



FACULTAD: INFORMÁTICA Y CIENCIAS APLICADAS
CARRERA: TÉCNICO EN INGENIERIA DE REDES COMPUTACIONALES



TEMA:

Desarrollo de una guía didáctica para la instalación y configuración de la tecnología Microsoft ISA Server 2004, dirigida al mejoramiento de las prácticas del laboratorio de redes de la Universidad Tecnológica de El Salvador.

Trabajo de graduación presentado por:

Eigner Iván Villacorta Rauda.
Juan Carlos Rivera Morales.
William Omar Moran Rosado.

Para optar al grado de:

TECNICO EN INGENIERIA DE REDES COMPUTACIONALES

SEPTIEMBRE 2007

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA.

PÀGINA DE AUTORIDADES

LIC. JOSÈ MAURICIO LOUCEL
RECTOR

ING. NELSON ZÀRATE SÀNCHEZ
VICERRECTOR ACADÈMICO

ING. LORENA DUQUE DE RODRIGUEZ
DECANO

JURADO EXAMINADOR

ING. VICENTE ZARCEÑO
PRESIDENTE

ING. SIGIFREDO PORTILLO
PRIMER VOCAL

ING. SALVADOR ALCIDEZ FRANCO
SEGUNDO VOCAL

SEPTIEMBRE 2007

San Salvador, El Salvador, Centroamérica.

ACTA DE EXAMEN PROFESIONAL



HABIÉNDOSE REUNIDO EL JURADO CALIFICADOR INTEGRADO POR:

ING. SIGFREDO EDUARDO PORTILLO, ING. SALVADOR ALCIDES FRANCO,

ING. VICENTE ZARCEÑO

A LAS 12:00 M. DEL DÍA: VIERNES, 20 DE JULIO DEL DOS MIL SIETE.

Y LUEGO DE HABER DELIBERADO SOBRE EL EXAMEN PROFESIONAL DE LOS ALUMNOS:

1- EIGNER IVAN VILLACORTA RAUDA CARNET 26-4218-2004

2- JUAN CARLOS RIVERA CARNET 26-1212-2002

3- WILLIAM OMAR MORAN ROSADO CARNET 26-3950-2004

QUIENES PRESENTARON DEFENSA DE SU TRABAJO DE GRADUACION TITULADO:

"DESARROLLO DE UNA GUIA DIDÁCTICA PARA LA INSTALACIÓN Y CONFIGURACIÓN DE LA TECNOLOGÍA MICROSOFT ISA SERVER 2004, DIRIGIDA AL MEJORAMIENTO DE LAS PRACTICAS DEL LABORATORIO DE REDES DE LA UNIVERSIDAD TECNOLÓGICA DE EL SALVADOR"

PARA OPTAR AL GRADO DE:

"TÉCNICO EN INGENIERIA DE REDES COMPUTACIONALES"

Y DEL CUAL TAMBIEN EVALUARON LOS CONOCIMIENTOS RELACIONADOS CON EL TEMA DEL MISMO. POR LO QUE ESTE JURADO RESUELVE DECLARAR EL EXAMEN COMO:

APROBADO

YA QUE CUMPLE CON LOS REQUISITOS ESTABLECIDOS EN EL REGLAMENTO DE GRADUACION DE LA UNIVERSIDAD.

SAN SALVADOR, 20 DE JULIO DEL DOS MIL SIETE.

F.

PRIMER VOCAL

ING. SIGFREDO EDUARDO PORTILLO

F.

SEGUNDO VOCAL

ING. SALVADOR ALCIDES FRANCO

F.

PRESIDENTE

ING. VICENTE ZARCEÑO

INDICE

Introducción

CAPÍTULO I

SITUACION PROBLEMÁTICA

1.0 Situación problemática.....	1
1.1 Enunciado del problema	2
1.2 Justificación del proyecto	2
1.3 Objetivos.....	3
1.3.1 Objetivo General	
1.3.2 Objetivos específicos	
1.4 Alcances.....	4
1.5 Delimitaciones.....	5
1.5.1 Geográfica	
1.5.2 Temporal	
1.5.3 Organizacional	
1.5.4 Especifica	
1.6 Estudios de factibilidad.....	6
1.6.1 Factibilidad Económica.....	6
1.6.2 Factibilidad Técnica.....	7
1.6.3 Factibilidad Operativa.....	11
1.7 Marco Teórico de Referencia.....	13
1.7.1 Introducción ISA Server.....	13
1.7.2 Componentes, servicios de ISA Server.....	15

1.7.3 Administración remota de ISA Server.....	18
1.7.4 Características de ISA Server.....	21
1.7.5 Tipos de Clientes que admite ISA Server.....	23
1.7.6 Escenarios de implementación.....	26
1.7.7 Resumen de características ISA Server 2004.....	39
1.7.8 Guía Rápida de instalación del software de servidor.....	43

CAPÍTULO II

PROYECTO TEMATICO

2.0 Proyecto Temático.....	45
2.1 Documentación técnica.....	48
2.1.1 ISA Server 2004.....	48
2.1.2 Características Técnicas de ISA 2004.....	50
2.2 SA Server 2006.....	57
2.2.1 Características Técnicas de ISA 2006.....	58
2.3 Ediciones de ISA Server.....	62
2.4 Squid GNU/Linux	64
2.5 Criterios de Evaluación.....	66
2.5.1 Evaluación Económica.....	66
2.5.2 Evaluación Técnica.....	66
2.6 Acoplamiento al laboratorio de redes de la UTEC.....	68
2.7 Tecnología y recursos seleccionados	70
2.8 Cronograma del proyecto temático.....	71
2.9 Oferta técnica.....	72

2.10 Oferta económica.....	73
----------------------------	----

CAPÍTULO III

PROTOTIPO

3.0 Manuales y CD de configuración de ISA Server 2004.....	76
3.1 Instalación de ISA Server 2004.....	76
3.2 Configuración de Proxy Web.....	85
3.3 Manual para la configuración de la Cachè Web.....	96
3.4 Configuración de las políticas de Firewall	102
3.5 Manual para crear una política http que impide Descargas mediante http con extensiones .exe.....	113
3.6 Configuración de Redes Perimetrales DMZ.....	121
3.7 Configuración de VPN.....	136
3.8 Descripción de CD interactivo.....	144
4.0 Conclusiones y recomendaciones.....	148
4.1 Conclusiones.....	148
4.2 Recomendaciones.....	149
4.3 Bibliografía.....	150
ANEXOS.....	151

INTRODUCCION

El presente documento aborda una de las problemáticas del laboratorio de redes de la Universidad Tecnológica de El Salvador, el cual es, la falta de orientación didáctica que este ofrece a los estudiantes que cursan la carrera Técnico en Ingeniería de Redes Computacionales, sobre la tecnología de seguridad de Microsoft ISA Server 2004, para lo cual, se desarrollará una guía didáctica que permita orientar a los estudiantes interesados en esta tecnología sobre las ventajas de instalar e implementar la tecnología del software Microsoft ISA Server 2004 en arquitectura cliente-Servidor.

La propuesta esta integrada por una guía didáctica que permita orientar y solventar las necesidades de información que demanden al momento de implementar la tecnología de Microsoft ISA Server 2004.

Para ello, se realizó una investigación en campo, a través de una encuesta de opinión, realizada a los estudiantes que cursan la carrera de técnico en Ingeniería de Redes Computacionales, el cual tuvo lugar en el laboratorio de redes de la Universidad Tecnológica de El Salvador en el período comprendido del 12 al 14 de abril de 2007 y 1 al 9 de junio del 2007.

CAPÍTULO I

SITUACIÓN PROBLEMÁTICA

1.0 SITUACIÓN PROBLEMÁTICA

El Laboratorio de Redes de la Universidad Tecnológica es el espacio didáctico y pedagógico, en el cual se realizan las diferentes prácticas que brindan los docentes de diversas asignaturas que comprende la carrera de Técnico en Ingeniería de Redes Computacionales.

Sin embargo, se ha observado que no se brinda una orientación sustancial sobre la seguridad en las Redes de Computadoras en Arquitectura Cliente – Servidor y específicamente de cómo instalar y configurar la tecnología de Microsoft ISA Server 2004. Software utilizado por muchas empresas y organizaciones para la administración de su seguridad en redes informáticas con los riesgos que hoy en día se observan con el aumento de las actividades empresariales en Internet y el cada vez mayor número de redes corporativas conectadas a ella cada día es más necesario la implementación de un servidor de seguridad para las empresas, que hacen uso del recurso de la Internet.

Es por ello, que se encuentra la necesidad de desarrollar un material educativo que entregue información tanto práctica como teórica de la tecnología de Microsoft ISA Server 2004.

Este material servirá para que las futuras generaciones de técnicos comprendan la necesidad de esta tecnología y los beneficios en materia de seguridad informática en un entorno de red.

1.1 ENUNCIADO DEL PROBLEMA

¿En qué medida el desarrollo de material educativo para el laboratorio de redes de la Universidad Tecnológica de El Salvador beneficiará a las futuras generaciones de la carrera de Técnico en Ingeniería de Redes Computacionales sobre el uso adecuado de la tecnología de Microsoft ISA Server 2004?

1.2 JUSTIFICACION DEL PROYECTO

El proyecto tendrá una clara orientación didáctica hacia el estudiante ya que mencionará lo que es necesario conocer para el uso adecuado de Microsoft ISA Server 2004.

Con esto se ayudará al estudiante a que solvante sus dudas acerca de la tecnología de Microsoft ISA Server 2004 y conozca más sobre la seguridad informática que brinda dicho software.

El proyecto ayudará al estudiante a solventar sus dudas de una manera rápida y práctica, evitando que utilice información poco confiable en la Web,

Así mismo apoyará a los docentes ya que este mismo podrá servir de referencia didáctica, ya que se brindara orientación tanto práctica como teórica en dicha guía.

En la práctica de hoy en día la seguridad informática para muchas empresas se encuentra basada en la implementación de la tecnología Microsoft ISA Server.

1.3 OBJETIVOS

1.3.1 Objetivo General

Desarrollar un material didáctico de la tecnología Microsoft ISA Server 2004, para ayudar al mejoramiento de las prácticas de laboratorio de redes de la carrera de Técnico en Ingeniería en Redes Computacionales de la Universidad Tecnológica de El Salvador.

1.3.2 Objetivos Específicos

1. Crear un manual didáctico de instalación de Microsoft ISA Server 2004.
2. Crear Manuales didácticos de las diferentes configuraciones y roles más utilizados de Microsoft ISA Server 2004.
3. Mejorar el sistema de prácticas de Universidad Tecnológica de El Salvador en cuanto a la utilización de Microsoft ISA Server 2004.
4. Solventar el problema de falta de contenido didáctico de la tecnología Microsoft ISA Server 2004.

1.4 ALCANCES

Con el desarrollo de una guía didáctica del software Microsoft ISA Server 2004, se brindará un apoyo tanto práctico como teórico a los estudiantes que cursan diversas asignaturas de la carrera de Técnico en Ingeniería de redes computacionales.

Con esta guía además se pretende que el estudiante tenga una noción de lo importante que es brindar seguridad a las redes informáticas y con ello encaminar al estudiante hacia una mayor profundización del tema.

Con la guía didáctica se logrará que el estudiante conozca como instalar el software en un servidor y se estudiará la manera de cómo configurarlo en sus roles mas importantes.

Se brindará un ejemplo práctico del funcionamiento del software a través de diferentes guías prácticas que el estudiante podrá desarrollar dentro del laboratorio de redes de la Universidad Tecnológica de El Salvador.

Así mismo se busca desarrollar con nuestra guía didáctica diversas políticas de seguridad que se logran implementar en un ambiente de redes Cliente Servidor con el software ISA Server 2004.

Los diferentes roles de Microsoft ISA Server 2004 que se estudiaran e investigarán se detallan continuación

- | | |
|---|---------------------------------------|
| 1. Configurar Proxy Web. | 4. Configurar políticas de firewall. |
| 2. Configurar Cache Web. | 5. Configurar Redes perimetrales DMZ. |
| 3. Configurar Directiva http para controlar las descargas de archivos a través de la extensión del nombre de archivo. | 6. Configurar VPN. |

1.5 DELIMITACIONES

1.5.1 Geográfica:

Universidad Tecnológica de El Salvador, ubica su campus sobre la calle Arce N. 1114, 1026, 1020. Administración académica, escuela de informática edificio Gabriela Mistral, 1ª. Calle Poniente y 19 Ave. Norte, San Salvador.

1.5.2 Temporal:

La guía didáctica del software Microsoft ISA Server 2004, tendrá una fecha de elaboración que comprenderá del mes de Marzo a Julio del 2007.

1.5.3 Organizacional:

La guía didáctica se elaborará para ser utilizado en las instalaciones de la Universidad Tecnológica de El Salvador, por la facultad de informática y ciencias aplicadas, escuela de informática.

1.5.4 Específica:

La guía didáctica tendrá su aplicación tanto práctico como teórica para beneficio de los estudiantes de la carrera de Técnico en Ingeniería de Redes Computacionales, en sus prácticas del laboratorio de redes de la Universidad Tecnológica de El Salvador, ubicado en la 5ª Planta del edificio Francisco Morazán, Calle Arce No. 1026, San Salvador.

1.6 ESTUDIOS DE FACTIBILIDAD

1.6.1 FACTIBILIDAD ECONÓMICA

La propuesta, es el desarrollo del material didáctico para el laboratorio de redes de la Universidad Tecnología de El Salvador, requiere la adquisición de las licencias del software MICROSOFT ISA SERVER, para su implementación.

ISA SERVER Y WIN 2003 SERVER LICENCIAS		
SOFTWARE	LICENCIA COMERCIAL	LICENCIA EDUCATIVA
ISA SERVER 2000	No se distribuye	El costo de licencias para uso educativo se encuentra entre el 10, 15% del costo de una licencia comercial.
ISA SERVER 2004	\$1,200	
ISA SERVER 2006	\$1,650	
WIN 2003 SERVER	\$920	
WIN 2003 SERVER R2	\$995	

1.6.2 FACTIBILIDAD TECNICA

ESPECIFICACIONES TECNICAS

REQUERIMIENTOS DEL SISTEMA PARA ISA SERVER			
ESPECIFICACIONES TECNICAS DE HARDWARE-SOFTWARE			
REQUISITOS	ISA SERVER 2000	ISA SERVER 2004	ISA SERVER 2006
CPU/Procesador	CPU compatible Pentium 300 MHz,o superior	Pentium III a 550 MHz o superior (ISA Server 2004 Standard Edition admite hasta cuatro CPU en un servidor)	PC con Pentium III a 733 MHz o superior.
Memoria	256 megabytes (MB) de RAM	256 MB de RAM o más (se recomienda)	512 MB de RAM mínimo. Recomendado 1 GB.
Espacio disponible en disco duro	20 MB de espacio disponible en disco duro. Una partición de disco duro local formateada con sistema de archivos NTFS	150 MB de espacio Partición local con formato NTFS disponible en el disco duro; se requiere espacio adicional para el contenido de la caché Web	150 MB de espacio Partición local formateada con sistema NTFS y al menos libre. Será necesario más espacio disponible para guardar el contenido de la cache Web.
Sistema operativo	Windows® 2000 Server o Windows® 2000 Advanced Server con Service Pack 1 o posterior, o Windows 2000 Datacenter Server.	Microsoft Windows 2000 Server o Advanced Server con Service Pack 4 o una version posterior; Windows 2000 Datacenter Server o Windows Server 2003 Standard Edition o Enterprise Edition	Microsoft Windows Server 2003 con Service Pack 1 (SP1) o Microsoft Windows Server 2003 R2.

Otros dispositivos	Adaptador de red compatible con Microsoft Windows® 2000 para comunicación con la red interna. Adaptador de red adicional, módem con Windows 2000® para la comunicación con el Internet o un servidor de transmisión.	Adaptador de red compatible con el sistema operativo del equipo para comunicarse con la red interna; un adaptador de red adicional, módem o adaptador RDSI (ISDN) para cada red adicional conectada al equipo ISA Server Unidad de CD-ROM o DVD-ROM Monitor VGA o de resolución superior Teclado y Microsoft Mouse o dispositivo señalador compatible	Tarjeta de red compatible con el sistema operativo para la comunicación con la red interna. Una tarjeta de red adicional, módem, o adaptador RDSI para cada red adicional a la cual se desee conectar el servidor ISA Server Un adaptador de red adicional, necesario para la comunicación intra-array si se va a instalar el NLB integrado en la Ed. Enterprise Unidad de CD-ROM o DVD-ROM Monitor VGA o de resolución superior Teclado y Microsoft Mouse o dispositivo señalador compatible
----------------------------------	--	---	--

ISA SERVER debe instalarse en un sistema operativo de red, se recomienda para ISA 2004

Windows 2003 Server, 2003 R2

Windows Server 2003 Requerimientos del Sistema				
Requerimiento	Standard	Enterprise	Datacenter	Web
CPU Mínima	133 MHz	• 133 MHz para x86 • 733 MHz para x64	• 400 MHz para x86 • 733 MHz para x64	133 MHz
CPU Mínima Recomendada	550 MHz	733 MHz	733 MHz	550 MHz
RAM Mínima	128 MB	128 MB	512 MB	128 MB
RAM Mínima Recomendada	256 MB	256 MB	1 GB	256 MB
RAM Máxima	• 4 GB para x86 • 32 GB para x64	• 32 GB para x86 • 512GB para x64	• 64 GB para x86 • 512GB para x64	2 GB
Número de Procesadores	Hasta 4	Hasta 8	• Mínimo 8 • Máximo 64	Hasta 2
Espacio para la instalación	1.5 GB	• 1.5 GB para x86 • 2.0 GB para x64	• 1.5 GB para x86 • 2.0 GB para x64	1.5 GB

Windows Server 2003 R2 Requerimientos del Sistema			
Requerimiento	Standard	Enterprise	Datacenter
CPU Mínima	133 MHz	• 133 MHz para x86 • 733 MHz para x64	• 400 MHz para x86 • 733 MHz para x64
CPU Mínima Recomendada	550 MHz	733 MHz	733 MHz
RAM Mínima	128 MB	128 MB	512 MB
RAM Mínima Recomendada	256 MB	256 MB	1 GB
RAM Máxima	• 4 GB para x86 • 32 GB para x64	• 64 GB para x86 • 1 TB para x64	• 128 GB para x86 • 1 TB para x64
Número de Procesadores	Hasta 4	Hasta 8	• Mínimo 8 • Máximo 64
Espacio para la instalación	1.5 GB	• 1.5 GB para x86 • 2.0 GB para x64	• 1.5 GB para x86 • 2.0 GB para x64

RECOMENDACIONES DE SOFTWARE

Debido los costos económicos de cada licencia del software ISA Server se opta por la utilización de ISA Server 2004 en comparación con ISA 2006, se observa una significativa reducción de costos, para efectos de estudio ISA Server 2004 es adecuado, aún no esta fuera del mercado con la llegada de la versión 2006, incluso algunas empresas aún utilizan ISA Server 2000. Además se recomienda la implementación de ISA SERVER en máquinas virtuales utilizando los siguientes software VMWARE Virtual Machine, Microsoft Virtual PC, de este modo se mantienen la configuración del equipo del laboratorio de redes en cuanto a sistemas operativos instalados en cada máquina.

RECOMENDACIONES DE HARDWARE

El desarrollo del material didáctico esta dirigido al laboratorio de redes de la Universidad Tecnología de El Salvador la cual cuenta con 30 máquinas, con las siguientes especificaciones de hardware.

LABORATOTIO DE REDES DE LA UNIVERSIDAD TECNOLOGICA ESPECIFICACIONES TECNICAS DEL HARDWARE	
Tamaño de disco duro	40GB
Memoria RAM	512MB
Velocidad del CPU	2.80GHZ
Sistemas Operativos	WIN XP Professional Edition Win 2003 server – virtual machine vmware

Cada sistema operativo en las máquinas del laboratorio de redes de la Universidad Tecnológica de El Salvador se encuentra previamente configurado, el uso de máquinas virtuales es recomendado en los laboratorios para sus prácticas, se observa la notificación en carteles al entrar al laboratorio. La implementación Microsoft ISA Server 2004 a Nivel de máquinas Virtuales permitirá conservar las configuraciones de los sistemas operativos previamente configurados en el equipo físico.

1.6.3 FACTIBILIDAD OPERATIVA

Resistencia al cambio: Con el estudio de campo efectuado se observa la falta del software ISA Server en laboratorio de redes de Universidad Tecnológica por lo tanto hay una buena aceptación por parte los estudiantes (usuarios del laboratorio de redes), el desarrollo de un material didáctico acerca del software de seguridad Microsoft ISA Server, el cual es necesario para adquirir el conocimiento de la tecnología.

Capacitaciones: Los estudiantes de la Universidad Tecnológica de El Salvador reflejan como respuesta la aceptación de recibir capacitaciones con el material didáctico a desarrollarse, además los estudiantes obtendrán más y mejores conocimientos del uso de software de seguridad podrán familiarizarse con

facilidad al ambiente de las redes informáticas en cuanto a la administración de seguridad la cual es muy importante.

Se recomienda capacitar al o los encargados del laboratorio de redes de la institución para asistir o dar apoyo practico-teórico a los, maestros y estudiantes en prácticas con el software ISA Server 2004.

Competencias: Los estudiantes de la Universidad Tecnológica de El Salvador obtendrán un mejor nivel de competencia académico-técnico, conocimiento que podría agregarse en el currículum de los Técnicos en Ingeniería de redes computaciones graduados de la institución.

La universidad ofrecerá a sus estudiantes conocimientos sobre el servidor de seguridad de Microsoft, incluso podrá mencionarlo en la descripción de la carrera, la cual es utilizada por los aspirantes interesados en estudiar en la Universidad Tecnológica de El Salvador.

En la práctica muchas empresas utilizan Microsoft ISA Server (Firewall) para administrar su seguridad y no ponerse en riesgo; para lo cual es necesario tener conocimientos previos.

Capacitando a los encargados del laboratorio de redes de la Universidad Tecnológica se pretende mejorar el nivel de conocimientos teóricos-prácticos del personal incrementando su perfil académico.

1.7 MARCO TEÓRICO DE REFERENCIA

1.7.1 Introducción ISA Server

ISA Server se remonta hasta su antecesor llamado Proxy Server 1.0, las primeras ediciones de este producto fueron puestas a la venta junto con la integración de Windows NT 4.0 para redes empresariales, sus primera ediciones fueron muy limitadas ya que solo soportaba algunos protocolos de Internet muy básicos y prácticamente las herramientas de seguridad no estaban presentes.

Microsoft lanzo luego una edición posterior llamada Proxy Server 2.0 el cual fue una evolución con muchos usos y funciones, una de las más grandes aplicaciones de estas herramientas fue el uso en base de datos, contaba también con un mayor soporte de protocolos, una mejora en servicios de caché filtrado de paquetes y una ejecución avanzada de seguridad sin embargo todavía contaba con funciones limitadas comparándolo con productos de terceros.

ISA Server fue la solución propuesta por Microsoft al integrar las nuevas plataformas Windows 2000 Server y Windows XP. ISA Server trajo consigo nuevos términos a la implementación y desarrollo de redes empresariales, tales como array, domain array, independent array, rules y array policy.

Con el creciente aumento de las actividades empresariales en Internet y el cada vez mayor número de redes corporativas conectadas a ella, cada vez es más

necesario disponer de una puerta de enlace a Internet eficaz y fácil de utilizar que proporcione una conexión segura al tiempo que mejore el rendimiento de la red. ISA Server protege la red y permite implementar la directiva de seguridad de su empresa mediante un amplio conjunto de reglas que permiten especificar qué sitios, protocolos y contenido pueden pasar a través del equipo con ISA Server. ISA Server supervisa las solicitudes y las respuestas transmitidas entre Internet y los equipos cliente internos, y controla quién tiene acceso a qué equipos de la red corporativa. ISA Server también controla a qué equipos de Internet tienen acceso los clientes internos.

ISA Server ofrece muchas opciones de seguridad, como el filtrado de paquetes y la detección de intrusos o software mal intencionado. Puede crear directivas de acceso basadas en la información de nivel de usuario o en las direcciones IP (Protocolo Internet) y controlar cuándo se aplican las reglas.

Puede utilizar ISA Server para definir una directiva de publicación, proteger los servidores de publicación internos y permitir que los clientes de Internet tengan acceso seguro a los mismos.

ISA Server implementa una caché para los objetos que se solicitan con más frecuencia. Puede configurar la caché para asegurarse de que contiene los datos utilizados con más frecuencia en su organización o los datos a los que los clientes de Internet tienen acceso con más frecuencia.

1.7.2 COMPONENTES, SERVICIOS DE ISA SERVER

ISA Server 2004

- **Firewall.**

Uno de los roles de configuración primarios para ISA Server 2004 es como un cortafuegos de Internet (Firewall). Este servicio de firewall provee funciones específicas de seguridad a nivel de usuarios, grupos de usuarios y direcciones IP; también soporta State Full Packet Inspection el cual es una solución donde los paquetes que pasan a través de un firewall son detectados y analizados a nivel de protocolo y conectividad.

En este rol, el Servidor de ISA proporciona una entrada segura para los usuarios que desean acceder los recursos en Internet y un cortafuego que previenen el acceso no autorizado y los ataques de entrar en la red. Como Firewall, el Servidor de ISA es el un punto de la entrada así como el límite de seguridad primario entre la red interna e Internet.

El Servidor de ISA se configura con una tarjeta de red conectada a Internet y una segunda tarjeta de red conectada a la red interior.

En algunos casos, el Servidor de ISA puede tener una tercera tarjeta de red que esta conectada a una red del perímetro (DMZ).

- **Directiva de acceso al exterior**

Puede utilizar ISA Server para configurar reglas para sitios, contenido y protocolos que permiten controlar el acceso de los clientes internos a Internet. Las reglas de sitios y contenido especifican a qué sitios y a qué contenido se puede tener acceso. Las reglas de protocolo indican si se puede utilizar un determinado protocolo para las comunicaciones entrantes o salientes.

- **Detección de intrusiones.**

Los mecanismos integrados de detección de intrusiones pueden avisarle cuando se inicie un determinado tipo de ataque contra su red. Por ejemplo, puede configurar el equipo en el que esté instalado ISA Server para avisarle si se detecta un intento de exploración de puertos.

- **Asistente de seguridad del sistema.**

El Asistente de seguridad de ISA Server permite bloquear los clientes de Windows con el nivel de seguridad adecuado, según las plantillas predefinidas.

- **Filtros de aplicación.**

ISA Server analiza y controla el tráfico específico de aplicación mediante filtros que inspeccionan los datos y distinguen cada aplicación. Puede habilitar el filtrado inteligente para el Protocolo de transferencia de hipertexto (HTTP), el Protocolo de transferencia de archivos (FTP), el Protocolo simple de transferencia de correo (SMTP), el correo electrónico, el protocolo de

conferencias H.323, las secuencias multimedia, las llamadas a procedimientos remotos (RPC) y muchos otros.

- **Compatibilidad con VPN.**

Incluye un sistema de acceso remoto seguro, basado en estándares, mediante los servicios integrados de red privada virtual (VPN) de MS Windows 2003.

- **Almacenamiento en caché jerárquico.**

Permite establecer una jerarquía de cachés, mediante el encadenamiento de equipos con ISA Server, que permite que los clientes tengan acceso desde la caché que esté más próxima geográficamente.

- **Caché inversa.**

ISA Server puede almacenar en caché el contenido HTTP y FTP de los servidores de publicación, lo que mejora su accesibilidad.

- **Almacenamiento en caché programado.**

Puede utilizar el servicio de descarga de contenido de caché programado para configurar el momento en el que el equipo con ISA Server debe descargar desde Internet a su caché el contenido que se solicita con más frecuencia.

- **Publicación segura en Web.**

Las reglas de publicación en Web permiten el acceso seguro a los servidores Web internos. Así mismo, conceden a los clientes externos acceso a los servidores internos, al tiempo que los protegen frente a accesos no autorizados.

1.7.3 ADMINISTRACIÓN REMOTA DE ISA SERVER

Para la administración remota de ISA Server sólo se necesita instalar Administración de ISA, que puede ejecutarse en Windows 2000 Professional o versiones posteriores.

En su lugar, puede instalar Servicios de Terminal Server en modo de Administración remota en el equipo que ejecuta ISA Server. Si lo hace, no tendrá que instalar la herramienta Administración de ISA en otro equipo para poder realizar las funciones de administración remota. En su lugar, puede utilizar una sesión de Servicios de Terminal Server para administrar ISA Server. Microsoft® Internet Security and Acceleration (ISA) Server 2004 permite administrar equipos servidor ISA desde otros equipos. Todas las tareas administrativas del servidor ISA se pueden realizar de forma remota, desde un equipo que ejecute el cliente de Servicios de Terminal Server, como una Conexión a escritorio remoto, o desde un equipo remoto que tenga instalado Microsoft Management Console (MMC).

También es posible administrar varios equipos servidor ISA desde un solo equipo servidor ISA.

Tanto Terminal Server como MMC tienen ciertas ventajas en la administración de equipos servidor ISA.

Terminal Server le permite ver el escritorio del equipo servidor ISA como si estuviera delante del monitor de éste, lo que aumenta la frecuencia de actualización, ya que la tarea de actualizar la vista la realiza el equipo servidor ISA y sólo hay que transmitir al equipo remoto la información de la imagen que está en el monitor. Sin embargo, cada sesión de Terminal Server sólo permite ver un equipo servidor ISA.

MMC tiene menor frecuencia de actualización que Terminal Server, ya que los cambios en la configuración que se puedan haber hecho se tienen que transmitir al equipo remoto. Sin embargo, MMC permite conectarse simultáneamente a muchos equipos servidor ISA y ver información de los mismos, lo que es útil para la administración central de equipos servidor ISA geográficamente dispersos o en aquellas situaciones en las que se ofrece consultoría a varias empresas que utilizan el servidor ISA. MMC forma parte de la instalación típica del servidor ISA, pero también se puede instalar como componente independiente para la administración de equipos servidor ISA.

Entornos de administración remota

Normalmente, el equipo servidor ISA estará alojado en una ubicación central con los restantes servidores corporativos, y no está cerca de la ubicación de la oficina. El servidor ISA se puede administrar desde otro equipo que se encuentre en la misma red que el equipo servidor ISA o desde un equipo

doméstico. Puede ofrecer servicios de consultoría a clientes que utilizan el servidor ISA para proteger sus redes y que son responsables del mantenimiento y supervisión de sus propios equipos servidor ISA. También puede administrar varios equipos servidor ISA ubicados en redes distintas. La administración remota le permite administrar el servidor ISA en todos estos casos.

Hay dos métodos de administración remota:

Administración remota mediante los Servicios de Terminal Server. Este método se recomienda para la administración desde un cliente de VPN.

Administración remota a través de Microsoft Management Console (MMC). MMC forma parte del servidor ISA, pero también se puede instalar sin la funcionalidad de servidor de seguridad del servidor ISA, sólo para administración.

MMC del servidor ISA se ejecuta en equipos que utilizan Windows® XP, Windows 2000 Professional o Windows 2000 Server.

La colocación del servidor ISA en relación con otras redes afecta al método de administración remota solamente en cuanto a la autenticación del cliente remoto. La provisión de credenciales difiere si el equipo servidor ISA está instalado en un grupo de trabajo, en lugar de en un dominio cuyo controlador reconozca credenciales de usuario. Ambas situaciones se tratan en los procedimientos que se incluyen en este documento.

La configuración de la administración remota exige la realización de cambios en la directiva del sistema de su equipo servidor ISA.

Se recomienda exportar la configuración de la directiva del sistema a un archivo antes de realizar cualquier cambio en la directiva, con el fin de poder volver fácilmente a la directiva original si es necesario.

1.7.4 CARACTERÍSTICAS DE ISA SERVER

ISA Server puede instalarse con las características de servidor de seguridad y caché. También puede instalar únicamente las funciones de servidor de seguridad o las de caché. Durante el proceso de instalación tendrá que elegir el modo de instalación: servidor de seguridad, caché o integrado.

En el modo de servidor de seguridad puede configurar reglas que controlen las comunicaciones entre su red corporativa e Internet, para así protegerlas. En este modo, también puede publicar servidores internos para compartir los datos de los mismos con los usuarios de Internet.

En el modo de caché, puede mejorar el rendimiento de la red y ahorrar ancho de banda si almacena más cerca de los usuarios los objetos a los que tienen acceso con mayor frecuencia. Puede poner en ruta las solicitudes de los usuarios de Internet al servidor Web más adecuado.

En el modo integrado están disponibles todas las características de caché y servidor de seguridad. Puede configurar una directiva que tenga en cuenta tanto las necesidades de rendimiento de la caché como las necesidades de seguridad.

Según el modo que seleccione, dispondrá de diferentes características. La siguiente tabla enumera qué características están disponibles en los modos de servidor de seguridad y de caché. En el modo integrado están disponibles todas las características.

CARACTERÍSTICAS DE ISA SERVER

Característica	Servidor de seguridad	Caché
Directiva de acceso	Sí	Sí (sólo los protocolos HTTP y HTTPS)
Filtros de aplicación	Sí	No
Configuración de caché	No	Sí
Compatibilidad con los clientes SecureNAT y del servidor de seguridad	Sí	No
Filtrado de paquetes	Sí	No
Supervisión en tiempo real	Sí	Sí
Informes	Sí	Sí
Publicación de servidores	Sí	No
Red privada virtual	Sí	No
Filtros Web	Sí	Sí
Publicación en Web	Sí	Sí

Compatibilidad con clientes de proxy Web	Sí	Sí
---	----	----

1.7.5 TIPOS DE CLIENTES QUE ADMITE ISA SERVER

- **Clientes de Proxy Web.** Los clientes de Proxy Web envían las solicitudes directamente a ISA Server, pero el acceso a Internet está limitado al explorador. Puede configurar como cliente de Proxy Web cualquier explorador Web compatible con HTTP 1.1 (versión del protocolo que se utiliza por estándar en los navegadores Web, se puede observar esta opción en las opciones de Internet y luego opciones avanzadas).
- **Clientes SecureNAT.** Los clientes de Traducción de direcciones de red segura (SecureNAT) proporcionan seguridad y almacenamiento en caché, pero no permiten realizar la autenticación en el nivel de usuario. Para configurar un cliente SecureNAT sólo tiene que establecer la puerta de enlace predeterminada en el equipo cliente como la dirección de Protocolo Internet (IP) del equipo con ISA Server. Como para configurar los clientes SecureNAT sólo es

necesario cambiar la puerta de enlace predeterminada, cualquier equipo que utilice el Protocolo de Control de Transporte/Protocolo Internet (TCP/IP) puede ser un cliente SecureNAT.

- **Clientes de servidor de seguridad.** Los clientes de servidor de seguridad restringen el acceso de cada usuario al exterior para las solicitudes que utilizan TCP y el Protocolo de datagramas de usuario (UDP). Para configurar un cliente de servidor de seguridad debe instalar el software correspondiente en cada equipo cliente. Sólo puede instalar el programa cliente del servidor de seguridad en aquellos equipos que utilicen Microsoft Windows Millennium Edition, Microsoft Windows 95 OSR2, Microsoft Windows 98, Windows NT 4.0 o Windows 2000.

Depende de las necesidades de la organización así se determina qué aplicaciones se necesitaran.

Si desea:	Utilice:
Mejorar el rendimiento de las solicitudes Web para los clientes internos	Clientes de Proxy Web.
Evitar la instalación de software cliente o la configuración de equipos cliente	Clientes SecureNAT. Los clientes SecureNAT no necesitan ninguna configuración específica ni ningún software

Publicar en servidores ubicados en la red interna	Clientes SecureNAT. Los servidores internos se pueden publicar como clientes SecureNAT, lo que elimina la necesidad de crear opciones de configuración especiales en cada servidor. No se recomienda configurar los servidores de publicación como clientes de servidor de seguridad.
Permitir el acceso a Internet sólo a los usuarios autenticados	Clientes de servidor de seguridad. En los clientes de servidor de seguridad puede configurar reglas para la directiva de acceso basadas en los usuarios

CLIENTES DE ISA SERVER VRS NAT, PROXY CLIENT

ISA Server admite los siguientes clientes:

- Clientes de Proxy Web
- Clientes de SecureNAT (Traducción de direcciones de red segura)
- Clientes de servidor de seguridad

En la siguiente tabla se muestran los tipos de cliente compatibles con ISA Server y se comparan la característica de cada uno de ellos.

Característica	Cliente SecureNAT	Cliente servidor de seguridad	Cliente de Proxy Web
Requiere instalación	No, pero es necesario modificar la configuración de la red.	Sí	No, requiere configurar el explorador Web
Compatibilidad con sistemas operativos	Cualquier sistema operativo compatible con el Protocolo de control de transporte/Protocolo Internet (TCP/IP).	Sólo plataformas Windows	Todas las plataformas TCP/IP

Protocolos admitidos	Los protocolos con conexiones principales y los protocolos definidos por los filtros de aplicación	Todas las aplicaciones Winsock	HTTP, HTTPS y FTP
Autenticación de nivel de usuario	No, sólo por dirección IP	Sí, también por dirección IP	El explorador Web pasa la información de autenticación
Publicación de servidores	No se requiere ni configuración	Requiere un archivo de configuración	N/D

1.7.6 ESCENARIOS DE IMPLEMENTACIÓN

Microsoft Internet Security and Acceleration (ISA) Server puede implementarse en diferentes topologías de red.

Esta sección describe algunas de las configuraciones de red más habituales. Aunque la configuración real de su red puede ser diferente de las que se describen aquí, los conceptos básicos y la lógica de la configuración le permitirán hacer una idea acerca de cómo aplicarlas a su configuración.

A continuación se incluyen las siguientes secciones:

- a. Servidores de seguridad y almacenamiento en caché en una red pequeña
- b. Conectar clientes remotos
- c. Escenarios de publicación en Web

- d. Escenarios de publicación en servidores seguros
- e. Escenarios con redes perimetrales

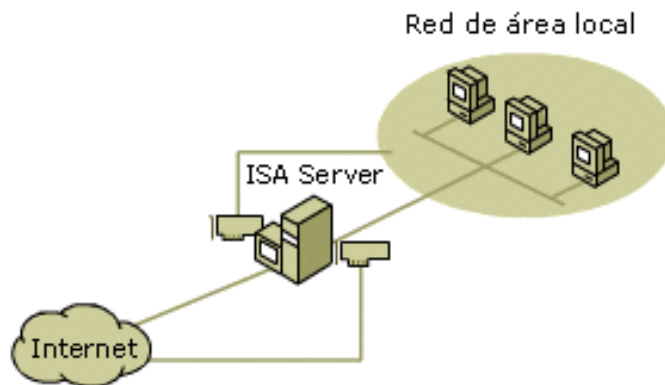
a. Servidores de seguridad y almacenamiento en caché en una red pequeña

Es posible implementar ISA Server en una red pequeña, lo que proporciona a los clientes internos la posibilidad de establecer conexiones seguras con la red. Debido a sus múltiples funciones, ISA Server también puede actuar como servidor de caché para los clientes internos.

Configuración de la red: En este escenario, ISA Server se instala en la red corporativa para actuar como conexión entre la red local e Internet. Los usuarios se configuran como clientes del Proxy Web o como clientes SecureNAT. Se crea una directiva de acceso en el equipo con ISA Server que estipula qué usuarios tienen acceso a Internet.

Configurar el equipo con ISA Server: ISA Server se instala como servidor independiente en modo integrado. Se configura una conexión de acceso telefónico con el Proveedor de servicios Internet (ISP). El equipo con ISA Server tiene una tarjeta de red conectada a la red interna y un módem para el acceso a Internet.

Además, en el equipo con ISA Server no se ejecuta ningún otro servicio (como exploradores Web, Outlook o Terminal Server).



Configurar los clientes: La mayoría de los usuarios sólo necesitan acceso Web. Por ello, el administrador configura la mayoría de los clientes como clientes del Proxy Web. En los equipos configurados como clientes de Proxy Web, los exploradores se configuran para que el servidor Proxy sea el equipo con ISA Server. El puerto configurado en el explorador Web para el servidor Proxy es el 8080, siempre y cuando la configuración de las solicitudes Web salientes en el equipo con ISA Server también corresponda al puerto 8080.

Algunos usuarios pueden utilizar protocolos de transmisión multimedia de Windows, por lo que sus equipos también están configurados como clientes SecureNAT. La puerta de enlace predeterminada para los clientes SecureNAT es la dirección IP del equipo con ISA Server. De este modo, todas las solicitudes dirigidas a Internet se reenviarán al equipo con ISA Server, que se encargará de ellas según indique la directiva de acceso.

Configurar la directiva de ISA Server: Después de configurar el equipo con ISA Server, el administrador utiliza Administración de ISA para implementar la directiva de acceso.

Sin embargo, antes de crear las reglas de directiva el administrador crea los siguientes elementos de directiva:

- Como los permisos de acceso a Internet son diferentes para cada departamento, se necesitan tres conjuntos de direcciones de cliente, uno para cada departamento. Cada conjunto de direcciones de cliente incluye las direcciones IP de los equipos de uno de estos tres departamentos: Ventas, Investigación y desarrollo y Recursos humanos.

- Las directrices de negocio especifican que durante la jornada laboral sólo se puede tener acceso a determinados sitios de Internet. Por tanto, el administrador crea un conjunto de destino, llamado Sitios para horario de trabajo, en el que incluye dichos sitios. De este modo es posible aplicar las reglas a un único conjunto de destinos.

- Por otra parte, las directrices del negocio permiten el acceso a Internet a todos los empleados después de la jornada de trabajo, por lo que el administrador crea un programa llamado Después del trabajo que puede utilizarse al crear las reglas que permiten el acceso a Internet en este horario.

- Como se utiliza una conexión de acceso telefónico a Internet, el administrador crea una entrada de marcado llamada Llamar_ISP. Esta entrada de marcado se

utilizará cada vez que el equipo con ISA Server necesite tener acceso a un objeto de Internet.

b. Conectar clientes remotos

Cada vez más empleados trabajan desde sus casas y utilizan desde sus equipos domésticos el acceso telefónico a la red corporativa. Por ello, es también cada vez más habitual que los empleados establezcan una conexión de red privada virtual (VPN). En esta situación, el usuario llama a su ISP local. En el otro extremo, uno de los servidores de la red corporativa está conectado a su ISP y se establece un túnel entre ambos.

Configuración de la red: ISA Server se instala como servidor independiente en modo integrado. En el equipo con ISA Server se configura una conexión de acceso telefónico a redes para llamar al Proveedor de servicios Internet (ISP). Además, el equipo con ISA Server dispone de una tarjeta de red conectada a la red interna.

El equipo con ISA Server está configurado como servidor VPN, lo que permite que determinados clientes remotos se comuniquen con los recursos de red.

Los clientes que se conectan con el equipo con ISA Server mediante VPN deben poder tener acceso a los recursos de la red corporativa, como DNS y WINS.

Los equipos cliente remotos deben tener configurada una conexión de acceso telefónico para llamar al ISP local.

Configurar ISA Server: Después de instalar ISA Server en el equipo, el administrador utiliza Administración de ISA para configurar el equipo como VPN de ISA Server. Para ello, el administrador:

Utiliza el Asistente para VPN entre el cliente y el servidor con el fin de configurar ISA Server de manera que acepte las conexiones de los clientes. El asistente:

- Configura Enrutamiento y acceso remoto como servidor VPN
- Exige los métodos de autenticación y cifrado
- Abre los filtros de paquetes estáticos en Enrutamiento y acceso remoto para permitir el Protocolo punto a punto (PPTP) y el Protocolo de túnel de capa 2 (L2TP) sobre los protocolos de Seguridad del Protocolo Internet (IPSec).

Crea una conexión de acceso telefónico a redes en el equipo cliente, configurada del siguiente modo:

- El tipo de conexión de red es VPN. (Para ello, seleccione Conectar a una red privada a través de Internet.)
- La dirección de destino es la dirección IP del VPN de ISA Server.

c. Escenarios de publicación en Web

Las funciones de publicación en Web de ISA Server resultan útiles para las organizaciones que desean publicar contenido en Web de forma segura.

ISA Server puede proteger el servidor Web de su organización en el que se aloja un sitio Web comercial o que proporciona acceso a los asociados comerciales. El equipo con ISA Server representa al servidor Web para el mundo exterior, mientras que el servidor Web mantiene el acceso a los servicios de red internos.

El servidor Web en el que se publica el contenido puede encontrarse en el mismo equipo que ISA Server o en otro diferente. En las siguientes secciones se muestran configuraciones de red para escenarios de publicación en Web.

Configurar el equipo con ISA Server: Independientemente de la configuración del escenario de publicación en Web, debe configurar ISA Server para escuchar las solicitudes Web entrantes. Las propiedades de las solicitudes Web entrantes especifican en qué direcciones IP y puertos del equipo con ISA Server se deben escuchar las solicitudes. Dichas propiedades también determinan la autenticación necesaria para el acceso a los servidores internos.

Configurar el servidor DNS: Si publica contenido en servidores Web, es posible que los clientes externos necesiten resolver sus nombres con el servidor DNS interno. En sí mismo, el servidor DNS interno es también un servidor de publicación. Si el servidor DNS es un cliente SecureNAT, no es necesario realizar ninguna configuración. Después de instalar ISA Server, cree una regla

de publicación en servidores en el equipo con ISA Server que publique el servidor DNS.

d. Escenario con un servidor Web en una red local:

En el escenario de publicación en Web que se describe a continuación, ISA Server protege el contenido de los servidores Web internos ubicados en los equipos de la red local.

La corporación que se utiliza como ejemplo publica dos sitios Web: <http://ejemplo.microsoft.com/Marketing> y <http://ejemplo.microsoft.com/Desarrollo>. El contenido de dichos sitios se encuentra en dos servidores Web internos diferentes: Mktg y Des, respectivamente. Cuando un usuario de Internet solicita un objeto de <http://ejemplo.microsoft.com/Marketing> o de <http://ejemplo.microsoft.com/Desarrollo>, la solicitud en realidad se envía al equipo con ISA Server, que a su vez la enruta al servidor Web apropiado.

El administrador debe realizar los siguientes pasos para publicar los servidores Web internos:

- Comprueba que el servidor DNS asigna el nombre de dominio completo a la dirección IP del equipo con ISA Server. Los clientes de Internet utilizan el nombre de dominio para solicitar el contenido.

-Configura las propiedades de ISA Server para las solicitudes Web entrantes.

La dirección IP debe incluir la dirección IP de la interfaz externa.

Crea los siguientes elementos de directiva:

-Un conjunto de destinos llamado Marketing, que debe incluir el equipo ejemplo.microsoft.com y la ruta de acceso \Marketing*. Se trata del encabezado de host con el que ISA Server intentará encontrar una coincidencia para poder enrutar la solicitud al servidor interno correcto.

-Un conjunto de destinos llamado Desarrollo, que debe incluir el equipo ejemplo.microsoft.com y la ruta de acceso \Desarrollo*.

Configura las siguientes reglas:

-Una regla de publicación en Web que publica el equipo Mktg, en la que el conjunto de destino configurado sea Marketing.

-Una regla de publicación en Web que publica el equipo Des, en la que el conjunto de destino configurado sea Desarrollo.

Utilizar reglas de publicación en Web para publicar un servidor Web en un equipo con ISA Server:

En este escenario, el administrador configura el equipo con ISA Server para escuchar las solicitudes entrantes en el puerto 80 de la tarjeta de interfaz externa. De manera predeterminada, el servidor Web también escucha las solicitudes entrantes en el puerto 80.

Para evitar este conflicto, el administrador debe realizar una de las siguientes acciones:

- Configurar el servidor Web para que escuche en un puerto distinto del 80 o en un adaptador de red diferente y, a continuación, crear una regla de publicación en Web en el equipo con ISA Server para reenviar las solicitudes al puerto apropiado del servidor Web.
- Configurar el servidor Web para verla reflejada en una dirección IP diferente. Por ejemplo, el servidor Web la puede ver reflejada en la dirección 127.0.0.1. De ese modo, el servidor Web sólo escuchará las solicitudes que provengan del equipo local. En realidad, estas solicitudes provienen de ISA Server.

Utilizar el filtrado de paquetes para publicar un servidor Web en un equipo con ISA Server:

Otra forma de publicar un servidor Web ubicado en el equipo con ISA Server es configurar filtros de paquetes IP. El filtro de paquetes IP pasa todos los paquetes que llegan al puerto 80 al servidor Web, que se encuentra en el equipo con ISA Server. El filtro de paquetes permite que el servidor Web escuche las solicitudes Web entrantes en el puerto 80.

e. Escenarios con redes perimetrales

Una red perimetral (denominada también *DMZ*, zona desmilitarizada y subred apantallada) es una pequeña red que se mantiene separada de la red privada de una organización y de Internet. La red perimetral permite que los

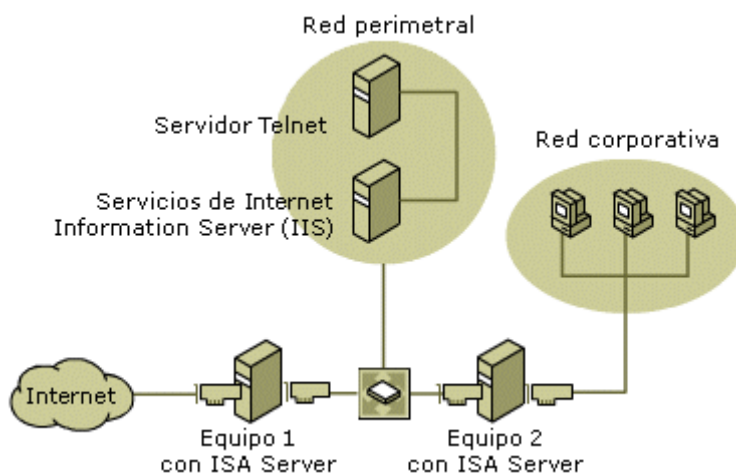
usuarios externos tengan acceso a los servidores que se encuentran en ella, al tiempo que impide el acceso a la red corporativa interna. Una organización también puede permitir el acceso limitado desde los equipos de las redes perimetrales a los equipos de la red interna.

Una red perimetral suele utilizarse para implementar los servidores Web y de correo electrónico de la compañía. Puede configurarse de una de estas formas:

- Configuración de red perimetral opuesto con opuesto, en la que hay dos equipos con ISA Server en cada lado de la red perimetral.
- Equipo con ISA Server de triple servicio, en el que el mismo equipo con ISA Server protege la red local y la red perimetral.

Escenario de red perimetral opuesto con opuesto

En este escenario hay dos equipos con ISA Server en cada lado de la red perimetral. (Una *red perimetral* también se denomina *DMZ*, *zona desmilitarizada* y *subred apantallada o blindada*.) La figura muestra una configuración de red perimetral opuesto con opuesto.



En esta configuración hay dos equipos con ISA Server conectados entre sí, uno de ellos conectado a Internet y el otro a la red local. La red perimetral se encuentra entre ambos servidores. Los dos servidores ISA están configurados en modo integrado o de servidor de seguridad, lo que reduce el riesgo de poner en peligro la seguridad, ya que un supuesto atacante tendría que infiltrarse en ambos sistemas para poder llegar a la red interna.

El administrador realiza los siguientes pasos para que los servidores de la red perimetral estén disponibles para los clientes externos, como los clientes de Internet:

- Configura la tabla de direcciones locales local (LAT) en el equipo con ISA Server conectado a la red corporativa (indicado como ISA Server 2) para que incluya las direcciones IP de los equipos de la red corporativa.

- Configura la LAT del equipo con ISA Server conectado a Internet para que incluya la dirección IP del servidor ISA conectado a la red corporativa y las direcciones IP de todos los servidores de publicación de la red perimetral.

- Crea una regla de publicación en Web para publicar el servidor IIS.

- Crea una regla de publicación en Web para publicar el servidor IIS y la configura para redirigir las solicitudes al sitio alojado.

Escenario de red perimetral de triple servicio

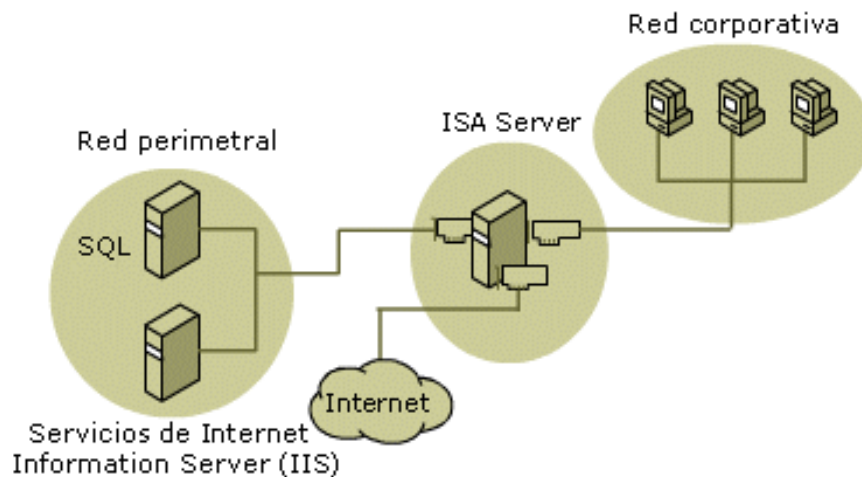
En este escenario se configura un único equipo con ISA Server con tres adaptadores de red.

-Uno de los adaptadores de red se conecta a los clientes internos de la red corporativa.

-El segundo adaptador de red se conecta con los servidores de la red corporativa, que se encuentran en la red perimetral. Las direcciones IP de la red perimetral no deben estar incluidas en la Tabla de Direcciones Locales (LAT).

-El tercer adaptador de red se conecta a Internet.

La figura muestra este escenario de red perimetral.



El administrador realiza los siguientes pasos para configurar una red perimetral con un equipo con ISA Server de triple servicio:

-Configura la tabla LAT para que incluya todas las direcciones de la red corporativa. La LAT no debe incluir las direcciones de la red perimetral.

-Habilita el filtrado de paquetes y el enrutamiento IP.

-Crea filtros de paquetes IP para cada uno de los servidores de la red perimetral. En cada filtro de paquetes IP se debe especificar el equipo local como la dirección IP del servidor de la red perimetral.

1.7.7 Resumen de características de ISA Server

ISA Server 2004 incluye numerosas características y mejoras, particularmente cuando se instala en un sistema donde se ejecuta Windows Server 2003.

Infraestructura de Seguridad

- Nuevo soporte de protocolos ampliado, permitiendo el control de acceso y el uso de cualquier protocolo, incluido los de nivel IP.
- Mejora la autenticación de usuarios con los métodos de Windows, RADIUS u otros que pueda generar el administrador a través del kit de desarrollo.
- Nuevo soporte para protocolos complejos que requieren múltiples conexiones primarias.
- Nuevas definiciones de protocolos personalizables.

- Nuevos grupos de usuarios de firewall, lo que incrementa la flexibilidad en el control de accesos.
- Nuevas credenciales de cliente de firewall restringidas al servicio Web Proxy.
- Mejora el control de aplicaciones de mensajería instantánea tales como MSN Messenger, a través de las políticas del firewall.
- Mejora los objetos de red.
- Mejoran los asistentes para la creación de reglas de firewall.
- Mejoran las reglas de firewall que representan una lista ordenada.
- Mejoran las políticas de acceso basadas en usuarios y grupos.
- Mejora el asistente de publicación para Outlook Web Access (OWA).
- Mejora el soporte para FTP.
- Mejora la redirección de puertos para reglas de publicación de servidores.
- Mejora la publicación Web segura.

Filtrado de nivel de aplicación

- Nuevo filtro HTTP basado en reglas.
- Nuevo bloqueo de acceso a todo contenido ejecutable.
- Nuevo control de descargas HTTP mediante extensión de archivo.
- Ahora el filtro HTTP se aplica a todas las conexiones cliente de ISA Server 2004.
- Nuevo control de acceso HTTP basado en firmas HTTP.

- Se permite el control de métodos HTTP.
- Conexiones Exchange RPC seguras obligatorias desde clientes Outlook MAPI.
- Posibilidad de configuración de políticas FTP.
- Nuevo traductor de enlaces.
- Nuevo control granular sobre opciones IP.

Múltiples redes

- Configuración de múltiples redes.
- Políticas particulares por red.
- Relaciones de red con enrutamiento y NAT.
- Mejora de la administración VPN
- Inspección dinámica del contenido en VPN
- Soporte de cliente SecureNAT para clientes VPN conectados al servidor VPN de ISA Server 2004
- Filtrado e inspección dinámica de contenido para comunicaciones por túnel VPN intersite
- Cuarentena VPN
- Publicación de servidores VPN
- Soporte para modo túnel IPSec para enlaces entre sites.

Acceso remoto seguro a servidores Microsoft

- Formularios generados por el firewall para autenticación basada en formularios.

- Asistente de publicación Outlook Web Access.
- Mejora el Delimitador de mensajes SMTP.
- Publicación de servidores VPN Microsoft.
- Acceso remoto a Servicios de Terminal utilizando VPN con SSL.
- Asistente de publicación servidor Web seguro.
- Cifrado obligatorio para conexiones seguras con Exchange usando RPC.
- Mejora la administración.
- Capacidad de exportación importación.
- Asistente de permisos delegados para roles de administrador de firewall.

Monitorización e informes

- Monitorización e informes en tiempo real.
- Facilidades de consulta al Log incorporadas.
- Monitorización y filtrado en tiempo real de las sesiones de firewall.
- Verificadores de conexión.
- Mejora la personalización de informes de ISA Server 2004.
- Nueva publicación de informes.
- Notificación por correo electrónico tras la creación de un informe.
- Ventana de tiempo personalizable para la creación de un informe.
- Log mejorado en SQL.
- Log en una base de datos MSDE.

Cache y Proxy para publicación Web

- Mejoran las reglas de caché.
- Mejora el mapeo de path para reglas de publicación Web.
- Nuevo soporte RADIUS para validación de cliente Web Proxy.
- Nueva delegación de la autenticación básica.
- Mantenimiento de la dirección IP de origen en las reglas de publicación Web.
- Autenticación SecurID para clientes Web Proxy.

1.7.8 GUÍA RÁPIDA DE INSTALACIÓN PARA ISASERVER 2004

Cuando instale ISA Server se le pedirá la siguiente información:

- Clave del CD (CD Key): Es el número de 10 dígitos que aparece en la parte posterior de la caja del CD-ROM de ISA Server (si utiliza versión de evaluación no lo pedirá).
 - Opciones de instalación: Puede seleccionar la instalación Estándar, Completa o Personalizada
 - Modo: Puede instalar ISA Server en modo de servidor de seguridad, de caché o integrado.
 - Configuración de la caché: Si instala ISA Server en los modos integrado o de caché, debe configurar que unidades de caché desea utilizar y el tamaño de la caché.
 - Configuración de la tabla de direcciones locales (LAT): Si instala ISA Server en los modos integrado o de servidor de seguridad, debe configurar los intervalos de direcciones que se incluirán en la LAT.
-
1. Inserte el CD-ROM de ISA Server en la unidad de CD-ROM o ejecute ISAautorun.exe desde la carpeta compartida de la red.

2. En el programa de instalación de Microsoft ISA Server, haga clic en **Instalar el servidor ISA**.
3. Si acepta los términos y condiciones indicados en el contrato de licencia para el usuario final, haga clic en **Continuar**.
4. Escriba el número de identificación del producto que aparece en la caja del producto.
5. Lea el contrato de licencia para el usuario final y, a continuación, si está de acuerdo con sus términos y condiciones, haga clic en **Aceptar**.
6. Haga clic en Instalación Estándar, Instalación Completa o Instalación Personalizada.
Si hace clic en **Instalación personalizada**, active las casillas de verificación correspondientes a los componentes de ISA Server que desea instalar. Puede elegir entre las siguientes:
 - Servicios del servidor ISA.
 - Servicios de complementos.
 - Herramientas de administración.
7. Haga clic en el modo del servidor ISA que desee instalar.
8. Cuando el programa de instalación le avise de que detendrá Servicios de Internet Information Server (IIS), si decide instalar ISA Server en el modo de caché o en el modo integrado, configure las unidades de caché.
9. Si instala ISA Server en modo de servidor de seguridad o en modo integrado, configure la LAT(tabla de direcciones locales)
10. Si desea ejecutar el Asistente de introducción al ejecutar ISA Server, active la casilla de verificación **Iniciar el Asistente para la introducción al administrador de ISA**.

CAPÍTULO II

PROYECTO TEMATICO

2.0 PROYECTO TEMÁTICO

La Universidad Tecnológica de El Salvador ubicada en la dirección siguiente: calle arce N° 1020 San Salvador, posee dentro de su oferta académica la carrera de Técnico en Ingeniería de Redes Computacionales la cual posee más de dos años de ser impartida en dicha institución educativa

La Universidad Tecnológica posee un centro de cómputo específico para redes, le han asignado el nombre de Laboratorio de Redes, en este lugar se realizan los estudios prácticos de los estudiantes de la carrera de Técnico en Ingeniería de Redes Computacionales. Las autoridades de la institución educativa han designado el respectivo pensum de materias a cursar para esta carrera, sin embargo durante el proceso de aprendizaje que realizan los estudiantes, existen deficiencias tanto prácticas como teóricas, específicamente en la educación que se les brinda de un software que es necesario para crear seguridad en las redes de computadoras, a este software se le conoce con el nombre de Microsoft ISA Server 2004, Según un estudio realizado previamente a los estudiantes de dicha carrera técnica, se ve reflejado un buen porcentaje de desconocimiento y un mayor porcentaje de apreciación e interés de los estudiantes para conocer más sobre este importante software.

Por tal razón se ve la necesidad de crear un material didáctico del software ISA Server 2004, que brinde información útil sobre dicho software y mejore las

destrezas educativas de los futuros Técnicos en Ingeniería de Redes Computacionales de la Universidad Tecnológica de El Salvador

La creación de este material didáctico se dividirá en las siguientes fases:

FASE 1

Definición de los contenidos.

El software: Microsoft ISA Server 2004, posee una considerable cantidad de teoría la cual se encuentra en el sitio Web de su fabricante el cual es: www.microsoft.com, gran parte del material teórico proviene de dicho sitio Web, el material didáctico a realizar debe acoplarse de tal manera que pueda ser incluido dentro de la carrera de Técnico en Ingeniería de Redes computacionales y a la vez tenga un espacio exclusivo en su ejecución práctica, por lo tanto, el material didáctico a realizar consiste en la creación de siete guías que permita realizar las prácticas más importantes que posee el software Microsoft ISA Server 2004 y su contenido teórico debe acoplarse de tal forma que el docente pueda brindar información clara y confiable en su cátedra optimizando el tiempo para poder brindar información de dicho software y generar interés al estudiante para que este se involucre en un estudio más profundo.

FASE 2

Selección de tecnología

La tecnología a utilizar en este material didáctico hace referencia al software que tiene como nombre: Microsoft ISA Server 2004, es de enfatizar que el

laboratorio de redes, posee computadoras con especificaciones técnicas apropiadas para ejecutar ISA Server 2004

FASE 3

Para generar el proyecto se brinda un material didáctico al docente y al estudiante que proporciona la información tanto teórica como practica del software Microsoft ISA Server 2004, en el cual se estudian los roles mas importantes del software, así mismo se brinda al estudiante guías practicas para poder ejecutarlos en el laboratorio de redes de la Universidad Tecnológica, de esta forma se dará como producto un material didáctico en el que se abarcan estudios prácticos y teóricos del software Microsoft ISA Server 2004, El estudiante se vera beneficiado por información actualizada que no se encuentra en biblioteca.

Con el producto desarrollar el estudiante que demuestre interés de investigación acerca del software, encuentre el manual y CD interactivo didáctico en el cual se muestra de una forma más dinámica y con recurso multimedia las prácticas realizadas, con dicho software, todo esto en un material didáctico esencial para la educación de aquel futuro Técnico en Ingeniería de Redes Computacionales de la Universidad Tecnológica de El Salvador.

2.1 DOCUMENTACIÓN TÉCNICA

2.1.1 MICROSOFT INTERNET SECURITY AND ACCELERATION

ISA SERVER 2004

Microsoft Internet Security and Acceleration (ISA) Server 2004 proporciona una protección avanzada, facilidad de uso y acceso rápido y seguro para todo tipo de redes.

ISA Server 2004, incluido en Microsoft Windows Server System™, es una solución segura, fácil de usar y rentable que ayuda a los profesionales de tecnologías de la información a combatir las nuevas amenazas de seguridad que surgen cada día.

ISA Server 2004 protege su red y permite implementar la directiva de seguridad de su empresa mediante un amplio conjunto de reglas que permiten especificar qué sitios, protocolos y contenido pueden pasar a través del equipo con ISA Server. ISA Server supervisa las solicitudes y las respuestas transmitidas entre Internet y los equipos cliente internos, y controla quién tiene acceso a qué equipos de la red corporativa. ISA Server también controla a qué equipos de Internet tienen acceso los clientes internos.

ISA Server 2004 ofrece muchas opciones de seguridad, como el filtrado de paquetes y la detección de intrusiones. Puede crear directivas de acceso

basadas en la información de nivel de usuario o en las direcciones IP (Protocolo Internet) y controlar cuándo se aplican las reglas.

Además, ISA Server permite la publicación segura en Internet. Puede utilizar ISA Server para definir una directiva de publicación, proteger los servidores de publicación internos y permitir que los clientes de Internet tengan acceso seguro a los mismos.

ISA Server implementa una caché para los objetos que se solicitan con más frecuencia. Puede configurar la caché para asegurarse de que contiene los datos utilizados con más frecuencia en su organización o los datos a los que los clientes de Internet tienen acceso con más frecuencia.

Usted puede utilizar ISA Server 2004 para crear grupos de usuarios firewall que consisten en grupos preexistentes en la base de datos de cuentas locales o el dominio de servicio de directorio Active Directory. Esto aumenta la flexibilidad para controlar el acceso sobre la base de membresía grupal o de un usuario, porque el administrador de firewall puede crear grupos de seguridad a partir de estos grupos existentes.

Esto elimina el requisito de que el administrador de firewall sea un administrador de dominio para acreditar grupos de seguridad pre fijados para control de acceso de entrada y salida.

2.1.2 CARACTERÍSTICAS TÉCNICAS DE ISA 2004

ISA Server 2004 ofrece las siguientes novedades y mejoras con respecto a versiones anteriores:

Protección avanzada

Filtro de Capa de Aplicación		
Nuevo o Mejorado	Característica	Descripción
Nuevo	Filtro de HTTP sobre una base por regla	La política de HTTP del ISA Server 2004 le permite al firewall realizar una inspección basada en el estado exhaustiva y profunda de HTTP (Filtro de capa de aplicación). El grado de inspección se configura por regla. Con esta capacidad, se pueden configurar trabas personalizadas para acceso de ingreso o salida de Internet.
Nuevo	Bloqueo de acceso a todos los contenidos ejecutables	La política de HTTP de Isa Server 2004 puede configurarse para bloquear todos los intentos de conexión a contenido ejecutable del sistema de operación Windows de Microsoft, más allá de la extensión del nombre del archivo que se utilice en la fuente.
Nuevo	Control de descargas de archivos HTTP a través de la extensión del nombre de archivo	La política HTTP de ISA Server 2004 le permite definir una política basada en la extensión del nombre del archivo, que incluya " permitir todos excepto un grupo especificado de extensiones" o " bloquear todos excepto un grupo específico".
Nuevo	El filtro de HTTP se aplica a todas las conexiones cliente de ISA Server 2004	Con la política ISA Server 2004, usted puede controlar el acceso HTTP para todas las conexiones cliente de ISA Server 2004.
Nuevo	Control de acceso HTTP basado en firmas HTTP	La profunda inspección de ISA Server 2004 puede ayudarle a crear "Firmas HTTP" comparadas con el Request URL, encabezadores Request, Request body, Response body. Esto le ofrece un control preciso sobre el contenido al que los usuarios internos y externos pueden acceder mediante el firewall de ISA Server 2004.

Filtro de Capa de Aplicación		
Nuevo o Mejorado	Característica	Descripción
Nuevo	Métodos HTTP de control permitidos	Estableciendo controles de acceso en el acceso del usuario para varios métodos, usted puede controlar cuáles son los métodos HTTP permitidos mediante el firewall. Por ejemplo, puede limitar el método POST HTTP para evitar que usuarios envíen datos a sitios WEB utilizando este método HTTP Post.
Nuevo	Política FTP	Puede configurar la política FTP de ISA Server 2004 para permitir a los usuarios subir o descargar archivos mediante FTP, o puede limitar el acceso FTP del usuario a realizar sólo descargas.

Seguridad y Firewall

Seguridad y Firewall		
Nuevo o Mejorado	Característica	Descripción
Nuevo	Soporte de protocolo extensivo	ISA Server 2004 le ofrece control sobre el uso y acceso de cualquier protocolo, incluidos los protocolos de nivel IP. Los usuarios pueden utilizar aplicaciones como ping y TRACERT para establecer conexiones VPN utilizando PPTP. Además, mediante ISA Server, se puede habilitar el tráfico IPSec.
Nuevo	Definiciones de protocolo fijadas por el usuario	Con ISA Server 2004, usted puede controlar el número de puerto de origen y el destino de cualquier protocolo al que le haya creado una norma firewall. Esto le otorga al administrador de firewall de ISA Server 2004 un alto nivel de control para permitir el ingreso y la salida de los paquetes a través del firewall.
Nuevo	Grupos de usuarios de firewall	Usted puede utilizar ISA Server 2004 para crear grupos de usuarios firewall que consisten en grupos preexistentes en la base de datos de cuentas locales o el dominio de servicio de directorio Active Directory. Esto aumenta la flexibilidad para controlar el acceso sobre la base de membresía grupal o de un usuario, porque el administrador de firewall puede crear grupos de seguridad a partir de estos grupos existentes. Esto elimina el requisito de que el administrador de firewall sea un administrador de dominio para acreditar grupos de seguridad pre fijados para control de acceso de entrada y salida.
Mejorado	Autenticación	Se pueden autenticar los usuarios utilizando Windows incorporado, RADIUS o el sistema de autenticación RSA u otro namespace. Proveedores terceros pueden utilizar un kit de desarrollo de software (SDK).

Seguridad y Firewall		
Nuevo o Mejorado	Característica	Descripción
Nuevo	Credenciales de cliente de firewall reenviadas al servicio de WEB Proxy	ISA Server 2004 le permite a los clientes de firewall acceder al WEB Caché con un filtro de HTTP sin requerir otra autenticación con el servicio Web Proxy.
Mejorado	Acceso a correo electrónico Hotmail basado en Web a través del firewall	El filtro de HTTP mejorado de ISA Server 2004 le permite a los usuarios acceder a Hotmail mediante una norma firewall fácil de configurar y no hace falta ninguna configuración especial para el cliente o el firewall.
Mejorado	Objetos de red	Con ISA Server 2004, usted puede expandir ampliamente la definición de objetos de red creando computadoras, redes, grupos de redes, rangos de direcciones, subredes, grupos de computadoras y grupos de nombre de dominio. Estos objetos de red se utilizan para definir lugares de origen y destino para las normas firewall.
Mejorado	Asistente de normas firewall	ISA Server 2004 incluye un nuevo grupo de Asistentes de normas que facilitan más que nunca la creación de una política de acceso. La política de acceso de ISA Server 2004 puede crearse mediante una sofisticada norma de firewall que puede utilizar para configurar cualquier elemento de política requerido en el instante. No es necesario ocultar el ayudante para crear un objeto de red; con el nuevo asistente se puede crear cualquier objeto o relación de red.
Mejorado	Las normas firewall representan una lista ordenada	Las reglas de firewall de ISA Server 2004 se encuentran representadas en una lista ordenada en la cual los parámetros de conexión se comparan primero con la norma principal de la lista. ISA Server 2004 recorre la lista de reglas hasta que encuentra la que se adecua a los parámetros de conexión y aplica la política de la norma adecuada. Este enfoque hacia la política de firewall facilita mucho más determinar por qué se acepta o rechaza un conexión específica.
Mejorado	Soporte FTP	ISA Server 2004 le ofrece acceso a Servidores FTP de Internet, analizando números de puertos alternados sin necesidad de una configuración especial en el firewall del cliente o el ISA Server 2004. La publicación del servidor FTP en números de puerto alternados sólo requiere de una simple Norma de Publicación de Servidor FTP.

Seguridad y Firewall		
Nuevo o Mejorado	Característica	Descripción
Mejorado	Redirección de Puerto para Normas de Publicación de Servidor FTP	Al utilizar ISA Server 2004, usted puede recibir una conexión en un número de puerto y redirigir el petitorio a un número de puerto diferente en el servidor publicado.
Mejorado	Publicación en Web Segura	Con ISA Server 2004, usted puede ubicar a los servidores detrás del firewall, ya sea en la red corporativa o en la red de perímetro (también denominada zona desmilitarizada [DMZ, por sus siglas en inglés] o subred examinada) y publicar sus servicios de manera segura. Con el ayudante de Publicación segura en WEB mejorado, usted puede crear una norma que le permita a los usuarios asegurar el acceso remoto SSL para los servidores de Web publicados.

Facilidad de uso

Interconexión múltiple		
Nuevo o Mejorado	Característica	Descripción
Nuevo	Configuración de red múltiple	Puede configurar una o más redes, cada una con relaciones distintas entre cada red. Las políticas de acceso se definen como relativas a las otras redes y no necesariamente relativas a una red interna en particular. ISA Server 2004 extiende las prestaciones de seguridad y firewall para aplicarlas al tráfico entre las redes y los objetos de red.
Nuevo	Políticas únicas por red	Las prestaciones de interconexión múltiple de ISA Server 2004 le permiten proteger su red de amenazas internas y externas a la seguridad, limitando la comunicación entre clientes aún en su propia organización. La funcionalidad de interconexión múltiple soporta escenarios de red perimetral sofisticados, y le ayuda a configurar cómo los clientes en diferentes redes pueden acceder la red perimetral.
Nuevo	Relaciones entre redes enrutadas y redes NAT	Puede utilizar ISA Server 2004 para definir relaciones de enrutador entre las redes, según el tipo de acceso y de comunicación que se requiera entre las redes. En algunos casos, usted puede desear comunicación más segura y menos transparente entre las redes. Para estos escenarios, puede definir una relación NAT, tal vez prefiera enrutar el tráfico mediante el ISA Server. En estos casos, puede definir una relación enrutada. Los paquetes que se transfieren entre las distintas redes están completamente expuestos a mecanismos de inspección basada en el estado y filtrado por parte del ISA Server 2004.

Acceso rápido y seguro

Acceso Remoto Seguro a los Servidores de Microsoft		
Nuevo o Mejorado	Característica	Descripción
Nuevo	Formularios generados por firewall para autenticación basada en formularios	ISA Server 2004 puede generar los formularios utilizados por sitios OWA para autenticación basada en formularios. Esto realza la seguridad para un acceso remoto a sitios OWA y evita que usuarios no autenticados contacten al servidor OWA.
Nuevo	Acceso Remoto a Servicios de Terminal utilizando SSL	Los ordenadores que utilizan el sistema operativo Windows Server 2003 de Microsoft soportan RDP sobre SSL para permitir una conexión segura SSL a los Servicios de Terminal de Windows Server 2003. Con ISA Server 2004, usted puede publicar de manera segura su Servidor de Terminal utilizando tecnología SSL segura.

Gestión

Gestión		
Nuevo o Mejorado	Característica	Descripción
Mejorado	Gestión	ISA Server 2004 incluye nuevas prestaciones de gestión, que facilitan la seguridad de sus redes. Las interfaces de usuarios nuevas incluyen Paneles de tareas, Paneles de ayuda, Un Asistente de Inicio mejorado, y un nuevo diseño para el Editor de Políticas Firewall.
Nuevo	Ingreso y salida de información	ISA Server 2004 presenta la capacidad de exportar e importar información de configuración. También puede utilizar esta prestación para guardar parámetros de configuración en un archivo XML, y luego importar la información del archivo a otro servidor.
Nuevo	Asistente de permisos delegados para roles de administración de firewall.	El Asistente de Delegación de Administración le ayudará a asignar roles administrativos a grupos y usuarios. Estos roles predefinidos delegan el nivel de control administrativo que tienen los usuarios dentro de los servicios de ISA Server 2004.

VPN – Redes privadas virtuales

Redes Privadas Virtuales		
Nuevo o Mejorado	Característica	Descripción
Mejorado	Administración de Redes Privadas Virtuales (VPN)	ISA Server 2004 incluye un mecanismo VPN más integrado, que se basa en la funcionalidad de Windows 2000 y Windows Server 2003.
Nuevo	Filtro de Inspección basada en el estado para VPN	Los clientes de VPN están configurados como una zona de red separada. Por lo tanto, usted puede crear distintas políticas para clientes VPN. El motor de normas de firewall controla discriminadamente los petitorios de los clientes VPN. El motor filtra e inspecciona exhaustivamente estos pedidos y, de manera dinámica, establece conexiones basadas en la política de acceso.
Nuevo	Soporte de Cliente SecureNat para clientes VPN conectados con el Servidor VPN de ISA Server 2004	ISA Server 2004 expande el soporte al cliente VPN permitiendo que clientes SecureNat accedan Internet sin que se instale un cliente firewall en el sistema de cliente. También puede consolidar la seguridad de red corporativa implementando en los clientes VPN SecureNAT una política de firewall basada en usuario/grupo.
Nuevo	Filtro de inspección basada en el estado para comunicaciones que se mueven a través de una conexión VPN sitio-a-sitio	ISA Server 2004 presenta filtrado e inspección basada en el estado para todas las comunicaciones que se mueven a través de una conexión VPN de sitio a sitio.
Nuevo	Cuarentena VPN	ISA Server 2004 aprovecha las herramientas de Cuarentena VPN de Windows Server 2003 para una mayor inspección e integración de cliente VPN de su política de firewall.
Nuevo	Servidores VPN publicados	Utilice las Normas de Publicación de Servidor de ISA Server 2004 para publicar protocolos IP y servidores PPTP. El Filtro de aplicación PPTP inteligente de ISA Server 2004 realiza la compleja gestión de conexión. Además, usted puede publicar fácilmente el servidor NAT-T L2TP/ IPsec VPN de Windows Server 2003 utilizando Server Publishing de ISA Server 2004.

Redes Privadas Virtuales		
Nuevo o Mejorado	Característica	Descripción
Nuevo	Soporte IPsec en modo túnel para vínculos sitio a sitio	ISA Server 2004 mejora el soporte de vínculo de sitio a sitio si usted utiliza el modo túnel IPsec como protocolo VPN. El soporte en modo túnel de IPsec aumenta significativamente la interoperabilidad de ISA Server 2004 con una amplia gama de soluciones VPN de terceros.

Web Cache y Web Proxy

Web Cache y Web Proxy		
Nuevo o Mejorado	Característica	Descripción
Mejorado	Normas de Caché	Con el mecanismo Norma de Caché de ISA Server usted puede configurar el modo en que los objetos guardados en el caché son recuperados y entregados desde el caché.
Mejorado	Dirección de Ruta para las Normas de Publicación en WEB	ISA Server 2004 mejora significativamente la flexibilidad de la publicación en Web porque usted puede redirigir la ruta enviada al firewall por el usuario a cualquier ruta que elija en el servidor de Web publicado.
Nuevo	Soporte RADIUS para la autenticación de cliente Web Proxy	Con ISA Server 2004, usted puede autenticar usuarios en el Directorio Activo y otras bases de datos de autenticación utilizando RADIUS para investigar el Directorio Activo. Las Normas de Publicación en Web también pueden utilizar RADIUS para autenticar conexiones de acceso remoto.
Nuevo	Delegación de autenticación básica	Los sitios Web publicados se encuentran protegidos contra el acceso no autenticado al exigir el firewall ISA Server 2004 para autenticar al usuario antes de reenviar la conexión al sitio Web publicado. Esto evita la explotación por parte de un usuario no autenticado del servidor de Web publicado.
Nuevo	Preservación de la dirección IP de origen en las Normas de Publicación en WEB	ISA Server 2004 le ofrece sobre una base por regla si el firewall debería reemplazar la dirección de IP original por sí misma o reenviar la dirección de IP original del cliente remoto al servidor Web.

2.2 MICROSOFT INTERNET SECURITY AND ACCELERATION 2006

ISA SERVER 2006

ISA Server 2006 es un gateway integrado de seguridad perimetral que le ayuda a proteger su entorno de TI frente a amenazas procedentes de Internet y además proporciona a sus usuarios un acceso remoto rápido y seguro a las aplicaciones y datos corporativos. ISA Server 2006 proporciona seguridad integrada, gestión eficiente y acceso seguro y rápido para todo tipo de redes.

ISA Server 2006 como un gateway para redes de sucursales que permite conectar y proteger los enlaces de sus redes de oficinas, utilizando el ancho de banda disponible con la máxima eficiencia. Dispone de funcionalidades como la compresión HTTP, el cache de contenidos (incluyendo las actualizaciones de software y funciones de VPN (Virtual Private Networks) entre sitios remotos, todo ello integrado junto con un potente filtrado de paquetes a nivel de aplicación. ISA Server 2006 es una forma efectiva de ampliar su red corporativa manteniendo los máximos estándares de seguridad y capacidad de gestión de los recursos.

Protección del acceso a Internet: con ISA Server 2006 las organizaciones pueden proteger sus entornos de TI frente a ataques y amenazas basadas en tecnologías de Internet, tanto de origen interno como externo. Su arquitectura híbrida Proxy-firewall, su potente inspección interna de paquetes, su capacidad para aplicar políticas con una alta granularidad y funcionalidades completas de

alerta y monitorización hacen posible una protección real para su red y una mayor facilidad de gestión de los recursos de conectividad.

ISA Server 2006 ofrece las siguientes novedades y mejoras con respecto a versiones anteriores:

2.2.1 CARACTERÍSTICAS TÉCNICAS DE ISA 2006

Protección de firewall avanzada

Nuevo o mejorado	Funcionalidad	Descripción
Mejorado	Asistentes de creación de reglas de Firewall	ISA Server 2006 incorpora una serie de asistentes para creación de reglas que facilitan la tarea de crear políticas de acceso. Las políticas de acceso en ISA Server 2006 pueden crearse a partir de una regla de firewall compleja que puede utilizarse para configurar cualquier elemento de política necesario. No hay que salir del asistente de reglas para crear ningún objeto de red. Cualquier objeto de red o relación puede crearse desde el mismo asistente.
Nuevo	Resistencia a los ataques por saturación	La nueva característica denominada "Resistencia al desbordamiento" protege a ISA Server 2006 frente a los ataques por saturación, que podrían dejar al servidor fuera de servicio de forma temporal o permanente, alterar su configuración o imposibilitar su administración.
Nuevo	Mejoras en la recuperación en caso de ataque	La "Resistencia al desbordamiento" permite una mejor recuperación en situación de ataques gracias a una optimización del proceso de registro de actividad (log), control del consumo de memoria y control de las peticiones DNS pendientes.

Redes Privadas Virtuales (VPN)

Nuevo o mejorado	Funcionalidad	Descripción
Nuevo	Asistente de conexión VPN para oficinas remotas	Este asistente configura automáticamente una conexión VPN site-to-site entre dos ubicaciones físicamente independientes.

Gestión

Nuevo o mejorado	Funcionalidad	Descripción
Mejorado	Asistentes fáciles de utilizar	Incluye nuevos asistentes de configuración para la publicación de Windows SharePoint Services, Exchange y sitios Web normales. Un nuevo asistente para la conexión VPN entre oficinas remotas permite configurar las conexiones VPN site-to-site.
Mejorado	Certificate Management	Ahora se pueden utilizar múltiples certificados para cada proceso Web en escucha ("listener") y utilizar distintos certificados para cada miembro del array. ISA Server 2006 ha simplificado la administración de certificados y reduce el coste total de propiedad (TCO) asociado al uso de certificados a la hora de publicar sitios Web.
Mejorado	Equipos de hardware basados en ISA Server	ISA Server 2006 Ed. Estándar y Enterprise ya disponibles en equipos de hardware preconfigurados.
Mejorado	Propagación de directivas de ámbito corporativo	Se mejora la arquitectura de base para una mayor eficiencia.

Autenticación

Nuevo o mejorado	Funcionalidad	Descripción
Mejorado	Autenticación	Los usuarios pueden autenticarse utilizando los métodos de validación incorporados en Windows, LDAP, RADIUS o RSA SecurID. Las configuraciones de front-end y backend se hacen por separado, para ganar en flexibilidad y granularidad. Se soporta SSO (Single Sign-On) para la autenticación en sitios Web. Las reglas se pueden aplicar a usuarios individuales o grupos de usuarios en cualquier espacio de nombres. Existe un SDK para que otros fabricantes puedan ampliar las funcionalidades e incorporar nuevos métodos de autenticación.
Nuevo	Single Sign-On (Logon único)	La función de logon único (SSO, Single Sign-On) permite a los usuarios el acceso a un grupo de sitios Web publicados sin necesidad de autenticarse de forma reiterada en cada sitio Web.
Mejorado	Autenticación basada en formularios Web	Ya está disponible la autenticación basada en formularios Web para todos los sitios Web publicados, no solamente para Outlook Web Access.
Mejorado	Control de sesión	ISA Server 2006 incluye mejoras en el control de sesiones basadas en cookies para lograr un mayor nivel de seguridad.
Nuevo	Soporte para autenticación LDAP	La autenticación LDAP permite a ISA Server autenticar contra el Directorio Activo sin necesidad de formar parte del dominio.

Publicación de servidores

Nuevo o mejorado	Funcionalidad	Descripción
Mejorado	Traducción de enlaces Web	Algunos sitios Web publicados incluyen referencias a nombres de máquinas internos. Puesto que, de cara a los clientes, solo existen los espacios de nombres del firewall ISA Server 2006 y el externo, y el espacio de nombres interno queda oculto, estas referencias aparecen como enlaces rotos. ISA Server 2006 incorpora una función de traducción de enlaces Web que se puede utilizar para crear un diccionario de definiciones para los nombres de máquina internos que se mapean con nombres válidos en Internet. ISA Server 2006 implementa la traducción automática de enlaces durante el proceso de publicación Web.
Nuevo	Traducción de enlaces Web entre arrays	Esta funcionalidad permite que los enlaces de contenidos Web que incluyen nombres de servidores internos se traduzcan a nombres públicos incluso en el caso de que el contenido Web esté publicado en un array distinto.

Rendimiento

Nuevo o mejorado	Funcionalidad	Descripción
Nuevo	Cache para BITS	ISA Server 2006 dispone de un mecanismo de cache para los datos recibidos mediante BITS. Cualquier regla de cache que se genere puede habilitarse para cachear datos BITS.
Nuevo	Balanceo de carga para publicación Web	ISA Server 2006 balancea automáticamente la carga de las peticiones realizadas desde el exterior hacia un array de servidores publicados.
Nuevo	Compresión HTTP	La compresión HTTP reduce el tamaño de los archivos mediante algoritmos que eliminan los datos redundantes durante la transmisión de paquetes HTTP.
Nuevo	Diffserv (Calidad de Servicio)	ISA Server 2006 incluye un nuevo sistema de priorización de paquetes (mediante el filtro Web Diffserv), que analiza el URL o el dominio y asigna una prioridad al paquete utilizando los bits Diffserv.

Acceso remoto seguro a los servidores Microsoft internos

Nuevo o mejorado	Funcionalidad	Descripción
Mejorado	Asistente de Publicación para OWA (Outlook Web Access).	Acceso remoto sin cliente mediante conexiones SSL desde el origen mismo de las VPN basadas en SSL. El Asistente de Publicación de Outlook Web Access (OWA) sirve de guía para crear una regla de firewall y la conexión SSL al servidor Exchange. Todos los elementos de la red pueden crearse desde el asistente, y no hay que salirse de él para crear un elemento de directiva.
Nuevo	Asistente de Publicación para servidores SharePoint.	Un nuevo asistente de publicación permite publicar múltiples sitios basados en Windows SharePoint Services a la vez, y resuelve la traducción automática de enlaces Web.
Nuevo	Soporte integrado para Exchange 2007	Soporte para el conjunto de funcionalidades de Exchange 2007 incluido de serie en ISA Server 2006.

2.3 EDICIONES DE ISA SERVER 2004, 2006 EDICIÓN ESTÁNDAR Y ENTERPRISE.

ISA Server se encuentra disponible en 2 ediciones que se encuentran diseñadas para cumplir las necesidades de todo tipo de empresas.

1. ISA Server Standard Edition.

Esta versión provee funciones de Firewall así como capacidades de Caché para pequeñas empresas.

2. ISA Server Enterprise Edition.

Esta versión está dirigida a satisfacer las necesidades de empresas con alto índice de volumen de negocio así como con un alto índice de acceso a Internet, permite crear políticas de acceso para centralizar la administración y provee tolerancia a fallos.

Característica	ISA ED. Estándar	ISA ED. Enterprise
Escalabilidad		
Redes	Sin limitación	Sin limitación Añade redes corporativas
Escalabilidad	Hasta 4 CPUs, 2-GB de RAM	Sin limitación (la que determine el S.O.)
Escalabilidad horizontal	Un solo servidor	Hasta 32 nodos mediante Balanceo de carga con NLB (Network Load Balancing)
Cache	Almacenamiento de servidor único	Sin límite (utilizando protocolo CARP - Cache Array Routing Protocol)
Disponibilidad		
Soporte para Windows Network Load Balancing (NLB)	No soportado	Sí (integrado)
Capacidad de manejo - Administración		
Políticas	Locales	Políticas de gestión del array de servidores y directivas corporativas mediante ADAM (Active Directory Application Mode)
Redes de oficinas	Importación y exportación manual de políticas	Políticas de nivel corporativo y de nivel de array de servidores
Monitorización y alertas	Consola de monitorización de un único servidor Management Pack para Microsoft Operations Manager (MOM)	Consola de monitorización multiservidor Management Pack para MOM
Múltiples redes	Mediante plantillas	Mediante plantillas

2.4 SQUID GNU/Linux

Otro producto que trabaja en forma similar al ISA SERVER 2004 es SQUID el cual es un Servidor Intermediario (Proxy) de alto desempeño que se ha venido desarrollando desde hace varios años y es hoy en día un muy popular y ampliamente utilizado entre los sistemas operativos como GNU/Linux y derivados de Unix®. Es muy confiable, robusto y versátil y se distribuye bajo los términos de la Licencia Pública General GNU (GNU/GPL). Siendo sustento lógico libre, está disponible el código fuente para quien así lo requiera.

Entre otras cosas, Squid puede funcionar como Servidor Intermediario (Proxy) y caché de contenido de Red para los protocolos HTTP, FTP, GOPHER y WAIS, Proxy de SSL, caché transparente, WWCP, aceleración HTTP, caché de consultas DNS y otras muchas más como filtración de contenido y control de acceso por IP y por usuario.

Squid consiste de un programa principal como servidor, un programa para búsqueda en servidores DNS, programas opcionales para reescribir solicitudes y realizar autenticación y algunas herramientas para administración y herramientas para clientes.

Squid ha sido desarrollado durante muchos años y se le considera muy completo y robusto. Soporta muchos protocolos, aunque se usa principalmente para HTTP y FTP. Se añade soporte también a TLS, SSL, Internet Gopher y HTTPS.

Squid posee las siguientes características:

1. Proxy y Caché de HTTP, FTP, y otras URLs
2. Proxy para SSL
3. Jerarquías de Caché
4. ICP, HTCP, CARP, Caché Digests
5. Caché transparente
6. WCCP (Squid v2.3 y superior)
7. Control de acceso
8. Aceleración de servidores http
9. SNMP
10. Caché de resolución DNS

2.5 CRITERIOS DE EVALUACIÓN

2.5.1 EVALUACIÓN ECONÓMICA

Desarrollo del material didáctico para el laboratorio de redes de la Universidad Tecnología De El Salvador, requiere la adquisición de las licencias del software MICROSOFT ISA SERVER, para su implementación.

LICENCIAS ISA SERVER		
SOFTWARE	LICENCIA COMERCIAL	LICENCIA ACADEMICA (10% aproximado)
ISA SERVER 2000	No se distribuye	No se distribuye
ISA SERVER 2004	\$1,200	\$120.00
ISA SERVER 2006	\$1,750	\$175.00
SQUID / LINUX	Licencia libre	Licencia libre

El costo de licencias para uso educativo se encuentra alrededor del 10% al costo de una licencia comercial.

2.5.2 EVALUACIÓN TÉCNICA

Parámetros de cumplimiento para la evaluación técnica.

Perfil a buscar

- Facilidad de acoplamiento al laboratorio de redes de la UTEC, en cuanto a software, hardware; actualizaciones de software, requerimientos de hardware.
- Proxy Web.
- Cache Web.
- Directiva HTTP para controlar las descargas de archivos a través de la extensión del nombre de archivo.
- Redes perimetrales DMZ
- Política de firewall.
- VPN.

- Costos.

MICROSOFT ISA 2004	Parámetros		MICROSOFT ISA 2006	Parámetros		SQUID LINUX	Parámetros	
Proxy Web.	√	12.5%	Proxy Web.	√	12.5%	Proxy Web.	√	12.5%
Cache Web.	√	12.5%	Cache Web.	√	12.5%	Cache Web.	√	12.5%
Directiva http.	√	12.5%	Directiva http.	√	12.5%	Directiva http.	X	
Redes perimetrales DMZ	√	12.5%	Redes perimetrales DMZ	√	12.5%	Redes perimetrales DMZ	X	
Políticas de firewall.	√	12.5%	Políticas de firewall.	√	12.5%	Políticas de firewall.	X	
VPN	√	12.5%	VPN	√	12.5%	VPN	X	
Facilidad de acoplamiento	√	12.5%	Facilidad de acoplamiento	X		Facilidad de acoplamiento	X	
Costos	√	12.5%	Costos	X		Costos	√	
PORCENTAJE	100%		75%		37.5%			
	ISA 2004		ISA 2006		SQUID			
	L. Comercial		L. Comercial muy Costosa		Licencia Libre			
	L. Académica		L. Académica mas costosa					

Porcentaje: Cada parámetro de cumplimiento refleja la octava parte del porcentaje total, de acuerdo a la siguiente norma. 100% dividido en 8(numero de parámetros de cumplimiento a buscar) dando como resultado 12.5% por cada parámetro, dando un valor igual a cada uno, se observa en la evaluación técnica y económica, que los productos ISA SERVER 2004 E ISA SERVER 2006, cumplen con los requerimientos mínimos que exige el proyecto.

2.6 ACOPLAMIENTO AL LABORATORIO DE REDES DE LA UTEC

El laboratorio de redes de la UTEC, cuenta con:

El laboratorio de redes utiliza Windows 2003 Server, en maquinas virtuales utilizando el software VMWARE Virtual Machina; ISA SERVER 2004 se instalara y configurara en las máquinas virtuales donde se encuentra instalado Windows 2003 Server

SOFTWARE

SOR: Windows 2003 Server Enterprise Edition.

Actualizaciones de software

SOFTWARE	ISA SERVER 2004
Sistemas Operativos	Microsoft Windows Server 2003 Standard Edition o Enterprise Edition. No requiere ninguna actualización del sistema operativo WINDOWS 2003 SERVER

SOFTWARE	ISA SERVER 2006
Sistemas Operativos	Microsoft Windows Server 2003 <u>con Service Pack 1</u> Microsoft Windows Server 2003 R2.

HARDWARE

El equipo del laboratorio de redes actual cuenta con los siguientes requerimientos de hardware

Tamaño de disco duro	40GB
Memoria RAM	512MB
Velocidad del CPU	2.80GHZ
Sistemas Operativos	Win 2003 server – virtual machine vmware

ISA 2004 Requerimientos de Hardware minimos

Memoria RAM	256MB o mas
Velocidad del CPU	Pentium III a 550 MHz o superior
Espacio de disco duro	150 MB de espacio Partición local con formato NTFS disponible en el disco duro; se requiere espacio adicional para el contenido de la caché Web

ISA 2006 Requerimientos de Hardware minimos

Memoria RAM	512MB se recomienda 1GB
Velocidad del CPU	Pentium III a 733 MHz o superior.
Espacio de disco duro	150 MB de espacio Partición local con formato NTFS disponible en el disco duro; se requiere espacio adicional para el contenido de la caché Web

Costos

ISA 2004 en comparación con su nueva versión ISA 2006 su costo es significativamente notable para buscar la economía del proyecto.

En el país la licencia comercial tiene un costo aproximado de \$ 1,200; sin embargo, si la Universidad Tecnológica de El Salvador hace las gestiones necesarias podría adquirir la licencia Académica alrededor del 10% del precio comercial.

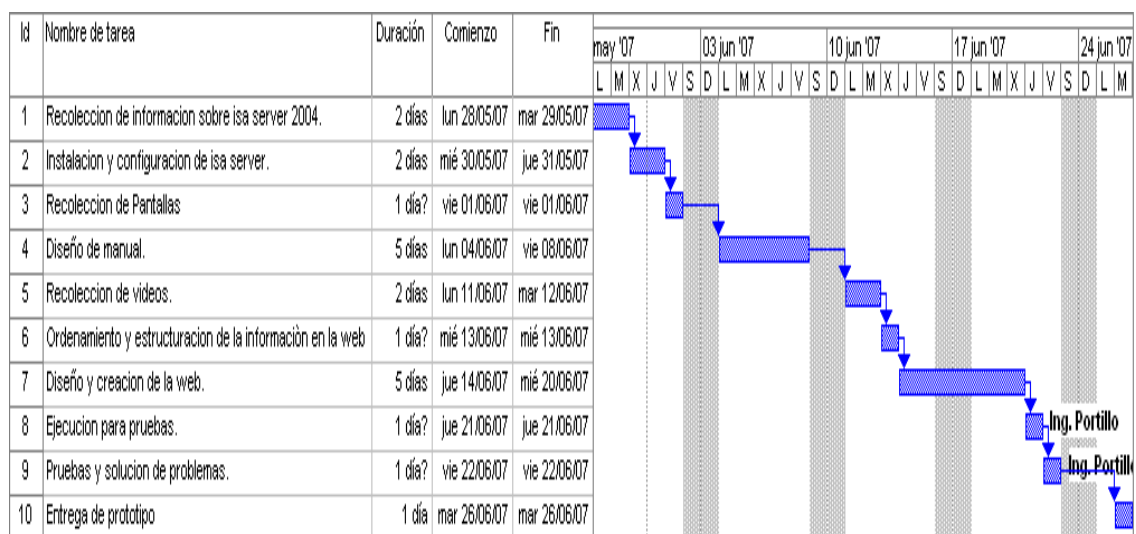
2.7 TECNOLOGÍA Y RECURSOS SELECCIONADOS

Tecnología y Recursos Seleccionados		
MICROSOFT ISA 2004	√	ISA 2004 cumple con todos los parámetros buscados en los 3 productos ya presentados, en comparación con su nueva versión 2006 su costo es significativamente notable buscando la economía. ISA 2004 llena el perfil buscado para la creación de la guía didáctica.
MICROSOFT ISA 2006	X	Es muy costoso, presenta un aumento significativo
SQUID LINUX	X	No Aplica a algunas Especificaciones técnicas requeridas.

2.8 CRONOGRAMA DEL PROYECTO TEMÁTICO

Listado de actividades para la creación del material didáctico comprendido en los meses de Mayo a Junio del 2007

Cronograma de actividades

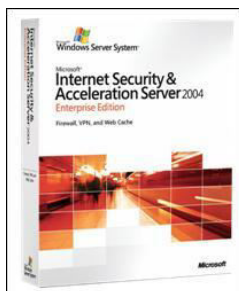


2.9 OFERTA TÉCNICA

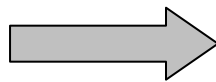
Con el desarrollo del material didáctico, de la tecnología Microsoft ISA Server 2004, se brindará un apoyo tanto teórico como práctico a estudiantes, profesores de las diversas asignaturas de la carrera de técnico en ingeniería de Redes Computacionales.

La guía didáctica brindará un ejemplo práctico del funcionamiento del software a través de diferentes guías prácticas relacionadas a los diferentes roles de Microsoft ISA Server 2004.

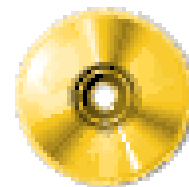
El producto a presentar constara con sus respectivos manuales acompañados de sus respectivo CD interactivo.



ISA Server 2004



Manuales



CD Interactivo

El CD interactivo contara con apoyo visual en diferentes formatos digitales como MS Word, html, y pequeños videos, el material didáctico tendrá su respectivo CD interactivo donde se podrán encontrar las versiones digitales.

Las diferentes guías a Crearse son:

- Instalación de Microsoft ISA Server 2004.
- Configuración de Proxy Web.
- Configuración de Cache Web.
- Configuración de políticas de Firewall.
- Configuración Directiva HTTP para controlar las descargas de archivos a través de la extensión del nombre de archivo.
- Configuración de redes perimetrales DMZ.
- Configuración de VPN.

2.10 OFERTA ECONÓMICA

LICENCIA COMERCIAL

LICENCIAS ISA SERVER		
SOFTWARE	LICENCIA COMERCIAL	
ISA SERVER 2004	\$1,200.00	El costo de una licencia comercial es demasiado costoso debido a su propósito destinado a empresas
ISA SERVER 2006	\$1,750.00	

LICENCIA ACADEMICA

LICENCIAS ISA SERVER		
SOFTWARE	LICENCIA ACADEMICA	
ISA SERVER 2004	\$120.00	El costo de licencias para uso educativo se encuentra alrededor del 10% al costo de una licencia comercial, su propósito educativo
ISA SERVER 2006	\$175.00	

La Universidad Tecnológica de El Salvador debe hacer los tramites pertinentes para lograr obtener este beneficio de las licencias académicas, adecuadas para la adquisición de un buen número de licencias del mismo software para este caso ISA Server 2004.

A la universidad Tecnológica de El Salvador se le presenta una oferta económica para la adquisición de las licencias del software Microsoft ISA Server 2004, el propósito a buscar en la adquisición de las licencias es la forma de trabajo que emplearan los estudiantes de la institución, tomando en cuenta el numero de licencias para poder utilizar en las practicas de dicho software

OFERTA ECONOMICA ISA SERVER 2004					
Propuesta 1		Propuesta 2		Propuesta 3	
La UTEC debe adquirir mínimo 25 licencias académicas de ISA SERVER 2004. Propósito, los estudiantes realizaran sus practicas de forma individual.		La UTEC debe adquirir 10 licencias académicas de ISA SERVER 2004. Propósito, los estudiantes realizaran sus practicas en pequeños grupos		La UTEC al no poder adquirir licencias académicas de ISA SERVER 2004, deberá comprar por lo menos una licencia comercial de ISA SERVER 2004 Propósito, los estudiantes realizaran sus practicas en grandes grupos	
Total 1	\$3000.00 25 licencias	Total 2	\$1200.00 10 Licencias	Total 3	\$1200.00 1 licencia comercial

Se recomienda la propuesta 1 por la posibilidad de desarrollar prácticas de laboratorio individuales, las cuales permitirán un mayor desarrollo en el proceso enseñanza – aprendizaje de los alumnos de la carrera Técnico en Ingeniería de Redes Computacionales de la Universidad Tecnológica de El Salvador.

CAPITULO III

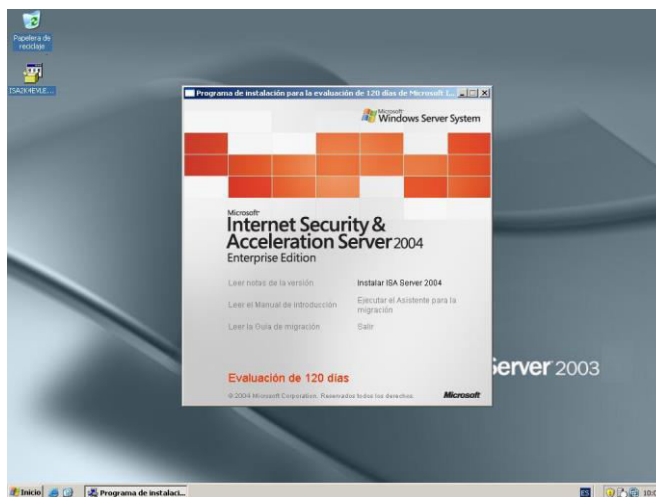
3.0 ENTREGA DE PROTOTIPO MANUALES Y CD DE CONFIGURACIÓN DE ISA SERVER 2004.

3.1 MANUAL PARA LA INSTALACIÓN DE ISA SERVER 2004

Objetivo: Que el estudiante observe el proceso de instalación del software ISA SERVER 2004.

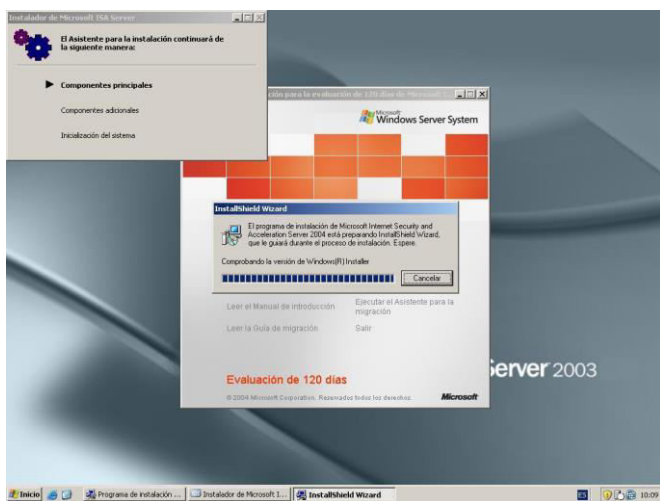
La configuración es un proceso relativamente simple, en el que se detallará cada paso para que el estudiante pueda observar el paso a paso de su instalación.

Se debe ejecutar el programa de instalación de ISA SERVER 2004, si esta trabajando con el CD original de instalación inserte el CD y espere la reproducción automática, si esta trabajando con una versión de evaluación como este caso debe ejecutar el archivo ISA2K4EVLE.exe. Cuando ejecute el archivo creará una carpeta en su disco C: con los archivos de instalación, luego debe esperar el inicio del programa de instalación de ISA SERVER.



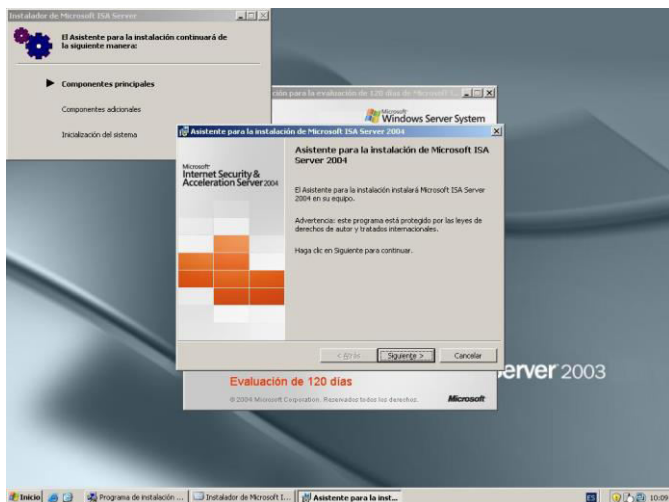
Pantalla N° 1

A continuación seleccionar la opción de Instalar ISA SERVER 2004.
En la pantalla nº 2, se observa el proceso que da inicio a la instalación del software.



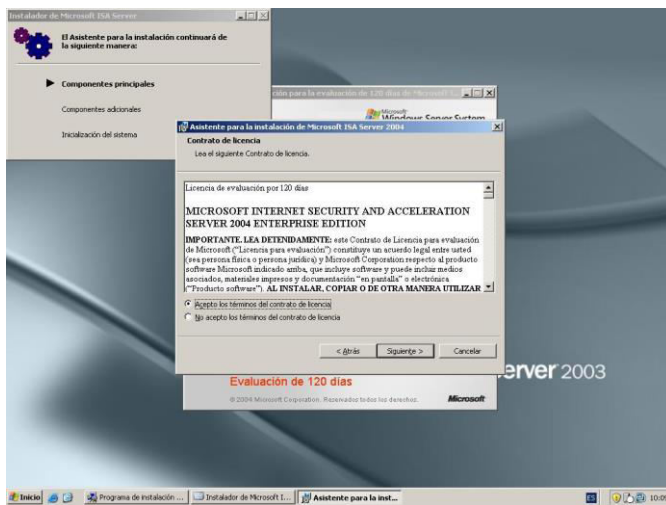
Pantalla nº 2

En la pantalla N° 3 inicia el asistente de instalación, seleccione el botón siguiente para continuar.



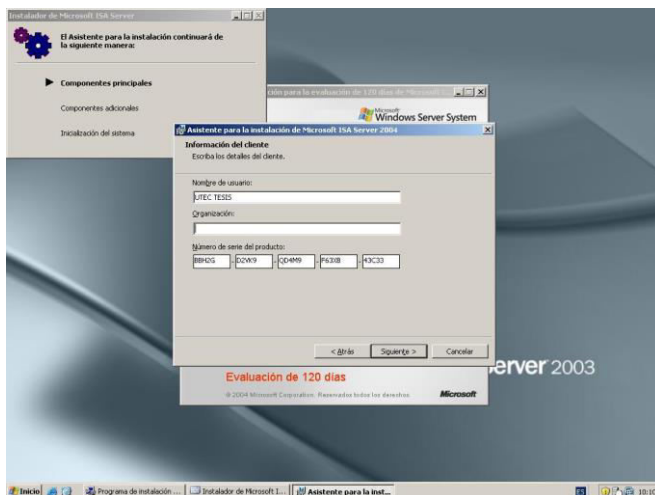
Pantalla N° 3

En la pantalla N° 4 se observa que el usuario debe aceptar los términos de la licencia para poder usar el producto seleccione la opción de **acepto los términos del contrato de la licencia**, luego elija el botón siguiente.



Pantalla N° 4

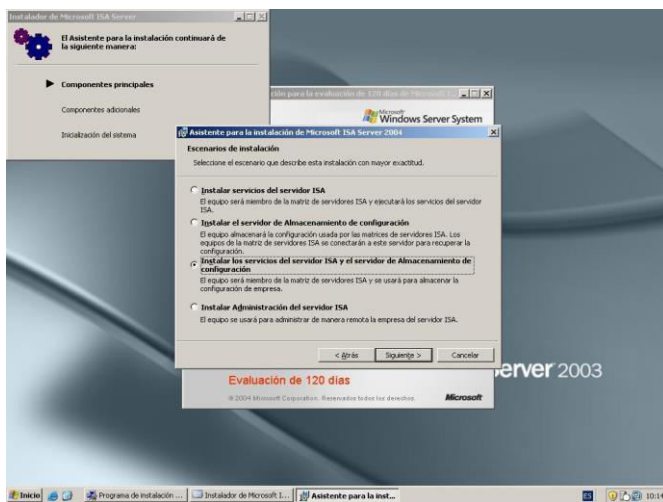
En la pantalla N° 5 el usuario debe proporcionar información, Nombre de usuario, Organización y el número de serie del producto (en este caso se esta utilizando un versión de evaluación dejamos el numero de serie incorporado), después seleccione el botón siguiente.



Pantalla N° 5

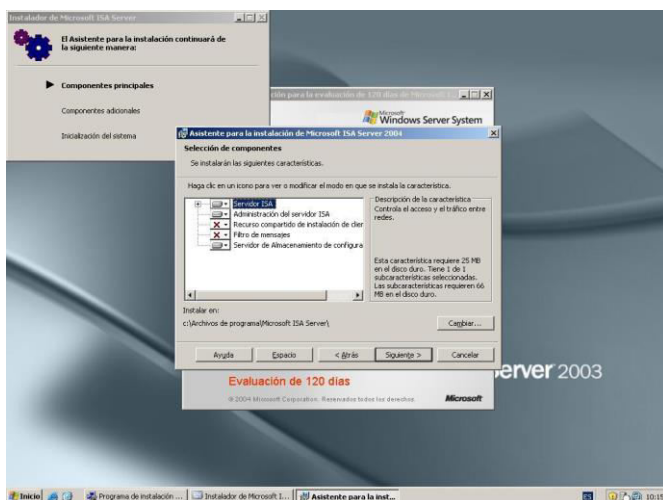
En la pantalla N° 6 el usuario debe elegir el escenario que describe el tipo de instalación a hacerse. Seleccione la tercera opción de **instalar los servicios del servidor ISA y el servidor de almacenamiento de configuración**, luego elija el botón siguiente.

NOTA: en la instalación de ISA SERVER 2004, debe escoger la tercera opción de **instalar los servicios del servidor ISA y el servidor de almacenamiento de configuración**. En la primera opción el servidor ISA requiere el servidor de almacenamiento. En la segunda opción el servidor de almacenamiento requiere del servidor ISA. En otro caso que exista otro servidor ISA o servidor de almacenamiento en la red.



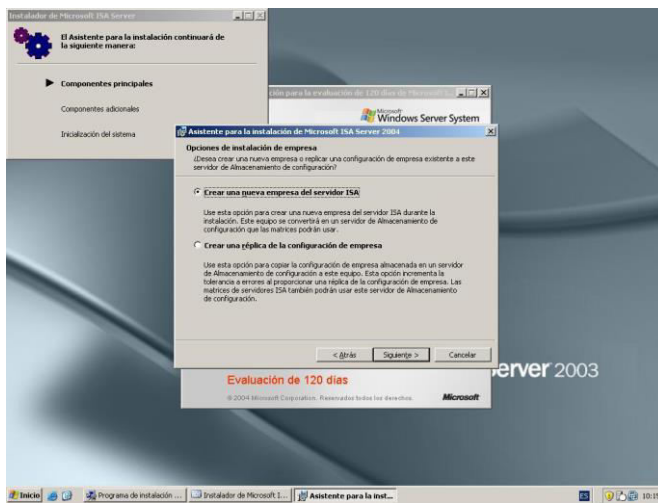
Pantalla N° 6

En la pantalla N° 7, el asistente muestra los componentes seleccionados a instalarse y además podemos seleccionar otro componente, el directorio destino, luego seleccione el botón siguiente.



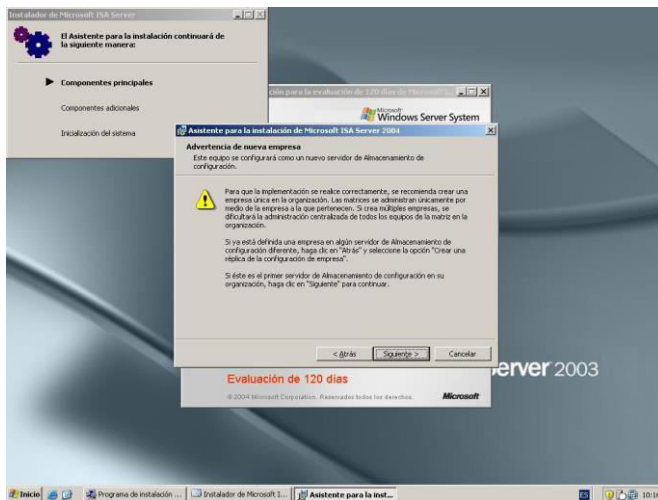
Pantalla N° 7

En la pantalla N° 8, se debe escoger la opción de **crear una nueva empresa del servidor ISA**. La opción se utiliza para copiar la configuración de un servidor de almacenamiento ya existente en la red.



Pantalla N° 8

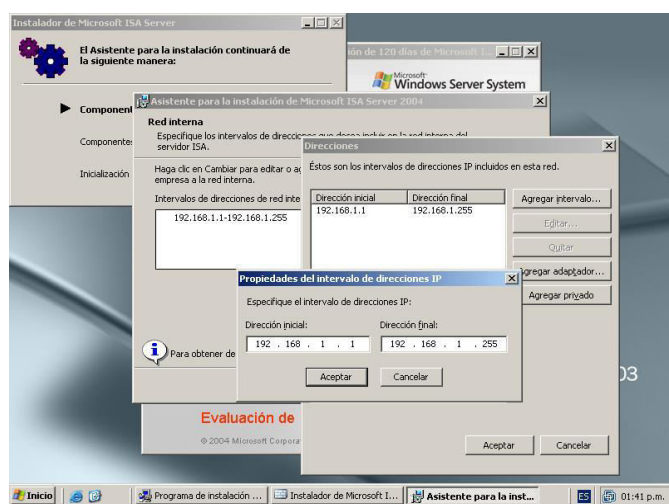
En la pantalla N° 9, el asistente notifica la creación de la nueva, elija el botón siguiente para continuar.



Pantalla N° 9

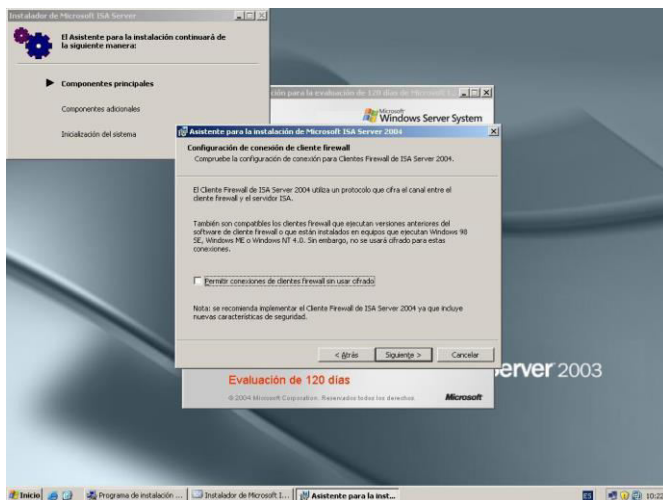
En la pantalla N° 10 se debe especificar el rango de direcciones IP para la red interna, seleccione cambiar, en el siguiente cuadro, elija agregar intervalo y escriba el siguiente rango utilizado para este caso dirección inicial 192.168.1.1, dirección final 192.168.1.255. Seleccione aceptar, después otro aceptar, por último siguiente, para continuar.

NOTA: En el caso de que la interfaz de red para la red privada ya esta previamente configurada con una dirección IP, Al agregar el rango de direcciones IP para la red interna de forma manual, debe coincidir con la con la dirección previamente configurada. En otro caso se puede agregar el rango de direcciones IP en la opción de agregar adaptador, se configura con automáticamente con los parámetros que posee la interfaz de red.



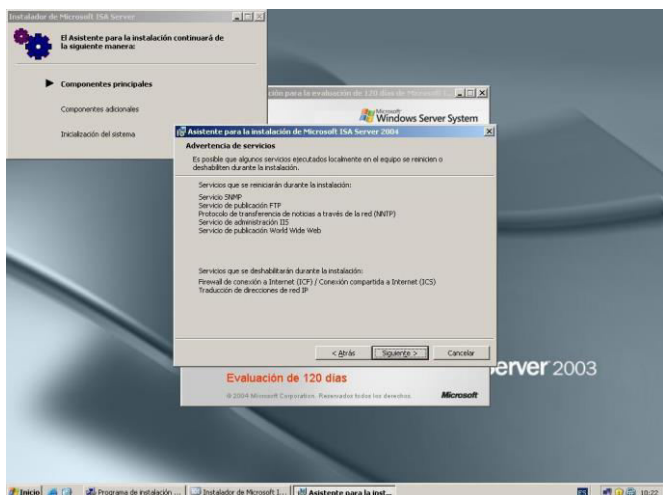
Pantalla N° 10

En la pantalla N° 11, el asistente de instalación pregunta si desea habilitar las conexiones cliente firewall sin usar cifrado, deseleccione la casilla para utilizar cifrado en las conexiones además es la configuración por default de ISA SERVER, luego elija siguiente.



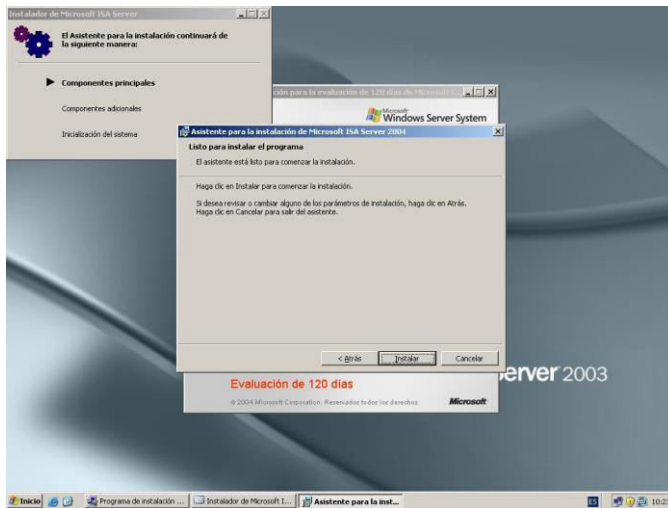
Pantalla N° 11

En la pantalla N° 12 el asistente de instalación hace una advertencia de los servicios que se reiniciarán y de los servicios a deshabilitarse durante la instalación, seleccione el botón siguiente para continuar.



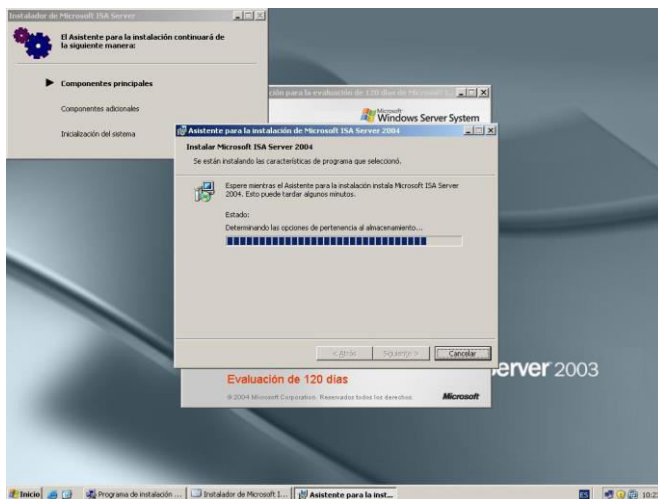
Pantalla N° 12

Antes de continuar con la instalación debe seleccionar el botón de instalar para empezar la instalación como se observa en la pantalla N° 13.



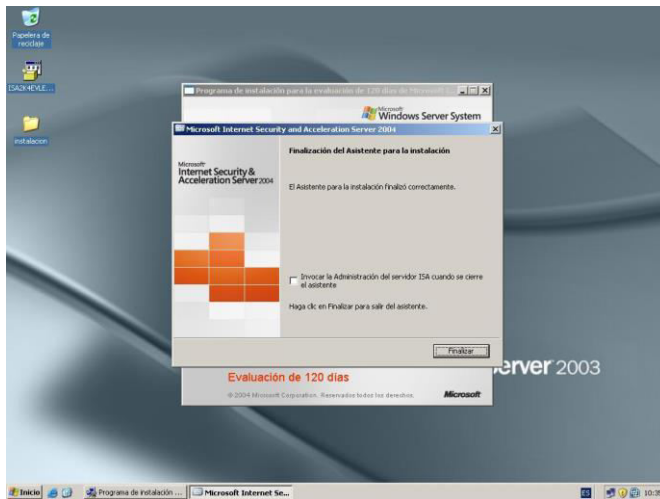
Pantalla N° 13

Ahora el usuario observará la instalación de ISA SERVER en el equipo el cual puede tardar algunos minutos como se observa en la pantalla N° 14.



Pantalla N° 14

En la pantalla N° 15 se observa que el usuario puede invocar la administración de ISA SERVER seleccione la casilla, luego seleccione el botón finalizar.



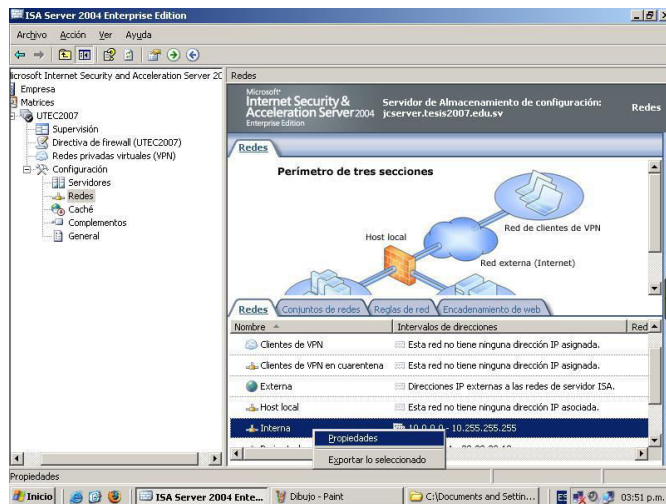
Pantalla N° 15

3.2 MANUAL PARA CONFIGURAR EL PROXY WEB DE ISA SERVER 2004.

Objetivo: Que el estudiante observe como se configura el proxy web.

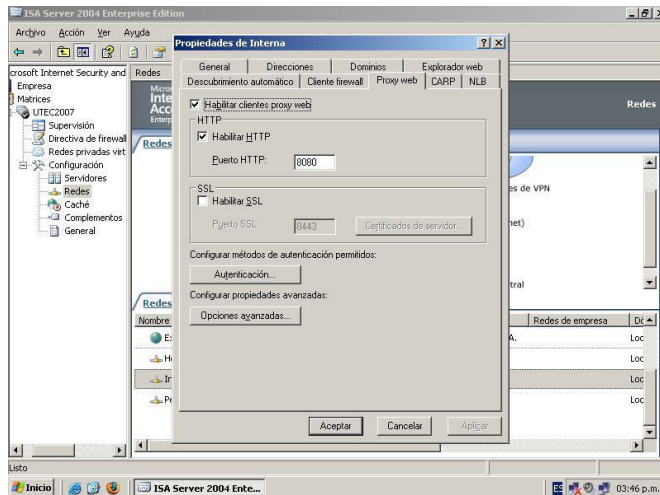
El siguiente paso consiste en la configuración del Proxy Web en ISA Server 2004. La configuración es un proceso relativamente simple, pero se detallará cada paso para asegurar de que el estudiante pueda observar el paso a paso para su configuración.

En la consola de administración de Microsoft Internet Security and Acceleration Server 2004, ubicar la opción y expandir la opción de **configuración**, luego elija **redes**, a continuación en el panel derecho ubicar en el listado de redes la **red interna**, haga clic derecho y elija **propiedades**, según se observa en la pantalla N° 1.



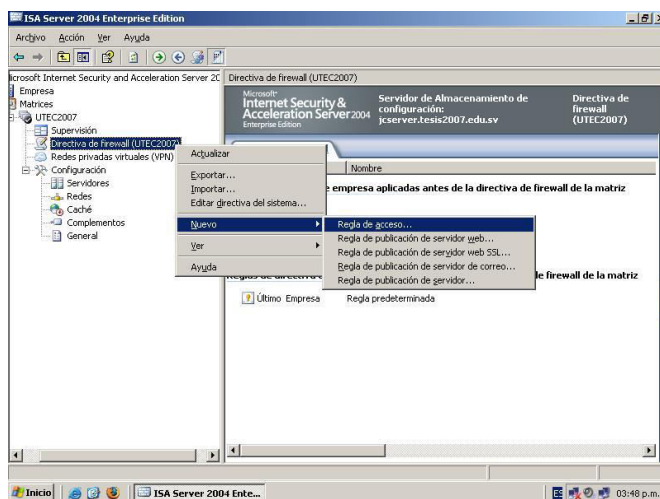
Pantalla N° 1

Se debe de acceder a las propiedades de la red interna como se observa en la pantalla N° 2, donde se debe activar la opción de **habilitar clientes Proxy Web, habilitar http, y el puerto 8080**, utilizado por default para este protocolo, luego seleccionamos aceptar.



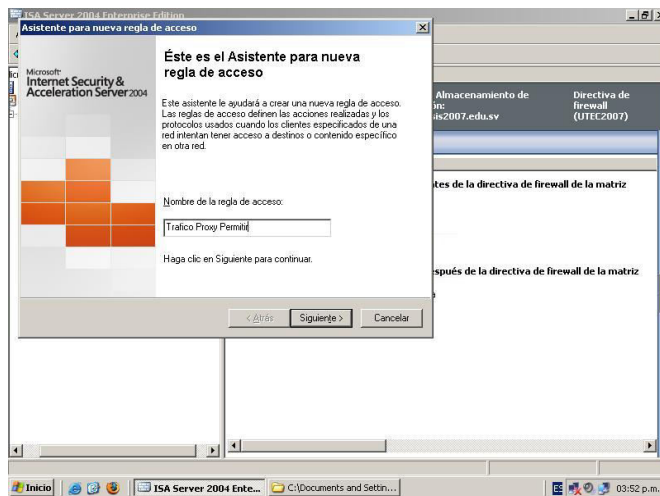
Pantalla N° 2

En la pantalla N° 3 se observa como se crea una nueva regla de acceso para habilitar el protocolo http, necesario para la configuración del Proxy Web. En la consola de administración de ISA SERVER ubicar la opción **directiva de firewall**, luego hacer clic derecho, seleccionar **nuevo, regla de acceso**.



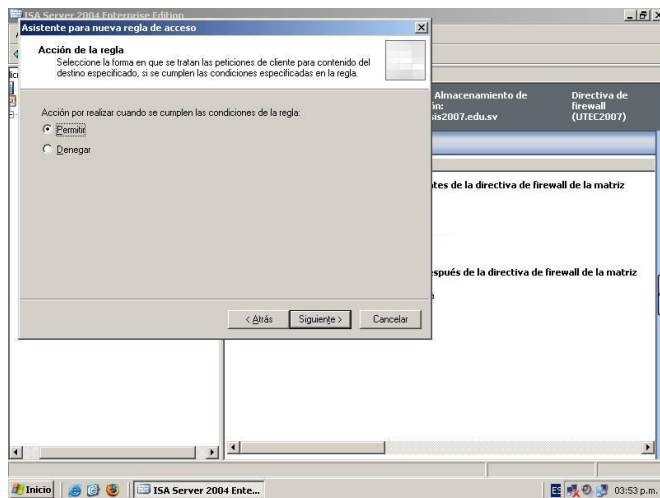
Pantalla N° 3

En la pantalla N° 4, se visualiza el asistente para la creación de la nueva regla de acceso, en donde debe agregar un nombre a la regla para este caso se utilizo trafico proxy permitir, después seleccionar el botón siguiente.



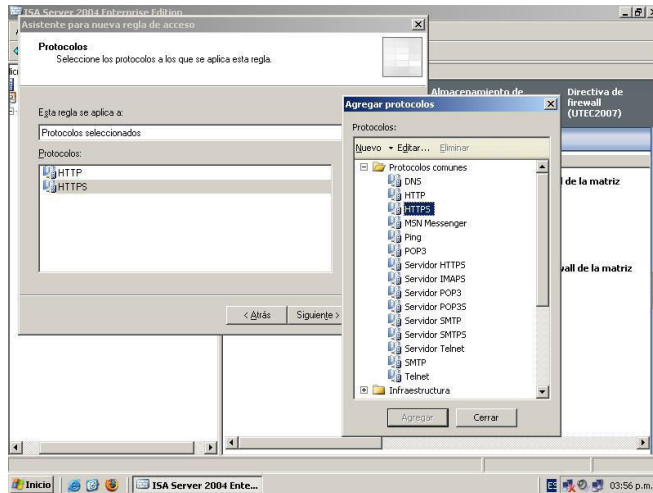
Pantalla n° 4

En la pantalla N° 5 el usuario debe determinar la acción de la regla, seleccione **permitir**, luego seleccione el botón siguiente.



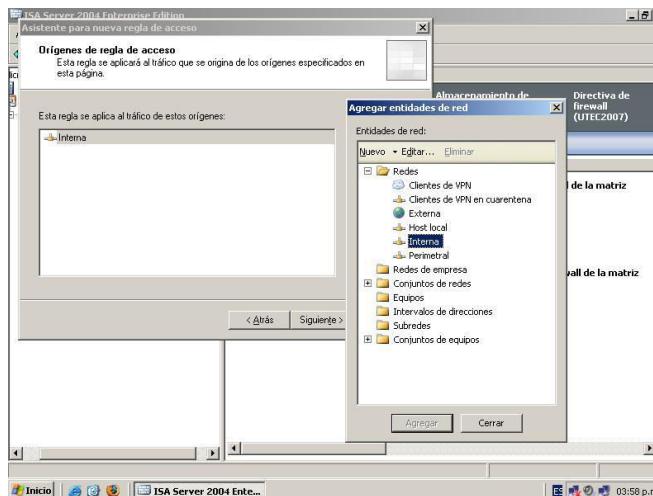
Pantalla N° 5

En la pantalla N° 6 se observa como el usuario debe seleccionar el tipo de protocolo que se aplicara a la regla, ubicar la opción agregar, luego en listado de protocolos buscar el protocolo http, seleccione agregar, también agregue el protocolo https (sitios con seguridad), después cerrar, por ultimo seleccione siguiente.



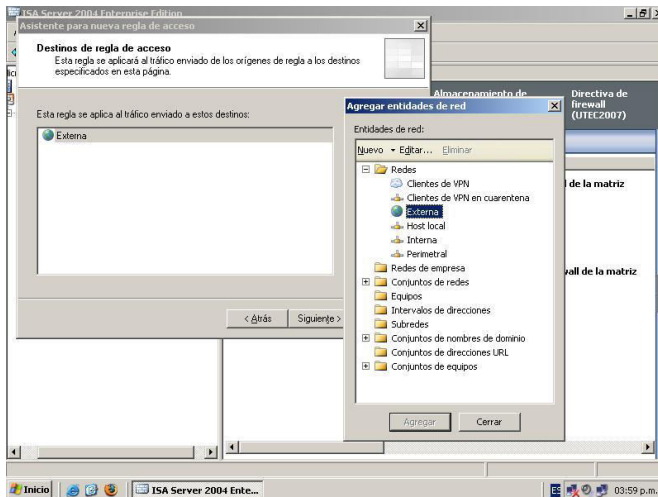
Pantalla N° 6

En la pantalla N° 7, se debe especificar el tráfico origen, ubique y seleccione agregar, luego en el listado buscar la opción red interna y elija el botón agregar, después cerrar, por ultimo seleccione el botón siguiente.



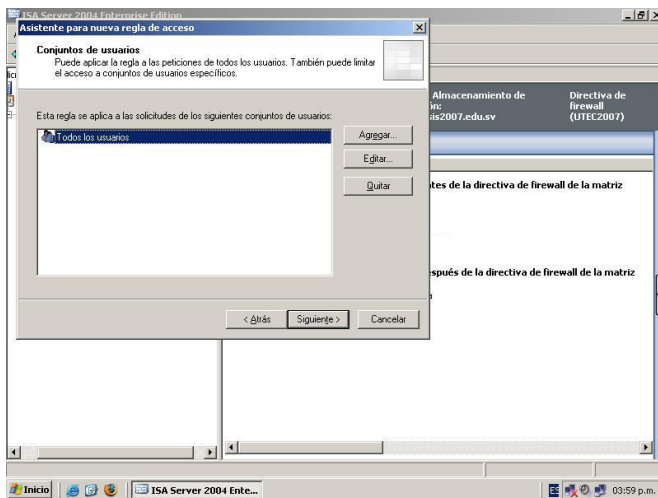
Pantalla N° 7

En la pantalla N° 8 se especifica el tráfico destino de la regla de acceso, ubique y seleccione agregar, luego en el listado buscar red externa y elija agregar, después cerrar, por ultimo seleccione siguiente.



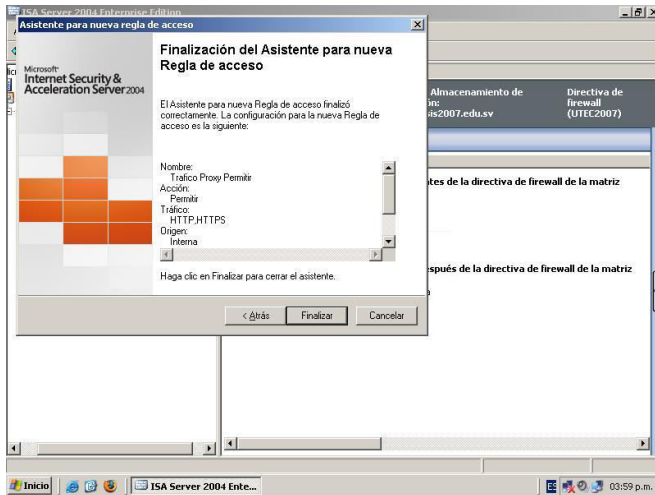
Pantalla N° 8

En la pantalla N° 9, debe determinar el conjunto de usuarios a los que se aplicará la regla de acceso, seleccione todos los usuarios, luego elija el botón siguiente.



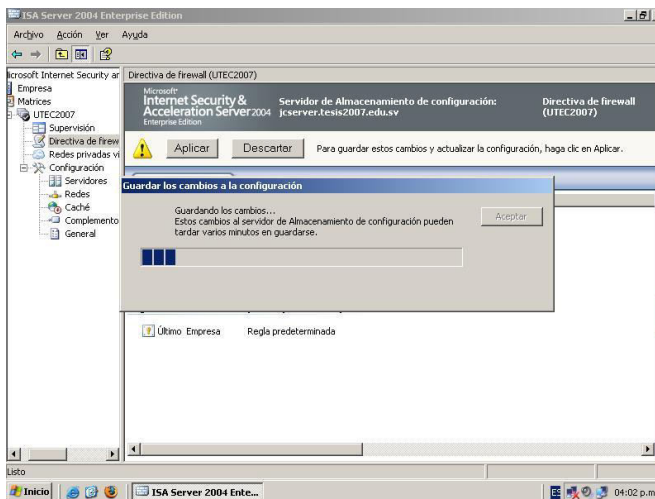
Pantalla N° 9

En la pantalla N° 10, se observa como se finaliza el asistente para la creación de la nueva regla de acceso, revisar la información, luego seleccione finalizar.



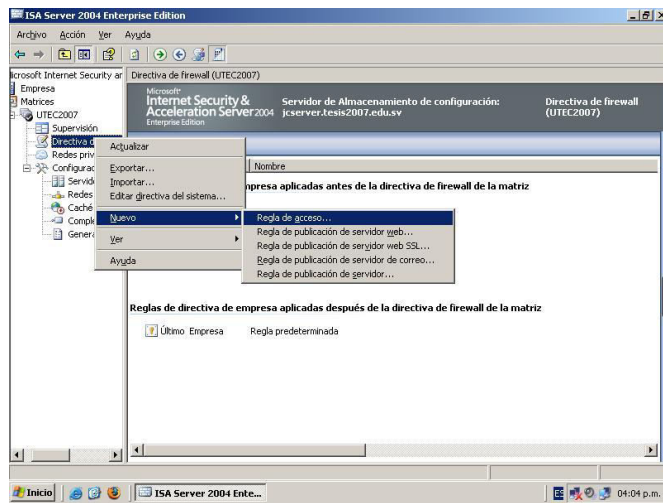
Pantalla N° 10

Para finalizar se debe aplicar los cambios a ISA SERVER, seleccionar la opción de aplicar, tal como se visualiza en la pantalla N° 11



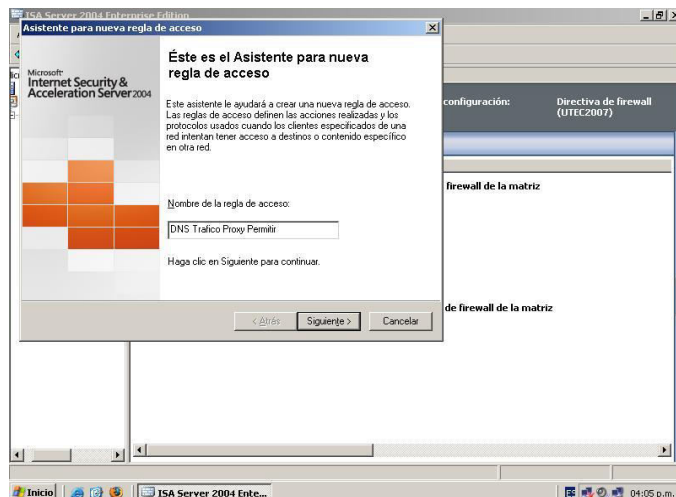
Pantalla N° 11

A continuación se creará una nueva regla de acceso del protocolo DNS para los clientes proxy Web. En la consola de administración de ISA SERVER ubicar la opción **directiva de firewall**, luego hacer clic derecho, seleccionar **nuevo, regla de acceso**. Como se observa en la pantalla N° 12.



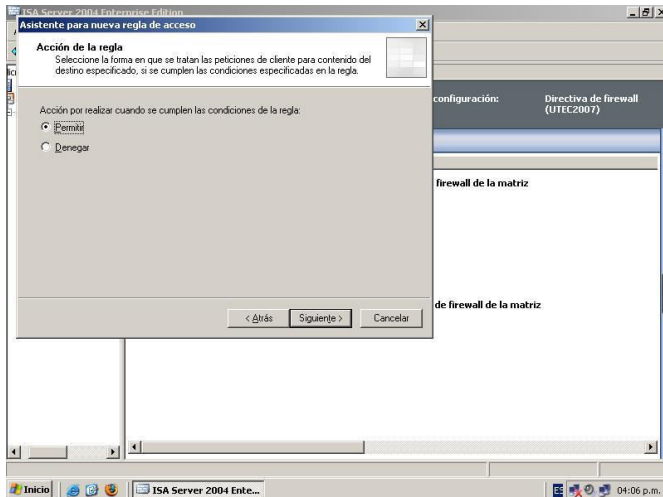
Pantalla N° 12

En la pantalla N° 13, se observa el inicio del asistente para la creación de la nueva regla de acceso, en donde debe agregar un nombre a la regla para este caso se utilizó DNS trafico proxy permitir, después seleccionar el botón siguiente.



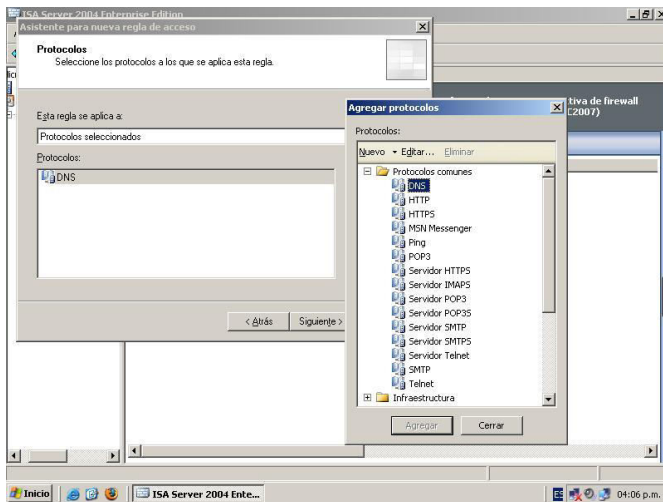
Pantalla 13

En la pantalla N° 14, se debe determinar la acción de la regla, seleccione **permitir**, luego siguiente.



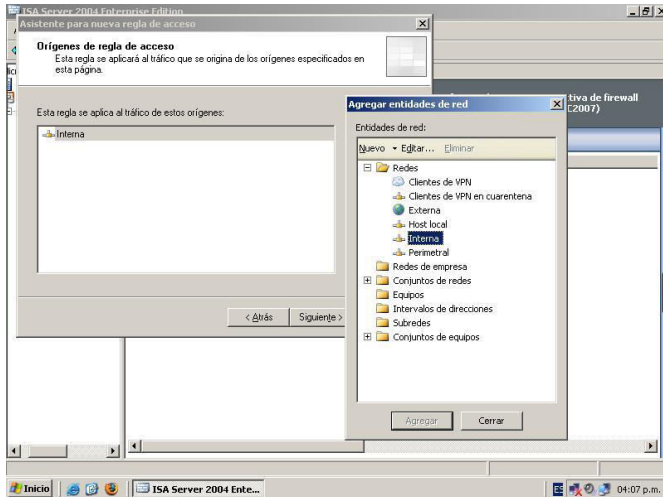
Pantalla N° 14

En la pantalla N° 15 se debe seleccionar el tipo de protocolo que se aplicara la regla, ubicar la opción agregar, luego en listado de protocolos buscar el protocolo DNS, seleccione agregar, después cerrar, por ultimo seleccione siguiente.



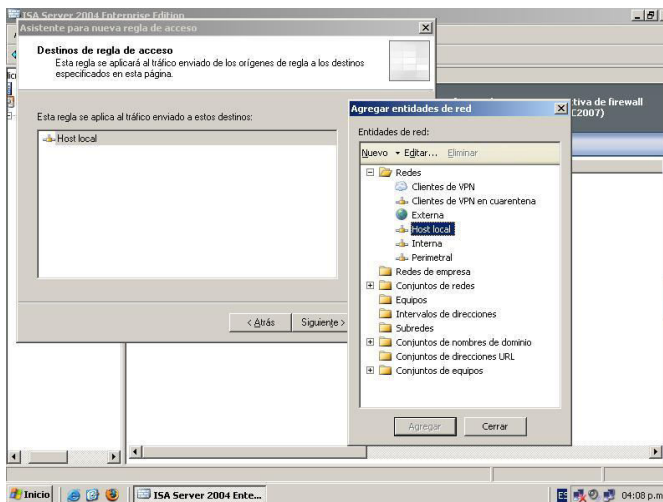
Pantalla N° 15

En la pantalla N° 16, se debe especificar el tráfico origen, ubique y seleccione agregar, luego en el listado buscar red interna y elija agregar, después cerrar, por ultimo seleccione siguiente.



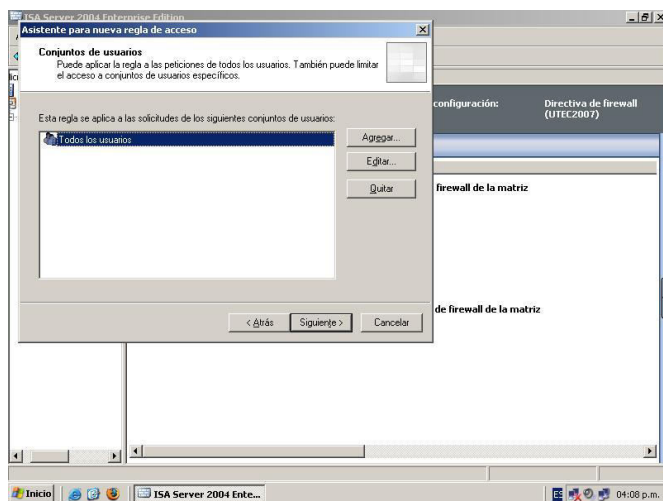
Pantalla N° 16

En la pantalla N° 17, se debe especificar el tráfico destino de la regla de acceso, ubique y seleccione agregar, luego en el listado buscar red host local (equipo donde ejecuta ISA Server, además se ejecuta DNS) y elija agregar, después cerrar, por ultimo seleccione siguiente.



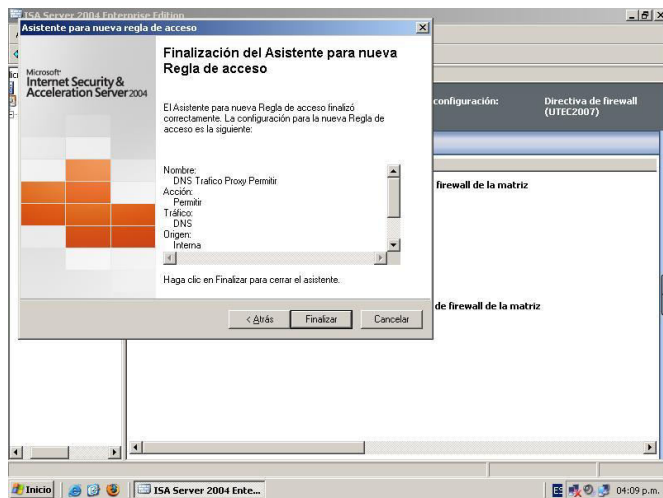
Pantalla N° 17

Debe determinar el conjunto de usuarios a los que se aplicará la regla de acceso, seleccione todos los usuarios, luego elija el botón siguiente, como se observa en la pantalla N° 18.



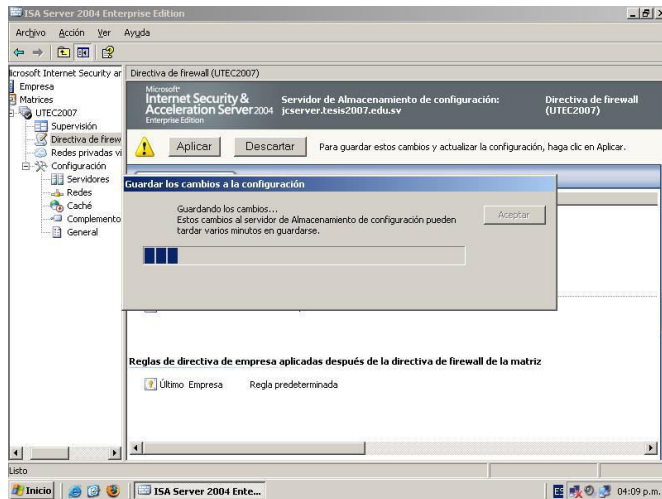
Pantalla N° 18

En la pantalla N° 19, se finaliza el asistente para la creación de la nueva regla de acceso, revisar la información, luego seleccione el botón finalizar.



Pantalla N° 19

Por último se debe aplicar los cambios a ISA SERVER, seleccionar la opción de aplicar, como se muestra en la pantalla N° 20.

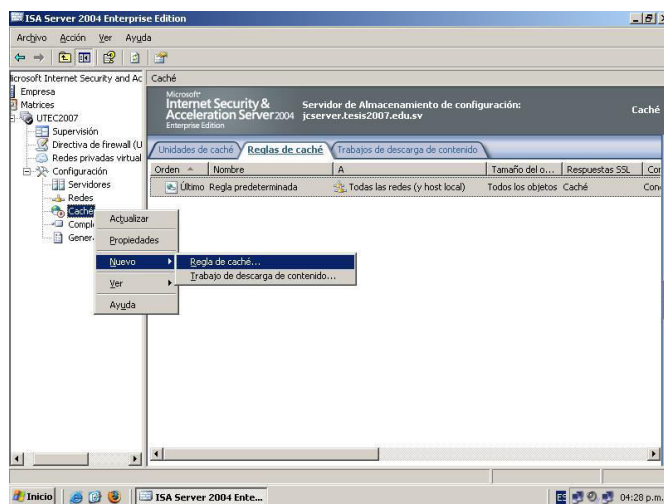


Pantalla N° 20

3.3 MANUAL PARA LA CONFIGURACIÓN DE LA CACHE WEB

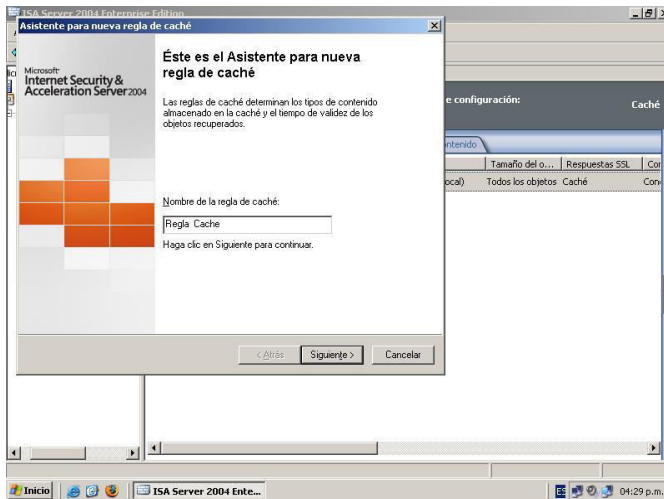
Objetivo: Que el estudiante observe el proceso para configurar la cachè web.
El siguiente paso consiste en configuración de la cache web de ISA Server 2004 para la red interna.

En la consola de administración de Microsoft Internet Security and Acceleration Server 2004, abra la opciones de configuración, luego en la opción Cache Haga click con el botón derecho, seleccione Nuevo, Regla cachè, como se observa en la pantalla N° 1



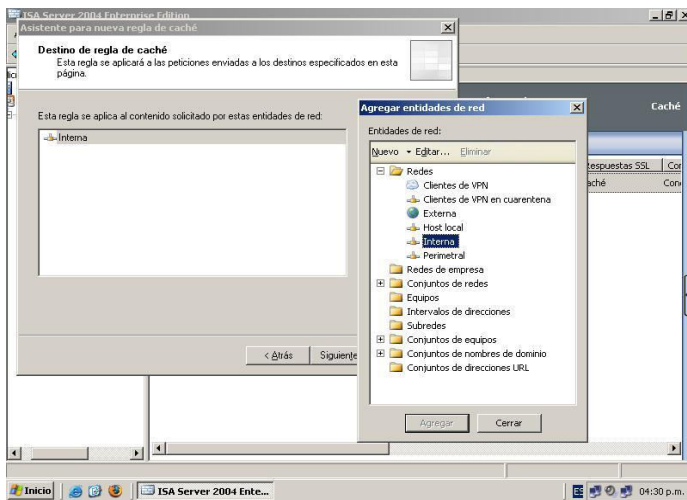
Pantalla N° 1

En la pantalla N° 2, se abrirá el asistente para nueva Regla Cachè, en donde se debe agregar un nombre para dicha regla para este caso se utilizo Regla Cachè.



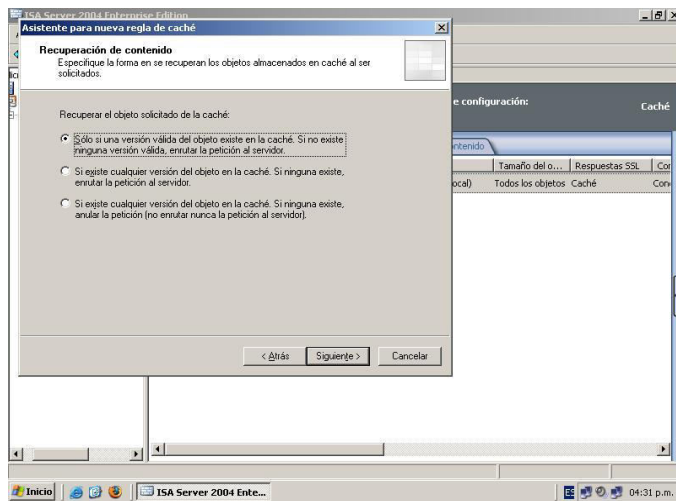
Pantalla N° 2

En el siguiente paso, es definir la red que solicita este servicio, elegir la opción agregar, buscar en entidades de red, expandir la opción de redes la primera, seleccionar la red Interna, seleccionar agregar y luego presione el botón cerrar, seleccionar el botón siguiente como se muestra en la Pantalla N° 3.



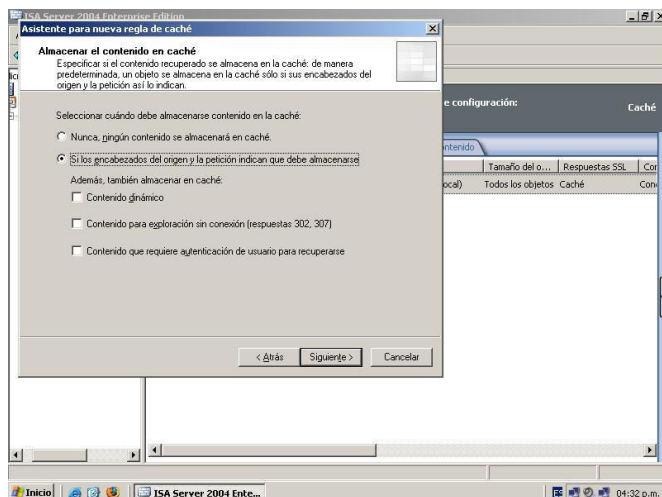
Pantalla N° 3

En la pantalla N° 4, se pregunta la forma en que se recuperan los objetos almacenados en cache al ser solicitados, en esta guía seleccionamos la opción **solo si una versión del objeto existe si no existe, enlutar la petición al servidor**, elegimos botón siguiente.



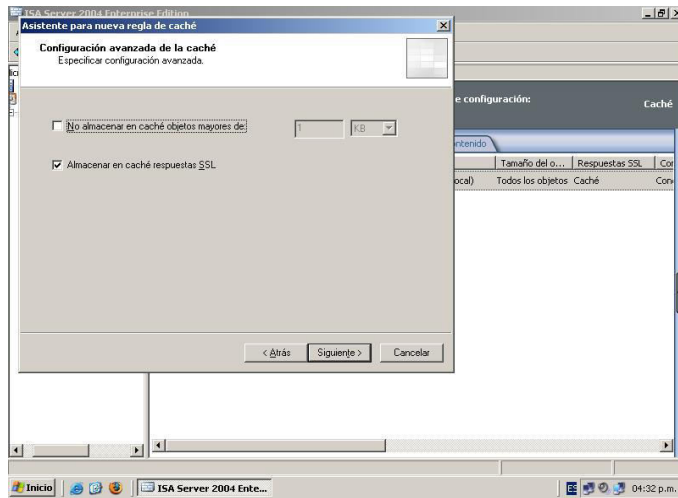
Pantalla N° 4

En la pantalla N° 5, el asistente nos pregunta cuando debe almacenarse el contenido en la cache, para esta guía se utilizo las opciones, **si los encabezados del origen y la petición indican que debe almacenarse**, luego seleccionar el botón siguiente.



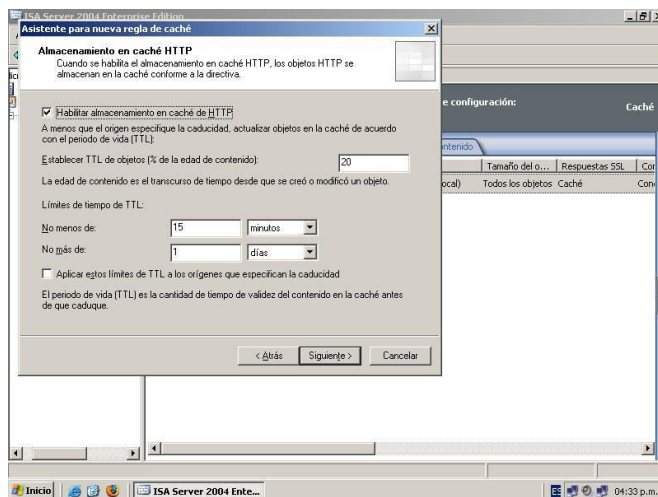
Pantalla N° 5

En la pantalla N° 6, se debe especificar algunos parámetros de la configuración avanzada de la cache, seleccionar la opción de almacenar en cache respuesta ssl, además no limitamos el tamaño de los objetos a almacenar, luego elegimos siguiente.



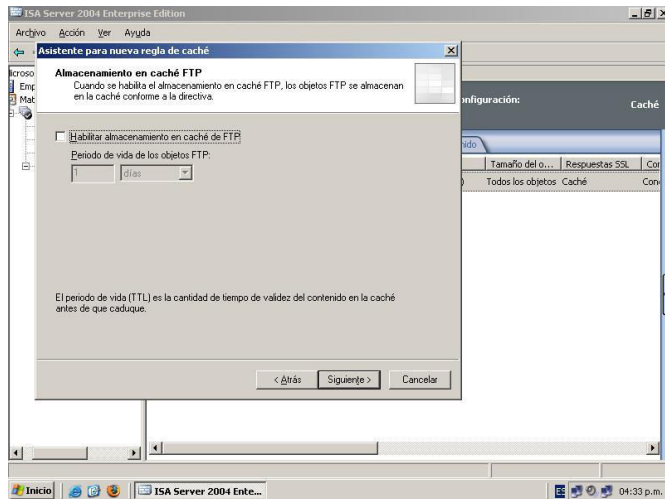
Pantalla N° 6

En la Pantalla N° 7, se debe habilitar el almacenamiento en cache de http, luego elegimos el botón siguiente.



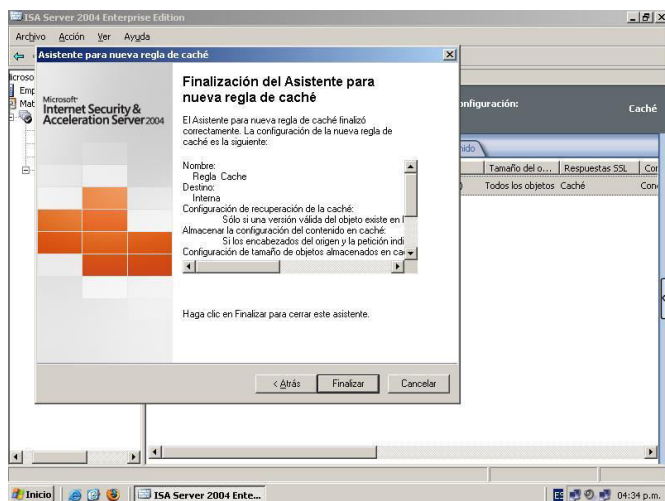
Pantalla N° 7

En la pantalla N° 8, el asistente pregunta si se desea habilitar el almacenamiento en cache de FTP, Para esta guía deseleccionamos la opción, luego elegimos el botón siguiente.



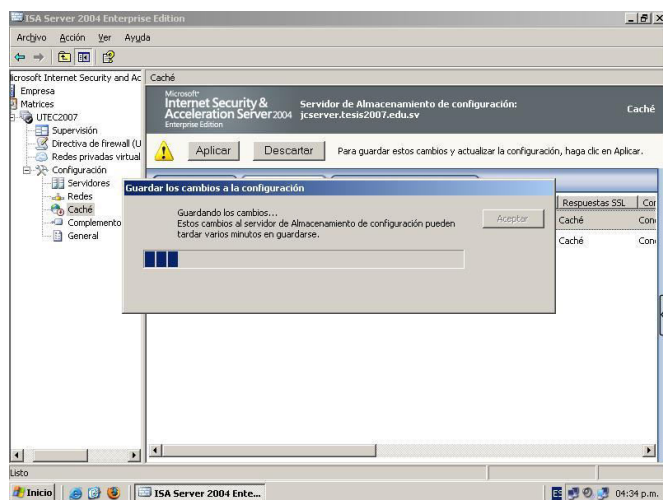
Pantalla N° 8

En la pantalla N° 9, se finaliza el asistente para la nueva regla cache, se revisa la información, luego elegir finalizar.



Pantalla N° 9

Por ultimo se aplica los cambios a ISA SERVER, seleccionar la opción de aplicar Tal como se muestra en la pantalla N° 10.



Pantalla N° 10

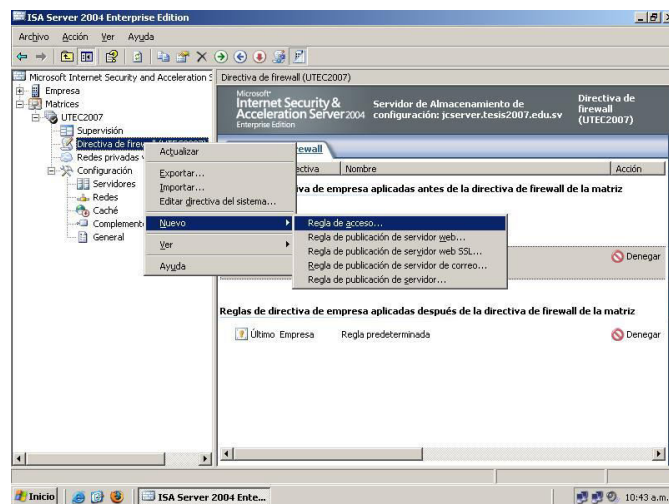
3.4 MANUAL PARA CONFIGURAR POLITICAS DE FIREWALL DE ISA SERVER 2004, BLOQUEAR MSN MESSENGER

Objetivo: Que el estudiante observe el proceso para configurar políticas de firewall de ISA SERVER 2004, para impedir el acceso de la aplicación MSN Messenger.

El siguiente paso consta con la configuración de las políticas de firewall en ISA Server 2004 a continuación se describe la configuración de una política de firewall para impedir el acceso de la aplicación MSN Messenger desde la red interna hacia la red externa.

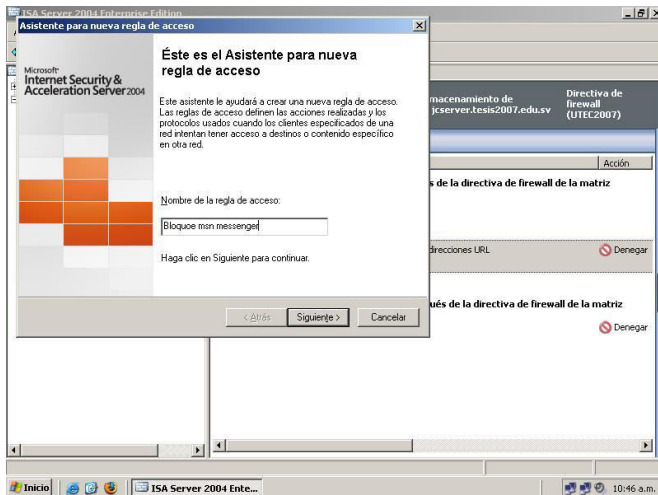
En la consola de administración de Microsoft Internet Security and Acceleration Server 2004, debe primero crear una regla de acceso para el protocolo http.

En consola de administración de ISA SERVER debe buscar la opción de políticas de firewall hacer click derecho sobre dicha opción, seleccionar nuevo, regla de acceso tal como se muestra en la pantalla N° 1.



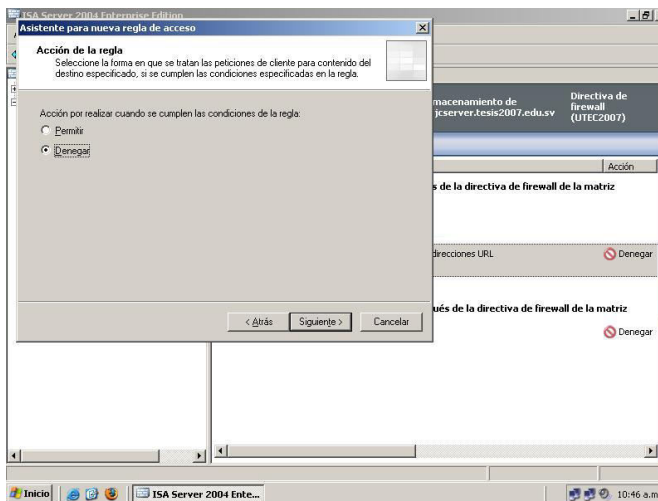
Pantalla N° 1

En la pantalla N° 2, se observa el asistente para la creación de la nueva regla de acceso, en donde debemos agregar un nombre a la regla, en este caso se le llamo bloqueo de msn Messenger, seleccionamos el botón siguiente.



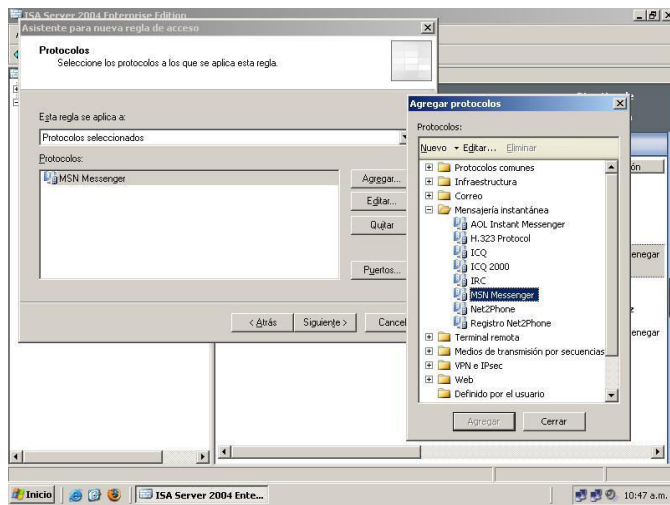
Pantalla N° 2

En la pantalla N° 3, se debe determinar la acción de la regla, seleccione **denegar**, luego seleccionamos el botón siguiente.



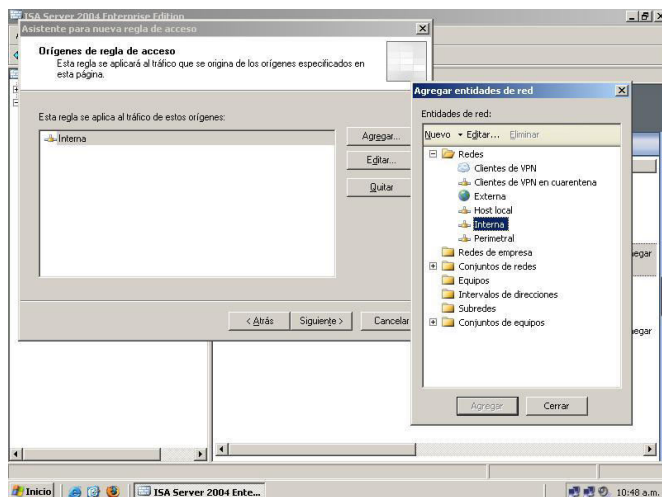
Pantalla N° 3

En la pantalla n° 4, se debe especificar los protocolos a los que se aplica la regla, ubique la opción de protocolos seleccionados, luego la opción de agregar buscar el protocolo MSN Messenger, opción agregar, luego cerrar, y por ultimo siguiente.



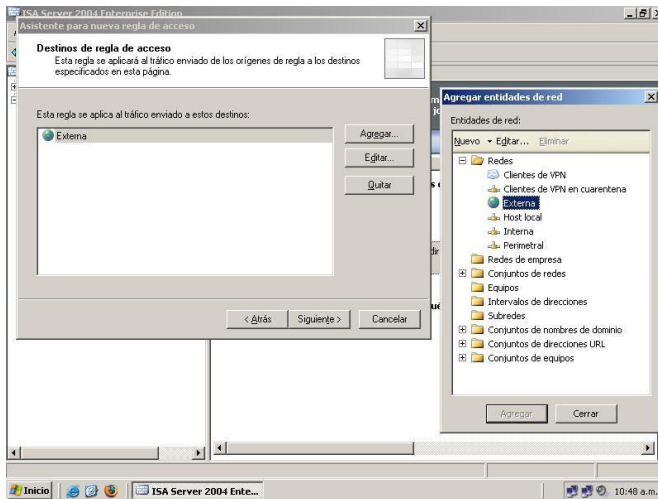
Pantalla N° 4

En la pantalla N° 5, debe especificar los orígenes de la regla de acceso, seleccione la opción de agregar, luego en entidades de de red ubicar la red interna y agregar, luego cerrar, por ultimo seleccione siguiente.



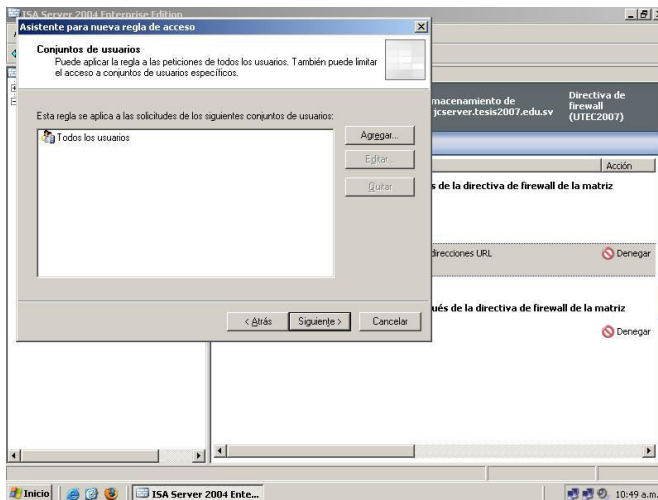
Pantalla N° 5

En la pantalla N° 6, se debe especificar los destinos de la regla de acceso, seleccione la opción de agregar, luego en entidades de red ubicar la red externa y agregar, luego cerrar, por ultimo seleccione siguiente.



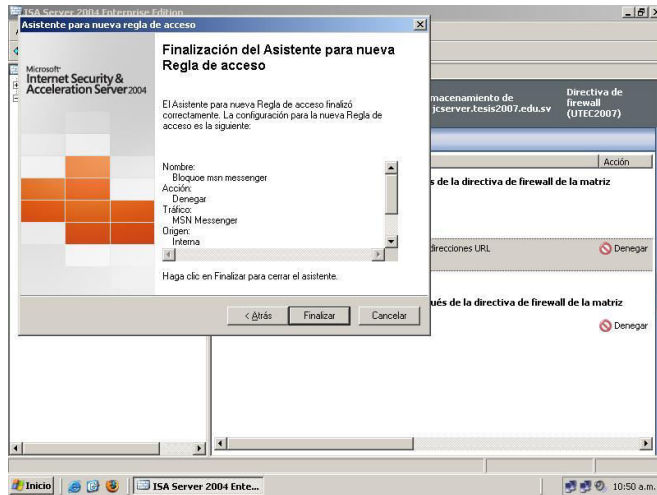
Pantalla N° 6

En la pantalla N° 7, se debe especificar el conjunto de usuarios a los que se aplicara la regla, seleccione, agregue todos los usuarios, luego elija siguiente.



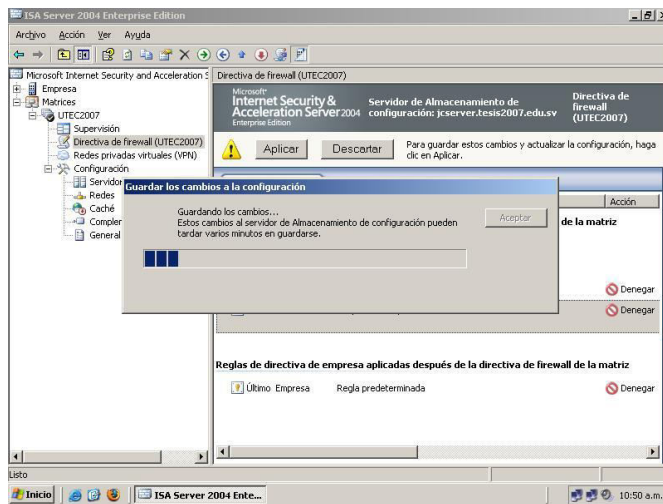
Pantalla N° 7

A continuación en la pantalla N° 8, se finaliza el asistente para la creación de la nueva regla de acceso, revise la información, seleccione el botón de finalizar.



Pantalla N° 8

Por último se debe aplicar los cambios a ISA SERVER, seleccione la opción de aplicar como se observa en la pantalla N° 9.



Pantalla N° 9

MANUAL PARA CONFIGURAR POLITICAS DE FIREWALL DE ISA SERVER 2004

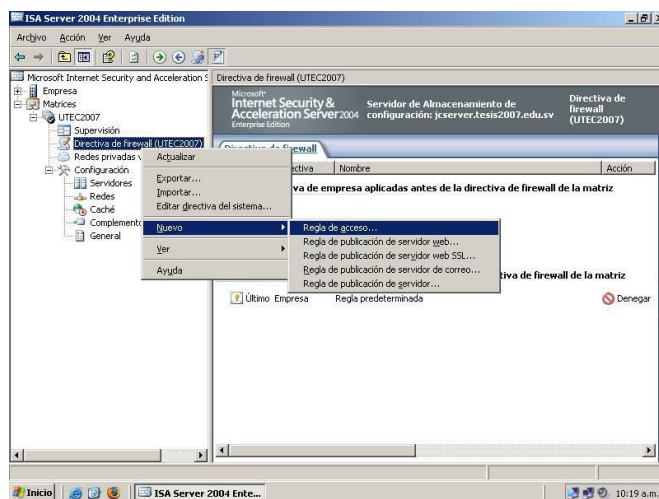
Objetivo: Que el estudiante observe el proceso para la configuración de una política de firewall, para impedir el acceso a un conjunto de direcciones URL.

El siguiente paso consta con la configuración de las políticas de firewall en ISA Server 2004 a continuación se describe la configuración de una política de firewall para impedir el acceso a un conjunto de direcciones URL, desde la red interna hacia la red externa.

NOTA: Previamente debe estar configurada una política de acceso que habilite el tráfico del protocolo http desde la red interna hacia la red externa, para luego crear políticas de firewall que impidan el acceso únicamente a un conjunto de direcciones URL determinado, tal cual se describe adelante.

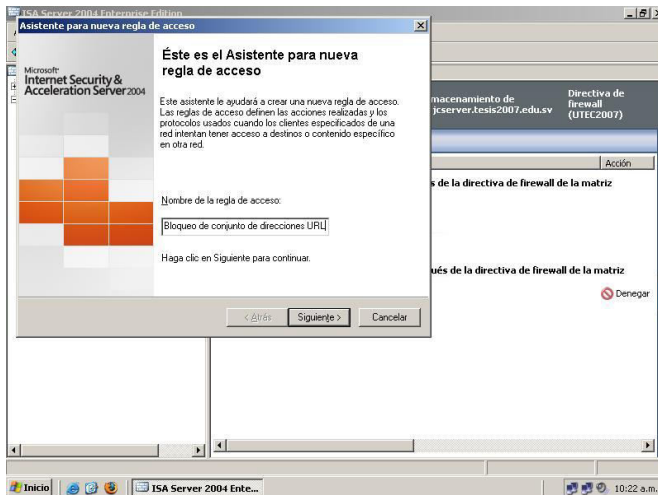
En la consola de administración de Microsoft Internet Security and Acceleration Server 2004, debe primero crear una regla de acceso para el protocolo http.

En consola de administración de ISA SERVER debe buscar la opción de políticas de firewall hacer click derecho sobre dicha opción, seleccionar nuevo, regla de acceso (pantalla N° 1).



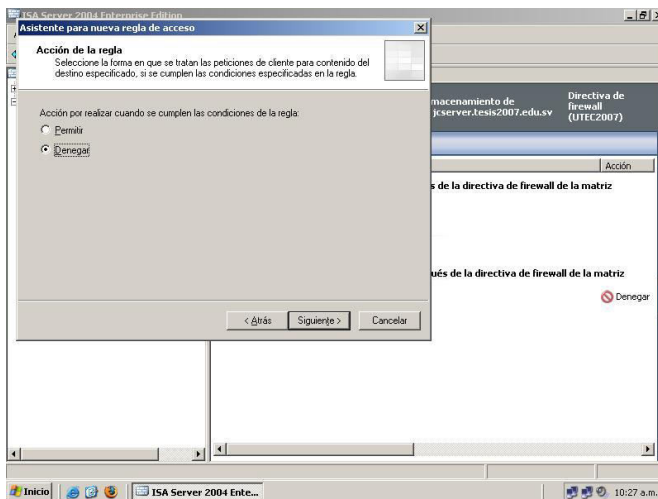
Pantalla N° 1

En la pantalla N° 2, se abrirá el asistente para la creación de la nueva regla de acceso, en donde debemos agregar un nombre a la regla, en este caso se le llamo bloqueo de conjunto de direcciones URL, seleccionamos siguiente.



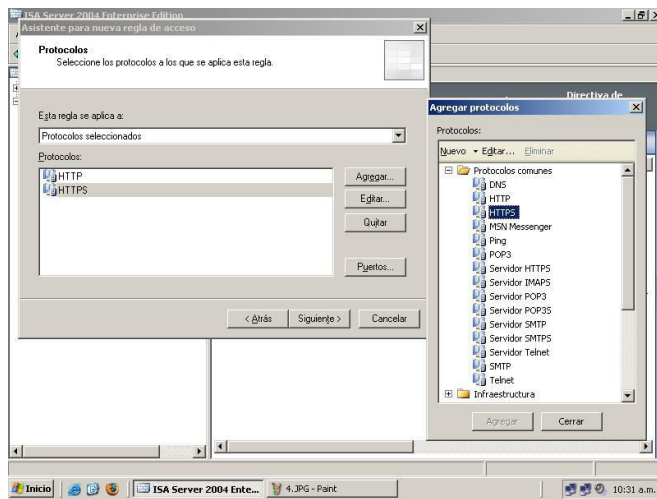
Pantalla N° 2

En la pantalla N° 3, se debe determinar la acción de la regla, seleccione **denegar**, luego seleccionar el botón siguiente.



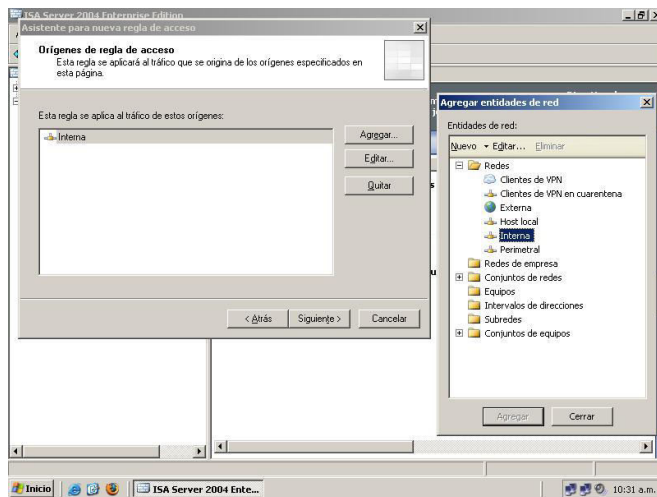
Pantalla N° 3

En la pantalla N° 4, se debe especificar los protocolos a los que se aplica la regla, ubique la opción de protocolos seleccionados, luego la opción de agregar buscar el protocolo HTTP, HTTPS, opción agregar, luego cerrar, y por ultimo seleccionar el botón siguiente.



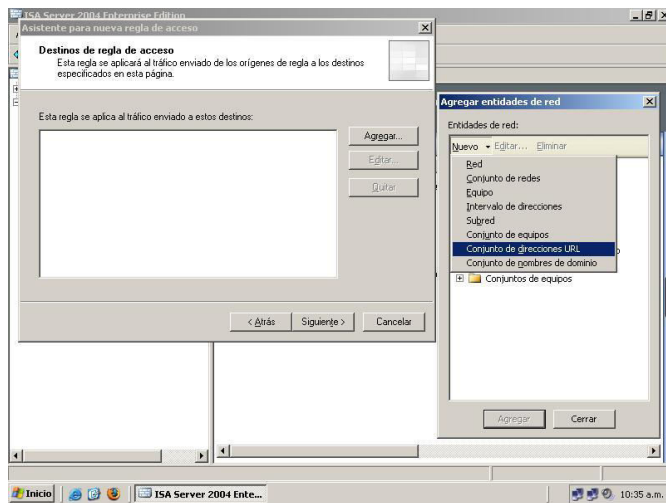
Pantalla N° 4

En la pantalla N° 5, debe especificar los orígenes de la regla de acceso, seleccione la opción de agregar, luego en entidades de de red ubicar la red interna y agregar, luego cerrar, por ultimo seleccione el botón siguiente.



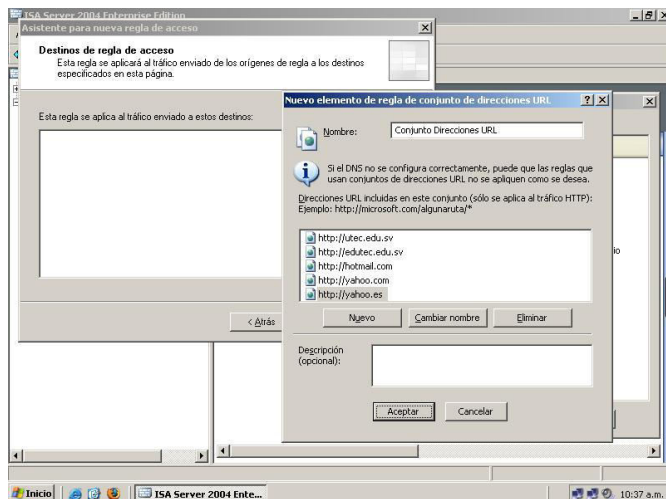
Pantalla N° 5

En la pantalla N° 6, se debe especificar los destinos de la regla de acceso, seleccione la opción de agregar, luego en entidades de de red seleccione el botón nuevo, y ubique la opción **conjunto de direcciones URL** para configurar un nuevo conjunto de direcciones.



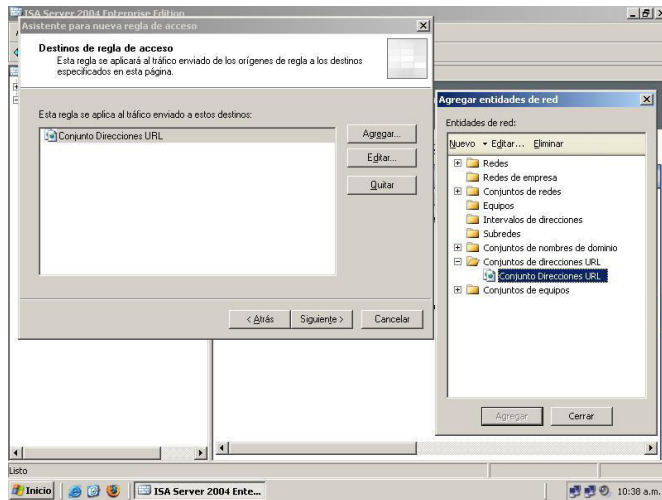
Pantalla N° 6

En la pantalla N° 7, especifique un nombre para el conjunto de direcciones URL, seleccione el botón nuevo, y agregue el nombre de la dirección URL que desee bloquear, en este caso se especificaron las direcciones de http://utec.edu.sv, http://edutec.edu.sv, http://hotmail.com, http://yahoo.com, http://yahoo.es, por ultimo seleccionar el botón siguiente.



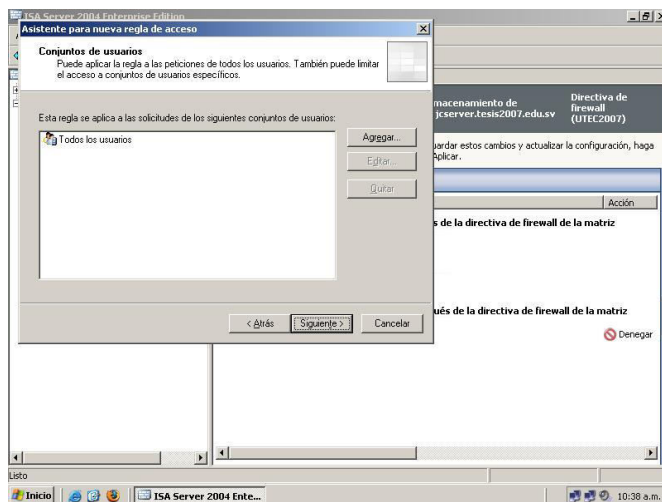
Pantalla N° 7

Después de haber configurado un nuevo conjunto de direcciones URL como se observa en la pantalla N° 8, especifique los destinos de la regla de acceso, seleccione la opción de agregar, luego en entidades de red ubicar el **nuevo conjunto de direcciones URL**, elija agregar, luego cerrar, por último seleccione el botón siguiente.



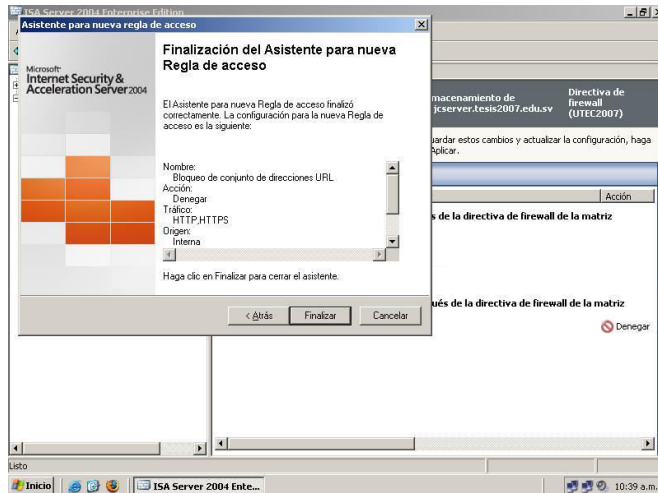
Pantalla N° 8

En la pantalla N° 9, se debe especificar el conjunto de usuarios a los que se aplicara la regla, seleccione, agregue todos los usuarios, luego elija siguiente.



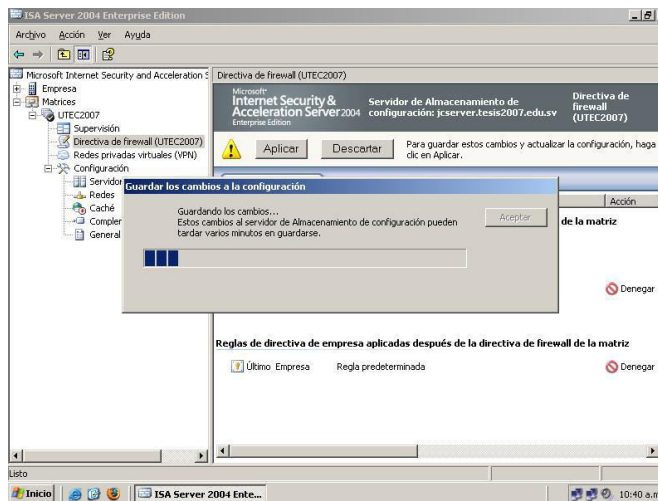
Pantalla N° 9

A continuación, finaliza el asistente para la creación de la nueva regla de acceso, revise la información, seleccione el botón finalizar (pantalla N° 10).



Pantalla N° 10

Por último, se debe aplicar los cambios a ISA SERVER, seleccione la opción de aplicar, como se observa en la pantalla N° 11.



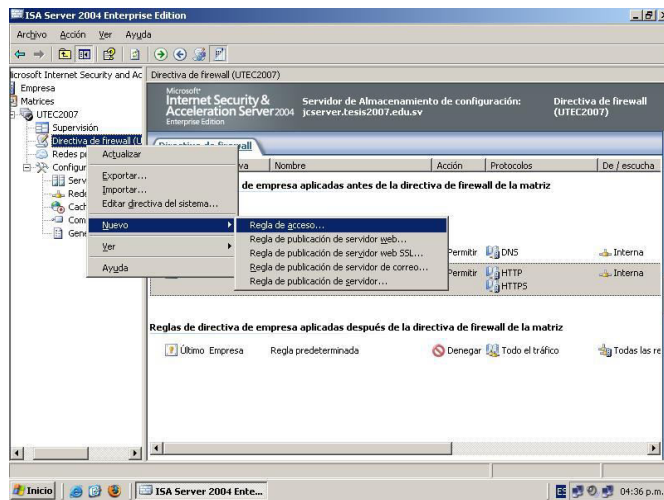
Pantalla N° 11

3.5 MANUAL PARA CREAR UNA POLÍTICA HTTP QUE IMPIDE DESCARGAS MEDIANTE HTTP CON EXTENSIONES .EXE.

Objetivo: Que el estudiante observe la creación de una política http, que impida descargas http con extensiones .exe en ISA SERVER 2004.

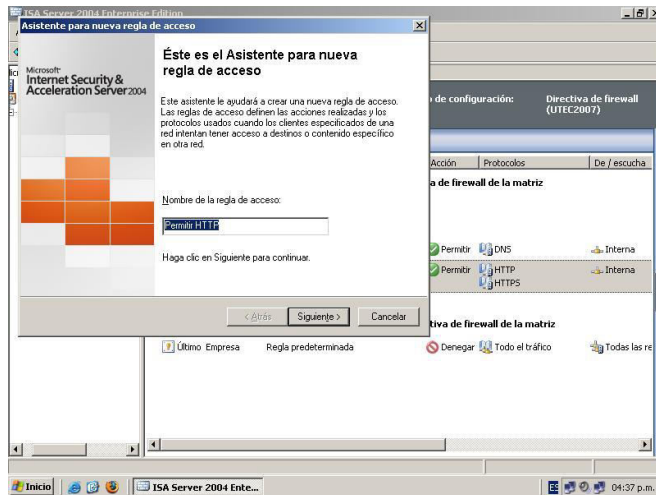
En la consola de administración de Microsoft Internet Security and Acceleration Server 2004, debe primero crear una regla de acceso para el protocolo http.

En consola de administración de ISA SERVER como se observa en la pantalla N° 1, debe buscar la opción de políticas de firewall hacer click derecho sobre dicha opción, seleccionar nuevo, regla de acceso.



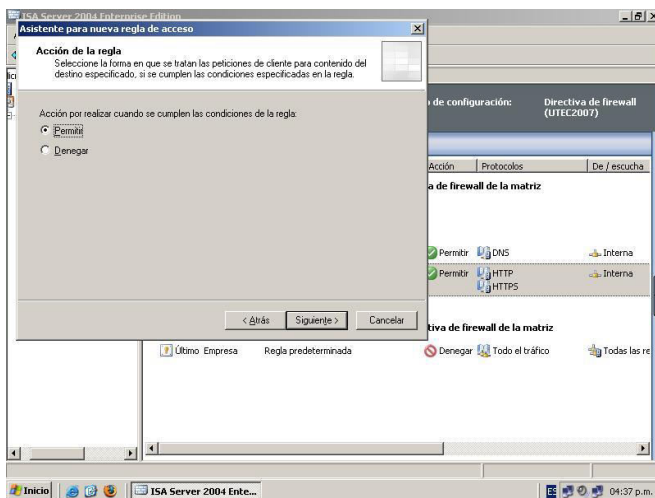
Pantalla N° 1

A continuación, como se observa en la pantalla N° 2, se abrirá el asistente para la creación de la nueva regla de acceso, en donde debemos agregar un nombre a la regla, en este caso se le llamo Permitir http, seleccionamos siguiente.



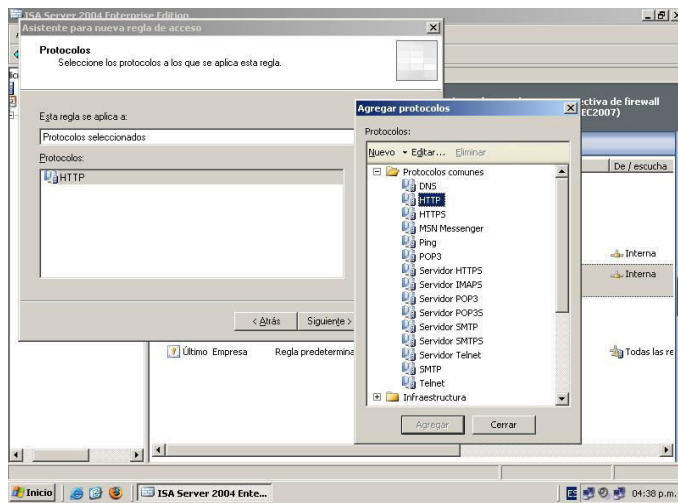
Pantalla N° 2

En la pantalla N° 3, se debe determinar la acción de la regla, seleccione **Permitir**, luego seleccionamos siguiente.



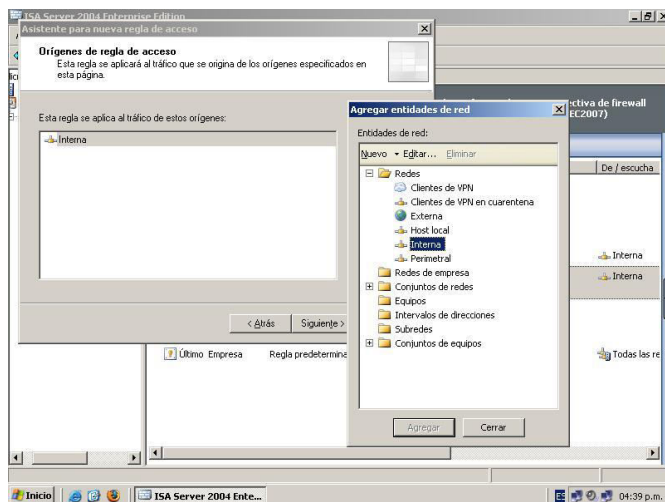
Pantalla N° 3

En la pantalla N° 4, debe especificar los protocolos a los que se aplica la regla, ubique la opción de protocolos seleccionados, luego la opción de agregar buscar el protocolo http, opción agregar, luego cerrar, y por ultimo seleccione el botón siguiente.



Pantalla N° 4

En la pantalla N° 5, se debe especificar los orígenes de la regla de acceso, seleccione la opción de agregar, luego en entidades de de red ubicar la red interna y agregar, luego cerrar, por ultimo seleccione siguiente.



Pantalla N° 5

ISA Server 2004 Enterprise Edition
Asistente para nueva regla de acceso

Destinos de regla de acceso

Esta regla se aplicará al tráfico enviado de los orígenes de regla a los destinos especificados en esta página.

Esta regla se aplica al tráfico enviado a estos destinos:

- Externa

< Atrás Siguiente >

Último Empresa Regla predeterminada

Agregar entidades de red

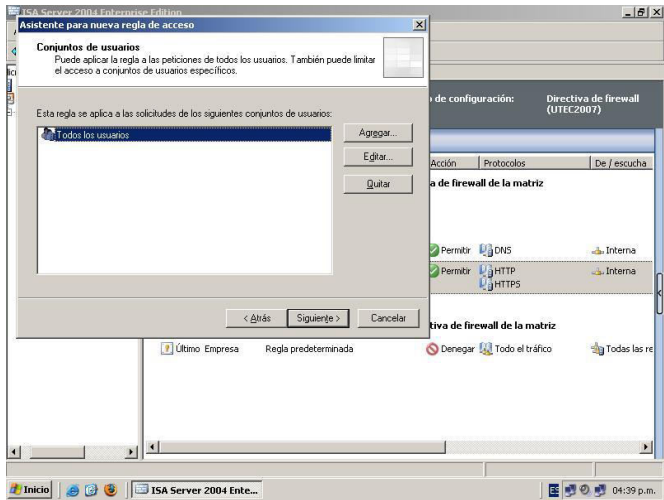
Entidades de red:

Nuevo Editar... Eliminar

- Redes
 - Clientes de VPN
 - Clientes de VPN en cuarentena
 - Externa**
 - Host local
 - Interna
 - Perimetral
- Redes de empresa
 - Conjuntos de redes
 - Equipos
 - Intervalos de direcciones
 - Subredes
- Conjuntos de nombres de dominio
- Conjuntos de direcciones URL
- Conjuntos de equipos

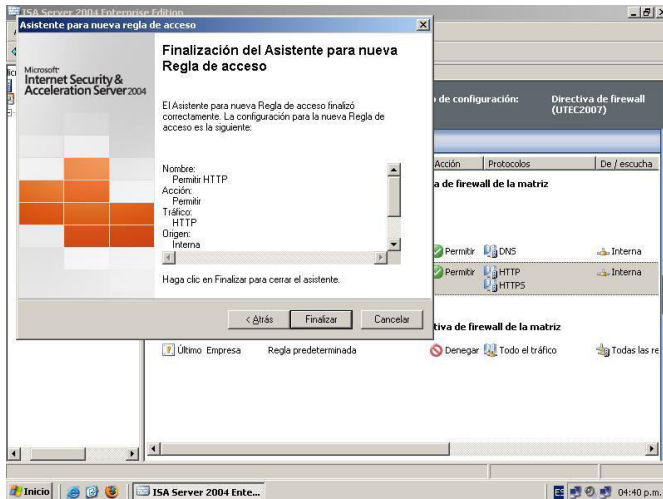
Agregar Cerrar

En la pantalla N° 7, se debe especificar el conjunto de usuarios a los que se aplicara la regla, seleccione, agregue todos los usuarios, luego elija el botón siguiente.



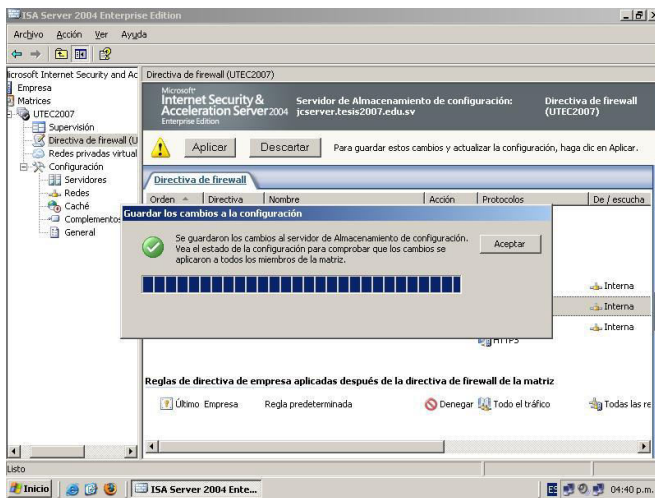
116

En la pantalla N° 8, se finaliza el asistente para la creación de la nueva regla de acceso, revise la información, seleccione el botón finalizar.



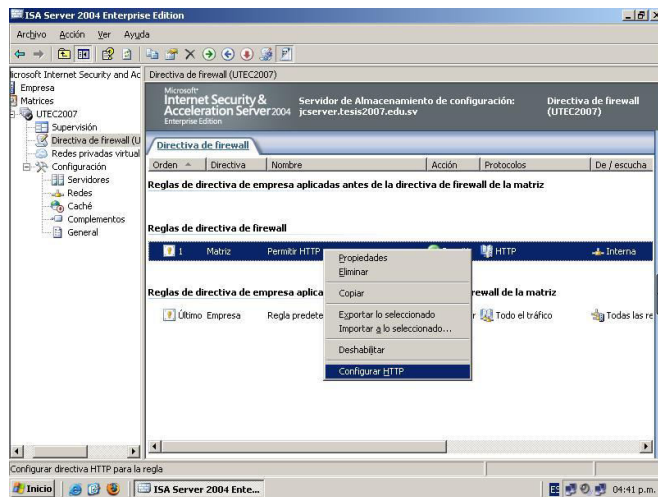
Pantalla N° 8

Por último como se observa en la pantalla N° 9, se debe aplicar los cambios a ISA SERVER, seleccione la opción de aplicar.



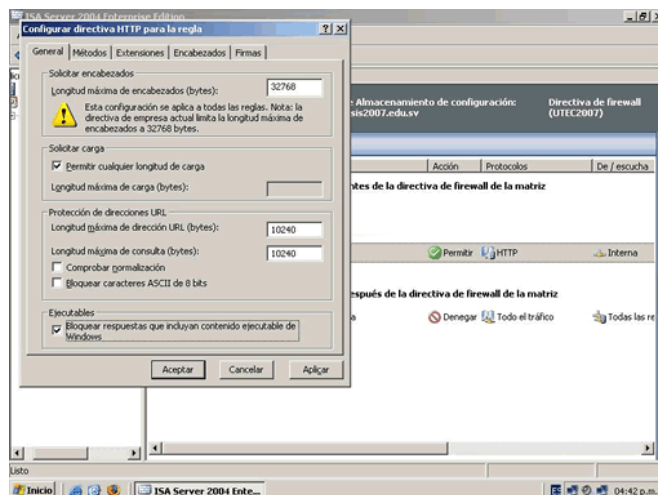
Pantalla N° 9

Después de haberse creado la regla de acceso http, se debe configurar la política http para impedir las descargas de archivos con extensiones .exe En la consola de administración de ISA SERVER y adentro de la opción directiva de firewall, hacer click derecho sobre la regla que se creó anteriormente, permitir http, ubique la opción de configurar http (ver pantalla N° 10).



Pantalla N° 10

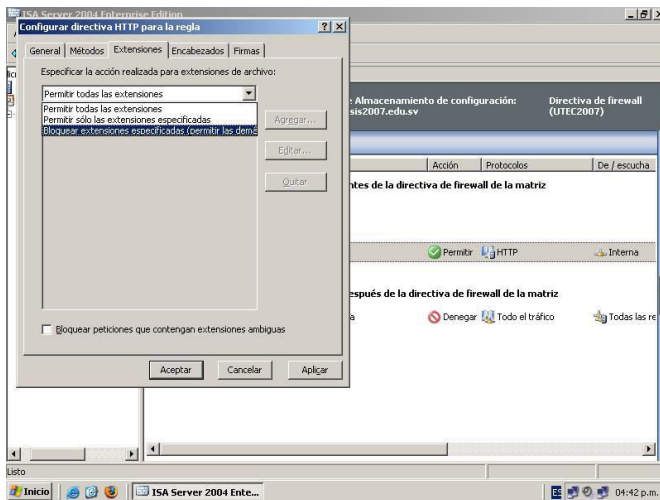
En la casilla general seleccionar la opción de bloquear respuestas que incluyan ejecutable de Windows, luego seleccionamos aceptar, tal como se muestra en la pantalla N° 11



Pantalla N° 11

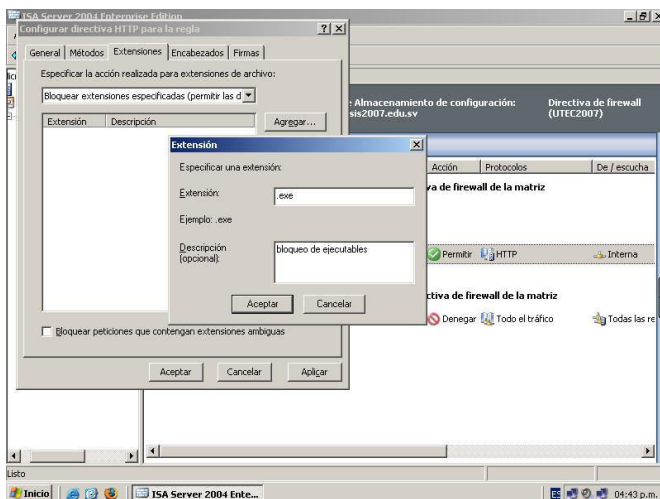
NOTA: Normalmente hasta aquí se puede bloquear las descargas con extensiones .exe. Existe otro método donde no solamente se pueden bloquear las extensiones .exe sino que también otro tipo de extensiones. rar, .zip, etc. A continuación se detalla.

Para bloquear extensiones .exe de diferente método repita el procedimiento de la pantalla N° 11, con la diferencia de que en lugar de elegir la casilla de opción general seleccione la casilla de extensiones. Especificar la acción a realizar para extensiones, ubique la opción de Bloquear extensiones especificadas.



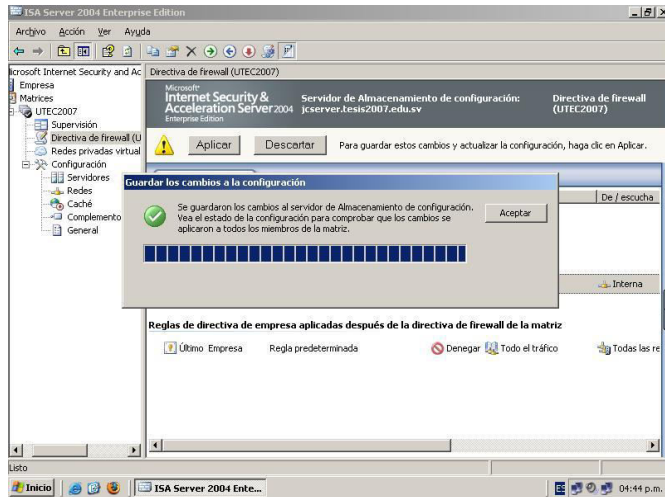
Pantalla N° 12

A continuación en la casilla de extensión digite el tipo de extensión a bloquear en este caso. Exe, (puede determinar algún otro tipo de extensión) y digite una pequeña descripción de la acción, luego seleccionar aceptar, aceptar (ver pantalla N° 13).



Pantalla N° 13

Para finalizar debe aplicar los cambios a ISA SERVER, seleccione la opción de aplicar, como se observa en la pantalla N° 14.

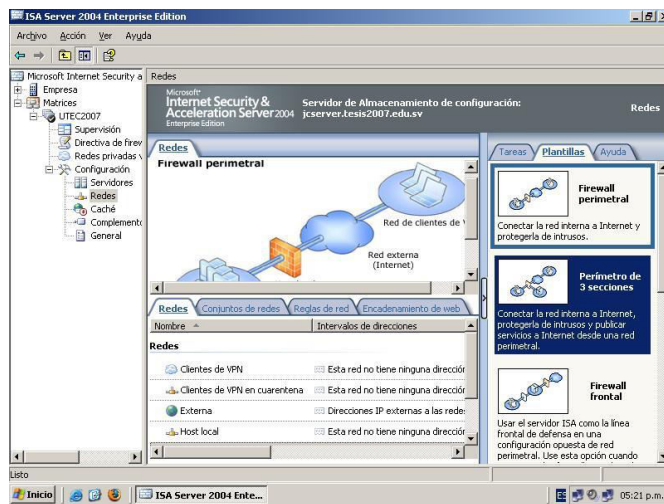


Pantalla N° 14

3.6 MANUAL PARA CONFIGURAR LA RED PERIMETRAL (DMZ)

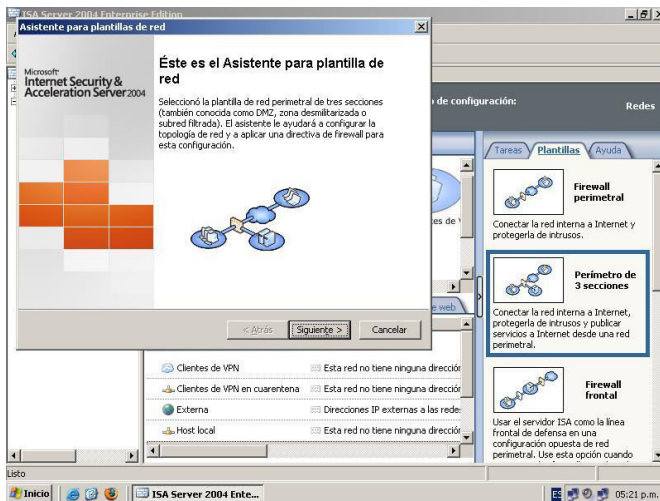
Objetivo: Que el estudiante observe la configuración de una red perimetral (DMZ) en ISA SERVER 2004.

En la consola de administración de Microsoft Internet Security and Acceleration Server 2004, ubicar la opción y expandir la opción de **configuración**, luego elija **redes**, a continuación abra el panel de tareas ubicado a lado derecho de la pantalla, abra la pestaña de **plantillas**, escoja en el listado perímetro de 3 secciones (ver pantalla N° 1).



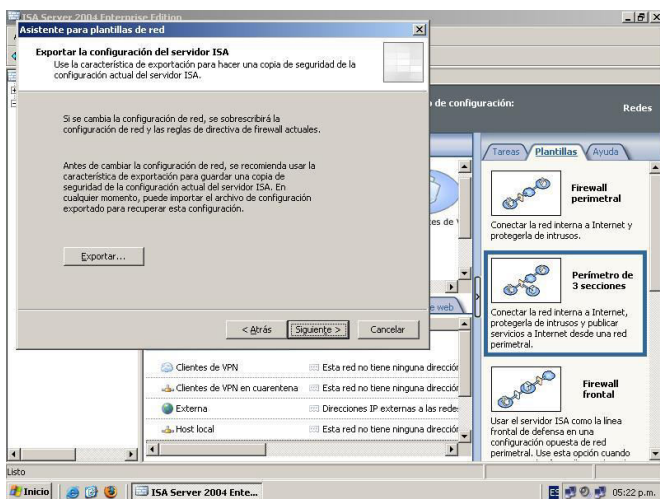
Pantalla N° 1

A continuación, en la pantalla N° 2, se observará el inicio del asistente para plantilla de red, seleccione el botón siguiente.



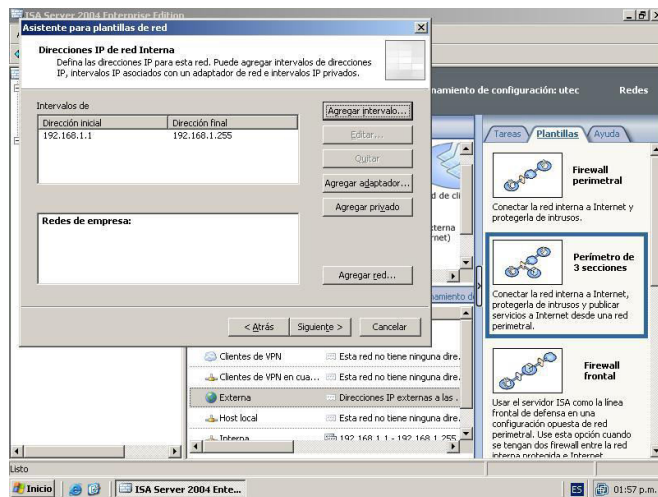
Pantalla N° 2

Este paso consta en exportar la configuración actual de ISA SERVER 2004, si no se va a guardar la configuración seleccione el botón siguiente (ver pantalla N° 3).



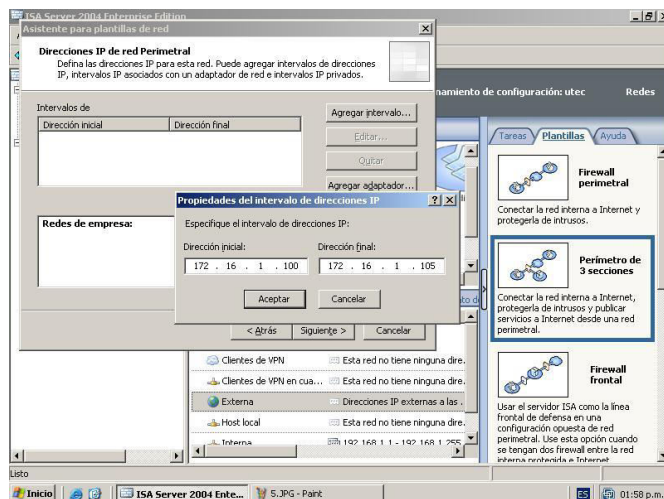
Pantalla N° 3

En la pantalla N° 4, se debe determinar el rango de direcciones de la red interna, en este caso debido a la instalación anterior de ISA SERVER 2004 ya se encuentra especificado un rango de direcciones para la red interna(192.168.1.1-192.168.1.255), se puede agregar manualmente un intervalo, o seleccionando un adaptador de red.



Pantalla N° 4

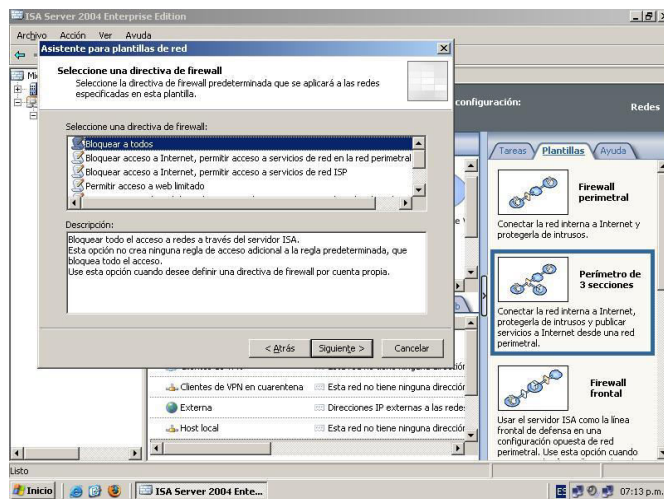
En la pantalla N° 5, se define el rango de direcciones para la red perimetral (DMZ), para agregar manualmente un rango de direcciones selecciones **agregar intervalo**, y especifique el siguiente rango utilizado para este caso, inicial(172.16.1.100), final(172.16.1.105), luego seleccione aceptar, después siguiente. También se logra determinar las direcciones agregando un adaptador de red.



Pantalla N° 5

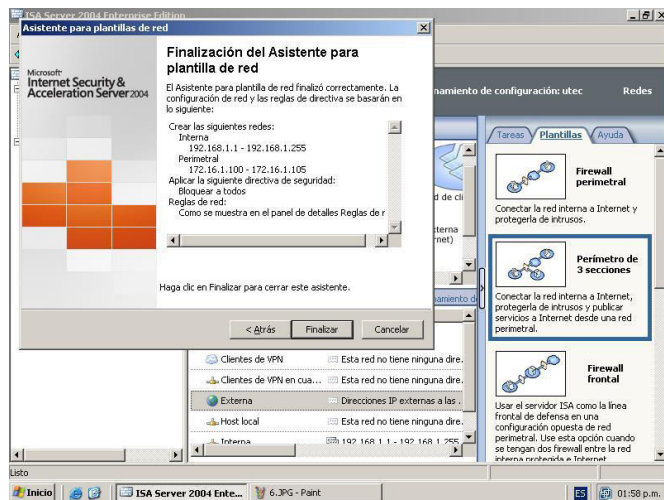
NOTA: la zona perimetral generalmente debe poseer direcciones públicas para que exista acceso desde cualquier parte del exterior a servicios públicos, depende del bloque de IP públicas que se adquieran de un ISP (proveedor de servicios)

En la pantalla N° 6, debe seleccionar una directiva de firewall predefinidas que posteriormente se aplicara, para este caso se selecciono la opción de **bloquear a todos**, para luego crear específicamente las reglas de acceso para la red perimetral.



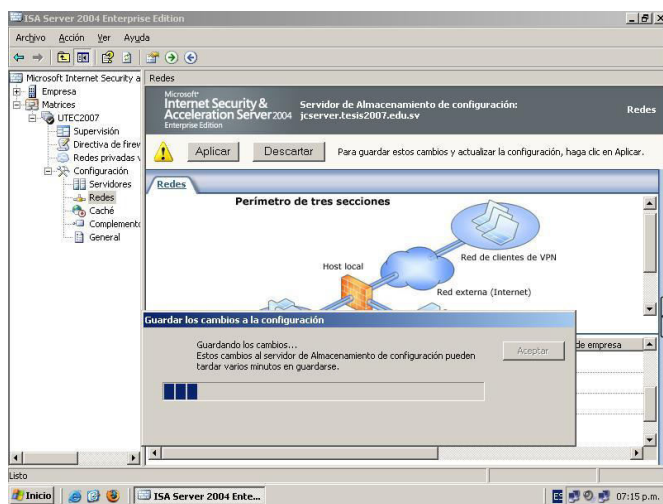
Pantalla N° 6

La pantalla N° 7, muestra la finalización del asistente para la plantilla de red, revise la información, seleccione el botón finalizar.



Pantalla N° 7

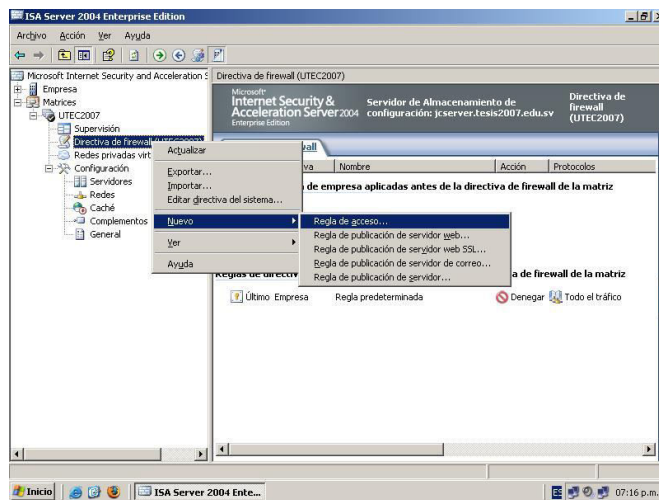
Para terminar la primera parte, se debe aplicar los cambios a ISA SERVER 2004, seleccione aplicar como se observa en la pantalla N° 8.



Pantalla N° 8

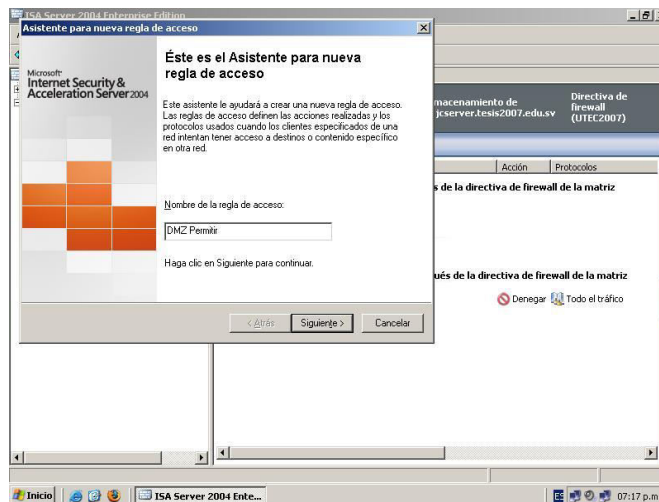
CONFIGURACION DE LAS REGLAS DE ACCESO PARA LA RED PERIMETRAL (DMZ)

En consola de administración de ISA SERVER debe buscar la opción de políticas de firewall hacer click derecho sobre dicha opción, seleccionar nuevo, regla de acceso. Primero debe crear una nueva regla de acceso a la red perimetral desde el exterior, habilitando específicamente los servicios a utilizarse (ver pantalla N° 9).



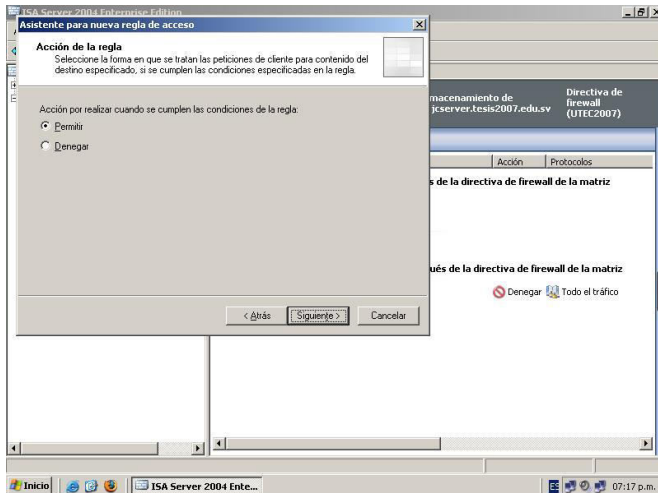
Pantalla N° 9

A continuación, se abrirá el asistente para la creación de la nueva regla de acceso, en donde debemos agregar un nombre a la regla, en este caso se le llamo DMZ Permitir, seleccionamos el botón siguiente (ver pantalla 10).



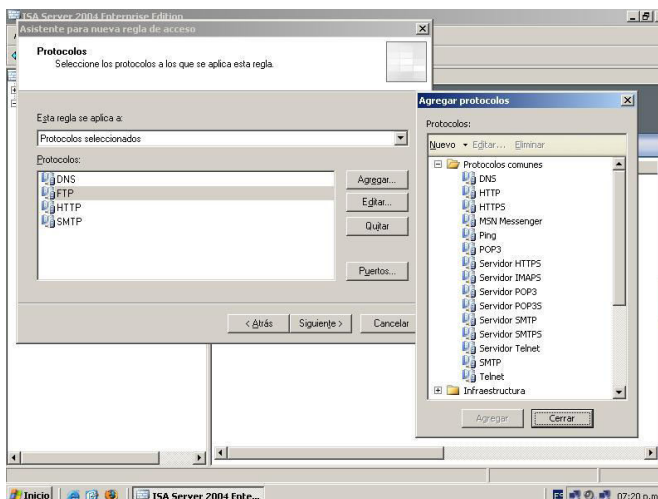
Pantalla N° 10

En la pantalla N° 11, se debe determinar la acción de la regla, seleccione **Permitir**, luego seleccionamos el botón siguiente.



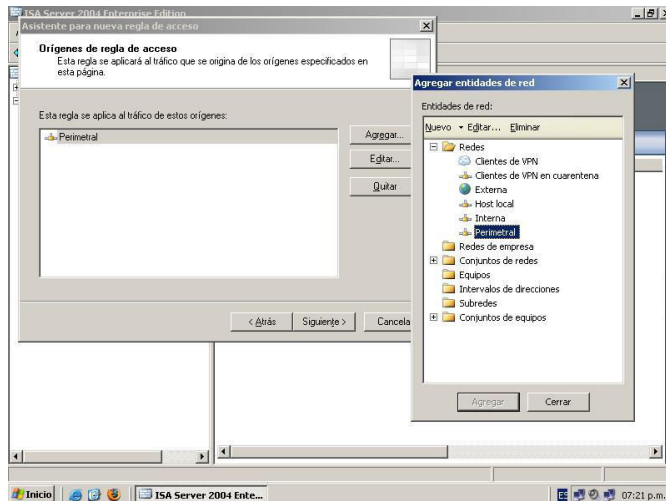
Pantalla N° 11

En la pantalla N° 12, debe especificar los protocolos a los que se aplica la regla los servicios que estarán disponibles en la red perimetral, ubique la opción de protocolos seleccionados, luego la opción de agregar buscar el protocolo HTTP, SMTP, DNS, FTP, Suponiendo que estos servicios estarán disponibles en la red perimetral, seleccione opción agregar por cada protocolo, luego cerrar, y por ultimo seleccione el botón siguiente.



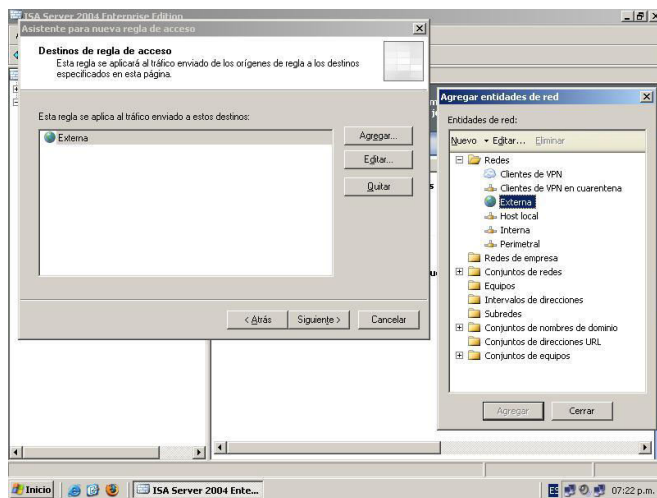
Pantalla N° 12

En la pantalla N° 13, debe especificar los orígenes de la regla de acceso, seleccione la opción de agregar, luego en entidades de de red ubicar la red perimetral y agregar, luego cerrar, por ultimo seleccione el botón siguiente.



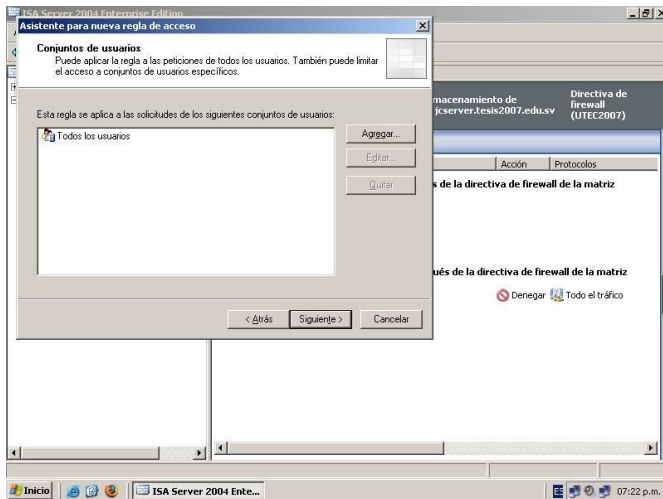
Pantalla N° 13

A continuación, se debe especificar los destinos de la regla de acceso, seleccione la opción de agregar, luego en entidades de de red ubicar la red externa (acceso del exterior) y agregar, luego cerrar, por ultimo seleccione el botón siguiente (ver Pantalla N° 14).



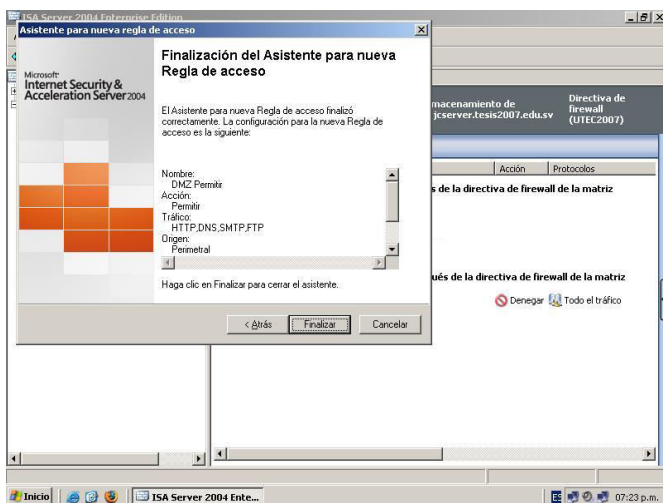
Pantalla N° 14

En la pantalla N° 15, se debe especificar el conjunto de usuarios a los que se aplicara la regla, seleccione, agregue todos los usuarios, luego elija el botón siguiente.



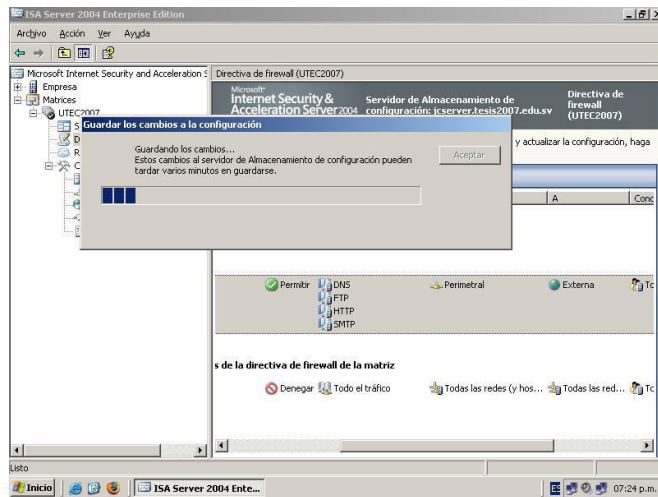
Pantalla N° 15

En la pantalla N° 16, finaliza el asistente para la creación de la nueva regla de acceso, revise la información, seleccione el botón Finalizar.



Pantalla N° 16

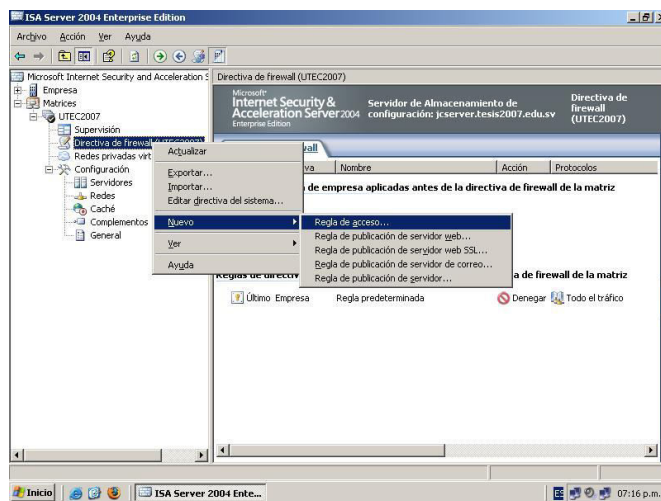
Por ultimo, se debe aplicar los cambios a ISA SERVER, seleccione la opción de aplicar (ver pantalla N° 17).



Pantalla N° 17

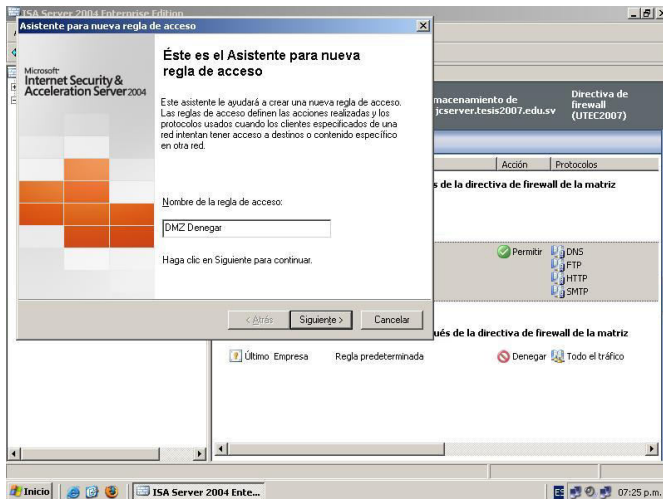
CONFIGURACION DE LAS REGLAS DE ACCESO PARA LA RED PERIMETRAL (DMZ)

En la consola de administración de ISA SERVER debe buscar la opción de políticas de firewall hacer click derecho sobre dicha opción, seleccionar nuevo, regla de acceso (ver pantalla N° 18). Segundo, debe crear una nueva regla de acceso a la red perimetral que bloquee el acceso desde la red interna (de esta forma solo se podrá acceder a la red perimetral desde el exterior de modo que los usuarios internos deberán salir primero al exterior para luego acceder desde el exterior), habilitando específicamente los servicios a utilizarse.



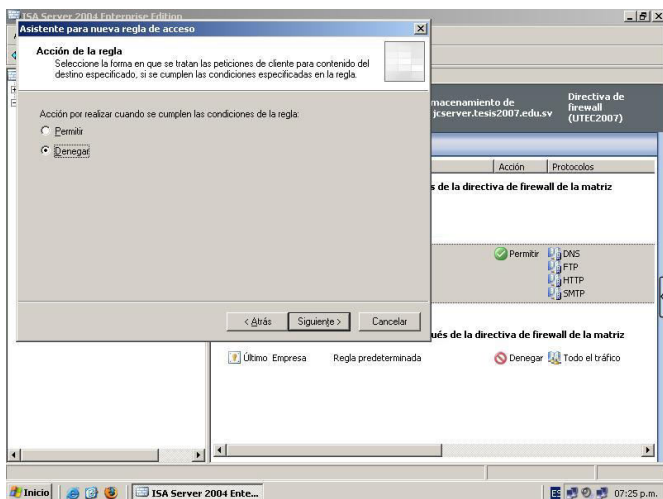
Pantalla N° 18

En la pantalla N° 19, se abrirá el asistente para la creación de la nueva regla de acceso, en donde debemos agregar un nombre a la regla, en este caso se llamo DMZ Denegar, seleccionamos el botón siguiente.



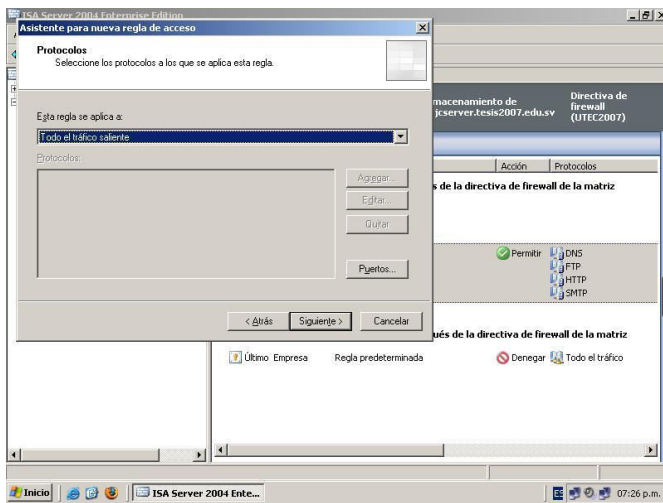
Pantalla N° 19

En la pantalla n° 20, se debe determinar la acción de la regla, seleccione **Denegar**, luego seleccionamos el botón siguiente.



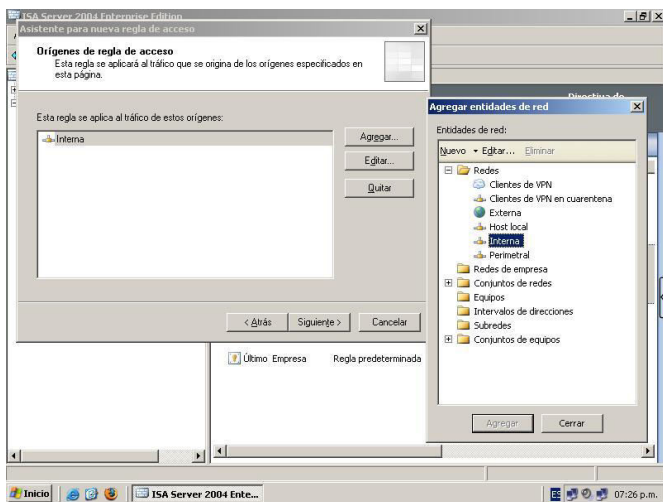
Pantalla N° 20

A continuación se debe especificar los protocolos a los que se aplica la regla los servicios que estarán disponibles en la red perimetral, ubique la opción de todo el trafico saliente (en principio la regla se configuro como denegar), por ultimo seleccionar el botón siguiente (ver pantalla N° 21).



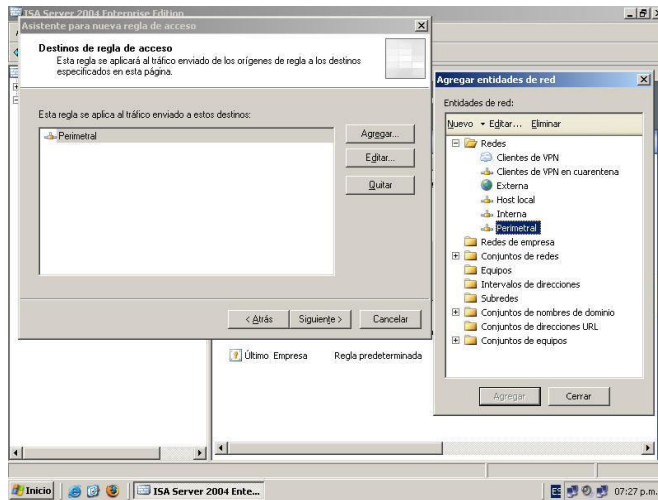
Pantalla N° 21

En la pantalla N° 22, se debe especificar los orígenes de la regla de acceso, seleccione la opción de agregar, luego en entidades de de red ubicar la red interna y agregar, luego cerrar, por ultimo seleccione el botón siguiente.



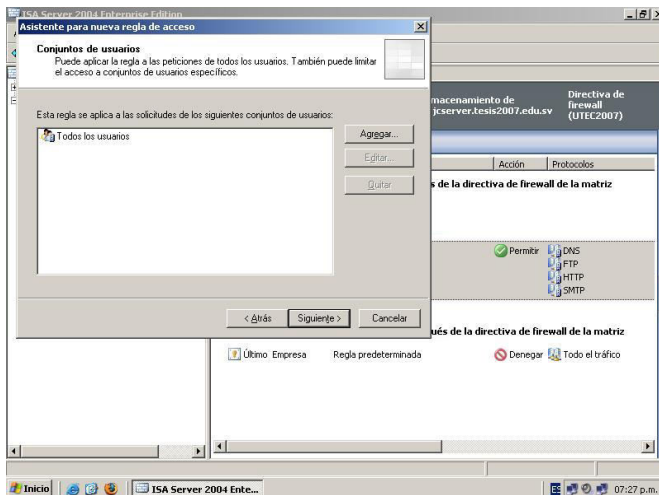
Pantalla N° 22

En la pantalla N° 23, se debe especificar los destinos de la regla de acceso, seleccione la opción de agregar, luego en entidades de red ubicar la red perimetral (bloquear el acceso directo, de esta manera los usuarios internos deberán primero salir a la red externa para luego a la perimetral) agregar, luego cerrar, por ultimo seleccione el botón siguiente.



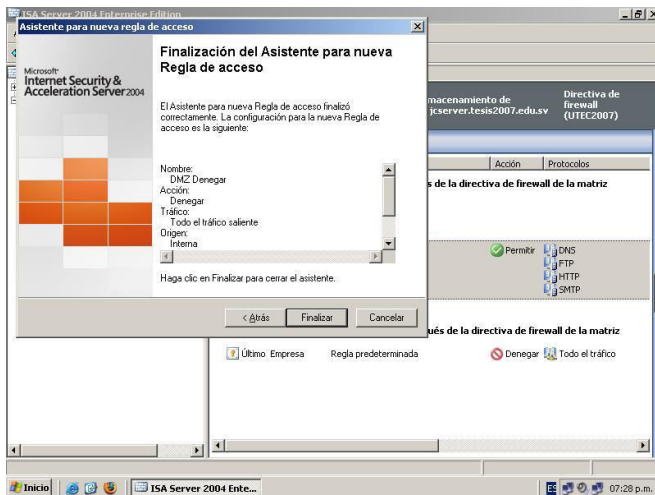
Pantalla N° 23

En la pantalla N° 24, se debe especificar el conjunto de usuarios a los que se aplicara la regla, seleccione, agregue todos los usuarios, luego elija el botón siguiente.



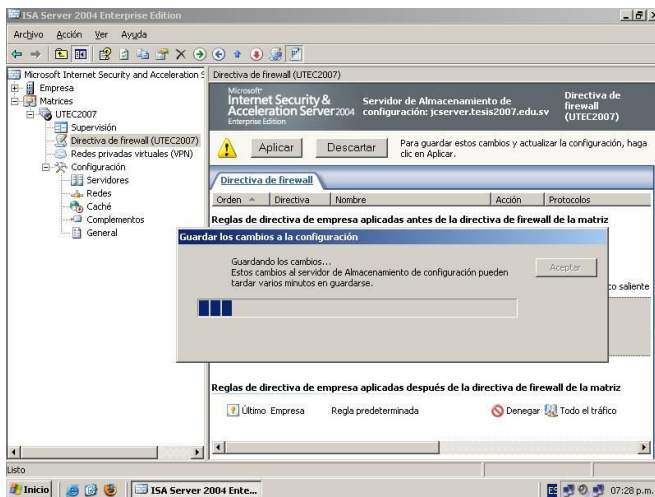
Pantalla N° 24

A continuación, finaliza el asistente para la creación de la nueva regla de acceso, revise la información, seleccione el botón Finalizar (ver pantalla N° 25).



Pantalla N° 25

Por ultimo se debe aplicar los cambios a ISA SERVER, seleccione la opción de aplicar (ver Pantalla N° 26).

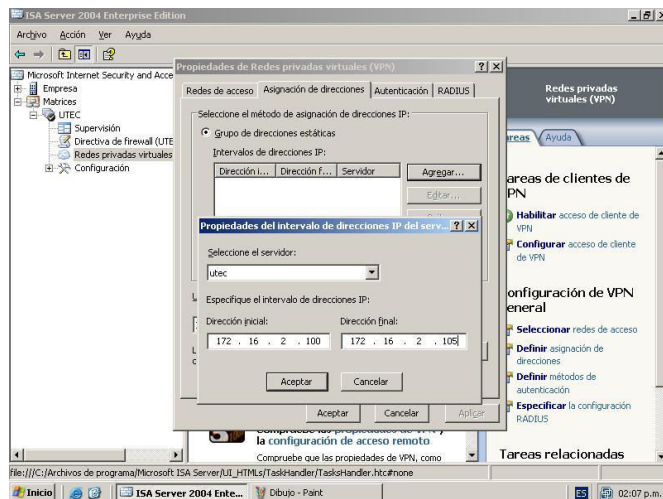


Pantalla N° 26

3.7 MANUAL PARA LA CONFIGURACIÓN DE VPN.

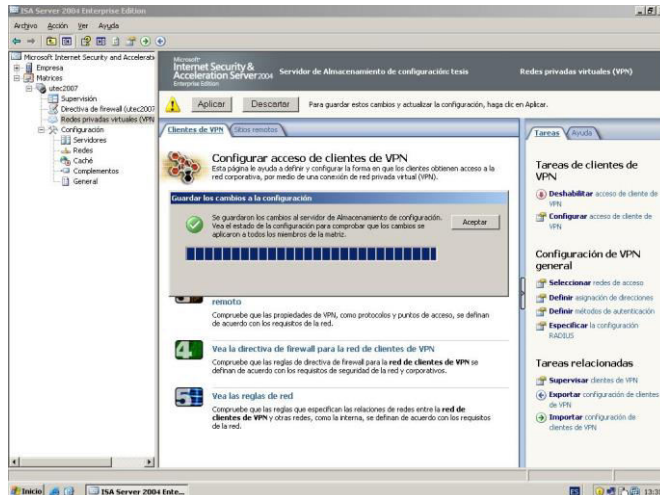
Objetivo: Que el estudiante observe la configuración de VPN a través del software, ISA SERVER 2004.

En la consola de administración de Microsoft Internet Security and Acceleration Server 2004, abra el panel de tareas del área izquierda de la pantalla, seleccione **Definir asignación de direcciones**, en las propiedades de VPN selecciones el botón agregar, después en la siguiente pantalla agregue el nombre del servidor VPN en este caso se llamo utec, luego defina un rango de direcciones en este caso se utilizo 172.16.2.100-172.16.2.105, luego aceptar, aceptar (ver pantalla N° 1).



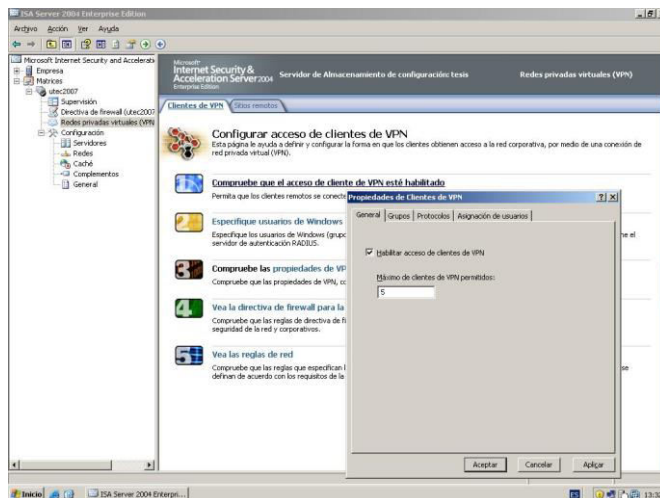
Pantalla N° 1

En la pantalla N° 2, se debe aplicar los cambios a ISA SERVER, seleccionar la opción de aplicar.



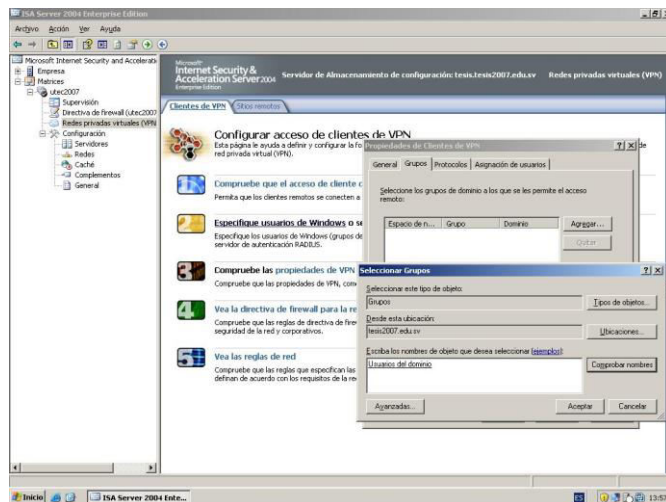
Pantalla N° 2

A continuación, debe habilitar el acceso de clientes VPN, busque la opción en el panel principal de tareas de VPN elija la opción 1, **Comprobar que el acceso de clientes VPN este activado**, defina el máximo de clientes VPN en este caso se utilizo 5, seleccione aceptar (Ver pantalla N° 3).



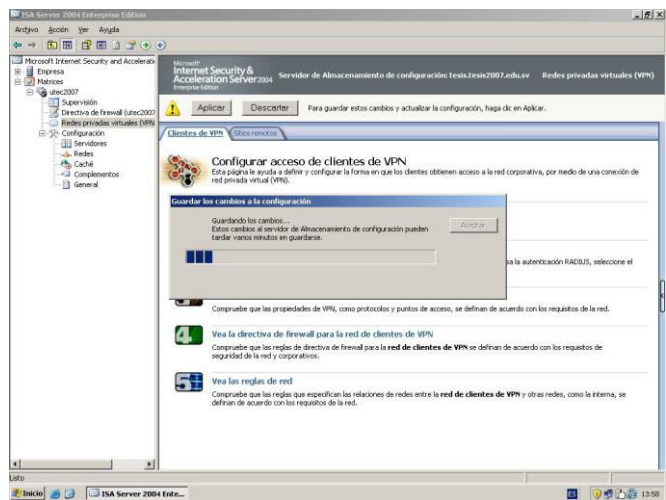
Pantalla N° 3

En la pantalla N° 4, se debe especificar los usuarios, busque la opción en el panel principal de tareas de VPN elija la opción 2, en las propiedades de VPN ubíquela la opción agregar después en la siguiente pantalla agregue el nombre de usuarios del dominio para este caso, seleccione comprobar nombre, por ultimo aceptar.



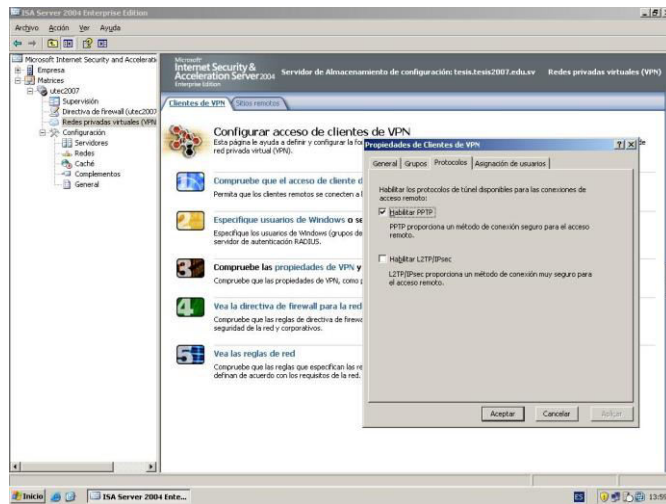
Pantalla N° 4

En la pantalla N° 5, seleccione el botón aceptar para realizar los cambios.



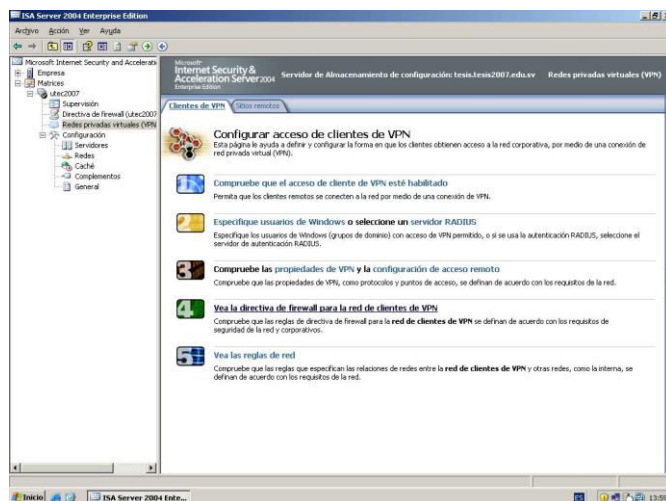
Pantalla N° 5

En la pantalla N° 6, se debe comprobar las propiedades VPN para ello habilite los protocolos, seleccione PPTP, luego aceptar



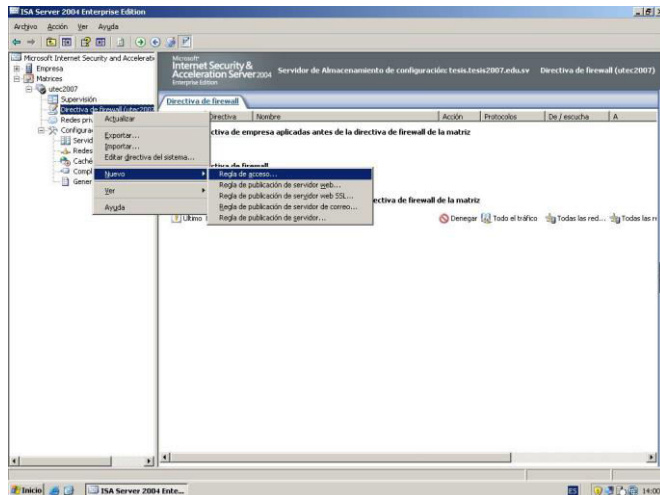
Pantalla N° 6

En el siguiente paso, debe crear una nueva directiva de acceso para habilitar los clientes VPN, seleccione la opción 4, vea la directiva de firewall (ver pantalla N° 7).



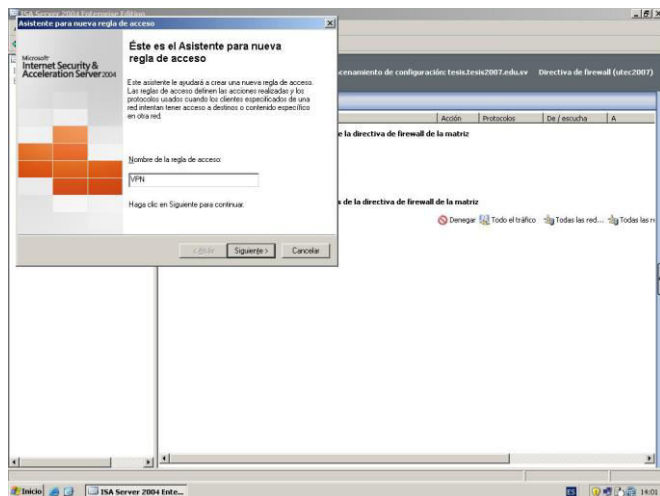
Pantalla N° 7

En la consola de administración de ISA SERVER, debe buscar la opción de políticas de firewall hacer click derecho sobre dicha opción, seleccionar nuevo, y a continuación regla de acceso (ver pantalla N° 8).



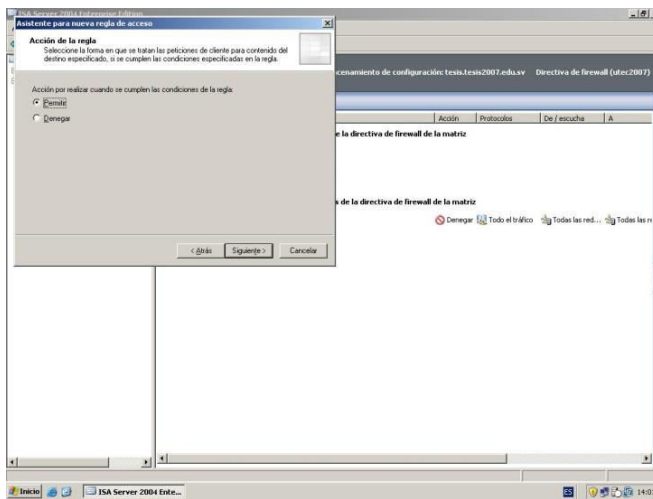
Pantalla N° 8

En la pantalla N° 9 se abrirá el asistente para la creación de la nueva regla de acceso, en donde debemos agregar un nombre a la regla, en este caso se le llamo VPN, seleccionamos siguiente.



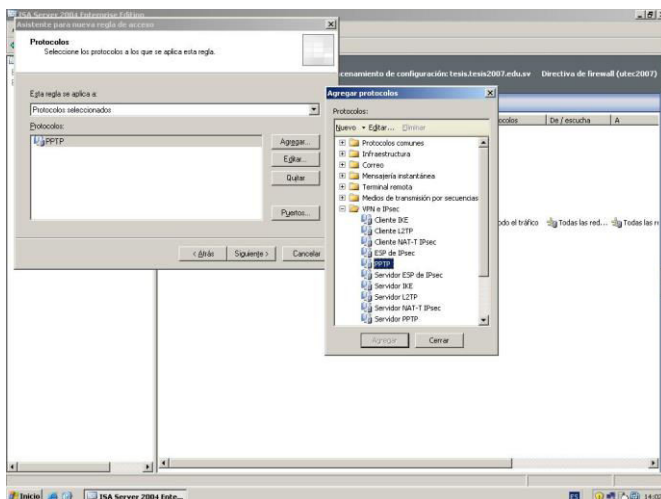
Pantalla N° 9

En la pantalla N° 10, se debe determinar la acción de la regla, seleccione **permitir**, luego seleccionar el botón siguiente.



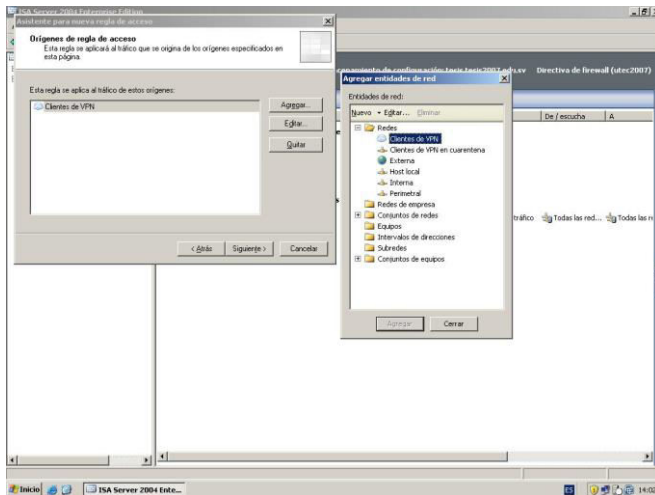
Pantalla N° 10

En la pantalla N° 11, debe especificar los protocolos a los que se aplica la regla, ubique la opción de protocolos seleccionados, luego la opción de agregar buscar en VPN busque PPTP, opción agregar, luego cerrar, y por ultimo seleccione el botón siguiente.



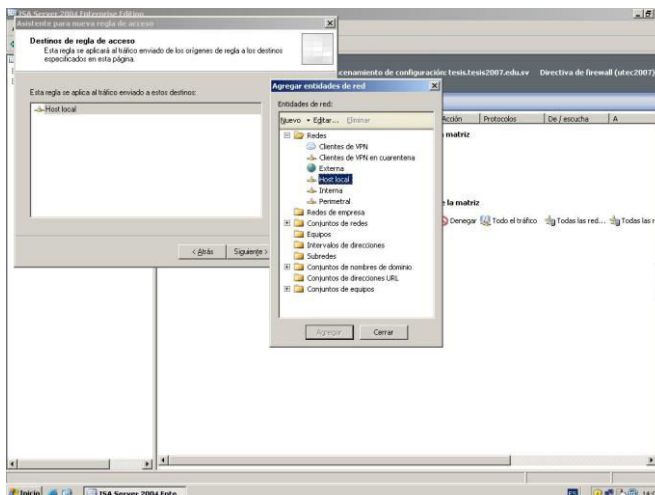
Pantalla N° 11

En la pantalla N° 12, debe especificar los orígenes de la regla de acceso, seleccione la opción de agregar, luego en entidades de red, ubicar Clientes VPN y agregar, luego cerrar, por ultimo seleccione siguiente.



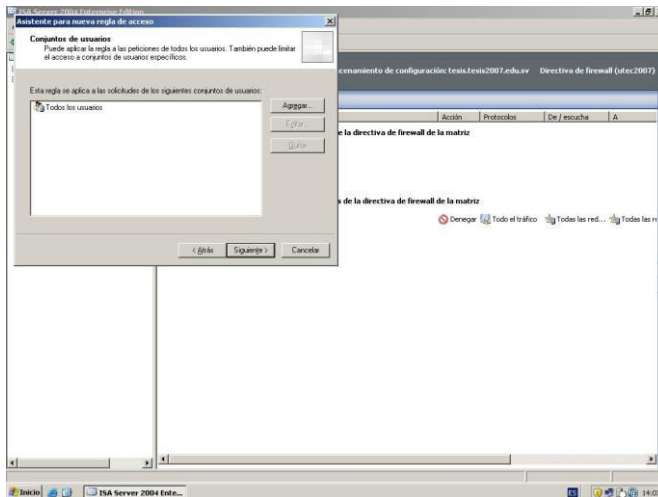
Pantalla N° 12

A continuación, se debe especificar los destinos de la regla de acceso, seleccione la opción de agregar, luego en entidades de red ubicar host local debido a que en este caso se está ejecutando active directory en el mismo equipo de ISA y agregar, luego cerrar, por ultimo seleccione siguiente (ver pantalla N° 13).



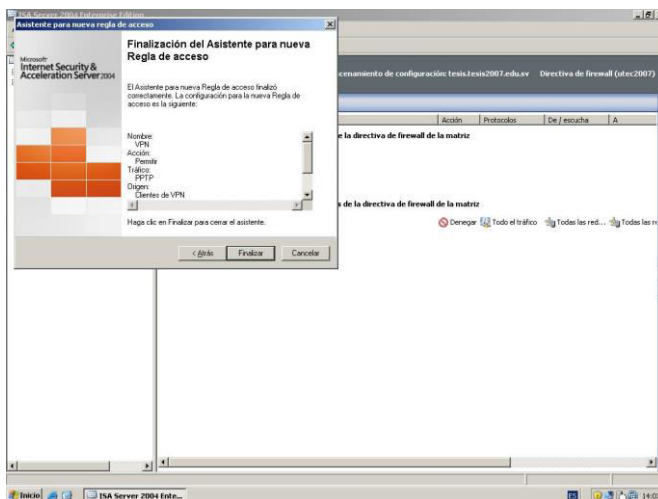
Pantalla N° 13

En la pantalla N° 14, se debe especificar el conjunto de usuarios a los que se aplicara la regla, seleccione, y a continuación agregue todos los usuarios, luego elija el botón siguiente.



Pantalla N° 14

A continuación, finaliza el asistente para la creación de la nueva regla de acceso, revise la información, seleccione el botón finalizar (ver pantalla N° 15).



Pantalla N° 15

3.8 CD INTERACTIVO COMO APOYO A LAS PRÁCTICAS DEL SOFTWARE MICROSOFT ISA SERVER 2004

Dentro de esta guía didáctica para la instalación y configuración de la tecnología Microsoft ISA SERVER 2004, se incluye un CD interactivo El cual sirve de ayuda al estudiante ya que muestra en video como se configuran las prácticas de los roles más importantes de dicho software orientado a la seguridad de las redes.

DESCRIPCIÓN

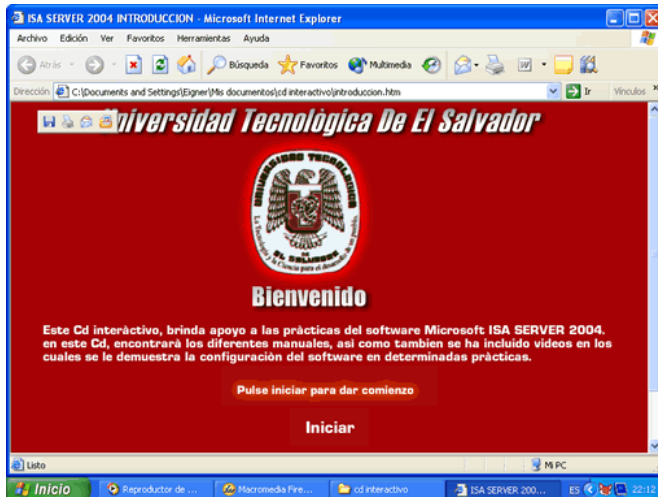
A continuación se menciona la forma de cómo funciona este CD y lo que observara el estudiante.

primero debe tener en cuenta, que el CD posee un auto ejecutable, por lo tanto automáticamente se cargará una pantalla al introducirlo a su unidad de lectura CD-ROM, posteriormente deberá elegir la opción de ver manuales, tal como se muestra en la pantalla N° 1.



Pantalla N° 1

Luego de haber seleccionado la opción ver manuales en la pantalla anterior, se le da la bienvenida al estudiante, para continuar se debe hacer clic sobre la palabra iniciar, ver pantalla N° 2:



Pantalla N° 2

3-En la pantalla N° 3, se deberá instalar un archivo, el cual servirá para poder visualizar los videos de las prácticas, se han colocado a disposición dos archivos, un archivo es para el navegador Internet Explorer y el otro archivo es para los usuarios que utilizan el navegador mozilla, es de tomar en cuenta que estos dos navegadores son los más utilizados en el ambiente informático actual.



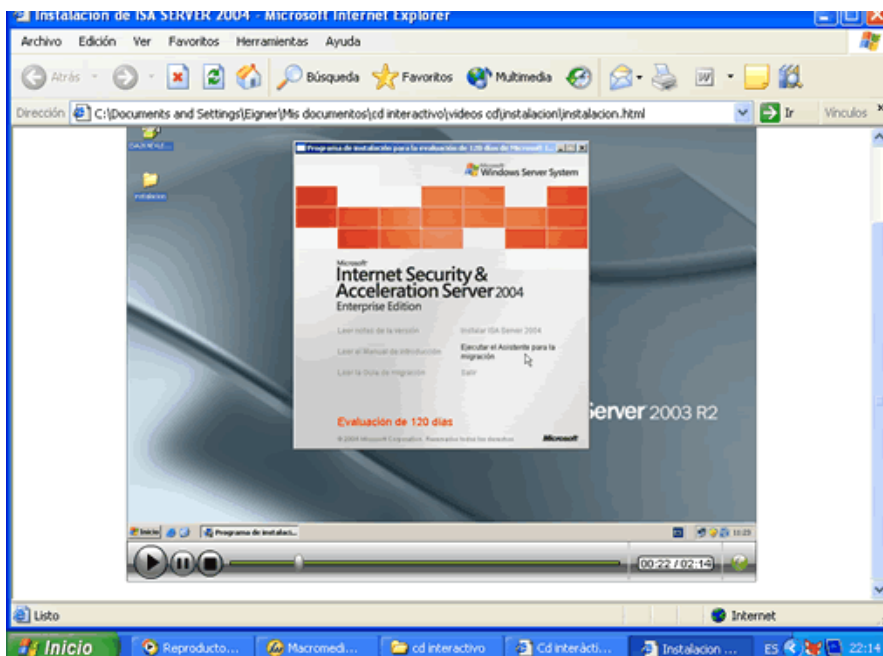
Pantalla N° 3

Una vez ya instalados los archivos correspondientes al navegador que el estudiante utiliza, podrá observar esta pantalla, a su lado izquierdo se observa un menú el cual le brinda la opción al estudiante que elija la practica que desee visualizar, al mismo tiempo encontrará la opción de ver manuales ya sea en el mismo CD o también puede imprimirlo ya que esta disponible en formato de Word solo haciendo un clic en ver manual, tal como se muestra en la pantalla N° 4



Pantalla N° 4

Al hacer clic sobre ver video, se muestra la siguiente pantalla que es el video de la configuración de una de las 7 prácticas disponibles en este CD interactivo, al final de este documento se anexa un CD interactivo el cual contiene toda esta información, la pantalla N° 5, muestra el desarrollo de una práctica en video.



Pantalla N° 5

4.0 CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

Actualmente no existe material educativo para capacitar a los estudiantes de la Carrera de Técnico en Ingeniería de Redes Computacionales de la Universidad Tecnológica de El Salvador, en el ambiente de seguridad informática, utilizando software para tal propósito, es por ello que se presenta, entre la comunidad educativa un manual para la instalación y configuración de ISA Server 2004 además como apoyo visual un CD interactivo que posee material didáctico que permitirá entregar información actualizada a los estudiantes que tengan acceso al este material. Microsoft ISA Server es uno de los software que ofrece mayor protección a nivel de firewall en el mercado local. Es decir ISA Server ofrece protección para inspeccionar y filtrar todo el tráfico que pasa de Internet a la red de área local.

Este material puede utilizarse en materias que se imparten en la escuela de informática tales como: sistemas Operativos de Red, Administración de Redes y cualquier otra materia que se pueda incluir o este contemplado en el contenido temático de dicha materia la seguridad en redes.

El grupo de investigación esta seguro que el material didáctico entregado ayudará en gran medida a la especialización sobre seguridad en redes, permitiendo a los estudiantes el uso de la tecnología de seguridad en redes informáticas.

4.2 RECOMENDACIONES

El grupo de investigación cree conveniente realizar las siguientes recomendaciones.

1. Dar continuidad al proyecto creando un CD interactivo que permita simular en tiempo real todas las opciones que posee el software ISA Server 2004.
2. Incluir en la curricula el uso del CD interactivo en el laboratorio de redes.
3. Permitir un proceso de mejora continua generando una opinión sobre el uso de un CD interactivo a través de encuesta de opinión a los usuarios del mismo.
4. Se recomienda crear otro CD interactivo para la nueva versión de ISA Server 2006.
5. Una vez realizada las observaciones por parte de los usuarios poder publicar en la Pág. Web de la Universidad Tecnológica de El salvador, una opción educativa para educaron a distancia.
6. Con lo anterior se recomienda estandarizar plantillas para que cualquier modulo de la curricula de la carrera pueda desarrollarse y publicarse en la Pág. Web de la institución.
7. Con todo lo anterior es posible la utilización de Internet como una herramienta al proceso de enseñanza aprendizaje de la carrera Técnico en Ingeniería de Redes Computacionales de la Universidad tecnológica de El Salvador y ser parte del proceso denominado E-Learning.

4.3 BILIOGRAFIA

Sitios Web, enlaces de referencia en línea.

Microsoft, ISA Server, descripción general, fecha de actualización 11 de julio de 2007.

<<http://www.microsoft.com/spain/isaserver/default.msp>> [Consulta: 30 Marzo 07]

Microsoft, ISA Server, Requerimientos del sistema para ISA Server 2004, fecha de actualización 18 de enero de 2006.

<<http://www.microsoft.com/latam/windowsserversystem/isaserver/info/sysreq.aspx>> [Consulta: 30 Marzo 07]

Microsoft, ISA Server, Requerimientos del sistema para ISA Server 2006, fecha de actualización 08 de Agosto de 2006.

<<http://www.microsoft.com/latam/windowsserversystem/isaserver/2006/sap.msp>> [Consulta: 02 Abril 07]

Microsoft, ISA Server, Soporte para ISA Server, fecha de actualización 20 de Junio de 2006.

<<http://www.microsoft.com/latam/windowsserversystem/isaserver/isupport/default.msp>> [Consulta: 05 Abril 07]

Microsoft, ISA Server, hoja de datos, fecha de actualización 18 de enero de 2006.

<<http://www.microsoft.com/latam/windowsserversystem/isaserver/info/datasheet.msp>> [Consulta: 10 Abril 07]

Microsoft, ISA Server, whitepapers, fecha de actualización 07 de Febrero de 2006.

<<http://www.microsoft.com/latam/windowsserversystem/isaserver/whitepapers/default.msp>> [Consulta: 23 Abril 07]

Microsoft, ISA Server, documentación del producto, fecha de actualización 03 de Enero de 2006.

<<http://www.microsoft.com/latam/windowsserversystem/isaserver/techres/documentacion.aspx>> [Consulta: 23 Abril 07]

Microsoft, ISA Server, documentación del producto, fecha de actualización 03 de Enero de 2006.

<<http://www.microsoft.com/latam/windowsserversystem/isaserver/techres/articulos.aspx>> [Consulta: 08 Marzo 07]

ANEXOS



Universidad Tecnológica de El Salvador
Facultad de informática y ciencias aplicadas

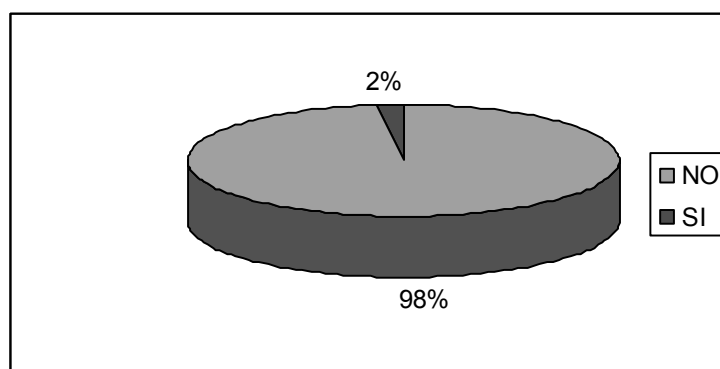
Cuestionario (basado en una encuesta hecha a 50 estudiantes)

Objetivo: el presente instrumento, tiene como finalidad recopilar información en campo, para conocer el estado actual del funcionamiento del laboratorio de redes, los servicios que brinda a los estudiantes y conocer si el laboratorio de redes permite ser utilizado como herramienta pedagógica en el uso del software Microsoft ISA Server 2004.

1-¿En lo que va de su carrera de técnico en ingeniería de redes computacionales, ha recibido orientación didáctica acerca del software Microsoft ISA Server 2004?

Número de estudiantes que dijeron que si: 1

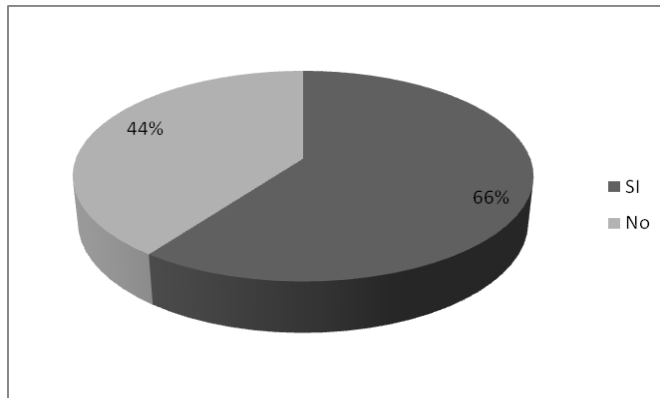
Número de estudiantes que dijeron que no: 49



2-¿Conoce algún tipo de software destinado a la seguridad de las redes informáticas?

Número de estudiantes que dijeron que si: 33

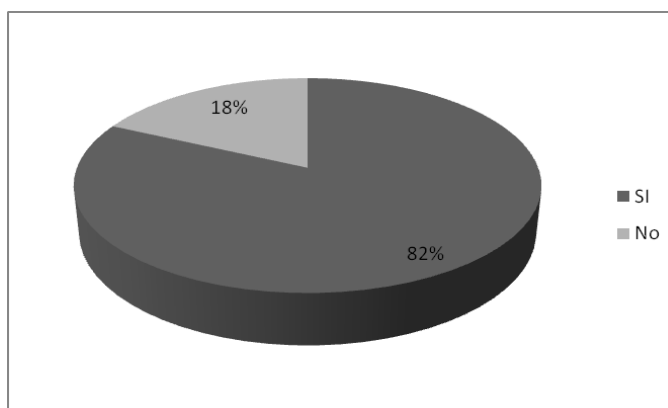
Número de estudiantes que dijeron que no: 17



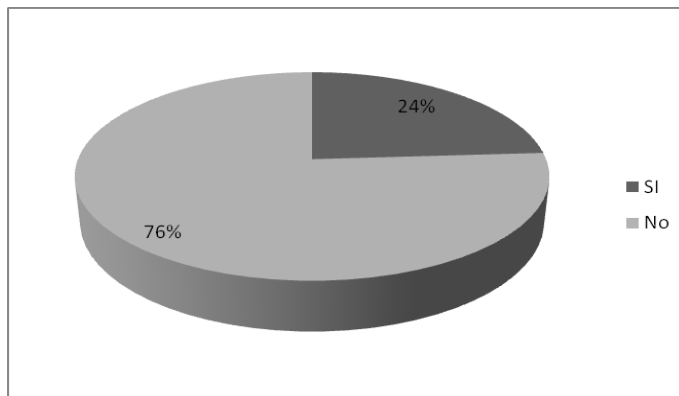
3-¿Le gustaría recibir capacitación didáctica del software Microsoft ISA Server 2004?

Número de estudiantes que dijeron que si: 41

Número de estudiantes que dijeron que no: 9



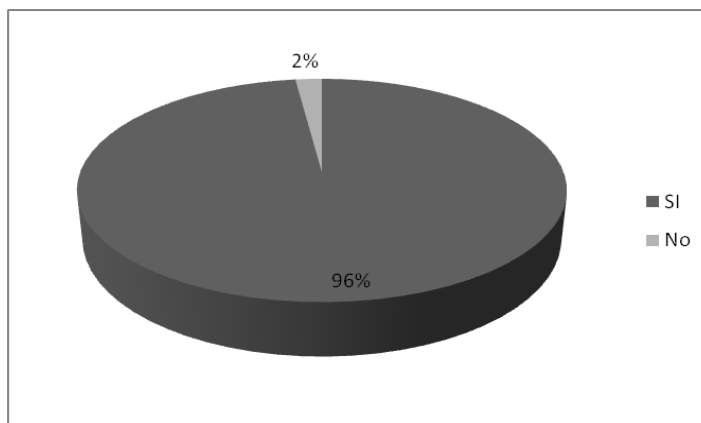
4-¿Conoce usted si el laboratorio de redes de la universidad tecnológica cuenta con el material didáctico para realizar un estudio teórico-practico del software Microsoft ISA Server 2004?



5-¿Considera usted necesario la creación de un material didáctico para el aprendizaje teórico practico de un software de seguridad para redes informáticas?

Número de personas que dijeron que si: 48

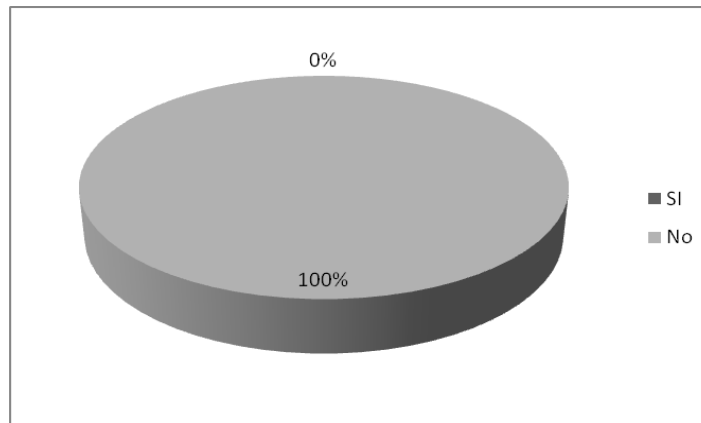
Número de personas que dijeron que no: 2



6-¿ha desarrollado usted prácticas en el laboratorio de redes acerca del software Microsoft ISA Server 2004?

Número de personas que dijeron que si: 0

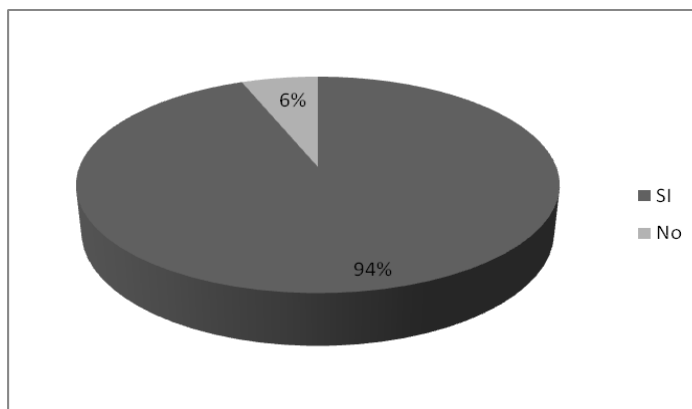
Número de personas que dijeron que no: 50



7-¿Considera usted necesario que deba existir seguridad en las redes informáticas?

Número de personas que dijeron que si: 47

Número de personas que dijeron que no: 3



8-¿Usted ha recibido material didáctico para trabajar en la instalación y configuración de software en el laboratorio de redes?

Número de personas que dijeron que si: 26

Número de personas que dijeron que no: 24

