puede ac	vidor filtra el res a continuación, le e liente con cualquie liente, que filtra, tados filtrado. El cortarse a Where.	sultado mediante e envía los resultad er cmdlet. Todo el . a continuación, filtrado del clie
DETALLADO: Conectando a ServidorUNACH.unach. DETALLADO: Conectado a ServidorUNACH.unach.e [PS] C:\Windows\system32>enable-transportage ADVERTENCIA: Para que los cambios surtan efe servicio siguiente: MSExchangeTransport [PS] C:\Windows\system32>get-transportagent	edu.ec du.ec. nt "EA Dkim Inbound cto, es necesario e	d Agent" el reinicio del
Identity	Enabled	Priority
Transport Rule Agent Text Messaging Routing Agent Text Messaging Delivery Agent EA DomainKeys Agent EA Dkim Inbound Agent	True True True True True True	1 2 3 4 5
[PS] C:\Windows\system32>Restart-Service "Ms [PS] C:\Windows\system32>_	ExchangeTransport"	-

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.

Getting Started	DKIM Configuratio	n	
DKIM Configuration	DKIM Configuration	> [New Domain]	
Sender Rules			
Plugin Journal	DomainKeys/DKIM s	ignature is based on the domain of sender email address. It is server name. For example, if you want to sign the email from	
SPF/DMARC Tool	*@emailarchitect.net	, then please input emailarchitect.net to Sender Domain.	
Documentation	Sender Domain:		
License Code	Selector:	s1024	
Uninstall	Active:		
	Signature	DKIM Only (recommended)	•
	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.

etting Started	Specify a pfx (p12) certificate for DKIM/DomainKeys key pair.
OKIM Configuration	
ender Rules	I do not have a key pair certificate for signature. Please create a new certificate (1024b
N	Certificate File Name:
Plugin Journal	
SPF/DMARC Tool	Cutificate Daylor fine Decement
Documentation	
	ТМРОО1
License Code	
Uninstall	Advanced Options
	Save Cancel Helo

Getting Started	Algorithm:	rsa-sha256 (securer)	•
OKIM Configuration	Specify a pfx (p12)	certificate for DKIM/DomainKeys key pair.	
Sender Rules	I have a key pair o	ertificate for DKIM/DomainKevs signature.	
Plugin Journal			
SPF/DMARC Tool	Certificate File Name	e: 86)\EAExchDomainKeys\certs\unach.edu.ec.pfx	srowse
Documentation	Certificate Protection	n Password:	
License Code	TMP001	Install current PFX certificate to machine store. (Op	otional)
Uninstall			
	Advanced Options .		
	Carrie Carried	Hele	

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 Domain Active 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":

DKIM Manager for IIS SMTP and Exchange Server				
Getting Started	DKIM Configuration	1		
DKIM Configuration	DKIM Configuration ->	[unach.edu.ec]		
Sender Rules				
Plugin Journal	DomainKeys/DKIM sig	gnature is based on the domain of sender email address. It is erver name. For example, if you want to sign the email from		
SPF/DMARC Tool	*@emailarchitect.net,	then please input emailarchitect.net to Sender Domain.		
Documentation	Sender Domain:	unach.edu.ec		
License Code		Export Public Key Deploy Key Test Public Key Test DKIM		
Uninstall	Selector:	s1024		
	Active:	v		
	Signature	DKIM Only (recommended)		
	Canonicalization	nofws/relaxed (recommended)		

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

xport Public	Key
If your doma	in is hosted by Windows DNS Server in local LAN, you can click here to deploy public key.
TXT Record:	s1024domainkey.unach.edu.ec
Public Key:	<pre>v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCuKVawUqK2wD4viVpv2mVmGyi8NQGawu 8nbe/NDigfjA+VYq2jsZo35pLbJpZdeCo+APOUXEs069iZ4u/wDAYLpp3A11XS5GP5aCrh8X 4qp1DgogSPmGqCB62B6EDrX9HS9RyIsj3ISX2s3BIVuvkQkPg7D+aFtZZ+ibqGbyc52wIDAQ AB</pre>
"t=y;" in pub DKIM/Doma	ic key record means Test mode , you can remove "t=y;" from your public key record after nKeys test is finished. [Help]
Test Mode:	
Please add t After the re ; DKIM publi s1024domai p=MIGfMA0GCS Yq2jsZo35Lb	he following TXT record (case sensitive) in unach.edu.ec DNS server. cord is created in DNS server, you can use Test Public Key to test it. c key zone file example: nkey.unach.edu.ec. IN TXT "v=DKIM1; k=rsa; qGSIb3DQEBAQUAA4GNADCBiQKBgQCuKVawUqK2wD4viVpv2mVmGyi8NQGawu8nbe/NDigfjA+V JpZdeCo+APOUXEs069iZ4u/wDAYLpp3A11XS5GP5aCrh8X4qp1DgogSPmGqCB6286EDrX9HS9R

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.

DKIM Manager for IIS	SMTP and Exchange Server
Getting Started	
DKIM Configuration	DomainKeys/DKIM -> [unach.edu.ec] -> Deploy Public Key
Sender Rules	If your domain is hosted by Windows DNS Server in local LAN, you can connect to DNS
Plugin Journal	is used.
SPF/DMARC Tool	If your domain is not hosted by Windows DNS Server, or DNS server is failed to connect, you
Documentation	should deploy public key manually. [Help]
License Code	DNS Server: localhost
Uninstall	User: (optional*)
	Password: (optional*)
	Connect to DNS Cancel
	Copyright © 2019 AdminSystem Software Limited. All rights reserved.

En la ventana síguiente se puede observar que se la clave púbica se ha añadió satisfactoriamente.

DKIM Configura	tion
DomainKeys/DKIM	-> [unach.edu.ec] -> Deploy Public Key
Please choose a zo and go to "Test Pu	ne to deploy DKIM public key. If the public key is deployed successfully, you o blic Key". If it is failed to deploy public key, please deploy public key manually.
Domain	Records
_msdcs.unach.edu.e	ec
unach.edu.ec	
Close	
Copyright © 2019	AdminSystem Software Limited. All rights reserved.

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.

DomainKeys/DKIM -> [unach.edu.ec] -> Deploy Public Key			
Please choose a zone t and go to "Test Public	to deploy DKIM public key. If the public key is deployed successfully, you Key". If it is failed to deploy public key, please deploy public key manually		
Domain	Records		
_msdcs.unach.edu.ec			
	_domainkey.unach.edu.ec IN TXT "o=~;"		
	s1024domainkey.unach.edu.ec IN TXT "v=DKIM1; k=rsa; p=		
unach.edu.ec	CSqGSIb3DQEBAQUAA4GNADCBiQKBgQCuKVawUqK2wD4viVpv2mVmGyi&		
	be/NDigfjA+VYq2jsZo35pLbJpZdeCo+APOUXEs069iZ4u/wDAYLpp34		
	aCrh8X4qplDgogSPmGqCB62B6EDrX9HS9RyIsj3ISX2s3BIVuvkQkPg7		
	ibqGbyc52wIDAQAB"		
Close			

3.1. Comprobación de implementación DKIM

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

Comandos: nslookup

set type=txt

s1024._domainkey.sudominio



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		
<mark>servicio siguiente: MSExchangeTransport</mark> [PS] C:\Windows\system32>get-transportagen(ţ	
Identity	Enabled	Priority
Transport Rule Agent Text Messaging Routing Agent Text Messaging Delivery Agent EA DomainKeys Agent EA Dkim Inbound Agent [PS] C:\Windows\system32>Restart-Service "Y [PS] C:\Windows\system32>get-transportagent	True True True True True IsExchangeTransport" t	1 2 3 4 5
Identity	Enabled	Priority
Transport Rule Agent Text Messaging Routing Agent Text Messaging Delivery Agent EA DomainKeys Agent EA Dkim Inbound Agent	True True True True True True	1 2 3 4 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"

DKIM Manager for IIS SM	MTP and Exchange Server				
Getting Started	SPF/DMARC Tool				
DKIM Configuration	SPE and DMARC record are also important to email server. The following tools help you to set				
Sender Rules	up SPF record and DMARC record in DNS server.				
Plugin Journal	SPF Record				
SPF/DMARC Tool	Sender Policy Framework (SPF) is a simple email-validation system designed to detect email				
Documentation	spoofing by providing a mechanism to allow receiving mail exchangers to check that incoming				
License Code	sender IP address.				
Uninstall					
	Please input your domain and click "Start" to set up SPF record.				
	Domain: unach.edu.ed Start Help				
	DMARC Record				

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.

🖡 Administrador del servidor						
Archivo Acción	Ver Ayuda					
🗢 🔿 🚈	🗙 🗐 🧟 📑					
rador del servidor (SE	RVIDORUNACH)	unach.edu.ec 12 regist	ros			Acciones
S		Nombre		Tipo	Datos	unach.edu.ec 🔺
Servicios de archivo	Activo Diroctory	domainkey				Acciones adicionales
Servidor DNS	e Active Directory	_msdcs				Actiones adicionales
DNS		Calification in the second sec				(igual que la carpeta princip 🔺
🖻 📋 SERVIDORUNA	ACH	🚞 _tcp				Acciones adicionales
🗄 🔃 Registros 🤅	globales	📫 _udp				Actiones adicionales
🖃 🧮 Zonas de b	púsqueda directa	DomainDnsZones				
E 📑 _msdc	s.unach.edu.ec	ForestDnsZones				
E 🛐 unach	.edu.ec	l 🔲 (iqual que la carpeta pri	ncipal)	Inicio de autoridad (SOA)	[33], servic	
	Actualizar archi	vo de datos del servidor	hcipal)	Servidor de nombres (NS)	servidoruni	
	voiver a cargar	- ^ ^ ^ ^	hcipal)	Host (A)	192.168.50	
	Alize pueve (Ch			Host (A)	192.168.50	
1 8 7 1	Alias nuevo (Cr	NAME)	hcipal)	lexto (IXI)	v=spf1mx	
🕀 🧮 Do	Dominio nuevo	ibio de correo (MA)				
🕀 📔 Fc	Delegación nue	Value				
🕀 🚞 Zonas de 🛛	Registros nuev	05				
🕀 🚞 Reenviado						
Servidor web (IIS)	Todas las tarea	is 🕨				
nóstico	Ver	۱.				
figuración	Eliminar					
ecenamiento	Actualizar					
	Exportar lista					
•	Propiedades				Þ	
Crea un registro de re	Ayuda					,

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

	IACT POLICE LZ POISTOS	_
Т	ipo de registro del recurso	×
1	Seleccione el tipo de registro del recurso:	
	Registro de servicio (SRV) Ruta directa (RT)	
	Servicios bien conocidos (WKS) Siguiente dominio (NXT)	
	Texto (TXT) X 25	Ļ
	Descripción: Registro de texto (TXT). Contiege una cadega de caracteres que	
	sirve como texto descriptivo que se asociará con un determinado nombre de dominio DNS. La semántica del texto descriptivo real utilizado como datos con este tipo de registro depende del nombre DNS donde se encuentran estos registros. (RFC 1035)	I
	Crear registro Cancela	ar

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.

luevo registro de recursos	×
Texto (TXT)	
Nombre de registro (si se deja en blanco, se usa el nombre del dominio primario):	
Nombre de dominio completo (FQDN):	
unach.edu.ec.	
Texto:	
v=spf1 mx a ip4: 192. 168. 10.0/24 ip4: 192. 168. 20.0/24 ip4: 192. 168	
Aceptar Cancelar	

Como se puede observar el registro se ha creado satisfactoriamente.

unach.edu.ec 12 registros		
Nombre	Тіро	Datos
🚞 _domainkey		
📳 _msdcs		
🚞 _sites		
🚞 _tcp		
🚞 _udp		
Communication Distances		
ForestDnsZones		
🗐 (igual que la carpeta principal)	Inicio de autoridad (SOA)	[33], servio
🗐 (igual que la carpeta principal)	Servidor de nombres (NS)	servidoruni
🗐 (igual que la carpeta principal)	Host (A)	192.168.50
servidorunach	Host (A)	192.168.50
(igual que la carpeta principal)	Texto (TXT)	v=spf1mx
•		F

3.2.1. Comprobación de implementación SPF

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

Comandos: nslookup

sudominio



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.

📠 Administrador del servidor						
Archivo Acción	Archivo Acción Ver Ayuda					
🗢 🔿 🚺 🗖	🗙 🗐 🧕 🗟					
rador del servidor (SE	RVIDORUNACH)	unach.edu.ec 12 regist	ros			Acciones
s		Nombre		Tipo	Datos	unach.edu.ec 🔺
Servicios de archivo		domainkey		1 100	00000	Auricean editionales
Servicios de dominio de	e Active Directory	msdcs				Acciones adicionales
Servidor DNS		sites				(iqual que la carpeta princip
	сн	tco				(igual que la carpeta principii
	lobales	📋 udp				Acciones adicionales
E Zonas de b	usqueda directa	DomainDnsZones				
E 📑 _msdc	s.unach.edu.ec	ForestDnsZones				
🗉 👩 unach.	edu.ec	🗐 (ioual que la carpeta pr	ncipal)	Inicio de autoridad (SOA)	[33], servic	
	Actualizar archi	vo de datos del servidor	hcipal)	Servidor de nombres (NS)	servidoruni	
E 🚺 🗉	Volver a cargar		hcipal)	Host (A)	192.168.50	
E 📜 -	Host nuevo (A	D AAAA)		Host (A)	192.168.50	
E 📃 -t	Alias nuevo (CN	IAME)	hcipal)	Texto (TXT)	v=spf1 mx	
비 브루날	Nuevo intercar	bio de correo (MX)				
	Dominio nuevo.					
Topas de	Delegación nue	va				
E Beenviade	Registros nuev	DS				
Servidor web (IIS)	Todas las tarea	s 🕨				
octerísticas	Ver	•				
figuración	Fliminar					
cenamiento	Actualizar					
	Exportar lista					
	exporter instant					
•	Propiedades				F	
Crea un registro de re	Ayuda					

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

Tipo de registro del recurso	×
Seleccione el tipo de registro del recurso:	
Registro de servicio (SRV) Ruta directa (RT) Servicios bien conocidos (WKS)	•
Siguiente dominio (NXT) Texto (TXT) X.25	•
Descripción:	
Registro de texto (TXT). Contiene una cadena de caracteres qu sirve como texto descriptivo que se asociará con un determinad nombre de dominio DNS. La semántica del texto descriptivo real utilizado como datos con este tipo de registro depende del nomb DNS donde se encuentran estos registros. (RFC 1035)	e 🔺 o
	~
Crear registro Ca	ncelar

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".

Propiedades de unach.edu.ec
Texto (TXT) Seguridad
Nombre de registro (si se deja en blanco, se usa el nombre del dominio primario):
(ìgual que la carpeta principal)
Nombre de dominio completo (FQDN):
unach.edu.ec
Texto:
Aceptar Cancelar Aplicar

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:) • Program Files (x86) • EAExchDomainKeys •			
elp			
🔻 🧾 Open 💌			
Name 🔻	-	Date modified	ŀ
🗑 uninst.exe		9/8/2017 6:36 PM	1
🚳 NgenMail.Net.dll		8/18/2017 9:39 A	١M
Interop.EADKIMMgrObjLib.dll		9/7/2017 10:09 A	١M
😰 eaexchdomainkeys.chm		9/8/2017 6:02 PM	4
EADKIMMgrObj.dll		9/8/2017 6:36 PM	4
OkimOutboundAgent.dll		9/7/2017 10:09 A	١M
DkimInboundAgent.dll.config		8/25/2017 9:56 A	M
🚳 DkimInboundAgent.dll		9/7/2017 9:24 AM	4
DKIM Plugin Manager		9/8/2017 6:36 PM	4
1		0/0/2017 0.20 01	

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,</pre> System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" /> <section name="ignoredGatewayIPAddressesForSpfCheck"</pre> type="System.Configuration.AppSettingsSection, System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" /> <section name="ignoredGatewayNameForSpfCheck"</pre> type="System.Configuration.AppSettingsSection, System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" /> <section name="ignoreSpfResultDomains" type="System.Configuration.AppSettingsSection,</pre> System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" /> <section name="dkimResultToReject" type="System.Configuration.AppSettingsSection,</pre> System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" /> <section name="ignoreBodyHashErrorDomains"</pre> type="System.Configuration.AppSettingsSection, System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" /> <section name="ignoreDkimResultDomains" type="System.Configuration.AppSettingsSection,</pre> System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" /> <section name="dmarcResultToReject" type="System.Configuration.AppSettingsSection,</pre> 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> <1 - -<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>

<!--

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.
</pre>
```

```
<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:

Configuración de nivel medio:

```
<spfResultToReject>
    <add key="fail" value="550 5.7.1 your message from [%source ip%] is against our SPF</pre>
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</pre>
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</pre>
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>
<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
temporal error with DMARC verification (temperror)" />
<add key="permerror" value="550 5.7.1 your message from [%header_from%] encountered a
temporal error with DMARC verification (permerror)" />
<add key="permerror" value="550 5.7.1 your message from [%header_from%] encountered a
```

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>
```