Deploying Avaya IP Office™ Platform SSL VPN Services

Issue 7
April 2023

Aviso

Si bien se hicieron esfuerzos razonables para asegurar que la información contenida en este documento esté completa y sea exacta en el momento de su impresión, Avaya no se responsabiliza por los errores. Avaya se reserva el derecho de realizar cambios y correcciones a la información contenida en este documento sin la obligación de notificar a ninguna persona u organización dichos cambios.

Exención de responsabilidad con respecto a la documentación

“Documentación” hace referencia a la información publicada en diversos medios, que puede incluir información del producto, instrucciones operativas y especificaciones de rendimiento, que se suelen poner a disposición de los usuarios de productos. La documentación no incluye material publicitario. Avaya no asume la responsabilidad por las modificaciones, adiciones o eliminaciones efectuadas en la versión original publicada de la Documentación, a menos que dichas modificaciones, adiciones o eliminaciones hayan sido realizadas por Avaya o expresamente a nombre de Avaya. El usuario final acuerda indemnizar y eximir de toda responsabilidad a Avaya, agentes de Avaya y empleados con respecto a todo reclamo, acción judicial, demanda y juicio que surgiere de o en relación con modificaciones, incorporaciones o eliminaciones posteriores en esta documentación realizadas por el usuario final.

Exención de responsabilidad con respecto a los vínculos

Avaya no asume la responsabilidad del contenido ni la fiabilidad de los enlaces a los sitios web incluidos en cualquier punto de este sitio o en la Documentación proporcionada por Avaya. Avaya no es responsable de la confiabilidad de ninguna información, instrucción ni contenido proporcionado en estos sitios y no necesariamente aprueba los productos, los servicios o la información descritos u ofrecidos por los mismos. Avaya no garantiza que estos vínculos funcionarán todo el tiempo ni tiene control de la disponibilidad de las páginas vinculadas.

Garantía

Avaya ofrece una garantía limitada para sus productos de hardware y software. Consulte su contrato de compraventa para establecer las condiciones de la garantía limitada. Además, el idioma de la garantía estándar de Avaya, así como la información relacionada con el soporte técnico para este producto durante el período de vigencia de la garantía, está disponible, tanto para los clientes como para otras personas interesadas, en el sitio web del soporte técnico de Avaya: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 o en el enlace “Warranty & Product Lifecycle” (Garantía y ciclo de vida del producto) o en el sitio web posterior designado por Avaya. Tenga en cuenta que si ha adquirido los productos de un Channel Partner de Avaya fuera de Estados Unidos y Canadá, la garantía es proporcionada por dicho Channel Partner y no por Avaya.

“**Servicio alojado**” significa una suscripción de servicio alojado por Avaya que Usted adquiere ya sea de Avaya o de un Channel Partner de Avaya (según corresponda) y que se describe detalladamente en SAS alojado u otra documentación de descripción del servicio sobre el servicio alojado correspondiente. Si compra una suscripción de servicio alojado, la garantía limitada anterior podría no ser aplicable, pero puede tener derecho a servicios de soporte técnico relacionados con el servicio alojado como se describe más adelante en los documentos de descripción del servicio para el servicio alojado correspondiente. Comuníquese con Avaya o el Channel Partner de Avaya (según corresponda) para obtener más información.

Servicio alojado

SE APLICA LO SIGUIENTE ÚNICAMENTE SI ADQUIERE UNA SUSCRIPCIÓN DE AVAYA A UN SERVICIO HOSPEDADO DE AVAYA O UN CHANNEL PARTNER DE AVAYA (SI CORRESPONDE), LOS TÉRMINOS DE USO PARA LOS SERVICIOS HOSPEDADOS ESTÁN DISPONIBLES EN EL SITIO WEB DE AVAYA HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO EN EL ENLACE “Avaya Terms of Use for Hosted Services” O EN LOS SITIOS FUTUROS QUE DESIGNE AVAYA, Y SE APLICAN A TODA PERSONA QUE TENGA ACCESO O USE EL SERVICIO HOSPEDADO. AL ACCEDER O USAR EL SERVICIO HOSPEDADO, O AL AUTORIZAR A TERCEROS A HACERLO, EN NOMBRE SUYO Y DE LA ENTIDAD PARA LA QUE ACCEDE O USA EL SERVICIO HOSPEDADO (EN ADELANTE, A LOS QUE SE HACE REFERENCIA INDISTINTAMENTE COMO “USTED” Y “USUARIO FINAL”), ACEPTA LOS TÉRMINOS DE USO. SI ACEPTA LOS TÉRMINOS DE USO EN NOMBRE DE UNA COMPAÑÍA U OTRA ENTIDAD LEGAL, USTED DECLARA QUE TIENE LA AUTORIDAD PARA VINCULAR A DICHA ENTIDAD CON LOS PRESENTES TÉRMINOS DE USO. SI NO CUENTA CON DICHA AUTORIDAD O SI NO ESTÁ DE ACUERDO CON LOS PRESENTES TÉRMINOS DE USO, NO DEBE ACCEDER NI USAR EL SERVICIO HOSPEDADO NI AUTORIZAR A TERCEROS A QUE ACCEDAN O USEN EL SERVICIO HOSPEDADO.

Licencias

LOS TÉRMINOS DE LICENCIA DE SOFTWARE DISPONIBLES EN EL SITIO WEB DE AVAYA, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, EN EL ENLACE “TÉRMINOS DE LICENCIA DE SOFTWARE DE AVAYA (Productos de Avaya)” O EN EL SITIO WEB POSTERIOR DESIGNADO POR AVAYA, SE APLICAN A CUALQUIER PERSONA QUE DESCARGUE, USE O INSTALE SOFTWARE DE AVAYA, ADQUIRIDO DE AVAYA INC., CUALQUIER SUBSIDIARIA DE AVAYA O UN CHANNEL PARTNER DE AVAYA (SEGÚN CORRESPONDA) BAJO UN ACUERDO COMERCIAL CON AVAYA O CON UN CHANNEL PARTNER DE AVAYA. A MENOS QUE AVAYA ACUERDE LO CONTRARIO POR ESCRITO, AVAYA NO OTORGA ESTA LICENCIA SI EL SOFTWARE FUE OBTENIDO DE ALGUIEN DISTINTO A AVAYA, UNA SUBSIDIARIA DE AVAYA O UN CHANNEL PARTNER DE AVAYA, RESERVÁNDOSE AVAYA EL DERECHO A EJERCER ACCIONES LEGALES EN SU CONTRA O EN CONTRA DE TERCEROS QUE USEN O VENDAN EL SOFTWARE SIN UNA LICENCIA. AL INSTALAR, DESCARGAR O UTILIZAR EL SOFTWARE, O AL AUTORIZAR A TERCEROS A HACERLO, USTED, EN NOMBRE DE SÍ MISMO Y DE LA ENTIDAD PARA LA QUE ESTÁ INSTALANDO, DESCARGANDO O UTILIZANDO EL SOFTWARE (DE AQUÍ EN MÁS DENOMINADOS DE FORMA INTERCAMBIABLE “USTED” Y “USUARIO FINAL”), ACEPTAN ESTOS TÉRMINOS Y CONDICIONES, Y CREAN UN CONTRATO VINCULANTE ENTRE USTED Y AVAYA INC. O LA SUBSIDIARIA DE AVAYA QUE CORRESPONDA (“AVAYA”).

Avaya le otorga una licencia dentro del alcance de los tipos de licencia que se describen a continuación, con la excepción de Heritage Nortel Software, para el que se detalla el alcance de la licencia a continuación. Siempre que la documentación de la orden no identifique expresamente un tipo de licencia, la licencia aplicable será una Licencia de sistema designado según se establece a continuación en la sección de Licencia de sistema designado (DS), según corresponda. La cantidad correspondiente de licencias y unidades de capacidad para la que se otorga la licencia será uno (1), a menos que una cantidad diferente de licencias o unidades de capacidad se especifique en la documentación u otros materiales disponibles para usted. “Software” significa programas de computadora en código objeto proporcionado por Avaya o un Channel Partner de Avaya, ya sea como productos independientes o preinstalados en productos de hardware, y cualquier mejora, actualización, revisión, corrección de falla o versiones modificadas del mismo. “Procesador designado” significa un dispositivo informático independiente único. “Servidor” significa un conjunto de Procesadores designados que aloja (ya sea física o virtualmente) una aplicación de software a la que pueden acceder varios usuarios. “Instancia” significa una única copia del software que se ejecuta en un momento determinado: (i) en una máquina física, o (ii) en un software instalado en una máquina virtual (“VM”) o una implementación similar.

Tipos de licencia

Licencia de sistemas designados (DS). El usuario final puede instalar y utilizar cada copia o una instancia del software únicamente: 1) en una cantidad de procesadores designados hasta el número que indica la orden; o 2) hasta la cantidad de instancias del software que indica la orden, la documentación o según lo autorice Avaya por escrito. Avaya puede exigir que el procesador designado sea indicado en la orden por tipo, número de serie, tecla de función, instancia, ubicación u otra designación específica, o que el usuario final proporcione a Avaya a través de medios electrónicos establecidos por Avaya específicamente para este propósito.

Licencia de usuarios simultáneos (CU). El usuario final puede instalar y usar el Software en varios procesadores designados o en uno o más servidores, siempre y cuando sólo el número de unidades con licencia obtenga acceso y use el Software en cualquier momento dado, según se indica en la orden, la documentación o según lo autorice Avaya por escrito. Una “unidad” se refiere a la unidad en la que Avaya, a su exclusivo criterio, fundamenta el precio de sus licencias y puede ser incluso, entre otros, un agente, puerto o usuario, una cuenta de correo electrónico o de correo de voz en nombre de una persona o función corporativa (por ejemplo, administrador web o centro de asistencia técnica) o una entrada de directorio en la base de datos administrativa utilizada por el software que permite que un usuario se conecte con el software. Las unidades pueden vincularse con un servidor específico identificado o una instancia del software.

Licencia de clúster (CL). El usuario final puede instalar y usar cada copia o una instancia del software solo hasta alcanzar la cantidad de clústeres que se indica en la orden, la documentación, o según lo autorice Avaya por escrito con una cantidad predeterminada de un [1] clúster, si no se indica.

Licencia empresarial (EN). El usuario final puede instalar y utilizar cada copia de una instancia del software solo para el uso de toda la empresa de una cantidad ilimitada de instancias del software según se indica en la orden, la documentación o según lo autorice Avaya por escrito.

Licencia del usuario identificado (NU). El usuario final puede: (i) instalar y utilizar cada copia o instancia del software en un solo procesador designado o servidor por usuario identificado autorizado (se define a continuación); o (ii) instalar y utilizar cada copia o instancia del software en un servidor siempre y cuando únicamente los usuarios identificados autorizados obtengan acceso y utilicen el software según se indica en la orden, la documentación, o según lo autorice Avaya por escrito. “Usuario identificado” se refiere a un usuario o dispositivo que ha sido expresamente autorizado por Avaya para tener acceso al software y utilizarlo. A entera discreción de Avaya, un “usuario identificado” puede ser incluso, entre otros, designado por nombre, función corporativa (por ejemplo, administrador web o centro de asistencia técnica), una cuenta de correo electrónico o de correo de voz a nombre de una persona o función corporativa, o una entrada de directorio en la base de datos administrativa utilizada por el software que permite que un usuario se conecte con el software.

Licencia Shrinkwrap (SR). El usuario final puede instalar y utilizar el software de acuerdo con los términos y las condiciones de los contratos de licencia vigentes, como las licencias “shrinkwrap” o “clickthrough” que acompañan o se aplican al software (“licencia shrinkwrap”) según se indica en la orden, la documentación, o según lo autorice Avaya por escrito.

Licencia de transacción (TR). El usuario final puede utilizar el software hasta la cantidad de transacciones que se especifica durante el período de tiempo especificado y según se indica en la orden, la documentación, o según lo autorice Avaya por escrito. Una “Transacción” significa la unidad a partir de la cual Avaya, a su solo criterio, basa la fijación de precio de su licenciamiento y puede ser, sin limitación, medida por el uso, acceso, interacción (entre el cliente/servidor o cliente/organización), u operación del Software dentro de un período de tiempo especificado (por ejemplo, por hora, por día, por mes). Algunos ejemplos de transacciones incluyen, a mero título enunciativo, cada saludo reproducido/mensaje en espera habilitado, cada promoción personalizada (en cualquier canal), cada operación de devolución de llamada, cada agente en vivo o sesión de chat en web, cada llamada enrutada o redirigida (en cualquier canal). El usuario final no puede exceder la cantidad de Transacciones sin el consentimiento previo de Avaya y el pago de una tasa adicional.

Heritage Nortel Software

“Heritage Nortel Software” significa el software que adquirió Avaya como parte de la compra de Nortel Enterprise Solutions Business en diciembre de 2009. El Heritage Nortel Software es el software contenido en la lista de productos Heritage Nortel Products ubicada en https://support.avaya.com/LicenseInfo en el enlace “Heritage Nortel Products” o el sitio web posterior designado por Avaya. Para el software Nortel heredado, Avaya otorga al cliente una licencia para utilizar el software Nortel heredado en virtud del presente documento únicamente en la medida de la activación autorizada o el nivel de uso autorizado, únicamente para el propósito especificado en la documentación y solamente como se incorpora, ejecuta o para comunicación con equipo Avaya. Los cargos por Heritage Nortel Software se podrían basar en el alcance de activación o el uso autorizado según se especifique en una orden o factura.

Copyright

Excepto donde se indique expresamente lo contrario, no se debe hacer uso de los materiales de este sitio, de la documentación, del software, del servicio alojado ni del hardware proporcionados por Avaya. Todo el contenido de este sitio, la documentación, el servicio alojado y los productos proporcionados por Avaya, incluida la selección, la disposición y el diseño del contenido, son de propiedad de Avaya o de sus licenciantes y están protegidos por leyes de derecho de autor y otras leyes de propiedad intelectual, incluidos los derechos de su género relacionados con la protección de las bases de datos. No debe modificar, copiar, reproducir, reeditar, cargar, publicar, transmitir ni distribuir de ninguna manera el contenido, en su totalidad o en parte, incluidos los códigos y el software, a menos que posea una autorización expresa de Avaya. La reproducción, transmisión, difusión, almacenamiento y/o uso no autorizado sin el consentimiento expreso por escrito de Avaya puede considerarse un delito penal o civil según la ley vigente.

Virtualización

Si el producto se implementa en una máquina virtual, se aplica lo siguiente. Cada producto tiene su propio código de pedido y tipos de licencia. A menos que se indique lo contrario, cada instancia de un producto debe pedirse por separado y tener una licencia independiente. Por ejemplo, si el cliente usuario final o el Channel Partner de Avaya prefieren instalar dos instancias del mismo tipo de producto, entonces se deben solicitar dos productos del mismo tipo.

Componentes de terceros

“Componentes de terceros” se refieren a ciertos programas de software y partes de estos incluidos en dicho software o servicio alojado que pueden contener software (incluido el software de código abierto) distribuido según contratos de terceros (“Componentes de terceros”), que incluyen condiciones sobre los derechos a utilizar ciertas partes del software (“Términos y condiciones de terceros”). Según se requiera, la información con respecto al código fuente de SO Linux distribuido (para aquellos productos que tienen código fuente de SO Linux distribuido) y que identifique a los titulares de derechos de autor de componentes de terceros y los términos y las condiciones de terceros que se aplican está disponible en los productos, la documentación o en el sitio web de Avaya: https://support.avaya.com/Copyright o el sitio web posterior designado por Avaya. Los términos de la licencia de software de código abierto que se proporcionan como Términos de terceros se corresponden con los derechos de licencia otorgados en estos Términos de licencia de software y pueden contener derechos adicionales que lo beneficien, como la modificación y distribución del software de código abierto. Los Términos de terceros tienen prioridad sobre estos Términos de licencia de software, únicamente con respecto a los Componentes de terceros aplicables, en la medida en que estos Términos de la licencia de software impongan mayores restricciones que los Términos de terceros aplicables.

Lo siguiente corresponde solo si el códec H.264 (AVC) se distribuye con el producto. ESTE PRODUCTO ESTÁ SUJETO A LA LICENCIA DE CARTERA DE PATENTES AVC PARA EL USO PERSONAL DE UN CONSUMIDOR Y OTROS USOS QUE NO IMPLIQUEN REMUNERACIÓN PARA (i) CODIFICAR VÍDEO QUE CUMPLA CON EL ESTÁNDAR AVC (“AVC VIDEO”) O (ii) DECODIFICAR VÍDEO AVC QUE UN CLIENTE CODIFICÓ DURANTE UNA ACTIVIDAD PERSONAL U OBTENIDO A TRAVÉS DE UN PROVEEDOR DE VÍDEO AUTORIZADO PARA SUMINISTRAR VÍDEO AVC. NO SE OTORGA LICENCIA NI SE IMPLICA PARA CUALQUIER OTRO USO. PARA OBTENER INFORMACIÓN ADICIONAL, PUEDE CONSULTAR MPEG LA, L.L.C. VISITE HTTP://WWW.MPEGLA.COM.

Proveedor de servicio

LO SIGUIENTE SE APLICA A LOS CHANNEL PARTNERS DE AVAYA QUE ALOJEN PRODUCTOS O SERVICIOS DE AVAYA. EL PRODUCTO O SERVICIO ALOJADO PUEDE USAR COMPONENTES DE TERCEROS SUJETOS A LOS TÉRMINOS DE TERCEROS Y REQUERIR QUE EL PROVEEDOR DE SERVICIOS TENGA UNA LICENCIA INDEPENDIENTE DIRECTA DE ESTOS TERCEROS. UN CHANNEL PARTNER DE AVAYA

QUE ALOJE PRODUCTOS DE AVAYA DEBE CONTAR CON AUTORIZACIÓN ESCRITA DE AVAYA, Y, EN CASO DE QUE DICHOS PRODUCTOS ALOJADOS UTILICEN O INCORPOREN SOFTWARE DE TERCEROS, LO QUE INCLUYE, A TÍTULO ENUNCIATIVO, SOFTWARE O CÓDECS DE MICROSOFT, EL CHANNEL PARTNER DE AVAYA DEBERÁ OBTENER DE FORMA INDEPENDIENTE Y A SU CARGO LOS ACUERDOS DE LICENCIA CORRESPONDIENTES, DIRECTAMENTE DEL PROVEEDOR DE TERCEROS.

CON RESPECTO A LOS CÓDECS, SI EL CHANNEL PARTNER DE AVAYA ALOJA PRODUCTOS QUE UTILIZAN O INCORPORAN LOS CÓDECS H.264 O H.265, EL CHANNEL PARTNER DE AVAYA RECONOCE Y MANIFIESTA ACUERDO CON QUE ES RESPONSABLE DE ASUMIR TODAS LAS TARIFAS Y/O REGALÍAS. EL CÓDEC H.264 (AVC) ESTÁ SUJETO A LA LICENCIA DE CARTERA DE PATENTES AVC PARA EL USO PERSONAL DE UN CONSUMIDOR Y OTROS USOS QUE NO IMPLIQUEN REMUNERACIÓN PARA (I) CODIFICAR VÍDEO QUE CUMPLA CON EL ESTÁNDAR AVC (“AVC VIDEO”) O (II) DECODIFICAR VÍDEO AVC QUE UN CONSUMIDOR CODIFICÓ DURANTE UNA ACTIVIDAD PERSONAL U OBTENIDO A TRAVÉS DE UN PROVEEDOR DE VÍDEO AUTORIZADO PARA SUMINISTRAR VÍDEO AVC. NO SE OTORGA LICENCIA NI SE IMPLICA PARA CUALQUIER OTRO USO. SE PODRÁ OBTENER INFORMACIÓN ADICIONAL SOBRE LOS CÓDECS H.264 (AVC) y H.265 (HEVC) DE MPEG LA, L.L.C. VISITE HTTP://WWW.MPEGLA.COM.

Cumplimiento de leyes

Usted reconoce y acepta que es su responsabilidad respetar las leyes y los reglamentos aplicables, incluidos, a mero título enunciativo, las leyes y los reglamentos relacionados con la grabación de llamadas, la privacidad de datos, la propiedad intelectual, el secreto comercial, el fraude, los derechos de interpretación musical, en el país o territorio en el cual se utiliza el producto de Avaya.

Prevención del fraude telefónico

El “fraude telefónico” se refiere al uso no autorizado de su sistema de telecomunicaciones por parte de un participante sin autorización (por ejemplo, una persona que no es un empleado, agente ni subcontratista corporativo o una persona que no trabaja en nombre de su compañía). Tenga en cuenta que pueden existir riesgos de Fraude telefónico asociados con su sistema y que, en tal caso, esto puede generar cargos adicionales considerables para sus servicios de telecomunicaciones.

Intervención en fraude telefónico de Avaya

Si sospecha que es víctima de fraude telefónico y necesita asistencia o soporte técnico, llame a la línea directa de Intervención en Fraude Telefónico del Centro de servicio técnico al +1-800-643-2353 para Estados Unidos y Canadá. Para obtener números de teléfono de soporte técnico adicionales, visite el sitio web de soporte técnico de Avaya: https://support.avaya.com o el sitio web posterior designado por Avaya.

Vulnerabilidades de seguridad

Puede encontrar información sobre las políticas de respaldo de seguridad de Avaya en la sección de Soporte técnico y políticas de seguridad de https://support.avaya.com/security.

Las sospechas de vulnerabilidades de la seguridad de productos de Avaya se manejan a través del Flujo de soporte técnico de seguridad de productos de Avaya (https://support.avaya.com/css/P8/documents/100161515).

Marcas comerciales

Las marcas comerciales, logotipos y marcas de servicio (“Marcas”) que aparecen en este sitio, la documentación, los servicios alojados y los productos proporcionados por Avaya son marcas registradas o no registradas de Avaya, sus afiliados, licenciantes, proveedores y otros terceros. Los usuarios no tienen permiso de usar dichas Marcas sin previo consentimiento por escrito de Avaya o dichos terceros que puedan ser propietarios de la Marca. Ningún contenido de este sitio, la documentación, los servicios alojados ni los productos deben considerarse como otorgamiento, por implicación, impedimento o de alguna otra forma, una licencia o derecho para usar las Marcas sin la autorización expresa por escrito de Avaya o del tercero correspondiente.

Avaya es una marca registrada de Avaya Inc.

Todas las demás marcas son propiedad de sus respectivos dueños.

Linux® es una marca comercial registrada de Linus Torvalds en EE. UU. y en otros países.

Contents

Capítulo 1: Cambios del documento desde la última versión

Se han realizado los siguientes cambios en este documento para IP Office versión 9.1.

Kit de desarrollo de software (SDK)

Para facilitar la configuración de los partners de la VPN SSL, hay dos SDK disponibles. Estos se describen en Configuración de una VPN SSL desde el SDK en la página 50.

Asistente de configuración rápida de AVG

Se actualizó el asistente de configuración rápida de AVG. Consulte el Apéndice A: ejemplo del Asistente de configuración rápida de AVG en la página 90.

Capítulo 2: Acerca del servicio VPN SSL

La solución de acceso remoto VPN SSL IP Office es una manera rápida y sencilla de configurar un acceso remoto seguro a velocidades de banda ancha. La solución está diseñada para proporcionar a Avaya y los socios de Avaya acceso remoto confiable que mejora la entrega de servicios mientras reduce el costo asociado a la entrega de servicios en el sitio. La solución permite a los socios de cualquier tipo crear una infraestructura que automatiza la gestión y el mantenimiento de los sistemas IP Office.

Servicios proporcionados por VPN SSL

El servicio de VPN SSL ofrece un túnel seguro entre el hardware de Avaya IP Office instalado en el lugar del cliente y Avaya VPN Gateway remoto (AVG). Este túnel seguro permite al personal de soporte técnico ofrecer a los clientes servicios de administración remota, como administración de fallas, control y administración. Permite que los administradores:

- reenvíen tráfico a través del servicio VPN SSL utilizando rutas de tunelización divididas y rutas estáticas
- controlen de manera remota IP Office a través del servicio VPN SSL en un servidor AVG utilizando System Status Application (SSA) o SysMonitor
- administren de manera remota los sistemas IP Office utilizando Avaya IP Office Manager o IP Office Manager for Server Edition
- reciban capturas de SNMP, entradas de registro del sistema y alarmas de correo electrónico SMTP de IP Office en un servicio VPN SSL conectado a un servidor AVG
- activen y desactiven el túnel con Manager o IP Office Manager for Server Edition
- activen y desactiven el túnel con códigos cortos, atención automática o administración basada en el conjunto
- ejecuten varias instancias del servicio VPN SSL simultáneamente

Vínculos relacionados

Opciones de implementación en la página 10
Modos de operación en la página 10
Arquitectura de sistema en la página 13
Requisitos y limitaciones del sistema en la página 16
Documentación relacionada en la página 16

Opciones de implementación

Servicios de soporte técnico remoto de Avaya

La solución VPN SSL es un elemento integral de Servicios de soporte técnico de IP Office (IPOSS), que permiten a Avaya proporcionar solución de problemas y soporte técnico líderes de la industria. El establecimiento de la conexión de VPN SSL con Avaya está ampliamente simplificado por la capacidad de integración automatizada. El proceso de integración incluye extracción de inventario, registro en GRT para crear el registro de base instalado y registro técnico para la conectividad remota con Avaya.

Para conocer detalles adicionales sobre la oferta de mantenimiento de IPOSS, vaya a la página Servicios de soporte técnico de IP Office en el Portal de ventas de Avaya.

Servicios de soporte técnico remoto proporcionados por los partners de Avaya

Además de la oferta de IPOSS, los partners tienen la opción de aprovechar el cliente VPN SSL en combinación con la solución Avaya VPN Gateway (AVG), para crear su propia infraestructura de VPN SSL. Este documento ofrece información y procedimientos para ayudar a los partners de Avaya que desean establecer su propia solución VPN SSL de acceso remoto, como parte de su soporte técnico de mantenimiento para sus clientes.

El partner configurado en la solución VPN SSL es compatible en los sistemas Standard Edition y Server Edition IP Office.

Vínculos relacionados

Acerca del servicio VPN SSL en la página 9

Modos de operación

Modos de operación

El servicio VPN SSL es compatible con el hardware IP500v2. El módulo de control IP500 no es compatible.

El VPN SSL es compatible con IP Office que funciona en los siguientes módulos. No compatible con modo branch

- Edición estándar de IP Office (modos Essential, Advanced y Preferred)
- Server Edition
  - Server Edition principal
  - Server Edition secundario
- Sistema de expansión Server Edition
  - Sistema de expansión Server Edition (V2), un sistema de expansión IP500v2
  - Sistema de expansión Server Edition (L), un sistema de expansión Linux
- Basic Edition

Nota:

Basic Edition solo es compatible en implementaciones utilizando los Servicios de soporte técnico de IP Office de Avaya (IPOSS). Basic Edition no es compatible con un VPN SSL implementado para los servicios de soporte técnico de los partners de Avaya.

Funciones compatibles

La funcionalidad disponible depende del modo de operación que esté usando. Esta sección proporciona una descripción general de la funcionalidad de VPN SSL y muestra una lista de las funciones disponibles en cada modo.

Funciones compatibles	Modo de operación			
	Standard Edition	Server Edition	Sistema de expansión Server Edition	Basic Edition
Conectividad				
Conexión siempre activada de VPN SSL en un servidor AVG	✔	✔	✔	✔
Rutas de tunelización divididas	✔	✔	✔	✔
Rutas estáticas	✔	✔	✔	✔
Instancias múltiples del servicio de VPN SSL ejecutándose simultáneamente	✔	✔	✔	✔
Acceso al dispositivo LAN (NAPT)	✔	✔	✔	—
Administración de fallas				
Generar trampas SNMP	✔	✔	✔	✔
Generar entradas de registro del sistema	✔	✔	✔	—
Generar notificaciones por correo electrónico para las alarmas	✔	✔	✔	—
Generar alarmas de prueba	✔	✔	✔	✔
Control y administración				
Administración remota utilizando Manager o IP Office Manager for Server Edition	✔	✔	✔	✔

Table continues…

Funciones compatibles	Modo de operación			
	Standard Edition	Server Edition	Sistema de expansión Server Edition	Basic Edition
Control remoto utilizando System Status Application	✔	✔	✔	✔
Control remoto utilizando SysMonitor	✔	✔	✔	✔
Activar y desactivar el servicio de VPN SSL a través de códigos cortos	✔	✔	✔	—
Activar y desactivar el servicio VPN SSL a través de menús basados en el conjunto	—	—	—	✔
Activar y desactivar el servicio VPN SSL a través de Manager o IP Office Manager for Server Edition	✔	✔	✔	—
Activar y desactivar el servicio VPN SSL utilizando atención automática	✔	✔	✔	—
Activar y desactivar el servicio VPN SSL utilizando las teclas programables de los teléfonos de escritorio de Avaya	✔	✔	✔	✔
Actualización remota de IP Office para las nuevas versiones	✔	✔	✔	✔

Herramientas de control y administración

Cuando el servicio de VPN SSL está conectado, puede administrar y controlar el sistema IP Office de manera remota a través del túnel.

Puede usar las siguientes herramientas para administrar, actualizar y configurar el sistema IP de manera remota:

- IP Office Manager: una aplicación administrativa que le permite ajustar las configuraciones de sistema para los sistemas IP Office Essential Edition.
  - IP Office Manager for Server Edition: cuando inicia IP Office Manager, puede elegir abrir una configuración utilizando el modo IP Office Manager for Server Edition. Este modo le permite administrar servidores Server Edition y sistemas de expansión.

- IP Office Basic Edition – Web Manager: una herramienta basada en el explorador que le permite ajustar las configuraciones del sistema para IP Office.

Puede usar las siguientes herramientas para controlar el sistema IP Office de manera remota:

- System Status Application (SSA): la System Status Application es una herramienta de diagnóstico que puede usar para controlar el estado de los sistemas IP Office. SSA informa eventos en tiempo real e históricos así como el estado y los datos de configuración.
- SysMonitor: la aplicación SysMonitor muestra la información de operación acerca del sistema IP Office. Puede capturar la información para registrar archivos para análisis.

Vínculos relacionados

Acerca del servicio VPN SSL en la página 9

Arquitectura de sistema

El servicio VPN SSL ofrece tunelización entre el hardware IP Office instalado en el lugar del cliente y un Avaya VPN Gateway (AVG) instalado en el sitio del proveedor de servicio. Use la información de esta sección para entender la arquitectura de red utilizada por el servicio VPN SSL.

Tarjetas de interfaz de red

Avaya recomienda que implemente el servidor AVG en una configuración de dos conexiones con dos tarjetas de interfaces de red (NIC). Una interfaz controla el tráfico privado entre el VPN SSL y la intranet de seguridad. Esta conexión permite al servicio VPN SSL acceder a los recursos internos y le permite configurar y administrar el sistema IP Office desde una estación de administración. La segunda interfaz controla el tráfico hacia y desde internet.

Enrutamiento

En el lugar del proveedor de servicios, puede configurar el enrutamiento corporativo entre el AVG y su red privada. En el mismo lugar del cliente, puede ubicar cada sistema IP Office en el lado privado de un enrutador corporativo. El enrutador corporativo no requiere cambios de configuración para que funcione el servicio VPN SSL.

IP Office reenvía datos al AVG en el servicio VPN SSL utilizando rutas de tunelización divididas o rutas estáticas. Debe usar una de estas opciones para enviar el tráfico a través del túnel VPN SSL:

- permitir que IP Office instale dinámicamente rutas de tunelización divididas cuando el servicio VPN SSL se conecte con AVG, y eliminar estas rutas cuando el servicio se desconecte
- configurar una ruta estática en IP Office Manager

Tunelización dividida:

Cuando instale y configure AVG, puede agregar subredes divididas o direcciones de host para un grupo. El sistema IP Office recibe la información de enrutamiento para el túnel de manera dinámica cuando el servicio VPN SSL se conecta correctamente con el AVG. Las rutas de redes divididas se eliminan cuando el servicio VPN SSL se desconecta de AVG.

Para recibir información sobre cómo configurar la tunelización dividida en el AVG utilizando Net Direct, consulte *Avaya VPN Gateway Administration Guide* (Guía de administración) (NN46120-105) y *Avaya VPN Gateway BBI Application Guide* (Guía de aplicación BBI) (NN46120-102). Para obtener información sobre cómo configurar la tunelización dividida utilizando la interfaz de la línea de comando, consulte *Guía de la aplicación CLI* (NN46120-101).

Rutas estáticas:

Como alternativa a la tunelización dividida, puede configurar una ruta estática directamente en el sistema IP Office. Cuando configura una ruta estática, el sistema usa la información de ruta IP configurada en el Manager para determinar el destino para el tráfico reenviado. Debe definir el servicio VPN SSL como el destino.

Use una ruta estática cuando:

- las rutas de tunelización divididas no son advertidas por el AVG y necesita enviar tráfico a través del túnel
- el servicio VPN SSL no está conectado en el AVG y usted desea poner en cola el tráfico a través del túnel cuando la conexión se restaura; en este caso, IP Office pone temporalmente en cola un pequeño número de paquetes que activan la conexión cuando el VPN SSL está en servicio, pero desconectado

Puede configurar varias rutas estáticas en el sistema IP Office.

Autenticación

Cada sistema IP Office es compatible con varios túneles VPN SSL. A cada instancia de un servicio VPN SSL se le asigna una dirección IP estática privada. Cuando conecta el servicio VPN SSL, AVG autentica el sistema IP Office. Para un pequeño número de sistemas IP Office, puede usar la base de datos local Avaya VPN Gateway (AVG) para crear los datos de usuarios necesarios para la autenticación. Para implementaciones más grandes, se recomienda que use un servidor RADIUS para la autenticación.

Acceso del agente de servicio

Los agentes de servicio ubicados en el sitio del proveedor de servicios pueden conectarse a cualquier sistema IP Office que tenga una conexión VPN SSL en servicio con AVG. Pueden monitorear y administrar el sistema IP Office de manera remota contactándose con la dirección IP del túnel VPN SSL, y pueden acceder a las direcciones IP de varios servicios VPN SSL simultáneamente.

El AVG asegura que los túneles VPN SSL no se puedan comunicar entre sí. No necesita definir configuraciones adicionales para asegurarse de que los túneles se mantengan seguros e independientes.

Administración de fallas

Un servidor de administración de fallas es un componente opcional en el servicio VPN SSL. Implemente un servidor de administración de fallas en el sitio del proveedor de servicios y use el servicio VPN SSL para enviar fallas de sistema a ese servidor. Puede configurar filtros de eventos para determinar qué fallas se informan. Por ejemplo, puede configurar filtros para informar eventos relacionados con la operación del sistema IP Office, y también puede reportar fallas que son específicas de la operación del servicio VPN SSL.

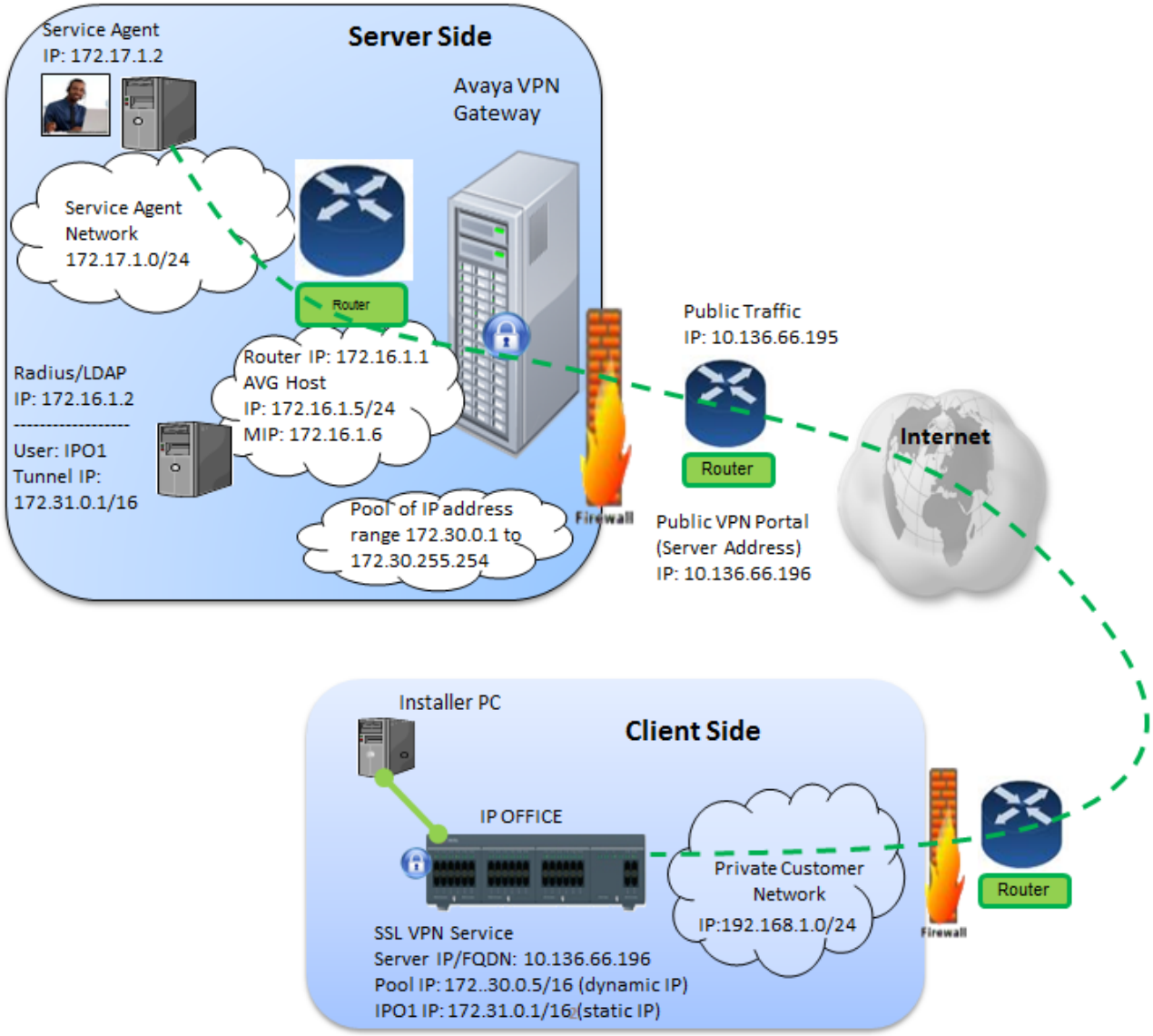
Avaya recomienda configurar el servicio VPN SSL Nombre de cuenta para que coincida con el nombre ID de dispositivo agente SNMP. La ID de dispositivo agente SNMP está configurada en IP Office Manager en el formulario **Sistema**, en **Eventos del sistema**, **Configuración**.

Atravesar el firewall

El servicio VPN SSL funciona de manera transparente por el firewall. No necesita configurar el enrutador corporativo para permitir el servicio VPN SSL si ya lo configuró para el tráfico HTTPS. El servicio VPN SSL usa el mismo puerto de destino para el tráfico TCP.

Ejemplo de arquitectura

El siguiente diagrama muestra un ejemplo de arquitectura utilizada por el servicio VPN SSL.



Vínculos relacionados

Acerca del servicio VPN SSL en la página 9

Requisitos y limitaciones del sistema

Requisitos

Ancho de banda:

Asegurar que el ancho de banda de carga sea al menos de 90 kB/s (720 kb/s) con una latencia no superior a 150 ms (recorrido completo). Esta especificación asegura que Avaya Global Services pueda proporcionar asistencia remota a través del servicio VPN SSL.

Autenticación:

- Para un pequeño número de sistemas IP Office, puede usar la base de datos local Avaya VPN Gateway (AVG) para crear los datos de usuarios necesarios para la autenticación.
- Las grandes implementaciones requieren un servidor RADIUS. Avaya recomienda que use el Servidor de encendido de motores de identidad de Avaya como el servidor RADIUS.
- El sistema IP Office usa certificados digitales para verificar la identidad del AVG al final del túnel VPN SSL. Debe configurar los certificados en AVG, y debe instalar los certificados X.509 necesarios en el almacén de certificados de IP Office.

Licencias:

El Servicio VPN SSL no requiere una clave de licencia.

Limitaciones

Redes pequeñas de la comunidad:

Si implementa los sistemas IP Office en una red Small Community Network (SCN), puede configurar un servicio VPN SSL entre nodos específicos en la SCN y el AVG. No puede usar la conexión VPN SSL para acceder de manera remota a otros nodos en la topología de SCN: el servicio VPN SSL solo se comunica con el sistema IP Office que es su punto final. Debe configurar un servicio VPN SSL para cada nodo en el SCN al que quiere acceder de manera remota.

Certificados:

Puede almacenar un máximo de 25 certificados en el almacén de certificados de seguridad de IP Office.

Versión HTTP:

Si ve un navegador con una versión de HTTP más reciente que 1.1, es posible que no puede conectarse a un dispositivo LAN utilizando NAPT VPN SSL. Si tiene problemas para conectarse a un dispositivo LAN, cambie las configuraciones del navegador para usar la versión 1.1 de HTML.

Vínculos relacionados

Acerca del servicio VPN SSL en la página 9

Documentación relacionada

Para instalar, configurar y administrar la solución VPN SSL, debe consultar la documentación para el sistema IP Office de Avaya, el Avaya VPN Gateway (AVG), y el Servidor de encendido

de motores de identidad de Avaya. Además, debe consultar la documentación proporcionada por otros proveedores para el soporte del hardware y software que se usa en su infraestructura de red.

Tenga la siguiente documentación de Avaya para respaldar la solución VPN SSL.

Avaya VPN Gatewaydocumentación

- *Guía de inicio de Avaya VMware - Avaya VPN Gateway* (NN46120-302)
- *Avaya VPN Gateway Guía del usuario* (NN46120-104)
- *Avaya VPN Gateway Guía de administración* (NN46120-105)
- *Avaya VPN Gateway Guía de aplicación BBI* (NN46120-102)
- *Avaya VPN Gateway Guía de aplicación CLI* (NN46120-101)

Documentación de IP Office de Avaya

- *Avaya IP Office Basic Edition – Web Manager*
- *Avaya Manager IP Office*
- *Administración de Voicemail Pro*
- *Instalación de Embedded Voicemail*

Documentación del Servidor de encendido de motores de identidad de Avaya

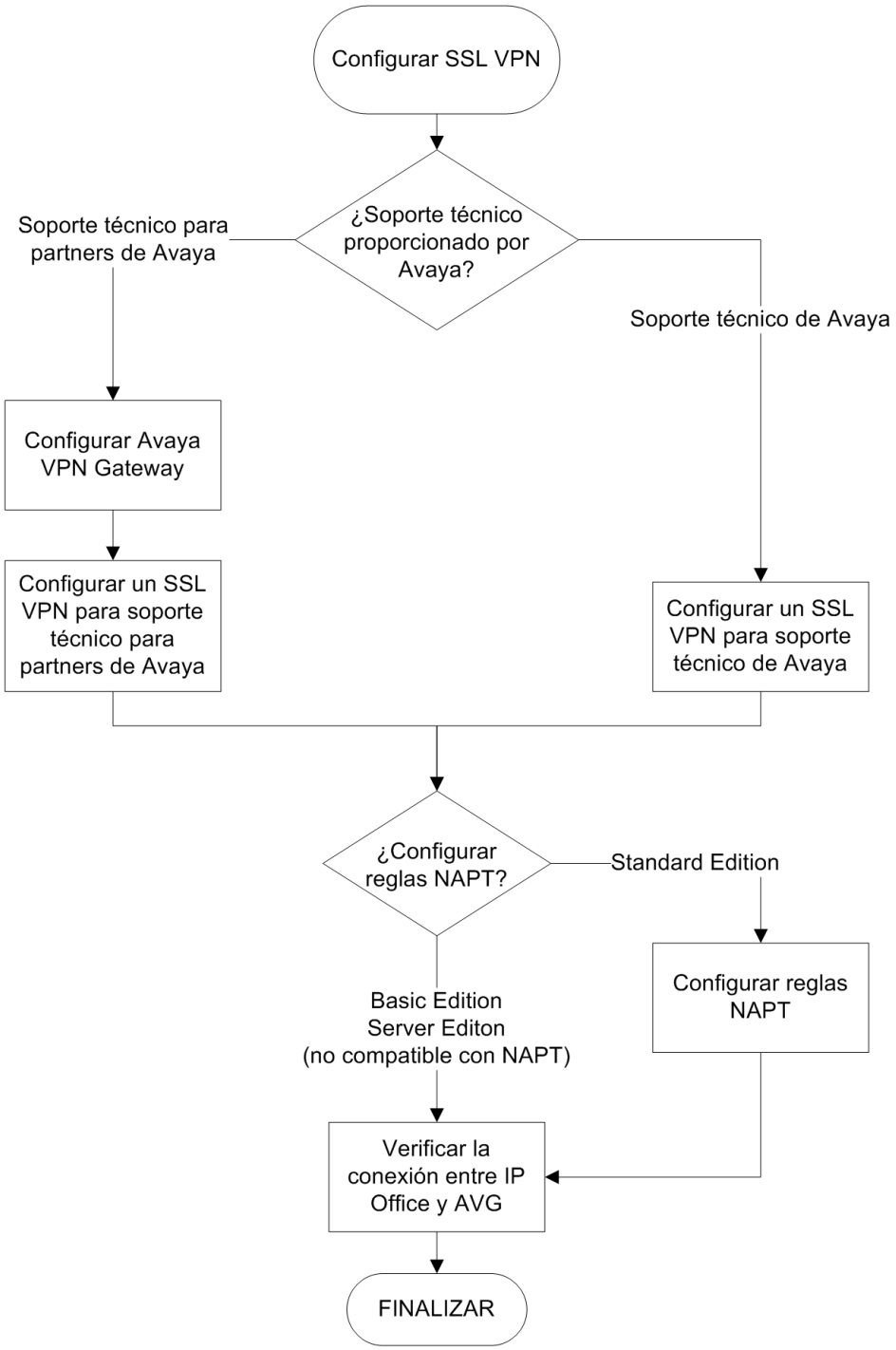
- *Servidor de encendido de motores de identidad de Avaya* (NN47280-500)

Vínculos relacionados

Acerca del servicio VPN SSL en la página 9

Capítulo 3: Flujo de trabajo para configurar un VPN SSL

Este flujo de trabajo de la siguiente página muestra la secuencia de tareas que realiza para configurar un VPN SSL.



Navegación

- Configuración de en la página 21
- Configuración de un VPN SSL para soporte técnico de Avaya en la página 34
- Configuración de un VPN SSL para soporte técnico para partners de Avaya en la página 37

- Reglas de la dirección de red y la conversión de puerto (NAPT) en la página 57
- Verificar la conexión entre y en la página 59

Capítulo 4: Configuración de Avaya VPN Gateway

Para proporcionar servicios de soporte técnico con la solución VPN SSL, los partner de Avaya deben configurar Avaya VPN Gateway (AVG)

Esta sección entrega información sobre las tareas que debe completar cuando instala y configura un AVG para respaldar una conexión VPN SSL con un sistema IP Office.

Antes de configurar el sistema IP Office para un servicio VPN SSL, debe configurar la infraestructura a la que se conecta el servicio. Esta sección cubre la configuración de la interoperación de AVG con un sistema IP Office. Para completar estas tareas, debe consultar la documentación del AVG, así como la documentación proporcionada por otros proveedores para respaldar el hardware y software utilizado en la infraestructura de red.

Las principales tareas requeridas para la implementación de Avaya VPN Gateway se describen en este capítulo. Estas son recomendaciones generales. Los detalles exactos de la implementación pueden variar dependiendo del entorno específico del partner de negocios.

Vínculos relacionados

Planificación y configuración inicial en la página 21
Flujo de tareas de la configuración de Avaya VPN Gateway en la página 22
Configuración básica de AVG: en la página 24
Activación de servicios de acceso remoto en la página 25
Ejecución del asistente de Net Direct en la página 25
Modificación del AVG predeterminado para VPN SSL en la página 26
Configuración de autenticación local en la página 28
Configuración de la autenticación de RADIUS en la página 29
Atributos de configuración del servidor RADIUS en la página 31

Planificación y configuración inicial

Ambiente personalizado

El cliente VPN SSL requiere que Avaya VPN Gateway (AVG) esté instalado en un entorno virtualizado como el servidor VPN Gateway. Los únicos entornos virtuales compatibles son los servidores ESX y ESXi. Existen tres modelos de AVG: 3050–VM, 3070–VM y 3090–VM. Para

las especificaciones de hardware para cada modelo, consulte *Guía de inicio de VMware, Avaya VPN Gateway* (NN46120-302). Puede descargar la colección completa de documentos AVG en http://support.avaya.com.

Información adicional sobre servidores VMware ESXi disponible en http://www.vmware.com.

Configuración de dos secciones

Instale Avaya VPN Gateway (AVG) en una configuración de dos secciones. Esto significa que el servidor AVG debe estar equipado con dos tarjetas de interfaces de red (NIC). Asigne una dirección IP estática para cada NIC.

- Una interfaz maneja tráfico privado y se utiliza como una interfaz de administración.
- La segunda interfaz maneja el acceso a internet y la tunelización VPN SSL.

Software AVG

Existen dos opciones para implementar el software AVG.

- Implementar dispositivos virtuales AVG OVF
- CDROM de instalación automática

Para la información de instalación y los procedimientos de AVG, consulte *Guía de inicio de VMware, Avaya VPN Gateway* (NN46120-302).

PC del Agente de servicio

Instale la PC del Agente de servicio (SA) en la red privada y configure el gateway predeterminado en la dirección IP del host de Avaya VPN Gateway (AVG).

Desde la PC de agente de servicio

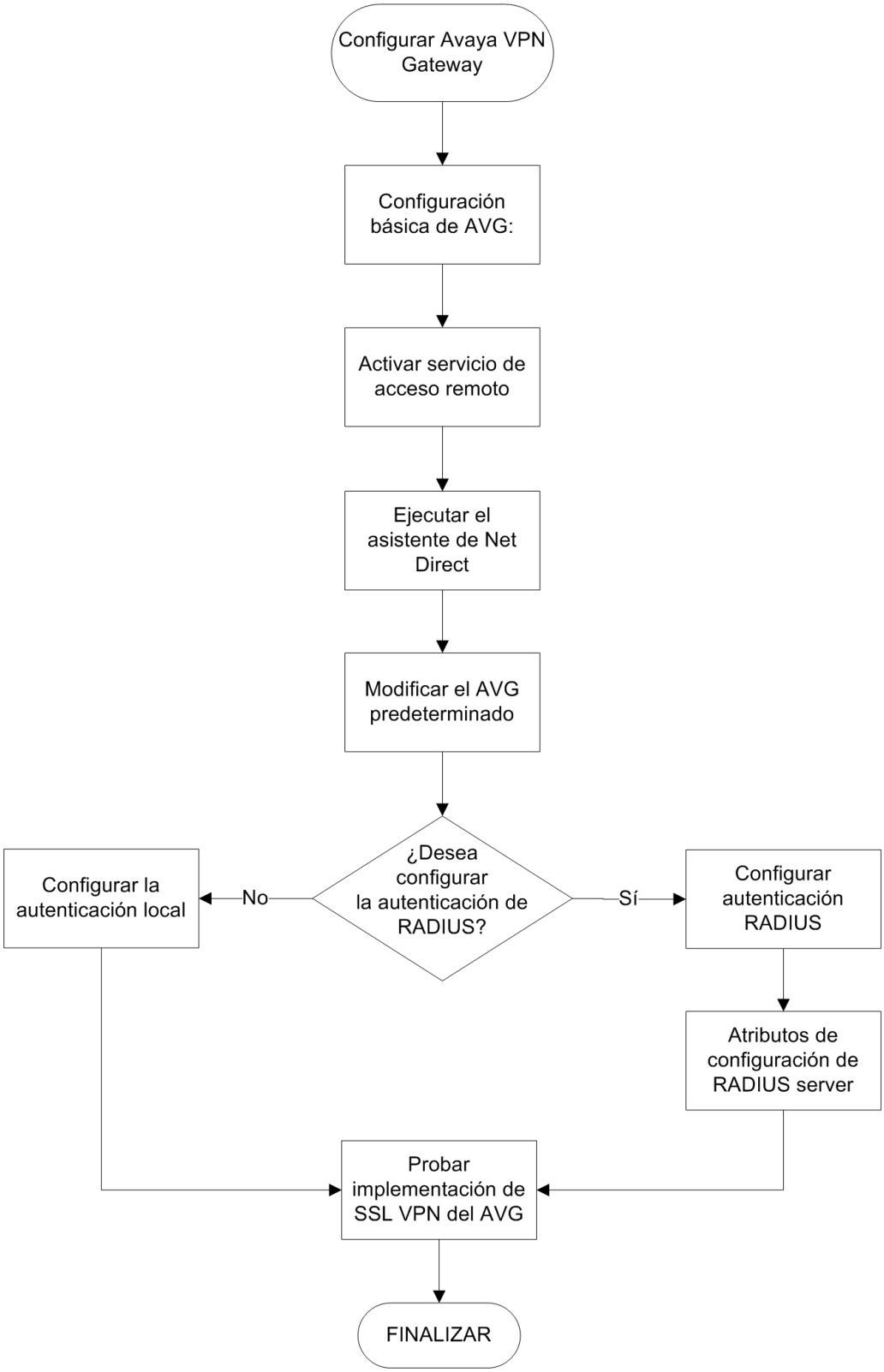
- La dirección IP de la interfaz de administración (MIP) se utiliza para iniciar una Interfaz basada en el navegador de administración (BBI) o una Interfaz de línea de comando (CLI) para configurar y monitorear el AVG.
- La dirección IP de tunelización de VPN SSL se utiliza para administrar y monitorear de manera remota los sistemas IP Office.

Vínculos relacionados

Configuración de Avaya VPN Gateway en la página 21

Flujo de tareas de la configuración de Avaya VPN Gateway

Este flujo de tareas le muestra la secuencia de procedimientos que realiza para configurar el AVG.


Configurar Avaya VPN Gateway
Configuración básica de AVG:
Activar servicio de acceso remoto
Ejecutar el asistente de Net Direct
Modificar el AVG predeterminado
¿Desea configurar la autenticación de RADIUS?
No
Sí
Configurar la autenticación local
Configurar autenticación RADIUS
Atributos de configuración de RADIUS server
Probar implementación de SSL VPN del AVG
FINALIZAR

Navegación

Vínculos relacionados

Configuración de Avaya VPN Gateway en la página 21

Configuración básica de AVG:

Configuración de AVG desde la PC de agente de servicio

La primera vez que inicia VPN, ingresará al menú **Configuración**. Este menú contiene el **nuevo** comando CLI. Este es un asistente de configuración inicial basado en CLI e intuitivo, para el AVG que ofrece la configuración predeterminada para activar rápidamente las conexiones de SSL desde IP Office. Es útil para la configuración y prueba iniciales. Esta es la manera más rápida de configurar inicialmente AVG. Como consecuencia, la Interfaz del administrador basada en el navegador (BBI) se puede usar para realizar los cambios recomendados para la conectividad VPN SSL. Para obtener información consulte *Guía de usuario de Avaya VPN Gateway* (NN46120-104).

Después de usar el nuevo comando para ejecutar el Asistente de configuración rápida, se crearon las siguientes configuraciones:

- A VPN. El VPN se define generalmente para acceder a una intranet, partes de una intranet o a una extranet.
- Un servidor SSL virtual de tipo portal. Se le asigna una dirección de IP de portal, en la que el usuario remoto debe conectarse para acceder al Portal. Si elige usar la función de VPN sin un Conmutador de aplicación, el servidor del portal se configura en el modo independiente.
- Un certificado de prueba se instaló y asignó al servidor de portal.
- El método de autenticación se configura en la base de datos local y usted tiene un usuario de prueba configurado. El usuario de prueba corresponde a un grupo denominado `trusted` cuyas reglas de acceso permiten acceder a todas las redes, los servicios y las rutas.
- Uno o varios de los nombres de dominio se agregan a la lista de búsqueda de DNS, que significa que el usuario remoto puede ingresar un nombre corto en los distintos campos de dirección del portal (por ejemplo, interior en lugar de interior.ejemplo.com si ejemplo.com se agrega a la lista de búsqueda).

- Si eligió activar la redirección de HTTP a HTTPS, un servidor adicional del tipo HTTP se creó para redirigir solicitudes realizadas con HTTP a HTTPS, porque el servidor del portal requiere una conexión SSL.

Encontrará un ejemplo impreso de ajustes de configuración en el archivo de registro Configuración rápida disponible en Apéndice A: ejemplo de archivo de registro de Configuración rápida de AVG en la página 90.

Vínculos relacionados

Configuración de Avaya VPN Gateway en la página 21

Activación de servicios de acceso remoto

Además de usar la consola VM local para configurar VPN, el administrador también necesita administrar el VPN utilizando una sesión TELNET o SSH, o a través de BBI. Para permitir la configuración remota de la puerta de enlace VPN, deben estar activados los servicios de acceso remoto.

Realice este procedimiento utilizando la Interfaz de línea de comando (CLI). Consulte los siguientes documentos AVG:

- *Avaya VPN Gateway para referencias de comando*
- *Avaya VPN Gateway de la guía de aplicación de CLI*

Procedimiento

1. Inicie sesión en el AVG.
2. Ingrese los siguientes comandos.

```
/cfg/sys/adm/.
        telnet on
        ssh on
/cfg/sys/adm/https/.
        cert 1
        ena true
/cfg/sys/adm/http/.
        ena true
apply
```

Vínculos relacionados

Configuración de Avaya VPN Gateway en la página 21

Ejecución del asistente de Net Direct

El asistente de Net Direct le permite crear un enlace en el portal que descarga e inicia una versión reducida de Avaya VPN Client, el cliente Net Direct. Ejecute el asistente Net Direct desde la Interfaz del administrador basada en el navegador (BBI). Consulte la *Guía de la aplicación Avaya VPN Gateway*.

Procedimiento

1. Inicie sesión en AVG BBI.

   En el panel de navegación de la izquierda, amplíe **Asistentes**.

2. Haga clic en **Asistente de Net Direct**.
3. En la página **Configuración de Net Direct para el VPN seleccionado**, seleccione el botón de opción **Activar Net Direct para este VPN**.
4. En la página **Configuración predeterminada de grupo de IP**:
   - Para **IPPool predeterminado**, seleccione **Local_pool**.
   - Ingrese las direcciones IP superiores e inferiores para el rango del grupo.

Vínculos relacionados

Configuración de Avaya VPN Gateway en la página 21

Modificación del AVG predeterminado para VPN SSL

Después de ejecutar los asistentes de configuración Configuración rápida y Net Direct, la configuración predeterminada debe modificarse para respaldar una conexión VPN SSL con un sistema IP Office.

Realice este procedimiento utilizando la interfaz basada en el explorador de AVG. Consulte la *Guía de la aplicación Avaya VPN Gateway*.

Este procedimiento está duplicado en el Apéndice B: modificación del AVG predeterminado para VPN SSL (con pantallas) en la página 94. Esta versión del procedimiento incluye capturas de pantalla de la interfaz del usuario.

Antes de empezar

Asegúrese de que la puerta de enlace predeterminada en AVG responda a las solicitudes ICMP. Si la puerta de enlace predeterminada no responde a las solicitudes de ICMP, el AVG no puede proporcionar los servicios VPN.

Procedimiento

1. Inicie sesión en el BBI de AVG como administrador.
2. En el panel de navegación de la izquierda, seleccione la ficha **Config** y luego **VPN Gateway** > **VPN1** > **Grupo de IP**.
3. Es posible que el VPN predeterminado de la configuración básica de AVG ya tenga un grupo local. Si no es así, debe agregar un grupo local al VPN predeterminado. En la página **Agregar nuevo grupo de dirección IP**, agregue un grupo local al VPN predeterminado.

4. En la página **Modificar grupo de dirección IP**, verifique que los valores de los campos **IP inferior** e **IP posterior** coincidan con los valores establecidos utilizando el asistente Configuración de Net Direct.
5. En la página **Grupo IP** > **Configuración de atributos de red**, seleccione la ficha **Atributos de red** e ingrese los valores de su red.
6. En la página **Grupo IP**, configure el **Grupo IP predeterminado** en el grupo local creado en el paso 3.
7. En la página **Configuración de acceso de cliente Net Direct**, verifique las configuraciones creadas por el asistente Configuración de Net Direct.
   - Asegúrese de que **Verificación de sesión inactiva** esté configurado en **desactivado**.
   - Asegúrese de que el encabezado de Net Direct esté configurado.
8. Defina el enlace del portal para iniciar el cliente de Net Direct. En la página **Configuración de conjunto de enlace de portal**, seleccione la ficha **Enlace de portal**. En el campo **Tipo de enlace**, seleccione **Net Direct**.
9. En la página **Redes para tunelización dividida**:
   - configure **Dividir modo de túnel** en **habilitado**
   - configure las rutas de tunelización divididas para alcanzar al agente de servicio en la red privada
10. Para VPN1, vaya a la página de grupos y seleccione **Grupo1**. En la página **Modificar un grupo**, configure el Grupo IP en el grupo local creado en el paso 3.
11. Vaya a la página **VPN1** > **Grupo1** > **Listas de acceso**. En la página **Lista de acceso de firewall**, cree una regla de acceso si no se creó de manera predeterminada.
12. Vaya a la página **VPN1** > **SSL**. En la página **Configuración de servidor**, en **Configuración de SSL** configure **Cifrados** en **AES256-SHA** para un cifrado sólido.
13. Vaya a la página **VPN1** > **Autorización** > **Servicios**. Elimine todos los servicios configurados en la configuración predeterminada ya que no son requeridos por VPN SSL.
14. Vaya a la página **VPN1** > **Autorización** > **Redes**. Configure el subgrupo de redes de autorización al que se hace referencia en una de las reglas de acceso que está configurado en **VPN1** > **Grupo1** > **Listas de acceso**.

    Nota:

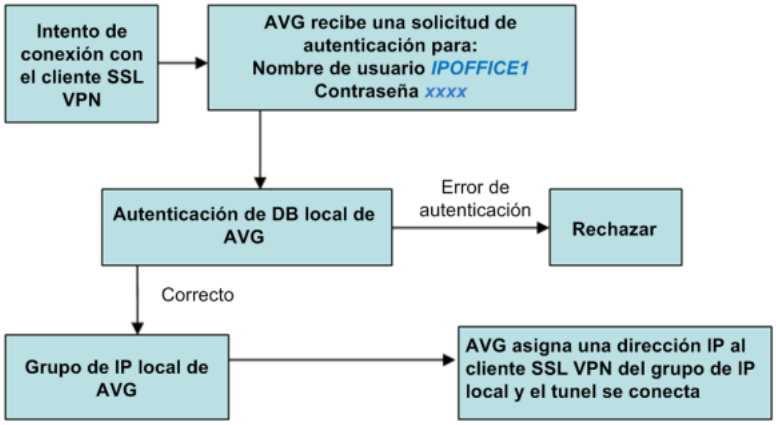
    Esta opción controla la comunicación interna en el túnel de la VPN SSL. La comunicación se habilita únicamente cuando se especifica una lista de redes “intranet” permitidas. La comunicación con clientes dentro de la VPN se bloquea de manera predeterminada.
15. Vaya a la página **VPN1** > **Configuración general** > **Sesión**. Configure **Tiempo de inactividad de sesión** en dos minutos.

Vínculos relacionados

Configuración de Avaya VPN Gateway en la página 21

Configuración de autenticación local

Para un pequeño número de sistemas IP Office, puede usar la base de datos local Avaya VPN Gateway (AVG) para crear los datos de usuarios necesarios para la autenticación. Esta es una manera rápida de configurar la autenticación cuando los servidores de autenticación externos RADIUS están disponibles. Configure un Grupo IP para asignar dinámicamente las direcciones IP a los usuarios locales. La siguiente figura muestra el flujo de autenticación del cliente VPN SSL y cómo se realiza la asignación de dirección de grupo IP.



Este procedimiento cubre los pasos manuales para configurar la autenticación local. También puede configurar la autenticación utilizando el asistente de autenticación de AVG.

Procedimiento

1. Para **VPN1**, vaya a la página **Configuración de grupo IP** y agregue un grupo IP local.
2. Vaya a **VPN1** > **Grupo IP** > **Agregar/modificar**. Configure el rango dinámico del grupo IP ingresando los valores en los campos **IP inferior** e **IP superior**.
3. Vaya a **VPN1** > **Grupo IP** > **Atributo de red**. Configure la **Máscara de red de cliente**.
4. En la página **Agregar un grupo**, agregue un nuevo grupo a VPN1.
5. Vaya a **VPN1** > **<Group_Name>** > **Modificar grupo**. Seleccione la ficha **General** y asigne un grupo local al grupo seleccionándolo en el campo **Grupo IP**.
6. Seleccione la ficha **Listas de acceso** y especifique la lista de acceso para el grupo de usuarios locales.
7. Seleccione la ficha **Conjunto de enlace** y asigne los conjuntos de listas.
8. Edite la configuración de autenticación de VPN. En la página **Servidores de autenticación**, agregue un nuevo servidor de autenticación.
9. Vaya a **VPN1** > **<Auth_Server_Name>** > **Agregar/modificar usuarios** y agregue usuarios al grupo.
10. Edite el servidor de autenticación y especifique la **Orden de autenticación**.

Vínculos relacionados

Configuración de Avaya VPN Gateway en la página 21

Configuración de la autenticación de RADIUS

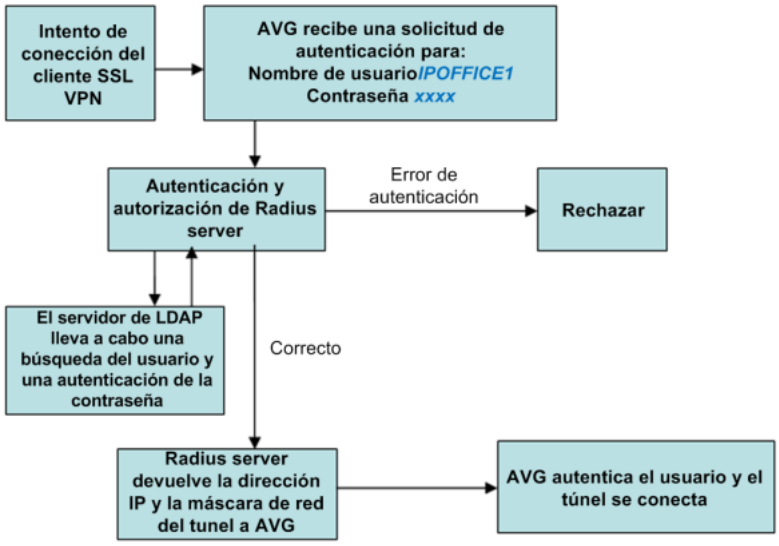
El beneficio clave de la autenticación de RADIUS es que el servicio de VPN SSL siempre está asignado a la misma dirección IP de túnel.

Para configurar la autenticación de RADIUS, debe instalar un servidor de RADIUS. Avaya recomienda Avaya Identity Engine para un servidor de Radius. Para obtener información y la descarga del software, vaya a http://support.avaya.com.

La información de autenticación del protocolo de RADIUS como la información de cuenta del usuario así como la información de túnel de VPN SSL como la dirección IP y la máscara de red deben almacenarse en la base de datos. Hay dos opciones posibles:

- Use la base de datos local de Identity Engine para almacenar la información de usuario y ofrecer tanto búsqueda y autenticación como servicios de autorización. La opción se puede usar para un pequeño número de usuarios. Identity Engine tiene un límite estricto de usuarios. Consulte la documentación para conocer el valor exacto.
- Use un servidor LDAP para almacenar las credenciales de usuarios y la información de túnel de VPN SSL tanto para servicio de búsqueda como de autenticación. Esta opción se adapta a situaciones de implementación para un gran número de usuarios.

Para la instalación del servidor LDAP, la documentación de Avaya Identity Engine Radius Server contiene opciones de configuración para servidores de LDAP de distintos proveedores. La autenticación de RADIUS con un servidor LDAP se ilustra en la figura a continuación. Tenga en cuenta que esta configuración del servidor de RADIUS en este procedimiento no requiere un servidor LDAP.



Este procedimiento cubre los pasos del manual para configurar la autenticación de RADIUS. También puede configurar la autenticación utilizando el asistente de autenticación de AVG.

Este procedimiento está duplicado en Apéndice C: configuración de autenticación de RADIUS (con pantallas) en la página 100. Esta versión del procedimiento incluye capturas de pantalla de la interfaz del usuario.

Procedimiento

1. Inicie sesión en el BBI de AVG como administrador.
2. En la página **Configuración del grupo de IP**, agregue un nuevo grupo de dirección IP para la autenticación de RADIUS.
3. En la página **Grupo de IP**, configure el **Grupo de IP predeterminado** en el grupo de dirección IP de autenticación de RADIUS que creó en el paso 2.
4. Modifique el VPN. En la página **Servidores de autenticación** > **Agregar nuevo servidor de autenticación**, complete los campos del servidor RADIUS.
5. Configure los ajustes del servidor de autenticación RADIUS. Tenga en cuenta que la ID de proveedor 1872 está asociada al proveedor Alteon e identifica a AVG. Seleccione la ficha **Configuración** y complete los siguientes campos.
   - **ID de proveedor: 1872**
   - **Tipo de proveedor: 1**
   - **Tiempo de espera: 10**
   - **ID de proveedor para ID de VPN: 1872**
   - **Tipo de proveedor para ID de VPN: 3**
6. Configure los atributos de red de RADIUS. Seleccione la ficha **Atributos de red** y complete los siguientes campos.

Configuración de ID de proveedor	Configuración de tipo de proveedor
Dirección IP del cliente: 1872	Dirección IP del cliente: 4
Máscara de red del cliente: 1872	Máscara de red del cliente: 5
Servidor NBNS primario: 1872	Servidor NBNS primario: 6
Servidor NBNS secundario: 1872	Servidor NBNS secundario: 7
Servidor DNS primario: 1872	Servidor DNS primario: 8

7. Configure los atributos del filtro. Seleccione la ficha Atributos de filtro y complete los siguientes campos>.
   - **Atributo de filtro de Radius: desactivado**
   - **ID de proveedor para atributo de filtro: 9**
   - **Tipo de proveedor para atributo de filtro: 1**
8. Especifique la dirección del servidor Radius. Seleccione la ficha **Servidores** en la página **Servidores RADIUS**.

9. Haga clic en **Agregar** y en la página **Modificar servidor RADIUS**, ingrese la dirección IP del servidor RADIUS y el secreto compartido.
10. Seleccione la ficha **Orden de autenticación** y especifique el orden preferido para los métodos de autenticación.

Vínculos relacionados

Configuración de Avaya VPN Gateway en la página 21

Atributos de configuración del servidor RADIUS

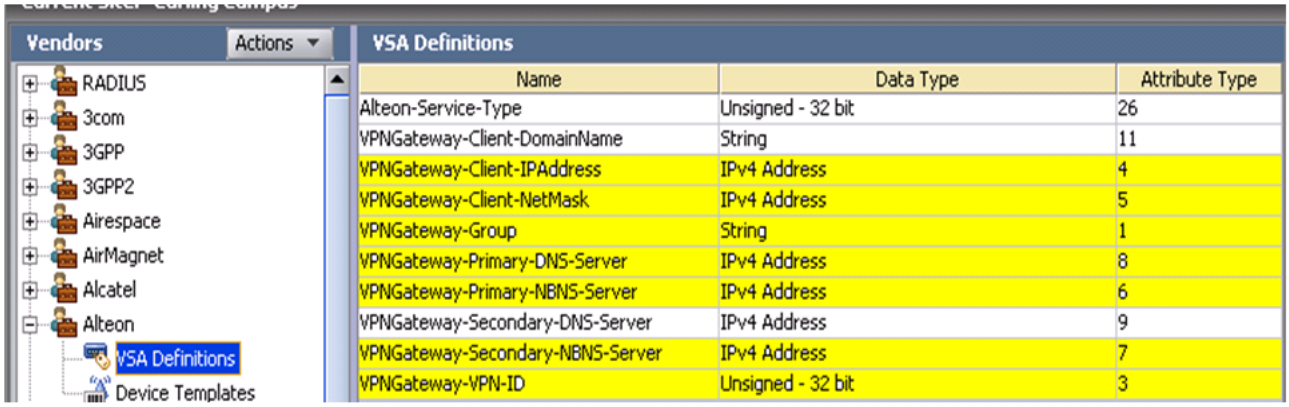
El servicio VPN SSL requiere un servidor de RADIUS. Avaya recomienda que use el Servidor de encendido de Avaya Identity Engines como el servidor RADIUS.

Cuando conecta el servicio VPN SSL, el Avaya VPN Gateway (AVG) autentica el sistema IP Office enviando una consulta a un servidor RADIUS externo. Esta sección muestra los atributos que debe configurar en el servidor de RADIUS.

Asignación del atributo del servidor RADIUS

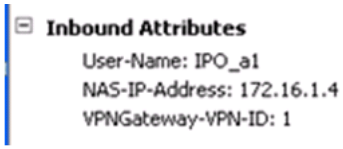
Los nombres del atributo Radius específico, y los tipos de datos asociados y los códigos de tipo de proveedor para el proveedor Alteon (AVG) están contenidos en la lista a continuación.

Los siguientes ejemplos se obtuvieron utilizando un servidor RADIUS Avaya Identity Engines. Los atributos destacados se configuraron como **Atributos de red** y **Configuración** en los ajustes del servidor RADIUS AVG.



Name	Data Type	Attribute Type
Alteon-Service-Type	Unsigned - 32 bit	26
VPNGateway-Client-DomainName	String	11
VPNGateway-Client-IPAddress	IPv4 Address	4
VPNGateway-Client-NetMask	IPv4 Address	5
VPNGateway-Group	String	1
VPNGateway-Primary-DNS-Server	IPv4 Address	8
VPNGateway-Primary-NBNS-Server	IPv4 Address	6
VPNGateway-Secondary-DNS-Server	IPv4 Address	9
VPNGateway-Secondary-NBNS-Server	IPv4 Address	7
VPNGateway-VPN-ID	Unsigned - 32 bit	3

• A continuación se muestran los atributos de entrada que provienen del AVG al Servidor Radius durante la solicitud de autenticación.



Los atributos de Radius que envía AVG son:

- o Dirección IP NAS (atributo genérico de radius) es la dirección IP del AVG IP.
- Nombre usuario (atributo genérico radius) es el nombre de cuenta del usuario
- VPNGateway-VPN-ID es un atributo de Alteon

El servidor IDEngine Radius tiene una asignación de atributo interno predeterminada para los atributos de Radius más conocidos como se ve en la tabla a continuación. Las filas resaltadas corresponden a los atributos de Radius contenidos en la SOLICITUD de Radius a continuación.

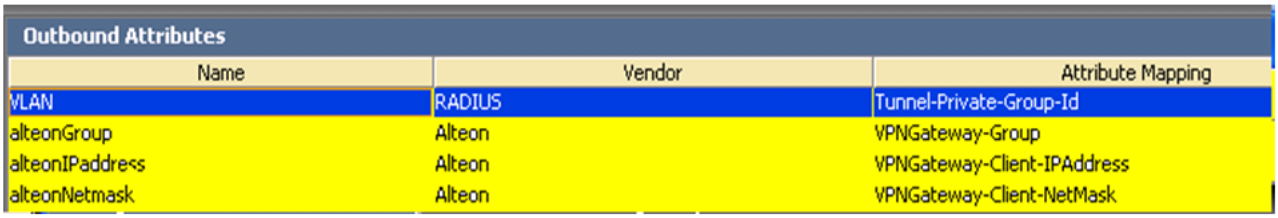
Inbound Attributes

Name	Vendor	Attribute Mapping
Inbound-Digest-Auth-Param	RADIUS	Digest-Auth-Param
Inbound-Digest-Domain	RADIUS	Digest-Domain
Inbound-Digest-Method	RADIUS	Digest-Method
Inbound-Digest-Nonce-Count	RADIUS	Digest-Nonce-Count
Inbound-Digest-Opaque	RADIUS	Digest-Opaque
Inbound-Digest-Qop	RADIUS	Digest-Qop
Inbound-Digest-Realm	RADIUS	Digest-Realm
Inbound-Digest-SIP-AOR	RADIUS	Digest-SIP-AOR
Inbound-Digest-URI	RADIUS	Digest-URI
Inbound-Digest-Username	RADIUS	Digest-Username
Inbound-Framed-Compression	RADIUS	Framed-Compression
Inbound-Framed-Interface-Id	RADIUS	Framed-Interface-Id
Inbound-Framed-IP-Address	RADIUS	Framed-IP-Address
Inbound-Framed-IP-Netmask	RADIUS	Framed-IP-Netmask
Inbound-Framed-MTU	RADIUS	Framed-MTU
Inbound-Framed-Pool	RADIUS	Framed-Pool
Inbound-Framed-Protocol	RADIUS	Framed-Protocol
Inbound-Login-IP-Host	RADIUS	Login-IP-Host
Inbound-NAS-Identifier	RADIUS	NAS-Identifier
Inbound-NAS-IP-Address	RADIUS	NAS-IP-Address
Inbound-NAS-Port	RADIUS	NAS-Port
Inbound-NAS-Port-Id	RADIUS	NAS-Port-Id
Inbound-NAS-Port-Type	RADIUS	NAS-Port-Type
Inbound-Port-Limit	RADIUS	Port-Limit
Inbound-Service-Type	RADIUS	Service-Type
Inbound-Tunnel-Client-Auth-Id	RADIUS	Tunnel-Client-Auth-Id
Inbound-Tunnel-Client-Endpoint	RADIUS	Tunnel-Client-Endpoint
Inbound-Tunnel-Medium-Type	RADIUS	Tunnel-Medium-Type
Inbound-Tunnel-Preference	RADIUS	Tunnel-Preference
Inbound-Tunnel-Private-Group-Id	RADIUS	Tunnel-Private-Group-Id
Inbound-Tunnel-Server-Auth-Id	RADIUS	Tunnel-Server-Auth-Id
Inbound-Tunnel-Server-Endpoint	RADIUS	Tunnel-Server-Endpoint
Inbound-Tunnel-Type	RADIUS	Tunnel-Type
Inbound-User-Name	RADIUS	User-Name

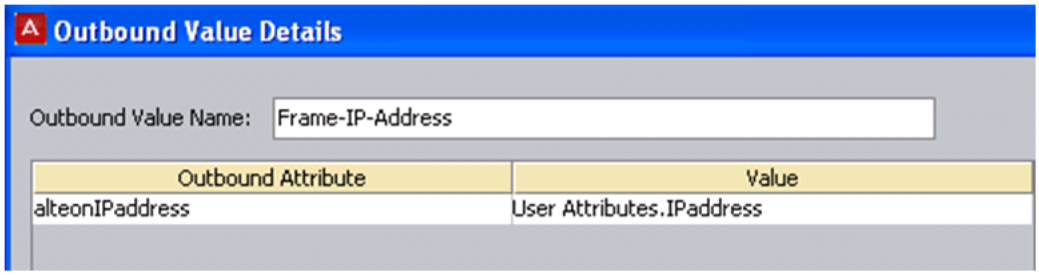
Los servidores de Radius evalúan los atributos de entrada utilizando reglas de autorización. La regla puede utilizar un atributo de entrada para verificar una condición o puede devolver el atributo de entrada en una RESPUESTA de Radius como un valor de salida. Si un atributo de entrada enviado por AVG requiere evaluación, pero no es parte del servidor Radius predeterminado que se configuró debe definirse como un atributo en el servidor Radius. Para conocer ejemplos de reglas de autenticación, consulte *Administración de IDEngine*.

• Los atributos de salida enviados al AVG desde el servidor Radius durante una RESPUESTA de autenticación que se muestran a continuación:

Los atributos de salida son los campos de datos que el servidor Radius usa para transportar datos de aprovisionamiento en VPN Gateway. Los atributos de salida son atributos genéricos o de protocolo de Radius tipo proveedor. Similar a los atributos de entrada los atributos de salida necesitan crearse si no son parte del conjunto predeterminado del servidor Radius. En el ejemplo anterior los tres atributos de salida Alteon (específico para AVG): “alteonGroup”, “alteonIPaddress” y “alteonNetmask” deben crearse en el servidor Radius como en el ejemplo a continuación:



Los valores de atributo de salida se pueden configurar en valores estáticos o se pueden asignar en atributos de usuario en la base de datos del servidor local Radius o en un repositorio LDAP. A continuación se muestra un ejemplo de un valor del atributo de salida asignado a un atributo de usuario de la base de datos:



Los valores de salida están asociados con reglas de autenticación y se envían a VPN Gateway como atributos de Radius cuando se evalúa la regla. Si la regla se evalúa en “Permitir” los valores de salida se utilizan para configurar las características de sesión del usuario. Cuando se evalúa la regla en “Rechazar” los valores de salida devueltos por lo general se utilizan para transmitir información en la causa del rechazo. Para obtener más información, consulte la documentación de IDEngine.

Vínculos relacionados

Configuración de Avaya VPN Gateway en la página 21

Capítulo 5: Configuración de un VPN SSL para soporte técnico de Avaya

Esta sección proporciona información acerca del proceso de configuración para IP Office cuando el proveedor de servicio es Avaya. Puede configurar automáticamente el VPN SSL utilizando el proceso integrado.

Puede configurar múltiples instancias del servicio VPN SSL y ejecutarlas consecutivamente.

Requisitos previos

Cuando configure un servicio VPN SSL, la dirección de la puerta de enlace VPN puede ser un FQDN. Debe configurar el servidor DNS para resolver las direcciones de FQDN. Configure los ajustes de DSN en el formulario de **Sistema** de IP Office Manager, en **DNS**.

Vínculos relacionados

[Configuración de un VPN SSL utilizando un archivo de integración](#) en la página 34
[Uso del archivo de integración para modificar un servicio existente](#) en la página 35

Configuración de un VPN SSL utilizando un archivo de integración

El archivo XML de integración está disponible en Avaya. Contiene la configuración requerida para establecer un túnel seguro entre IP Office y un servidor AVG. Al importar el archivo XML de integración, se aplica la configuración, y se instalan uno o varios certificados TLS.

Al configurar el servicio SSL VPN en un nuevo sistema, debe comenzar generando un archivo de inventario del sistema IP Office. Cuando registra el sistema IP Office, el archivo de inventario que generó se carga en el GRT y los datos del inventario se completan en la base de datos Avaya Customer Support (ACS). Después de activar el soporte técnico remoto, puede descargar el archivo de integración XML desde el sitio web de GRT y cargarlo en su sistema IP Office.

El proceso de integración configura:

- Configuración del servicio SSL VPN
- Códigos cortos para activar y desactivar el servicio SSL VPN
- capturas de alarmas SNMP

- Uno o más certificados TLS en el depósito de certificados de confianza de IP Office

Realice este procedimiento utilizando el cliente IP Office Web Manager de Avaya.

Advertencia:

El proceso de integración crea automáticamente un servicio SSL VPN en la configuración del sistema cuando el archivo de integración se carga en el sistema. Se debe tener cuidado de no eliminar o modificar esa excepción de servicio cuando Avaya lo aconseje.

Antes de empezar

Antes de comenzar, debe tener los códigos de hardware y la descripción de catálogo del sistema IP Office. Por ejemplo, “IP OFFICE 500 VERSION 2 CONTROL UNIT TAA” es un código de hardware y una descripción de catálogo.

Procedimiento

1. Seleccione **Herramientas > Integración**.

   Aparece el cuadro de diálogo Integración.

2. Si el código de hardware para el sistema IP Office termina con las letras TAA, seleccione la casilla de verificación que está junto a la indicación **¿Usa hardware de la serie TAA?**
3. Haga clic en **Obtener el archivo de inventario** para generar un inventario de su sistema IP Office.
4. Haga clic en **Registrar IP Office**.

   Se abre un explorador y navega al sitio web GRT.

5. Inicie sesión en el sitio web e ingrese los datos requeridos para el sistema IP Office.
6. Seleccione **Soporte técnico remoto** para el sistema IP Office.
7. Haga clic en **Descargar** y guarde el archivo de integración.
8. Examine la ubicación donde guardó el archivo de integración y haga clic en **Cargar**.

   Aparece un mensaje para confirmar que el archivo de integración se instaló correctamente.

Vínculos relacionados

Configuración de un VPN SSL para soporte técnico de Avaya en la página 34

Uso del archivo de integración para modificar un servicio existente

Puede usar el archivo de integración para configurar el servicio VPN SSL. El archivo de integración contiene las configuraciones requeridas para establecer un túnel seguro entre IP Office y un servidor AVG. Use este procedimiento cuando ya haya configurado el servicio VPN SSL en un sistema IP Office y necesite actualizar o modificar la configuración VPN SSL.

Realice este procedimiento desde la interfaz IP Office Web Manager de Avaya.

Antes de empezar

Antes de comenzar, debe tener los códigos de hardware y la descripción de catálogo del sistema IP Office. Por ejemplo, “IP OFFICE 500 VERSION 2 CONTROL UNIT TAA” es un código de hardware y una descripción de catálogo.

Procedimiento

1. Seleccione **Herramientas > Integración**.

   Aparece el cuadro de diálogo Integración.

2. Este paso es opcional. Para generar un inventario del sistema IP Office, realice lo siguiente:
   - Si el código de hardware para el sistema IP Office termina con las letras TAA, seleccione la casilla de verificación que está junto a la indicación **¿Usa hardware de la serie TAA?**
   - Haga clic en **Obtener el archivo de inventario**.
3. Haga clic en **Modificar**.

   Se abre un explorador y navega al sitio web de Avaya.

4. Inicie sesión en el sitio web.

   Aparece la página Administración de conectividad remota / contraseña de IP Office.

5. Haga clic en **Existing IP Office SSL VPN Remote Connectivity** (Conectividad remota VPN SSL de IP Office existente).
6. Seleccione **Regenerate on-boarding file (existing properties)** (Regenerar archivo de integración [propiedades existentes]).
7. Ingrese el nombre del servicio VPN SSL y el nombre de cuenta VPN SSL en los campos correspondientes.
8. Haga clic en **Submit** (Enviar).
9. Seleccione si desea recibir el archivo de integración actualizado por correo electrónico o si desea descargarlo y seguir las indicaciones en pantalla.
10. Cuando haya descargado o recibido el archivo de integración actualizado, guárdelo en el sistema local.
11. Examine la ubicación donde guardó el archivo de integración y haga clic en **Cargar** en la interfaz de Web Manager.

    Aparece un mensaje para confirmar que el archivo de integración se instaló correctamente.

Vínculos relacionados

Configuración de un VPN SSL para soporte técnico de Avaya en la página 34

Capítulo 6: Configurar un VPN SSL para soporte técnico para partners de Avaya

Los proveedores de servicios de terceros pueden utilizar su propia Avaya VPN Gateway para implementar el servicio técnico al cliente remoto mediante la tecnología VPN SSL de IP Office.

Para el soporte técnico de proveedores de servicios de terceros, el VPN SSL puede configurarse manualmente a través de la aplicación Manager. Puede configurar un sistema en modo Estándar o un sistema Server Edition. La configuración manual no es admitida para el modo Basic Edition.

Puede configurar múltiples instancias del servicio VPN SSL y ejecutarlas consecutivamente.

Requisitos previos

Cuando configure un servicio VPN SSL, la dirección de la puerta de enlace VPN puede ser un FQDN. Debe configurar el servidor DNS para resolver las direcciones de FQDN. Configure los ajustes de DNS en el formulario de **Sistema** de IP Office Manager, en **DNS**.

Configuración de un VPN SSL para los procedimientos de soporte técnico de partners de Avaya

En la lista que se incluye a continuación, se muestra la secuencia de procedimientos que realiza para configurar un VPN SSL para el soporte técnico de socios.

- Configuración del servicio VPN SSL en la página 38
- Instalación de un certificado en la página 39
- Configuración de códigos abreviados en la página 41
- Configuración de notificaciones de alarma en la página 45
- Configuración de una ruta estática en la página 49
- Verificación de la conexión con en la página 59
- Envío de una alarma de prueba en la página 61

Vínculos relacionados

Configuración del servicio VPN SSL en la página 38
Instalación de un certificado en la página 39
Configuración de códigos cortos en la página 41
Cómo configurar notificaciones de alarma en la página 45
Configuración de una ruta estática en la página 49

Configuración del servicio VPN SSL

Use este procedimiento para configurar el servicio VPN SSL.

Realice este procedimiento en la interfaz de Manager. Si está configurando un sistema Server Edition, use el modo IP Office Manager for Server Edition.

Antes de empezar

Debe conocer el valor de las siguientes variables de configuración.

Tabla 1: Ficha Servicio

Variable	Descripción
Nombre del servicio	Ingrese un nombre para el nuevo servicio VPN SSL.
Nombre de cuenta	Ingrese el nombre de cuenta de servicio VPN SSL. Este nombre de cuenta se usa para autenticar el servicio VPN SSL cuando se conecta con el AVG. **Sistemas Server Edition:** Si está configurando un sistema Server Edition, Avaya recomienda que configure el mismo nombre tanto para la cuenta del servicio VPN SSL como la ID del dispositivo agente SNMP. Cuando estas configuraciones coincidan, el personal de soporte técnico puede usar esta información para identificar la dirección del túnel VPN SSL. Puede configurar solo una ID de dispositivo agente SNMP por sistema. Si está configurando varias instancias del servicio VPN SSL, elija uno de los nombres de cuenta de servicio de VPN SSL para que coincida con el ID de dispositivo agente SNMP según sus necesidades de soporte técnico. También puede ver la ID del dispositivo seleccionando **Red** de la lista de navegación y seleccionando un sistema Server Edition; la pantalla muestra un resumen de configuraciones para el sistema seleccionado.
Contraseña de la cuenta	Ingrese la contraseña para la cuenta del servicio VPN SSL.
Confirmar contraseña	Confirme la contraseña para la cuenta del servicio VPN SSL.
Dirección del servidor	Ingrese la dirección de la puerta de enlace VPN. La dirección puede ser una dirección FQDN o IPv4.
Tipo de servidor	Seleccionar AVG.
Número de puerto del servidor	Seleccione un número de puerto. El número de puerto predeterminado es 443.

Tabla 2: Ficha Sesión

Variable	Descripción
Protocolo Preferido de transferencia de datos	Seleccione TCP; este es el protocolo utilizado por el servicio VPN SSL para el transporte de datos. Si selecciona UDP como el protocolo, cuando configure la conexión, UDP aparece en este campo, pero el servicio VPN SSL vuelve a TCP.
Intervalo de latidos	Ingrese la duración del intervalo entre los mensajes de latidos en segundos. El valor predeterminado es de 30 segundos.
Reintentos de latido	Ingrese el número de mensajes de latidos no reconocidos que IP Office envía a AVG antes de determinar que AVG no responde. Cuando se alcance este número de mensajes de latidos consecutivos y AVG no los reconozca, IP Office termina la conexión. El valor predeterminado es 4.
Intervalo de reconexión luego de una falla	El intervalo de espera antes de que el servicio VPN SSL intente restablecer una conexión con el AVG. El intervalo comienza cuando el túnel VPN SSL está activo y realiza un intento exitoso de conectarse con el AVG, o cuando se pierde la conexión con AVG. El valor predeterminado es 60 segundos.

Procedimiento

1. En la lista de navegación, haga clic con el botón secundario en **Servicio**.
2. Seleccione **Nuevo** > **servicio de VPN SSL**.
3. En la ficha **Servicio**, configure los valores que aparecen en la siguiente tabla.
4. Seleccione la ficha **Sesión** y configure los valores que aparecen en la siguiente tabla.
5. Seleccione la ficha **Respaldo** y elija una de las siguientes opciones:
   - para activar el servicio y establecer una conexión VPN SSL, asegúrese de que la opción **En respaldo** esté desmarcada
   - para configurar el servicio sin establecer una conexión VPN SSL, seleccione la opción **En respaldo**
6. Haga clic en **Aceptar**.
7. Haga clic en el icono **Guardar** para guardar la configuración.

Vínculos relacionados

Configurar un VPN SSL para soporte técnico para partners de Avaya en la página 37

Instalación de un certificado

El servicio VPN SSL usa certificados digitales para verificar la identidad de los dispositivos en cada extremo del túnel VPN SSL. Este procedimiento describe cómo instalar un certificado en el almacén de certificados de confianza de IP Office.

Manager contiene una opción de menú que le permite restaurar la configuración predeterminada de seguridad en IP Office. Si restaura la configuración predeterminada de seguridad, y el servicio VPN SSL no se vuelve a conectar con AVG después de unos minutos, debe volver a agregar el certificado en el almacén de certificados de confianza.

De manera similar, la aplicación Security Manager le permite eliminar el certificado del almacén de certificados de confianza. Si elimina el certificado mediante Security Manager y el servicio VPN SSL ya se había conectado con AVG, el servicio VPN SSL se desconecta la próxima vez que el túnel vuelva a negociar la clave secreta. Esta renegociación se lleva a cabo de manera predeterminada cada 8 horas y puede realizarse en intervalos diferentes, dependiendo de la configuración establecida en AVG. Si el servicio VPN SSL se desconecta durante una renegociación o si usted desactiva el servicio antes de la próxima renegociación, no podrá activar el servicio VPN SSL otra vez hasta que haya instalado el certificado requerido en el almacén de certificados de confianza.

Antes de empezar

Debe instalar uno de los siguientes tipos de certificados:

- el certificado AVG autofirmado del portal de VPN al que se conecta el servicio VPN SSL de IP Office;
- el certificado del CA que firmó el certificado de AVG

Procedimiento

1. Seleccione **Archivo > Avanzado > Configuración de seguridad**.

   Un cuadro de diálogo muestra los sistemas IP Office.

2. Haga clic en la casilla de verificación para seleccionar el sistema IP Office donde desea instalar el certificado.
3. Haga clic en **Aceptar**.

   Aparece un cuadro de diálogo.

4. En el campo **Nombre de usuario del servicio**, introduzca el nombre de usuario del administrador de IP Office.
5. En el campo **Contraseña de usuario de servicio**, ingrese la contraseña del administrador IP Office.
6. Haga clic en **Aceptar**.

   Se aceptan las credenciales.

7. En el panel de navegación, seleccione **Seguridad > Sistema** y seleccione el nombre de la configuración.
8. En la ficha **Certificados**, haga clic en **Agregar**.

   Aparece un cuadro de diálogo que le indica que seleccione una fuente para el certificado.

9. Seleccione **Pegar desde el portapapeles** y haga clic en **Aceptar**.

   Se abre un cuadro de diálogo para capturar el texto del certificado.

10. Copie el certificado y pegue el texto en la ventana abierta. Debe incluir las líneas `-----BEGIN CERTIFICATE-----` y `-----END CERTIFICATE-----`.
11. Haga clic en **Aceptar**.

    Aparece el nombre del certificado en la lista Certificados instalados.

Vínculos relacionados

Configurar un VPN SSL para soporte técnico para partners de Avaya en la página 37

Configuración de códigos cortos

El sistema IP Office le permite configurar códigos cortos. Estos códigos cortos activan una acción específica cuando marca el código corto en un deskphone conectado al sistema IP Office. Para obtener información sobre cómo programar los botones del teléfono con códigos cortos, consulte la documentación de IP Office Manager.

Puede configurar códigos cortos y usarlos para activar y desactivar el servicio VPN SSL. Cuando usa los códigos cortos para activar o desactivar el servicio VPN SSL, el servicio se mantiene aprovisionado en el sistema; los códigos cortos activan el servicio o lo dejan en estado de respaldo.

El sistema IP Office incluye un conjunto de funciones previamente definidas a las que puede acceder a través de códigos cortos. Puede usar las siguientes funciones previamente definidas para crear códigos cortos que activan y desactivan el servicio VPN SSL:

- Borrar servicio nocturno de grupo de búsqueda: activa el servicio VPN SSL
- Establecer servicio nocturno de grupo de búsqueda: activa el servicio VPN SSL

Estos códigos abreviados se encuentran disponibles para uso interno y debe marcarlos desde un teléfono que esté conectado al sistema IP Office. Si desea usar los códigos cortos desde un teléfono externo, puede configurar una atención automática. La operadora automática le permite marcar en el sistema IP Office desde un número de teléfono externo y activar los códigos cortos utilizando un sistema de menú.

Vínculos relacionados

Configurar un VPN SSL para soporte técnico para partners de Avaya en la página 37
Configuración de un código corto para permitir el servicio VPN SSL en la página 41
Configuración de un código corto para desactivar el servicio VPN SSL en la página 42
Configuración de una operadora automática en la página 43

Configuración de un código corto para permitir el servicio VPN SSL

Use este procedimiento para configurar un código corto que active el servicio VPN SSL cuando se marque el código desde un deskphone conectado al sistema IP Office.

Procedimiento

1. En la lista de navegación, seleccione **Código corto**.

   Aparece la lista de códigos cortos predeterminados.

2. Haga clic con el botón secundario y seleccione **Nuevo**.

   Aparece la ficha Código corto.

3. En el campo **Código**, ingrese ***775*x*1**, donde la *x* representa una instancia del servicio VPN SSL, que va de 1 a 9. Por ejemplo, si tiene dos instancias configuradas del servicio VPN SSL, y está configurando códigos cortos para la primera instancia, ingrese ***77511**.

   Nota:

   Puede asignar números diferentes al código corto. Para que sea más sencillo de usar, Avaya recomienda que use *775, que representa *SSL en un teclado de marcación.

4. En la lista **Función**, seleccione **Borrar servicio nocturno de grupo de búsqueda**.

5. En el campo **Número de teléfono**, ingrese el nombre del servicio VPN SSL entre comillas. Por ejemplo, si el nombre del servicio es Service1, ingrese `"Service1"`.

   Use el nombre del servicio VPN SSL que ingresó cuando creó el servicio VPN SSL. Consulte Configuración del servicio en la página 38 VPN SSL para obtener información acerca de esta configuración.

6. Haga clic en **Aceptar**.

7. Haga clic en el icono **Guardar** para guardar los cambios de la configuración.

Vínculos relacionados

Configuración de códigos cortos en la página 41

Configuración de un código corto para desactivar el servicio VPN SSL

Use este procedimiento para configurar un código corto que desactive el servicio VPN SSL cuando se marque el código desde un deskphone conectado al sistema IP Office.

Procedimiento

1. En la lista de navegación, seleccione **Código corto**.

   Aparece la lista de códigos cortos predeterminados.

2. Haga clic con el botón secundario y seleccione **Nuevo**.

   Aparece la ficha Código corto.

3. En el campo **Código**, ingrese ***775*x*0**, donde la *x* representa una instancia del servicio VPN SSL, que va de 1 a 9. Por ejemplo, si tiene dos instancias configuradas del servicio VPN SSL, y está configurando códigos cortos para la primera instancia, ingrese ***77510**.

Nota:

Puede asignar números diferentes al código corto. Para que sea más sencillo de usar, Avaya recomienda que use *775, que representa *SSL en un teclado de marcación.

4. En la lista **Función**, seleccione **Establecer servicio nocturno de grupo de búsqueda**.
5. En el campo **Número de teléfono**, ingrese el nombre del servicio VPN SSL entre comillas. Por ejemplo, si el nombre del servicio es Service1, ingrese `"Service1"`.

   Use el nombre del servicio VPN SSL que ingresó cuando creó el servicio VPN SSL. Consulte Configuración del servicio VPN SSL en la página 38 para obtener información acerca de esta configuración.
6. Haga clic en **Aceptar**.
7. Haga clic en el icono **Guardar** para guardar los cambios de la configuración.

Vínculos relacionados

Configuración de códigos cortos en la página 41

Configuración de una operadora automática

Use este procedimiento para configurar una operadora automática. La operadora automática le permite acceder al sistema IP Office desde un número de teléfono interno o externo, y usar un menú para activar o desactivar el servicio VPN SSL.

Antes de empezar

Debe configurar códigos cortos. Consulte Configuración de códigos cortos en la página 41.

Si está utilizando Avaya Voicemail Pro, debe configurar un módulo para transferencia asistida antes de comenzar este procedimiento. Para obtener más información, consulte *Administración de* Voicemail Pro (15–601063).

Acerca de esta tarea

En este procedimiento, usted crea una operadora automática y luego asigna llamadas entrantes a la operadora automática. Este ejemplo usa 0 para activar el servicio VPN SSL y 1 para desactivarlo, pero puede asignar estas funciones a cualquier tecla del teclado de marcación.

Procedimiento

1. Seleccione una de las siguientes opciones:
   - Si usa Embedded Voicemail, seleccione **Operadora automática** en la lista de navegación.
   - Si usa Voicemail Pro, comience este procedimiento en el paso 12 en la página 44.
2. Haga clic con el botón secundario y seleccione **Nuevo**.
3. En el campo **Nombre**, ingrese el nombre para la operadora automática.
4. Seleccione la ficha **Acciones**.
5. Seleccione la entrada para la tecla **0** y haga clic en el botón **Editar**.

6. En la lista **Acción**, seleccione una de las siguientes opciones:
   - Seleccione la transferencia **Transferencia normal**.
   - Seleccione **Transferencia**.
7. En la lista **Destino**, escriba el código corto que configuró para activar el servicio y haga clic en **Aceptar**.
8. Seleccione la entrada para la tecla **1** y haga clic en el botón **Editar**.
9. En la lista **Acción**, seleccione una de las siguientes opciones:
   - Seleccione la transferencia **Transferencia normal**.
   - Seleccione **Transferencia**.
10. En la lista **Destino**, escriba el código corto que configuró para desactivar el servicio y haga clic en **Aceptar**.
11. Haga clic en el icono **Guardar** para guardar los cambios de la configuración.
12. En la lista de navegación, seleccione **Ruta de llamada entrante**.
13. En la ficha **Estándar**, configure el campo **Capacidad del portador** en **Cualquier llamada de voz**.
14. En la lista **Id. de grupo de líneas**, seleccione la línea que desea usar para activar y desactivar el servicio VPN SSL.
15. Seleccione la ficha **Destino**.
16. Elija una de las siguientes opciones:
    - Si usa Embedded Voicemail, seleccione la operadora automática que configuró desde la lista **Destino**.
    - Si usa Voicemail Pro, escriba `VM:<name>` en la lista **Destino**, donde `<name>` es el nombre del módulo Voicemail Pro.
17. Haga clic en **Aceptar**.
18. Haga clic en el icono **Guardar** para guardar los cambios de la configuración.

Pasos siguientes

Puede registrar indicaciones para la operadora automática. Para obtener más información acerca de cómo registrar indicaciones, consulte la documentación para el sistema de correo de voz. Si está usando Embedded Voicemail, consulte la *Instalación de Embedded Voicemail*. Si está usando Voicemail Pro, consulte *Administración de Voicemail Pro*.

Vínculos relacionados

Configuración de códigos cortos en la página 41

Cómo configurar notificaciones de alarma

La configuración de la administración de fallas es opcional para el servicio de VPN SSL. Si configura la administración de fallas, puede configurar los filtros para determinar los tipos de eventos que se le notifican. Por ejemplo, puede recibir notificaciones sobre fallas relacionadas con el servicio de VPN SSL o puede recibir notificaciones de fallas relacionadas con el sistema IP Office.

Cuando configure la administración de fallas, debe definir los destinos de las alarmas donde se informen fallas del sistema. Puede configurar los siguientes destinos para el informe de alarmas:

- Trampas de SNMP informadas en una LAN local o en un servidor remoto
- notificaciones por correo electrónico informadas a un servidor SMTP en una LAN local o un servidor SMTP remoto
- entradas de registro del sistema informadas en una LAN local o en un servidor remoto

Los destinos de alarmas que configura dependen del modo de operación que utiliza. La siguiente tabla muestra listas de destinos de alarmas compatibles con cada modo.

Destino de alarma	Modo de operación			
	Essential Edition	IP Office Server Edition	Sistema de expansión Server Edition	Basic Edition
Trampas de SNMP				
SNMP en una LAN local	✔	✔	✔	✔
SNMP en un servicio VPN SSL	✔	✔	✔	✔
Notificaciones por correo electrónico				
Servidor SMTP en una LAN local	✔	✔	✔	—
Servidor SMTP en un túnel VPN SSL	✔	✔	✔	—
Entradas de registro del sistema				
Servidor de registro del sistema en una LAN local	✔	✔	✔	—
Servidor de registro del sistema en un túnel VPN SSL	✔	✔	✔	—

Vínculos relacionados

Configurar un VPN SSL para soporte técnico para partners de Avaya en la página 37
Configuración de los destinos de captura SNMP en la página 46
Configuración de notificaciones de alarma de correo electrónico en la página 47

Configuración de las entradas de registro del sistema en la página 48

Configuración de los destinos de captura SNMP

Use el siguiente procedimiento para reportar las fallas de sistemas como capturas SNMP. Puede configurar filtros para determinar los tipos de eventos que generan capturas SNMP. Por ejemplo, puede generar capturas SNMP para fallas relacionadas con el servicio VPN SSL, o puede generar capturas SNMP para fallas relacionadas con el sistema IP Office.

Antes de empezar

Cuando defina una dirección IP de destino para un evento de fallas, el sistema usa una tabla de enrutamiento IP para determinar qué interfaz usar cuando envíe el evento de falla. El destino debe ser una dirección IPv4 para que la captura SNMP se enrute correctamente al servidor de administración de fallas.

Debe configurar un oyente de capturas en la computadora de destino donde se reportan las capturas SNMP.

Procedimiento

1. En la lista de navegación, haga clic en **Sistema** y seleccione la ficha **Eventos del sistema**.

   Manager muestra una ficha **Configuración** y una ficha **Alarmas**.
2. En la ficha **Configuración**, seleccione la opción **SNMP habilitado**.
3. En el campo **Comunidad**, ingrese `public`.
4. En la ficha **Alarmas**, haga clic en **Agregar**.
5. Seleccione **Captura** e ingrese una dirección de destino para las capturas SNMP en el campo **Dirección IP**. .
6. Ingrese un número de puerto o use el número de puerto predeterminado (162).
7. En el campo **Comunidad**, ingrese `public`.
8. En la lista **Eventos**, elija el filtro del evento:
   - Seleccione **Servicio** para generar las capturas SNMP para fallas relacionadas con el servicio VPN SSL.
   - Seleccione los eventos relacionados con la operación del sistema IP Office para los que desea generar capturas SNMP. Para obtener información de estas opciones, consulte *IP Office Manager*.
9. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.
10. Haga clic en **Aceptar** en la ficha Alarmas.
11. Haga clic en el icono **Guardar** para guardar los cambios de la configuración.

Vínculos relacionados

Cómo configurar notificaciones de alarma en la página 45

Configuración de notificaciones de alarma de correo electrónico

Use el siguiente procedimiento para recibir notificaciones de correo electrónico sobre fallas cuando se presentan. Puede ajustar los filtros para determinar los tipos de eventos que se le notificarán. Por ejemplo, puede recibir notificaciones sobre fallas relacionadas con el servicio de VPN SSL o puede recibir notificaciones de fallas relacionadas con el sistema IP Office.

Antes de empezar

Debe configurar un servidor de correo electrónico SMTP en la computadora que está usando para la administración de fallas. También debe configurar un cliente de correo electrónico en la computadora donde desea recibir las notificaciones de correo electrónico.

Cuando defina una dirección de destino para un evento de fallas, el sistema usa una tabla de enrutamiento IP para determinar qué interfaz usar cuando envíe el evento de falla. El destino debe ser una dirección IPv4 para que la notificación se enrute correctamente al servidor de administración de fallas.

Procedimiento

1. En la lista de navegación, haga clic en **Sistema** y seleccione la ficha **Eventos del sistema**.

   Manager muestra una ficha **Configuración** y una ficha **Alarmas**.
2. En la ficha **Alarmas**, haga clic en **Agregar**.
3. Seleccione la opción **Correo electrónico** e ingrese la dirección donde desea recibir las notificaciones de correo electrónico en el campo **Correo electrónico**.
4. En la lista **Eventos**, elija el filtro del evento:
   - Seleccione **Servicio** para recibir notificaciones acerca de las fallas relacionadas con el servicio VPN SSL.
   - Seleccione los eventos relacionados con la operación del sistema IP Office del que desea recibir notificaciones. Para obtener información de estas opciones, consulte *IP Office Manager*.
5. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.
6. Haga clic en **Aceptar** en la ficha Alarmas.
7. Seleccione la ficha **SMTP**.
8. En el campo **Dirección IP**, ingrese la dirección IP del servidor SMTP.
9. En el campo **Puerto**, ingrese el número de puerto del servidor SMTP.
10. En el campo **Dirección de origen**, ingrese la dirección de correo electrónico que el sistema IP Office usará para enviar notificaciones de correo electrónico.
11. Seleccione **Servidor requiere autenticación**.
12. En los campos **Nombre de usuario** y **Contraseña**, ingrese las credenciales requeridas para iniciar sesión en el servidor SMTP.
13. Haga clic en **Aceptar**.

14. Haga clic en el icono **Guardar** para guardar los cambios de la configuración.

Vínculos relacionados

Cómo configurar notificaciones de alarma en la página 45

Configuración de las entradas de registro del sistema

Use el siguiente procedimiento para reportar las fallas de sistemas como entradas de registro del sistema. Puede ajustar los filtros para determinar los tipos de eventos que se notificarán. Por ejemplo, puede reportar fallas relacionadas con el servicio VPN SSL o puede reportar fallas relacionadas con el sistema IP Office.

Antes de empezar

Debe configurar un cliente de registros del sistema en el servidor donde desea que se informen las fallas del sistema.

Cuando defina una dirección IP de destino para un evento de fallas, el sistema usa una tabla de enrutamiento IP para determinar qué interfaz usar cuando envíe el evento de falla. El destino debe ser una dirección IPv4 para que la notificación se enrute correctamente al servidor de administración de fallas.

Procedimiento

1. En la lista de navegación, haga clic en **Sistema** y seleccione la ficha **Eventos del sistema**.

   Manager muestra una ficha **Configuración** y una ficha **Alarmas**.
2. En la ficha **Alarmas**, haga clic en **Agregar**.
3. Seleccione la opción **Registro del sistema** e ingrese la dirección IP del servidor donde el cliente de entradas de registro está configurado en el campo **Dirección IP**.
4. Ingrese el número de puerto del servidor donde el cliente de entradas de registro del sistema está configurado en el campo **Puerto**.
5. En la lista **Eventos**, elija el filtro del evento:
   - Seleccione **Servicio** para reportar fallas relacionadas con el servicio VPN SSL.
   - Seleccione los eventos relacionados con la operación del sistema IP Office del que desea recibir notificaciones. Para obtener información de estas opciones, consulte *IP Office Manager*.
6. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.
7. Haga clic en **Aceptar** en la ficha **Alarmas**.
8. Haga clic en el icono **Guardar** para guardar los cambios de la configuración.

Vínculos relacionados

Cómo configurar notificaciones de alarma en la página 45

Configuración de una ruta estática

Cuando configura rutas de tunelización divididas en el AVG, el sistema IP Office recibe la información de enrutamiento dinámicamente para el túnel cuando el servicio VPN SSL se conecta con el AVG. Sin embargo, también tiene la opción de configurar una ruta estática. Esta sección proporciona información que le ayuda a determinar si configurará una ruta estática, y ofrece un procedimiento para configurarla.

Cuando configura una ruta estática, el sistema usa la información de ruta IP configurada Manager para determinar el destino para el tráfico reenviado. Puede definir el servicio VPN SSL como el destino.

Use una ruta estática cuando:

- las rutas de tunelización divididas no son advertidas por el AVG y necesita enviar tráfico a través del túnel
- el servicio VPN SSL no está conectado al AVG y usted desea poner en cola el tráfico que se reenviará a través del túnel cuando la conexión esté restaurada

Antes de empezar

Antes de comenzar, debe tener la siguiente información:

- la dirección de la subred remota; esta es la subred ubicada en la red privada donde está instalado el AVG
- la máscara de subred aplicada a la dirección de subred
- el nombre de servicio de VPN SSL que desea usar para enviar tráfico a esta subred remota

Procedimiento

1. En la lista de navegación, seleccione **ruta IP**.
2. Haga clic con el botón secundario y seleccione **Nuevo**.
3. En el campo **Dirección IP**, ingrese la dirección de la subred remota ubicada en el sitio donde está instalado el AVG.
4. En el campo **Máscara de subred**, ingrese la máscara de subred aplicada a la subred remota.
5. En el campo **Dirección IP de puerta de enlace**, asegúrese de que la dirección IP de la puerta de enlace esté configurada en 0.0.0.0.
6. En la lista **Destino**, seleccione el nombre del servicio VPN SSL.

Vínculos relacionados

Configurar un VPN SSL para soporte técnico para partners de Avaya en la página 37

Capítulo 7: Configuración de Avaya Partner SSL VPN mediante SDK

Los proveedores de servicios de terceros pueden utilizar su propia Avaya VPN Gateway para implementar el servicio técnico al cliente remoto mediante la tecnología VPN SSL de IP Office.

Para el servicio técnico del proveedor de servicios de terceros, el VPN SSL se puede configurar mediante el Kit de desarrollo de software (SDK). El SDK está diseñado para permitir que los socios configuren sus propios AVG mediante la automatización de algunos aspectos del registro de IP Office y el proceso de integración, o todos ellos. El proceso automatizado reemplaza los procedimientos utilizados para la configuración manual.

Opciones de SDK

Existen dos SDK de integración:

- SDK de integración
- SDK Express de integración

SDK de integración:

Para cada nueva instalación de IP Office, SDK de integración se ejecuta en el servidor web del socio para generar el archivo xml de integración cargado en IP Office mediante Web Manager. Mediante este proceso, se configura el túnel VPN SSL desde IP Office del cliente en el AVG del socio.

SDK Express de integración:

SDK Express de integración se puede ejecutar desconectado, sin una conexión a Internet. Al ejecutar SDK, IP Office se integra inmediatamente, luego recopila todos los registros y archivos de proceso de integración relevantes en un archivo zip. En este punto, el túnel VPN SSL intenta conectarse al AVG, pero se produce un error de autenticación. Cuando el socio procesa el contenido del archivo zip para crear las credenciales de VPN SSL del sitio del cliente asociado, AVG acepta el establecimiento del túnel VPN SSL.

Códigos abreviados

IP Office admite diversas instancias del servicio VPN SSL. Esto significa que pueden existir dos servicios VPN SSL simultáneos conectados activamente: uno en AVG de Avaya Support y el otro en AVG del socio. Cuando dos servicios VPN SSL están configurados en IP Office, Avaya recomienda utilizar las convenciones de nombre y enumeración de código abreviado que se indican a continuación para el servicio Avaya Support SSL VPN y el servicio Partner SSL VPN. Las convenciones se basan en lo siguiente:

- Los dígitos 775 = SSL en un teclado de marcación telefónico.

- El valor del cuarto dígito de 1 o 2 es para la instancia de servicio.
- En cuanto al valor del quinto dígito, 1 = habilitado y 0 = deshabilitado.

Servicio Avaya Support SSL VPN:

- Nombre del servicio: AVAYA_SUPPORT.
- Código abreviado para habilitar el servicio AVAYA_SUPPORT: 77511.
- Código abreviado para deshabilitar el servicio AVAYA_SUPPORT: 77510.

Servicio Partner SSL VPN:

- Nombre del servicio: BP_SUPPORT.
- Código abreviado para habilitar el servicio BP_SUPPORT: 77521.
- Código abreviado para deshabilitar el servicio BP_SUPPORT: 77520.

Requisitos previos

- En la máquina donde se ejecutará el SDK, debe tener instalado Java 1.6 o una versión posterior.
- La dirección IP del túnel no debe ser entre 172.22.0.0 y 172.25.255.255. Este intervalo de dirección está reservado para Avaya Support.

Vínculos relacionados

Descarga del SDK en la página 51
Descarga del archivo de inventario de IP Office en la página 51
Cómo utilizar el SDK de integración en la página 52
Cómo utilizar SDK Express de integración en la página 55

Descarga del SDK

Puede descargar el SDK de integración y el SDK Express de integración en el sitio web de Avaya DevConnect en http://www.devconnectprogram.com/

Vínculos relacionados

Configuración de Avaya Partner SSL VPN mediante SDK en la página 50

Descarga del archivo de inventario de IP Office

Este procedimiento proporciona el método manual para descargar el archivo de inventario de IP Office utilizando Web Manager. SDK Express de integración ofrece las herramientas necesarias para automatizar la descarga sin uso de Web Manager. Para obtener información, consulte la documentación que se incluye con SDK Express de integración.

Procedimiento

1. Inicie sesión en Web Manager. En un explorador web, introduzca la dirección IP del sistema IP Office en el formato `http://<ip_address>/index.html`.

   Se abre la página de índice del servidor.
2. Haga clic en **IP Office Web Manager**.
3. En la página de inicio de sesión, introduzca un nombre de usuario y contraseña, y haga clic en **Iniciar sesión**.
4. En la página Solución, haga clic en el menú del servidor que se encuentra a la derecha del servidor y seleccione **Integración**.
5. En la página Integración, haga clic en **Obtener archivo de inventario**.

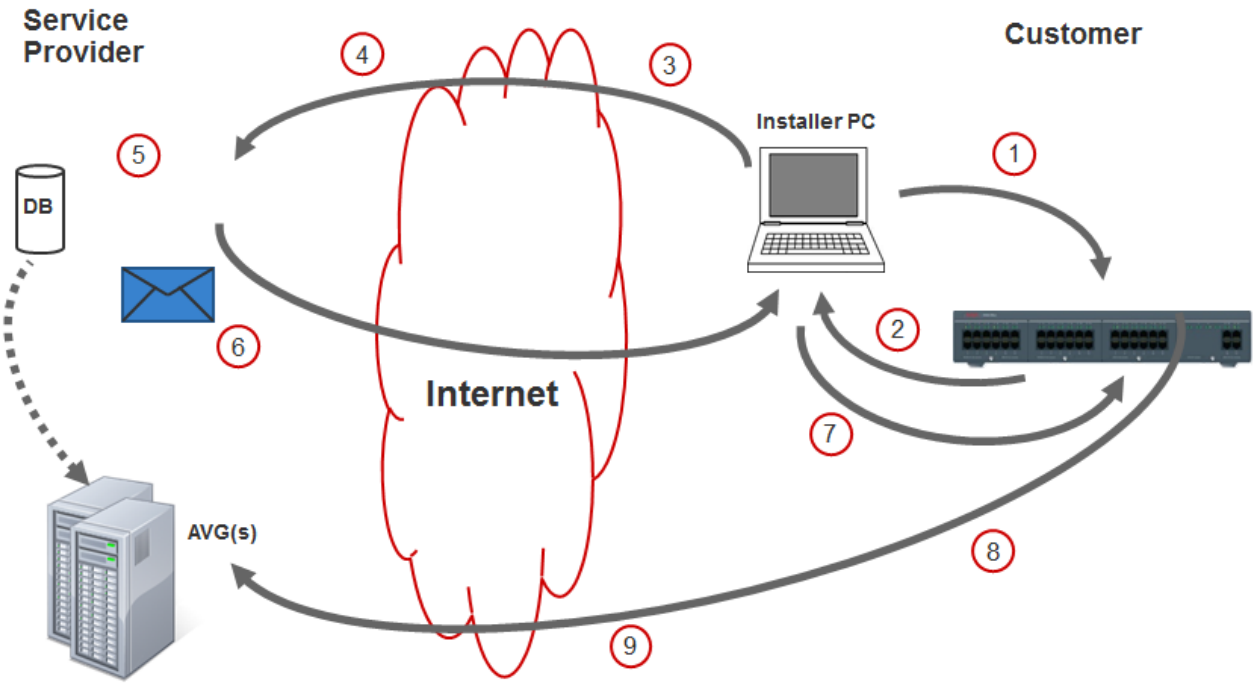
   El archivo de inventario se descarga en la PC del instalador.

Vínculos relacionados

[Configuración de Avaya Partner SSL VPN mediante SDK](#) en la página 50

Cómo utilizar el SDK de integración

Proceso de configuración de VPN SSL mediante el SDK de integración



1	Defina la siguiente configuración de IP Office: • ID del sistema • Licencias • Interfaces LAN • Servidor DNS
2	En el sitio del cliente, descargue el archivo XML de inventario de IP Office en la PC del instalador.
3	Cargue el archivo de inventario en el sitio del socio.
4	Almacene las credenciales de VPN SSL en la base de datos.
5	Ejecute la herramienta SDK de integración.
6	Envíe por correo electrónico o cargue el archivo xml de integración en la PC del instalador.
7	Cargue el archivo xml de integración en IP Office.
8	El servicio VPN SSL se conecta a AVG.
9	Use SSA para verificar la conectividad de VPN SSL.

Vínculos relacionados

Configuración de Avaya Partner SSL VPN mediante SDK en la página 50
Almacenamiento de las credenciales de VPN SSL en la base de datos de AVG en la página 53
Cómo ejecutar el SDK de integración en la página 53
Cómo cargar el archivo de integración y verificar el VPN SSL en la página 54

Almacenamiento de las credenciales de VPN SSL en la base de datos de AVG

Si utiliza la base de datos de AVG local, agregue las credenciales en la interfaz de configuración de AVG.

Si utiliza la base de datos de LDAP o una base de datos de RADIUS, use la interfaz correspondiente para agregar las credenciales a la base de datos.

Vínculos relacionados

Cómo utilizar el SDK de integración en la página 52

Cómo ejecutar el SDK de integración

El SDK se puede ejecutar de dos maneras:

- Invoque el contenedor de la línea de comandos de script por lote de DOS de integración con los parámetros relevantes y los nombres de archivos de entrada/salida.
- Utilice las API de JAVA publicadas.

Para obtener información, consulte la guía del desarrollador de SDK incluida en el archivo zip de SDK.

La salida de SDK es el archivo de integración xml. Transfiera el archivo a la PC del instalador en el sitio del cliente.

Vínculos relacionados

Cómo utilizar el SDK de integración en la página 52

Cómo cargar el archivo de integración y verificar el VPN SSL

Procedimiento

1. Inicie sesión en Web Manager. En un explorador web, introduzca la dirección IP del sistema IP Office en el formato `http://<ip_address>/index.html`.

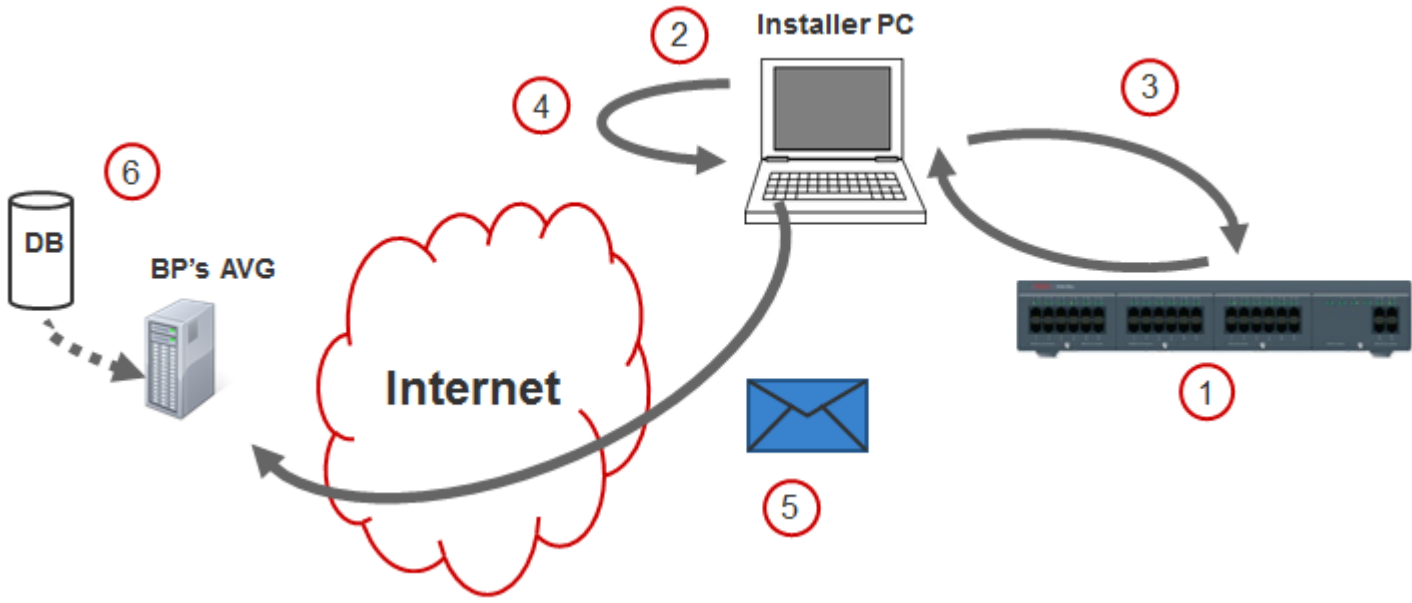
   Se abre la página de índice del servidor.
2. Haga clic en **IP Office Web Manager**.
3. En la página de inicio de sesión, introduzca un nombre de usuario y contraseña, y haga clic en **Iniciar sesión**.
4. En la página Solución, haga clic en el menú del servidor que se encuentra a la derecha del servidor y seleccione **Integración**.
5. En la página Integración, en el panel número 3, haga clic en **Examinar** y navegue hasta la ubicación del archivo xml de integración.
6. Haga clic en **Cargar**.
7. Verifique la conectividad de VPN SSL con la aplicación SSA.

Vínculos relacionados

Cómo utilizar el SDK de integración en la página 52

Cómo utilizar SDK Express de integración

Proceso de configuración de VPN SSL mediante SDK Express de integración



1	Defina la siguiente configuración de IP Office: • ID del sistema • Licencias • Interfaces LAN • Servidor DNS
2	Ejecute la herramienta SDK Express de integración.
3	La herramienta SDK Express de integración intercambia archivos con IP Office.
4	La herramienta SDK Express de integración crea un archivo zip que contiene todos los archivos requeridos para la integración. Repita los pasos 1 a 3 para todos los sistemas de IP Office.
5	Transfiera los archivos zip de manera segura al sitio del socio. Por ejemplo, utilice un servicio de hospedaje de archivos o un servicio de almacenamiento en la nube para transferir el archivo.
6	Procese todos los archivos de integración para crear el túnel VPN SSL.

Vínculos relacionados

Configuración de Avaya Partner SSL VPN mediante SDK en la página 50
Cómo ejecutar SDK Express de integración en la página 56
Procesamiento de archivos zip de SDK Express de integración en la página 56

Cómo ejecutar SDK Express de integración

Este procedimiento proporciona información sobre la interfaz de usuario de la línea de comandos predeterminada. Además, se proporciona una API de JAVA para facilitar la creación de una interfaz de usuario alternativa. La interfaz de la línea de comandos predeterminada recopila la información utilizada para crear el archivo de propiedades como una entrada en la API de JAVA.

Por ejemplo, se podría crear una aplicación móvil con un formulario para recopilar la información necesaria. A continuación, se invoca la API de JAVA que luego se comunica con IP Office para completar el proceso de registro y crear el archivo zip resultante.

Procedimiento

1. Modifique el archivo `default_parameters.txt`.
2. Ejecute el archivo `sslvpnOnboardingExpress.bat` de SDK Express de integración utilizando los parámetros de comando correctos.

   El SDK Express de integración crea un archivo zip que contiene los archivos requeridos para configurar el VPN SSL para IP Office. El archivo zip está almacenado en la carpeta `sslvpn_OUTPUT`.

Pasos siguientes

Transfiera los archivos zip de manera segura al sitio del socio. Por ejemplo, utilice un servicio de hospedaje de archivos o un servicio de almacenamiento en la nube para transferir el archivo.

Vínculos relacionados

Cómo utilizar SDK Express de integración en la página 55

Procesamiento de archivos zip de SDK Express de integración

Una vez que el archivo zip generado por el SDK se transfirió al sitio del socio, las credenciales del túnel VPN SSL para la instalación del cliente se configuran en AVG, Radius o LDAP. Una vez completo este proceso, el túnel VPN SSL se conectará con AVG correctamente.

Si usted utiliza un servicio de almacenamiento de archivos en nube compartida, el procesamiento del archivo zip en el sitio del socio se puede realizar en segundos. Esto permite que el instalador inicie SSA inmediatamente después de ejecutar el script de Express de integración para verificar que la conectividad del túnel VPN SSL sea funcional.

Vínculos relacionados

Cómo utilizar SDK Express de integración en la página 55

Capítulo 8: Reglas de la dirección de red y la conversión de puerto (NAPT)

Utilice un servicio de VPN SSL y las reglas de dirección de red y conversión de puerto (NAPT) para establecer las sesiones de comunicación remota con dispositivos LAN como un módulo UCM de IP Office. Para conectar un dispositivo LAN a una red IP Office privada, el proveedor de servicios de soporte técnico inicia una aplicación de comunicación en una PC ubicada en el sitio del proveedor de servicios remoto y especifica los siguientes parámetros de configuración para la sesión:

- la dirección IP de un túnel VPN SSL
- el número de puerto externo para el dispositivo LAN

IP Office utiliza reglas de NAPT para asignar la dirección IP del túnel y el número de puerto externo en la dirección IP correcta y el número de puerto en la red privada.

Vínculos relacionados

Configuración de las reglas NAPT en la página 57
Eliminación de una regla NAPT en la página 58

Configuración de las reglas NAPT

Realice este procedimiento en la interfaz de Manager. Puede configurar hasta 64 reglas.

Cuando configure una regla NAPT, debe seleccionar un tipo de aplicación. Están disponibles las siguientes opciones de aplicación:

- Personalizar
- VMPro
- one-X Portal
- SSH
- TELNET
- RDP (Protocolo de escritorio remoto)
- Web Control

Puede usar el ajuste **Personalizado** para configurar una regla NAPT para el nuevo tipo de aplicación. También puede usar la configuración **Personalizada** con un **Número de puerto**

externo modificado para abrir dos sesiones de comunicación concurrentes utilizando la misma aplicación para conectar el mismo dispositivo LAN. Por ejemplo, para activar las sesiones de SSH concurrentes en la misma dirección IP, las dos reglas NAPT serán similares a lo siguiente.

Aplicación	Protocolo	Número de puerto externo	Dirección IP interna	Número de puerto interno
SSH	TCP	22	192.168.40.1	22
Personalizar	TCP	221	192.168.40.1	22

Procedimiento

1. En la lista de navegación, seleccione **Servicio**.
2. En la lista **Servicio**, seleccione el servicio VPN SSL en que desea configurar las reglas NAPT.
3. En el panel de detalles del servicio, seleccione la ficha **NAPT**.
4. En **Aplicación**, abra la lista desplegable y seleccione un tipo de aplicación.

   El campo **Protocolo** y los campos **Número de puerto** se completan automáticamente con los valores predeterminados.
5. (Opcional) Si desea configurar una aplicación **Personalizada**, modifique el campo **Número de puerto externo**.
6. Repita los pasos 4 y 5 para configurar reglas adicionales.

Vínculos relacionados

Reglas de la dirección de red y la conversión de puerto (NAPT) en la página 57

Eliminación de una regla NAPT

Procedimiento

Para eliminar una regla NAPT, use la columna vacía de la izquierda de la tabla. Haga clic con el botón secundario en la celda vacía junto a la regla que desea eliminar y seleccione el icono de eliminación.

Vínculos relacionados

Reglas de la dirección de red y la conversión de puerto (NAPT) en la página 57

Capítulo 9: Verificar la conexión entre IP Office y AVG

Utilice los procedimientos de este capítulo para probar la conexión entre el sistema IP Office y AVG.

Vínculos relacionados

Verificación de la conexión con SysMonitor en la página 59
Verificación de la implementación AVG VPN SSL utilizando System Status Application en la página 60
Verificación de la conexión utilizando AVG BBI en la página 60
Envío de una alarma de prueba en la página 61

Verificación de la conexión con SysMonitor

Puede usar System Status Application (SSA) para verificar que el túnel VPN SSL está en servicio. Inicie la SSA y verifique que los ajustes de la configuración de túnel estén en la lista.

También puede seguir los pasos a continuación para usar SysMonitor para verificar la conexión VPN SSL entre el sistema IP Office y el AVG.

Procedimiento

1. Seleccione **Start > Programs > IP Office > Monitor**.

   La aplicación SysMonitor se conecta con el servidor IP Office y muestra un registro del sistema.

2. Seleccione las opciones **Filters > Trace** (Filtros > Seguimiento) y haga clic en la ficha **VPN**.

3. En el área VPN SSL, verifique que **Session** (Sesión) y **Session State** (Estado de la sesión) estén habilitadas. Haga clic en **Aceptar**.

   El registro de SysMonitor muestra la actividad para el servicio VPN SSL bajo el nombre que configuró para el servicio.

4. Ubique el nombre del servicio y revise la siguiente información:

Cambio de estado de la sesión	Cuando active el servicio VPN SSL, el estado de sesión progresa por las siguientes etapas: • resolución del nombre de dominio • inicio de la sesión • conexión de la dirección IP de IP Office en la dirección IP de la puerta de enlace del VPN Si IP Office no puede resolver el nombre de dominio, aparece el siguiente mensaje de error: “DNS failed to resolve host name <x.x.x> and reached MAX retries. Restart session.” (DNS no pudo resolver el nombre de host <x.x.x> y llegó a las entradas MAX. Reinicie sesión)

Vínculos relacionados

Verificar la conexión entre IP Office y AVG en la página 59

Verificación de la implementación AVG VPN SSL utilizando System Status Application

Realice estas acciones para probar la implementación de AVG SSL.

1. Inicie IP Office System Status Application (SSA) y verifique que el túnel VPN SSL esté **En servicio** y que se muestre **Dirección IP de túnel**.
2. Haga ping en IP Office de manera remota. Desde la computadora Agente de servicio, inicie una ventana de comando y ejecute un comando de ping utilizando la dirección IP del túnel. El ping debe ser correcto.

Vínculos relacionados

Verificar la conexión entre IP Office y AVG en la página 59

Verificación de la conexión utilizando AVG BBI

Procedimiento

1. Inicie sesión en AVG BBI.
2. En el panel de navegación de la izquierda, expanda **Monitor**.
3. En **Monitor**, seleccione **Usuarios**.
4. La columna **IP de origen** muestra:
   - la dirección IP de IP Office

- la dirección IP del túnel VPN SSL asignada al usuario local.

Vínculos relacionados

Verificar la conexión entre IP Office y AVG en la página 59

Envío de una alarma de prueba

Use este procedimiento para enviar una alarma de prueba desde la System Status Application (SSA). Use la alarma de prueba para generar un evento de falla.

Antes de empezar

Debe tener definido un destino para la alarma. Cuando defina una dirección IP de destino para el evento de fallas, el sistema usa una tabla de enrutamiento IP para determinar qué interfaz usar cuando envíe el evento de falla.

Procedimiento

1. Inicie SSA utilizando uno de los siguientes métodos:
   - Inicie SSA desde el DVD de administración IP Office.
   - Seleccione **Inicio > Programas > IP Office > System Status**.
   - Desde Manager o IP Office Manager for Server Edition, seleccione **Archivo > Avanzado > System Status**.
2. Seleccione **Alarmas > Servicio** desde la lista de navegación.
3. Haga clic en el botón **Alarma de prueba**.

   La tabla muestra los resultados de la prueba:

Valor	Descripción
Última fecha de error	La fecha y la alarma en que ocurrió la alarma.
Ocurrencias	El número de veces que ocurrió la alarma desde la última vez que se reinició la unidad de control o que se borró.
Descripción de error	Las alarmas de prueba muestran el mensaje “Operator initiated test alarm” (El operador inició alarma de prueba).

   Si configuró un destino de alarma para una captura SNMP, la alarma de prueba genera la siguiente información:

```
Enterprise: ipoGenTraps
Bindings (8)
Binding #1: ipoGTEventStdSeverity.0 *** (int32) major(4)
Binding #2: ipoGTEventDateTime.0 *** (octets)
Binding #3: ipoGTEventDevID.0 *** (octets)
Binding #4: sysDescr.0 *** (octets)
Binding #5: ipoGTEventReason.0 *** (int32) testAlarm(39)
Binding #6: ipoGTEventData.0 *** (octets)
Binding #7: ipoGTEventAlarmDescription.0 *** (octets) Operator initiated test
```

```
alarm - do not process
Binding #8: ipoGTEventAlarmRemedialAction.0 *** (octets) (zero-length)
```

Vínculos relacionados

Verificar la conexión entre IP Office y AVG en la página 59

Capítulo 10: Cómo controlar y administrar el sistema IP Office

Cuando el servicio de VPN SSL está conectado, puede controlar el sistema IP Office de manera remota a través del túnel. También puede administrar y actualizar el sistema IP Office de manera remota. El servicio VPN SSL le permite usar aplicaciones nativas y basadas en la web como si estuvieran directamente conectadas a una interfaz LAN. Esta sección ofrece información acerca de las aplicaciones compatibles y cómo usarlas.

Herramientas de control

Puede usar las siguientes herramientas para controlar el sistema IP Office de manera remota:

- System Status Application (SSA): la System Status Application es una herramienta de diagnóstico que puede usar para controlar el estado de los sistemas IP Office. SSA informa eventos en tiempo real e históricos así como el estado y los datos de configuración.
- SysMonitor: la aplicación SysMonitor muestra la información de operación acerca del sistema IP Office. Puede capturar la información para registrar archivos para análisis.

Herramientas de administración

Puede usar las siguientes herramientas para administrar, actualizar y configurar el sistema IP Office de manera remota:

- IP Office Manager: una aplicación administrativa que le permite ajustar las configuraciones de sistema para los sistemas IP Office Essential Edition.
  - IP Office Manager for Server Edition: cuando inicia IP Office Manager, puede elegir abrir una configuración utilizando el modo IP Office Manager for Server Edition. Este modo le permite administrar servidores Server Edition y sistemas de expansión.
- IP Office Basic Edition – Web Manager: una herramienta basada en el explorador que le permite ajustar las configuraciones del sistema para IP Office.

Informes de fallas

Puede usar el servicio VPN SSL para enviar fallas de sistemas a un servidor remoto de administración de fallas ubicado en el sitio del proveedor de servicios donde está instalado AVG. Puede configurar filtros de eventos para determinar qué fallas son compatibles, y configurar los destinos donde se envían las fallas.

Para obtener más información acerca de informes de falla, consulte Configuración de notificaciones de alarma en la página 45

Modos de operación

Las herramientas que puede usar para controlar y administrar el sistema IP Office dependen del modo de operación que utilice. La siguiente tabla muestra las herramientas compatibles en cada modo.

Herramientas	Modo de operación			
	Essential Edition	IP Office Server Edition	Sistema de expansión Server Edition	Basic Edition
SSA	✔	✔	✔	✔
SysMonitor	✔	✔	✔	✔
Manager (Simplificado)	—	—	—	✔
Manager (Estándar) y IP Office Manager for Server Edition	✔	✔	✔	—
Web Manager	—	—	—	✔
Informes de fallas	✔	✔	✔	✔

Vínculos relacionados

Control de IP Office de manera remota utilizando SSA en la página 64
Control de IP Office de manera remota con SysMonitor en la página 65
Control remoto de los dispositivos LAN utilizando el túnel SSL VPN en la página 66
Configuración de IP Office de manera remota con Web Manager en la página 66
Configuración de IP Office de manera remota con Manager en la página 67
Configuración remota de sistemas Server Edition usando IP Office Manager for Server Edition en la página 68
Configuración remota de sistemas Server Edition usando Web Control en la página 69

Control de IP Office de manera remota utilizando SSA

Use este procedimiento para conectar el System Status Application (SSA) en IP Office a través del túnel VPN SSL.

Antes de empezar

El túnel VPN SSL debe estar en servicio y debe tener la siguiente información:

- la dirección IP del túnel VPN SSL

- el nombre de usuario para la cuenta del administrador de IP Office
- la contraseña para la cuenta del administrador IP Office

Procedimiento

1. Inicie SSA utilizando uno de los siguientes métodos:
   - Inicie SSA desde el DVD de administración IP Office.
   - Seleccione **Inicio > Programas > IP Office > System Status**.
   - Desde Manager o IP Office Manager for Server Edition, seleccione **Archivo > Avanzado > System Status**.
2. En el campo **Dirección IP de unidad de control**, ingrese la dirección IP del túnel VPN SSL.
3. En el campo **Nombre de usuario**, ingrese el nombre de usuario para el administrador de IP Office.
4. En el campo **Contraseña**, ingrese la contraseña para la cuenta del administrador de IP Office
5. Haga clic en **Inicio de sesión**.

Vínculos relacionados

Cómo controlar y administrar el sistema IP Office en la página 63

Control de IP Office de manera remota con SysMonitor

Use este procedimiento para conectar la aplicación SysMonitor a través IP Office del túnel VPN SSL.

Antes de empezar

El túnel VPN SSL debe estar en servicio y debe tener la siguiente información:

- la dirección IP del túnel VPN SSL
- la contraseña para la cuenta del administrador IP Office

Procedimiento

1. Seleccione **Start > Programs > IP Office > Monitor.**
2. Haga clic en el icono **Select Unit** (Seleccionar unidad).

   Aparece un cuadro de diálogo.
3. En el campo **Dirección IP de unidad de control**, ingrese la dirección IP del túnel VPN SSL.
4. En el campo **Password** (Contraseña), ingrese la contraseña para la cuenta del administrador de IP Office.

5. Haga clic en el botón de exploración junto al campo **Trace Log Settings Filename** (Nombre de archivo de configuración de registro de seguimiento) y explore la ubicación donde desea guardar el registro de seguimiento y haga clic **Open** (Abrir).
6. Haga clic en **Aceptar**.

Vínculos relacionados

Cómo controlar y administrar el sistema IP Office en la página 63

Control remoto de los dispositivos LAN utilizando el túnel SSL VPN

Utilice este procedimiento para conectarse a un dispositivo LAN en la red IP Office a través del túnel SSL VPN utilizando la dirección de red y la conversión de puerto (NAPT). Puede conectar un dispositivo LAN utilizando una aplicación de comunicación que tenga una regla NAPT configurada. Para obtener información sobre la configuración de las reglas NAPT, consulte Reglas de la dirección de red y la conversión de puerto (NAPT) en la página 57.

Antes de empezar

El túnel VPN SSL debe estar en servicio y debe tener la siguiente información:

- la dirección IP del túnel VPN SSL
- el número de puerto externo configurado en la regla NAPT para el dispositivo LAN al que está conectado

Procedimiento

1. Abra la aplicación de comunicación que está usando para conectarse a un dispositivo LAN a través del túnel SSL VPN.
2. Establezca una sesión de comunicación utilizando la dirección IP del túnel SSL VPN y el número de puerto externo del dispositivo LAN.

Vínculos relacionados

Cómo controlar y administrar el sistema IP Office en la página 63

Configuración de IP Office de manera remota con Web Manager

Use este procedimiento para conectar la aplicación Web Manager a través IP Office del túnel VPN SSL.

Para obtener información sobre cómo usar la aplicación Web Manager para configurar el sistema IP Office, consulte *Avaya IP Office Basic Edition – Web Manager.*

Antes de empezar

El túnel VPN SSL debe estar en servicio y debe tener la siguiente información:

- la dirección IP del túnel VPN SSL
- el nombre de cuenta para la cuenta del administrador de IP Office
- la contraseña para la cuenta del administrador IP Office

Procedimiento

1. En un navegador, ingrese la dirección IP para la administración web utilizando el siguiente formato: `https://10.0.0.1:8443/webmanagement/WebManagement.html`, donde *10.0.0.1* es la dirección IP del túnel VPN SSL.

   Si el navegador responde con una advertencia de seguridad, siga las configuraciones de menú que aparecen para continuar con la conexión.

2. Cuando aparezca el menú de inicio de sesión, ingrese el nombre de usuario y la contraseña para la administración del sistema.
3. Haga clic en **Inicio de sesión**.

   Aparece la página de inicio para la administración web del sistema.

Vínculos relacionados

Cómo controlar y administrar el sistema IP Office en la página 63

Configuración de IP Office de manera remota con Manager

Puede usar Manager para administrar el sistema de IP Office de manera remota a través del túnel VPN SSL. Cuando usa Manager a través del túnel VPN SSL, el descubrimiento automático del sistema IP Office no es compatible. Debe configurar la dirección IP del sistema al que desea conectarse. Use este procedimiento para conectar la aplicación Manager a través IP Office del túnel VPN SSL.

Para obtener información acerca de cómo configurar Manager, y cómo usarlo para administrar un sistema IP Office, consulte *Avaya IP Office Manager*.

Antes de empezar

El túnel VPN SSL debe estar en servicio y debe tener la siguiente información:

- la dirección IP del túnel VPN SSL
- el nombre de cuenta para la cuenta del administrador de IP Office
- la contraseña para la cuenta del administrador de IP Office

Procedimiento

1. Seleccione **Start > Programs > IP Office > Manager**.
2. Haga clic en el icono **Abrir configuración desde IP Office**.

   Aparece el cuadro de diálogo Seleccionar IP Office.

3. Ingrese la dirección IP del túnel VPN SSL en el campo **Dirección de Unidad/Difusión** y haga clic en **Actualizar**.
4. Seleccione el sistema IP Office que desee configurar y haga clic en **Aceptar**.

   Aparece el cuadro de diálogo Inicio de sesión del usuario para servicio de configuración.
5. Ingrese el nombre de usuario para el administrador de IP Office en el campo **Nombre de usuario del servicio**, e ingrese la contraseña para la cuenta del administrador IP Office en el campo **Contraseña de usuario de servicio**. Haga clic en **Aceptar**.

Vínculos relacionados

Cómo controlar y administrar el sistema IP Office en la página 63

Configuración remota de sistemas Server Edition usando IP Office Manager for Server Edition

Puede usar el IP Office Manager for Server Edition para administrar los siguientes sistemas de manera remota a través del túnel VPN SSL:

- Server Edition principal
- Server Edition secundario
- Sistema de expansión Server Edition

Antes de empezar

El túnel VPN SSL debe estar en servicio y debe tener la siguiente información:

- la dirección IP del túnel VPN SSL
- el nombre de cuenta para la cuenta del administrador de IP Office Manager for Server Edition
- la contraseña para la cuenta del administrador IP Office Manager for Server Edition

Acerca de esta tarea

Para configurar sistemas Server Edition de manera remota, debe configurar un servicio VPN SSL entre el AVG y el Server Edition principal. Puede aplicar cambios de configuración en los sistemas Server Edition que están conectados con el Servidor primario. Debe configurar un servicio VPN SSL entre cada sistema Server Edition y el AVG.

Use este procedimiento para conectar el IP Office Manager for Server Edition a través Server Edition principal del túnel VPN SSL.

Para obtener información acerca de cómo usar el IP Office Manager for Server Edition, consulte *Avaya IP Office Manager*.

Procedimiento

1. Seleccione **Start > Programs > IP Office > Manager**.

2. Seleccione **Archivo > Preferencias**.
3. Seleccione **Usar acceso remoto para Multi-Site** y haga clic en **Aceptar**.
4. Haga clic en el icono **Abrir configuración desde IP Office**.

   Aparece el cuadro de diálogo Seleccionar IP Office.
5. Ingrese la dirección IP del túnel VPN SSL en el campo **Dirección de Unidad/Difusión** y haga clic en **Actualizar**.
6. Seleccione el sistema de Server Edition que desea configurar.

   Cuando selecciona el sistema Server Edition, aparece la opción Abrir con Server Edition y se activa de manera predeterminada.
7. Si está conectado a un Server Edition principal y desea realizar cambios de configuración en los sistemas Server Edition que están conectados, seleccione **Utilizar Acceso remoto**. Si está conectado directamente con el sistema Server Edition que desea configurar, no necesita seleccionar esta opción.
8. Haga clic en **Aceptar**.

   Aparece el cuadro de diálogo Inicio de sesión del usuario para servicio de configuración.
9. Ingrese el nombre de usuario para el administrador de IP Office Manager for Server Edition en el campo **Nombre de usuario del servicio**, e ingrese la contraseña para la cuenta del administrador IP Office Manager for Server Edition en el campo **Contraseña de usuario de servicio**. Haga clic en **Aceptar**.
10. En la lista de navegación, seleccione **Red**.

    Aparece la pantalla Resumen. Una tabla al final de la pantalla muestra una lista de todos los sistemas Server Edition.
11. Seleccione el sistema de Server Edition que desea configurar.

    La pantalla Resumen muestra la información de configuración para el sistema seleccionado.

Vínculos relacionados

Cómo controlar y administrar el sistema IP Office en la página 63

Configuración remota de sistemas Server Edition usando Web Control

Puede usar la interfaz Web Control para iniciar el IP Office Manager for Server Edition y administrar los sistemas Server Edition de manera remota a través del túnel VPN SSL.

Puede usar el IP Office Manager for Server Edition para administrar los siguientes sistemas de manera remota a través del túnel VPN SSL:

- Server Edition principal
- Server Edition secundario
- Sistema de expansión Server Edition

Antes de empezar

El túnel VPN SSL debe estar en servicio y debe tener la siguiente información:

- la dirección IP del túnel VPN SSL
- el nombre de cuenta para la cuenta del administrador de Web Control
- la contraseña para la cuenta del administrador de Web Control

Acerca de esta tarea

Para configurar sistemas Server Edition de manera remota, debe configurar un servicio VPN SSL entre el AVG y el Server Edition principal. Puede aplicar cambios de configuración en los sistemas Server Edition que están conectados con el Servidor primario. Debe configurar un servicio VPN SSL entre cada sistema Server Edition y AVG.

Use este procedimiento para iniciar el IP Office Manager for Server Edition a través de la interfaz Web Control y usarlo para conectar un Server Edition principal a través del túnel VPN SSL.

Para obtener información acerca de cómo usar el IP Office Manager for Server Edition, consulte *Avaya IP Office Manager*.

Procedimiento

1. Abra un navegador e ingrese `https://<IP address>:7070`, donde <*IP address*> es la dirección del túnel VPN SSL configurado para el Server Edition principal.
2. Ingrese las credenciales del administrador en los campos **Inicio de sesión** y **Contraseña** y haga clic en **Inicio de sesión**.

   Aparece la pantalla Inicio y muestra una lista de los Servidores Server Edition y los Sistemas de expansión.
3. Haga clic en **Administrar**.

   Se abre el IP Office Manager for Server Edition y muestra un pantalla de resumen.
4. Seleccione **Archivo > Cerrar** para cerrar la configuración.
5. Seleccione **Archivo > Preferencias**.
6. Seleccione **Usar acceso remoto para Multi-Site** y haga clic en **Aceptar**.
7. Haga clic en el icono **Abrir configuración desde IP Office**.

   Aparece el cuadro de diálogo Seleccionar IP Office.
8. Ingrese la dirección IP del túnel VPN SSL en el campo **Dirección de Unidad/Difusión** y haga clic en **Actualizar**.
9. Seleccione el servidor Server Edition.

Cuando selecciona el sistema Server Edition, aparece la opción Abrir con Server Edition y se activa de manera predeterminada.

10. Seleccione **Utilizar Acceso remoto** y haga clic en **Aceptar**.

    Aparece el cuadro de diálogo Inicio de sesión del usuario para servicio de configuración.

11. Ingrese el nombre de usuario para el administrador de IP Office Manager for Server Edition en el campo **Nombre de usuario del servicio**, e ingrese la contraseña para la cuenta del administrador de IP Office Manager for Server Edition en el campo **Contraseña de usuario de servicio**. Haga clic en **Aceptar**.

    Se abre el IP Office Manager for Server Edition y muestra un pantalla de resumen.

12. En la tabla al final de la pantalla, seleccione el Server Edition principal.
13. En la lista **Abrir. . .** del lado derecho de la pantalla, haga clic en **Configuración**.

    Aparece un árbol de navegación para el sistema.

14. Después de configurar el sistema seleccionado y guardar los cambios, seleccione **Red** desde la lista de navegación para volver a la pantalla **Resumen**.
15. Para configurar otros sistemas Server Edition que están conectados al servidor Server Edition principal, seleccione el sistema desde la tabla en la parte inferior de la pantalla Resumen.

    La pantalla Resumen muestra la información de configuración para el sistema seleccionado.

Vínculos relacionados

Cómo controlar y administrar el sistema IP Office en la página 63

Capítulo 10: Actualización IP Office de manera remota

Usted usa el túnel VPN SSL para actualizar el sistema de IP Office desde el sitio del proveedor de servicio. Esta función está disponible cuando actualiza un sistema Versión 8.1 a una versión superior de software.

Cuando usa Manager a través del túnel VPN SSL, el descubrimiento automático del sistema IP Office no es compatible.

Realice este procedimiento en el sitio del proveedor de servicios, utilizando la interfaz Manager instalada en el servidor de agente de servicio. Si está configurando un sistema Server Edition, use el modo IP Office Manager for Server Edition.

Antes de empezar

En el sitio del proveedor de servicios, el DVD de administración IP Office que contiene la nueva versión de software debe instalarse en el PC del Agente de servicio.

El túnel VPN SSL debe estar en servicio y debe tener la siguiente información:

- la dirección IP del túnel VPN SSL

Procedimiento

1. Seleccione **Archivo > Preferencias > Detección**.
2. En el campo **Criterios de búsqueda de IP**, ingrese la dirección IP del túnel VPN SSL y haga clic en **Aceptar**.
3. Seleccione **Archivo > Avanzado > Actualizar**.

   Aparece el asistente de actualización.

   Nota:

   Si aparece un cuadro de diálogo que le indica abrir el archivo de configuración, haga clic en Cancelar y continúe con este paso. No necesita abrir un archivo de configuración antes de realizar una actualización.
4. En el campo **Dirección de Unidad/Difusión**, ingrese la dirección IP del túnel VPN SSL y haga clic en **Actualizar**.

   No ingrese una dirección de difusión. Las direcciones de difusión no son compatibles para actualizaciones remotas en una conexión VPN SSL.

5. Haga clic en la casilla de verificación para seleccionar el sistema que desea actualizar y haga clic en **Actualizar**.

   Después de que se complete la actualización, IP Office se reinicia y el servicio VPN SSL se reconecta automáticamente.

Capítulo 11: Control del servicio VPN SSL

Además de controlar el sistema de IP Office, también puede controlar el túnel VPN SSL. Esta sección ofrece información acerca de las herramientas de control disponible para el servicio VPN SSL y cómo usarlas.

Puede usar las siguientes herramientas para controlar el servicio VPN SSL:

- System Status Application (SSA): System Status Application es una herramienta de diagnóstico que puede usar para controlar el estado del túnel VPN SSL. SSA informa eventos en tiempo real e históricos.
- SysMonitor: la aplicación SysMonitor muestra información de funcionamiento del túnel VPN SSL. Puede capturar la información para registrar archivos para análisis. Use esta herramienta para reunir información solo cuando lo solicite el personal de soporte técnico.
- Informe de fallas: el servicio VPN SSL genera fallas para sus propios componentes cuando ocurre un problema. Puede configurar filtros de eventos para que pueda recibir notificaciones cuando se presenten estas fallas, y puede configurar los destinos cuando se envíen las notificaciones. Para obtener información acerca de cómo configurar filtros de eventos y configurar destinos, consulte Configuración de notificaciones de alarma en la página 45.

Vínculos relacionados

Visualización del estado del túnel en la página 74
Control de alarmas con SSA en la página 77
Solución de problemas del servicio VPN SSL en la página 79

Visualización del estado del túnel

Use el siguiente procedimiento para ver la condición del túnel VPN SSL utilizando System Status Application (SSA).

Procedimiento

1. Inicie SSA utilizando uno de los siguientes métodos:
   - Inicie SSA desde el DVD de administración IP Office.
   - Seleccione **Inicio > Programas > IP Office > System Status**.
   - Desde Manager, seleccione **Archivo > Avanzado > System Status**.

2. Seleccione **Conexión en red IP > VPN SSL** de la lista de navegación.

   Una tabla resumen muestra información de cada servicio de VPN SSL que está configurado.

3. Para ver información detallada acerca del servicio VPN SSL específico, resalte el servicio VPN SSL y haga clic en **Seleccionar**.

   Una tabla detallada muestra información de estado acerca del servicio VPN SSL seleccionado.

Vínculos relacionados

Control del servicio VPN SSL en la página 74
Descripciones de campo de Estado del túnel: tabla de resumen en la página 75
Descripciones de campo de Estado de túnel: tabla de detalles en la página 76

Descripciones de campo de Estado del túnel: tabla de resumen

System Status Application (SSA) muestra el siguiente resumen para el servicio VPN SSL:

Valor	Descripción
Nombre	El nombre del servicio VPN SSL configurado en IP Office.
Estado de servicio	Indica si el VPN SSL está activo o en respaldo.
Hora de última conexión	La marca de tiempo de la última conexión correcta.
Hora de última desconexión	La marca de tiempo de la última desconexión.
Dirección IP de túnel	La dirección IP del túnel VPN SSL.
Total latidos perdidos	Un conteo acumulativo de latidos perdidos. El conteo se reinicia a 0 cuando reinicia IP Office, o si desaprovisiona el servicio VPN SSL en Manager.
Total sustentaciones perdidas	Los keepalives se usan para conexiones UDP. UDP no es compatible con el servicio VPN SSL; el valor es 0.
Extremo TCP local	La dirección IP de TCP y el número de puerto de IP Office.
Extremo TCP remoto	Esta es la dirección pública y el número de puerto del AVG. El VIP del AVG.
Extremo UDP local	UDP no es compatible con el servicio VPN SSL; el valor es 0.
Extremo UDP remoto	UDP no es compatible con el servicio VPN SSL; el valor es 0.

Vínculos relacionados

Visualización del estado del túnel en la página 74

Descripciones de campo de Estado de túnel: tabla de detalles

System Status Application (SSA) muestra los siguientes detalles para el servicio VPN SSL:

Valor	Descripción
Nombre del servicio	El nombre del servicio configurado en IP Office.
Estado de servicio	Indica si el VPN SSL está activo o en respaldo.
Nombre de cuenta	El nombre de cuenta del servicio VPN SSL. Este nombre de cuenta se usa para autenticar el servicio VPN SSL cuando se conecta con el AVG.
Dirección del servidor	La dirección del servidor de la puerta de enlace del VPN en el sitio del proveedor de servicios. La dirección que se muestra puede ser una dirección IPv4 o una dirección Fully Qualified Domain Name (FQDN).
Tipo de servidor	El servicio VPN SSL es compatible con la puerta de enlace VPN de Avaya. El tipo de servidor es AVG.
Protocolo	El protocolo utilizado por el servicio VPN SSL para transporte de datos es TCP. Si selecciona UDP como el protocolo, cuando configure la conexión, UDP aparece en este campo, pero el servicio VPN SSL vuelve a TCP.
Última fecha y hora de conexión	La marca de tiempo de la última conexión correcta.
Última fecha y hora de desconexión	La marca de tiempo de la última desconexión.
Dirección IP de túnel	La dirección IP del túnel VPN SSL.
Máscara de subred del túnel	La máscara de subred del túnel VPN SSL.
La dirección IP de la puerta de enlace del túnel	La dirección IP de la puerta de enlace predeterminada de IP Office.
Dominio del túnel	La dirección de dominio del túnel.
La dirección IP TCP local	La dirección IP TCP de IP Office.
Puerto TCP local	El puerto TCP de IP Office. El número de puerto es dinámico.
Dirección IP TCP remota	La dirección IP TCP del servidor AVG.
Puerto TCP remoto	El puerto TCP del servidor AVG. El número de puerto predeterminado es 443.
La dirección IP UDP local	UDP no es compatible con el servicio VPN SSL; el valor es 0.
Puerto UDP local	UDP no es compatible con el servicio VPN SSL; el valor es 0.
Dirección IP UDP remota	UDP no es compatible con el servicio VPN SSL; el valor es 0.

Table continues…

Valor	Descripción
Puerto UDP remoto	UDP no es compatible con el servicio VPN SSL; el valor es 0.
DNS primario	La dirección del servidor DNS primario en el AVG. Esta dirección se entrega para propósitos de información y no la utiliza IP Office.
DNS secundario	La dirección del servidor DNS secundario configurada en el AVG. Esta dirección se entrega para propósitos de información y no la utiliza IP Office.
WINS primario	El WINS primario configurado en el AVG. Esta dirección se entrega para propósitos de información y no la utiliza IP Office.
WINS secundario	El WINS secundario en el AVG. Esta dirección se entrega para propósitos de información y no la utiliza IP Office.
Total latidos perdidos	Un conteo acumulativo de latidos perdidos. El conteo se reinicia a 0 cuando reinicia IP Office, o si desaprovisiona el servicio VPN SSL en Manager.
Total sustentaciones perdidas	Los keepalives se usan para conexiones UDP. UDP no es compatible con el servicio VPN SSL; el valor es 0.

Vínculos relacionados

Visualización del estado del túnel en la página 74

Control de alarmas con SSA

Use este procedimiento para ver fallas de sistemas en el servicio VPN SSL que se informaron en el System Status Application (SSA).

Procedimiento

1. Inicie SSA utilizando uno de los siguientes métodos:
   - Inicie SSA desde el DVD de administración IP Office.
   - Seleccione **Inicio > Programas > IP Office > System Status**.
   - Desde Manager, seleccione **Archivo > Avanzado > System Status**.
2. Seleccione **Alarmas > Servicio** desde la lista de navegación.

   Una tabla muestra las fallas de sistema. Las fallas de sistemas que se relacionan con el servicio VPN SSL se identifican en el nombre de servicio.

Vínculos relacionados

Control del servicio VPN SSL en la página 74

Descripciones de alarma SSA en la página 78

Descripciones de alarma SSA

Las siguientes fallas de sistemas se relacionan con el servicio VPN SSL y se informan en el System Status Application (SSA).

Nombre	Descripción
Última fecha de error	La fecha y la alarma en que ocurrió la alarma.
Ocurrencias	El número de veces que ocurrió la alarma desde la última vez que se reinició la unidad de control o que se borró.
Descripción de error	Las alarmas relacionadas con el servicio VPN SSL muestran los siguientes mensajes de error, seguidos por el nombre del servicio de VPN SSL: • SSL VPN fuera de servicio debido a mantenimiento planificado. • SSL VPN fuera de servicio debido a que no se puede conectar con el servidor o a que hubo una falla en la red. • SSL VPN fuera de servicio debido a una falla en la negociación de la sesión TLS. • SSL VPN fuera de servicio debido a una falla en la renegociación clave de la sesión TLS. • SSL VPN fuera de servicio debido a la falta de recursos en IP Office. • SSL VPN fuera de servicio debido a un error interno en IP Office. • SSL VPN fuera de servicio debido a demasiados mensajes de latido perdidos. • SSL VPN fuera de servicio debido a una falla en la resolución del servidor FQDN. • SSL VPN fuera de servicio debido a que se detectó una dirección IP duplicada en otra interfaz IP Office. • SSL VPN fuera de servicio debido a una falla en la autenticación. • SSL VPN fuera de servicio debido a un error de protocolo SOCKS. • SSL VPN fuera de servicio debido a que el servidor ha informado acerca de un error.

Vínculos relacionados

Control de alarmas con SSA en la página 77

Solución de problemas del servicio VPN SSL

Puede usar la información captada por SysMonitor para solucionar problemas de conectividad. SysMonitor captura información que puede ayudar a solucionar problemas cuando el servicio VPN SSL no se conecte con el AVG y el System Status Application (SSA) no proporcione suficiente información para identificar la causa original de la falla.

Use este procedimiento para reunir información solo cuando lo solicite el personal de soporte técnico.

Procedimiento

1. Seleccione **Start > Programs > IP Office > Monitor**.

   La aplicación SysMonitor se conecta con el servidor IP Office y muestra un registro del sistema.

2. Seleccione las opciones **Filters > Trace** (Filtros > Seguimiento) y haga clic en la ficha **VPN**.
3. En el área VPN SSL, seleccione los filtros especificados por soporte técnico.
4. Haga clic en **OK** (Aceptar)

   El registro de SysMonitor muestra la actividad para el servicio VPN SSL bajo el nombre que configuró para el servicio.

Vínculos relacionados

Control del servicio VPN SSL en la página 74
Descripciones de resultados de SysMonitor en la página 79

Descripciones de resultados de SysMonitor

La siguiente tabla muestra una lista de filtros que puede seleccionar en SysMonitor, y describe los resultados que cada filtro genera. Esta información está diseñada para personal de soporte técnico cuando solucionen los problemas del servicio VPN SSL.

Nombre	Descripción
Configuration (Configuración)	Muestra información acerca de cuándo se agregó, modificó o eliminó el servicio VPN SSL.

Table continues…

Nombre	Descripción
Session (Sesión)	Muestra información acerca del estado del servicio VPN SSL, por ejemplo si el túnel está activo o en respaldo, o intentando conectarse. Cuando el servicio VPN SSL está conectado, este muestra los parámetros de túnel VPN SSL negociados con AVG.
SessionState	Muestra información acerca del estado cuando ocurre un evento. Los estados definidos son: Idle (Inactivo), Connecting (Conectando), Connected (Conectado), Disconnecting (Desconectando), WaitingToStart (Esperando inicio) y NeedsRestart (Debe reiniciarse).
Fsm	Se usa para conexiones UDP. UDP no es compatible con el servicio VPN SSL; no se generó resultado.
Socks	Muestra eventos apilados de SOCKS activados por mensajes de señalización.
SocksState	Muestra los estados internos de la pila de SOCKS cuando se procesan mensajes de señalización SOCKS5.
Heartbeat (Latidos)	Muestra información acerca de cuando se envían y se reciben mensajes de latidos.
Keepalive	Se usa para conexiones UDP. UDP no es compatible con el servicio VPN SSL; no se generó resultado.
SignalingPktRx	Muestra la secuencias de bytes del paquete de señalización SOCKS recibido de AVG.
SignalingPktTx	Muestra la secuencias de bytes del paquete de señalización SOCKS enviado a AVG.
DataPktRx	Muestra una subred de datagramas, comenzando con el paquete de datos recibido por el túnel VPN SSL desde AVG y aprobado en el sistema IP Office.
DataPktTx	Muestra una subred de datagramas, comenzando por los paquetes de datos enviados por la interfaz del túnel VPN SSL en el AVG.
TunnelInterface (Interfaz del túnel)	Muestra información acerca de las interacciones entre la interfaz del túnel VPN SSL y la pila de IP de IP Office.
TunnelRoutes (Rutas del túnel)	Muestra información acerca de las rutas de tunelización divididas instaladas y eliminadas de la tabla de rutas de IP Office.

Vínculos relacionados

[Solución de problemas del servicio VPN SSL](#) en la página 79

Capítulo 12: Mantenimiento del servicio de VPN SSL

Esta sección describe las tareas que realiza en una base constante después de que el servicio VPN SSL se configuró y conectó.

Use la información en esta sección para realizar las siguientes tareas de navegación:

- sacar el túnel de servicio y volver a ponerlo en funcionamiento
- cambiar la contraseña para la cuenta VPN SSL

Vínculos relacionados

Activación y desactivación del servicio en la página 81
Restablecimiento de la contraseña en la página 87

Activación y desactivación del servicio

Después de configurar el servicio VPN SSL, puede usar las siguientes interfaces para activar o desactivar el túnel.

- Manager
- System Status Application(SSA)
- códigos cortos marcados en deskphones de Avaya
- teclas programables en deskphones compatibles de Avaya
- una configuración de operadora automática configurada en sistemas Embedded Voicemail o Voicemail Pro
- administradores basados en el conjunto en deskphones compatibles de Avaya

Los métodos disponibles dependen del modo de operación que utilice.

La siguiente tabla muestra los métodos compatibles en cada modo de operación:

Método	Modo de operación			
	Essential Edition	IP Office Server Edition	Sistema de expansión Server Edition	Basic Edition
Manager	✔	✔	✔	—
SSA	✔	✔	✔	—
Códigos cortos marcados en deskphones de Avaya	✔	✔	✔	—
Teclas programables en deskphones de Avaya	✔	✔	✔	—
Operadora automática en sistemas Embedded Voicemail o Voicemail Pro	✔	✔	✔	—
Administración basada en el conjunto	—	—	—	✔

Vínculos relacionados

Mantenimiento del servicio de VPN SSL en la página 81
Activación del servicio con Manager en la página 82
Desactivación del servicio con Manager en la página 83
Activación del servicio con SSA en la página 83
Desactivación del servicio con SSA en la página 84
Activación del servicio con un código corto en la página 84
Desactivación del servicio con un código corto en la página 85
Activación y desactivación del servicio con administración basada en el conjunto en la página 85
Activación y desactivación del servicio con las teclas programables en la página 86

Activación del servicio con Manager

Use este procedimiento para activar el servicio VPN SSL desde la interfaz de Manager. Si está configurando un sistema Server Edition, use el modo IP Office Manager for Server Edition.

El servicio de VPN SSL debe tener el estado En Respaldo antes de comenzar.

Procedimiento

1. En la lista de navegación, haga clic con el botón secundario en **Servicio**.

   La lista se amplía para mostrar los servicios configurados en el sistema.
2. Seleccione el servicio VPN SSL que desea activar.
3. Seleccione la ficha **Reserva** y desmarque la opción **En Respaldo**.
4. Haga clic en **Aceptar**.
5. Haga clic en el icono **Guardar** para guardar la configuración.

Vínculos relacionados

Activación y desactivación del servicio en la página 81

Desactivación del servicio con Manager

Use este procedimiento para desactivar el servicio VPN SSL desde la interfaz de Manager. Si está configurando un sistema Server Edition, use el modo IP Office Manager for Server Edition.

El servicio de VPN SSL debe tener el estado En servicio antes de comenzar.

Procedimiento

1. En la lista de navegación, haga clic con el botón secundario en **Servicio**.

   La lista se amplía para mostrar los servicios configurados en el sistema.
2. Seleccione el servicio VPN SSL que desea desactivar.
3. Seleccione la ficha **Respaldo** y seleccione la opción **En Respaldo**.
4. Haga clic en **Aceptar**.
5. Haga clic en el icono **Guardar** para guardar la configuración.

Vínculos relacionados

Activación y desactivación del servicio en la página 81

Activación del servicio con SSA

Use este procedimiento para activar el servicio VPN SSL desde System Status Application (SSA). El servicio de VPN SSL debe tener el estado En Respaldo antes de comenzar.

Procedimiento

1. Inicie SSA utilizando uno de los siguientes métodos:
   - Inicie SSA desde el DVD de administración IP Office.
   - Seleccione **Inicio > Programas > IP Office > System Status**.
   - Desde Manager, seleccione **Archivo > Avanzado > System Status**.
2. Seleccione **Conexión en red IP > VPN SSL** de la lista de navegación.
3. Seleccione el servicio VPN SSL que desea activar de la lista.

4. Haga clic en el botón **Establecer en Servicio**.

   El estado cambia a En servicio.

Vínculos relacionados

Activación y desactivación del servicio en la página 81

Desactivación del servicio con SSA

Use este procedimiento para desactivar el servicio VPN SSL desde System Status Application (SSA). El servicio de VPN SSL debe tener el estado En servicio antes de comenzar.

Procedimiento

1. Inicie SSA utilizando uno de los siguientes métodos:
   - Inicie SSA desde el DVD de administración IP Office.
   - Seleccione **Inicio > Programas > IP Office > System Status**.
   - Desde Manager o IP Office Manager for Server Edition, seleccione **Archivo > Avanzado > System Status**.
2. Seleccione **Conexión en red IP > VPN SSL** de la lista de navegación.
3. Seleccione el servicio VPN SSL que desea activar de la lista.
4. Haga clic en el botón **Establecer en servicio de respaldo**.

   Aparece un cuadro de diálogo de confirmación.
5. Haga clic en **Sí**.

   El sistema genera una alarma para confirmar que el servicio VPN SSL está desactivado.
6. Para ver la alarma, seleccione **Alarmas > Servicio** en la lista de navegación.

   La alarma muestra el siguiente mensaje: “SSL VPN fuera de servicio debido a mantenimiento planificado” seguido del nombre del servicio.

Vínculos relacionados

Activación y desactivación del servicio en la página 81

Activación del servicio con un código corto

Use este procedimiento para activar el servicio VPN SSL marcando un código corto desde un deskphone. El servicio de VPN SSL debe tener el estado En Respaldo antes de comenzar.

Antes de empezar

Esta función está disponible solo si el administrador del sistema configuró códigos cortos en el sistema IP Office. Para obtener más información, consulte Configuración de códigos cortos en la página 41. Antes de comenzar, debe conocer el nombre que el administrador del sistema configuró en el código corto para identificar el servicio VPN SSL.

Procedimiento

Desde un deskphone conectado en el sistema IP Office, ingrese ***775x1**, donde *x* representa una instancia de servicio VPN SSL, que va de 1 a 9. Por ejemplo, si el administrador del sistema configuró el código corto de modo que el **1** identifica el servicio VPN SSL, ingrese ***77511**.

La conexión VPN SSL entra en servicio.

Vínculos relacionados

Activación y desactivación del servicio en la página 81

Desactivación del servicio con un código corto

Use este procedimiento para desactivar el servicio VPN SSL marcando un código corto desde un deskphone. El servicio de VPN SSL debe tener el estado En servicio antes de comenzar.

Antes de empezar

Esta función está disponible solo si el administrador del sistema configuró códigos cortos en el sistema IP Office. Para obtener más información, consulte Configuración de códigos cortos en la página 41. Antes de comenzar, debe conocer el nombre que el administrador del sistema configuró en el código corto para identificar el servicio VPN SSL.

Procedimiento

Desde un deskphone conectado en el sistema IP Office, ingrese ***775x0**, donde *x* representa una instancia de servicio VPN SSL, que va de 1 a 9. Por ejemplo, si el administrador del sistema configuró el código corto de modo que el **1** identifica el servicio VPN SSL, ingrese ***77510**.

La conexión VPN SSL queda en respaldo.

Vínculos relacionados

Activación y desactivación del servicio en la página 81

Activación y desactivación del servicio con administración basada en el conjunto

En algunos modelos de teléfonos Avaya, puede usar teclas programables para activar y desactivar el servicio VPN SSL. Esta sección proporciona información acerca de esta función y los teléfonos que son compatibles.

Antes de empezar

Debe configurar los Derechos de sistema del teléfono antes de que esta función esté disponible. Para obtener más información acerca de cómo configurar los Derechos de sistema del teléfono, consulte *IP Office Manager*.

El teléfono debe estar conectado a uno de los primeros dos puertos de la primera tarjeta en la plataforma IP500 V2.

Acerca de esta tarea

Puede usar teclas programables para activar y desactivar el servicio VPN SSL en los siguientes teléfonos Avaya:

- Deskphones ETR 18D y ETR 34D
- Deskphone digital 1416
- Deskphone digital 1408
- Deskphone digital 9504
- 9508, Deskphones digitales
- Deskphones digitales T7316 y 7316E
- Deskphones digitales M7310 y M7324

El siguiente procedimiento proporciona una guía general para acceder a la función VPN SSL en estos teléfonos. Para obtener información detallada de las opciones de menú, consulte la guía del usuario para el teléfono.

Procedimiento

1. Los menús que debe navegar para acceder a la función VPN SSL dependen del modelo de teléfono que use. Use uno de los siguientes métodos para acceder a la función VPN SSL:
   - Seleccione **Admin > Administración del sistema > Parámetros del sistema** y desplácese para ubicar el servicio VPN SSL.
   - Seleccione **Admin > Función** y desplácese para ubicar el servicio VPN SSL.
   - Seleccione **Admin** y oprima **#775** para acceder al menú VPN SSL.
2. Oprima la tecla programable que corresponde para activar o desactivar el servicio.

Vínculos relacionados

Activación y desactivación del servicio en la página 81

Activación y desactivación del servicio con las teclas programables

Algunos modelos de teléfonos Avaya incluyen teclas programables. Puede usar estas teclas como acceso directo de modo que no tenga que ingresar un código de función o navegar por los menús de la interfaz del teléfono para activar una función. El administrador del sistema puede configurar una tecla programable que permita activar y desactivar el servicio VPN SSL.

Si el administrador de sistemas configuró una tecla programable en el teléfono para el servicio VPN SSL, aparece una etiqueta junto a la tecla programable del teléfono.

Oprima la tecla para alternar el servicio VPN SSL entre activado (en servicio) y desactivado (en respaldo).

El estado del servicio VPN SSL aparece junto a la tecla del teléfono. La manera en que aparece el estado depende del modelo del teléfono. Por ejemplo, algunos teléfonos muestran un icono, y

otros usan LED para indicar el estado de una función. Cuando el icono muestra las luces LED, el servicio VPN SSL está activado.

Cuando oprime la tecla para desactivar el servicio VPN SSL, el icono ya no aparece y el LED se apaga.

Vínculos relacionados

Activación y desactivación del servicio en la página 81

Restablecimiento de la contraseña

Esta sección describe los métodos que puede usar para restaurar la contraseña para el servicio VPN SSL.

Hay dos métodos para restablecer la contraseña del servicio VPN SSL.

- Puede cambiar la contraseña en el archivo de integración y volver a importarlo.
- Puede cambiar la contraseña con Manager.

Para ambos métodos, también debe cambiar la contraseña que se configuró en el servicio VPN SSL del servidor RADIUS.

Vínculos relacionados

Mantenimiento del servicio de VPN SSL en la página 81
Restablecimiento de la contraseña con un archivo de integración en la página 87
Restablecimiento de la contraseña con Manager en la página 88

Restablecimiento de la contraseña con un archivo de integración

Use este procedimiento cuando ya haya configurado el servicio VPN SSL en un sistema IP Office y necesite modificar la contraseña para el servicio VPN SSL.

Realice este procedimiento desde la interfaz de IP Office Web Manager de Avaya en el sitio del cliente.

Antes de empezar

Antes de comenzar, debe tener la siguiente información:

- el nombre del servicio VPN SSL
- el nombre de cuenta se usa para autenticar el servicio VPN SSL cuando se conecta con el AVG.

Puede usar System Status Application (SSA) para buscar el nombre del servicio VPN SSL y el nombre de cuenta. Para obtener más información, consulte Visualización de la condición del túnel en la página 74.

También debe restablecer la contraseña para el servicio VPN SSL en el servidor RADIUS.

Procedimiento

1. Seleccione **Herramientas > Integración**.

   Aparece el cuadro de diálogo Integración.

2. Haga clic en **Modificar**.

   Se abre un explorador y navega al sitio web de Avaya.

3. Inicie sesión en el sitio web.

   Aparece la página Administración de conectividad remota / contraseña de IP Office.

4. Haga clic en **Existing IP Office SSL VPN Remote Connectivity** (Conectividad remota VPN SSL de IP Office existente).

5. Seleccione **Password Reset** (Restablecer contraseña).

   Aparece el nombre del servicio VPN SSL predeterminado.

6. Asegúrese de que el nombre del servicio que aparece coincida con el nombre del servicio VPN SSL para el que desea restablecer la contraseña. Si el nombre del servicio predeterminado no coincide, ingrese el nombre del servicio,

7. Ingrese el nombre de cuenta de VPN SSL.

8. Haga clic en **Submit** (Enviar).

9. Seleccione si desea recibir el archivo de integración actualizado por correo electrónico o si desea descargarlo y seguir las indicaciones en pantalla.

10. Cuando haya descargado o recibido el archivo de integración actualizado, guárdelo en el sistema local.

11. Examine la ubicación donde guardó el archivo de integración y haga clic en **Cargar** en la interfaz de Web Manager.

    Aparece un mensaje para confirmar que el archivo de integración se instaló correctamente.

Pasos siguientes

Después de restablecer la contraseña, confirme que el servicio VPN SSL se haya reconectado correctamente con AVG siguiendo el procedimiento Visualización de la condición del túnel en la página 74.

Vínculos relacionados

Restablecimiento de la contraseña en la página 87

Restablecimiento de la contraseña con Manager

Use este procedimiento para modificar la contraseña para el servicio VPN SSL. Realice este procedimiento desde la interfaz Manager en el sitio del cliente. Si está configurando un sistema Server Edition, use el modo IP Office Manager for Server Edition.

Antes de empezar

También debe restablecer la contraseña para el servicio VPN SSL en el servidor RADIUS.

Procedimiento

1. En la lista de navegación, seleccione **Servicio**.
2. Seleccione el nombre del servicio VPN SSL.
3. Seleccione la ficha **Sesión** e ingrese la nueva contraseña para la cuenta del servicio VPN SSL en el campo **Contraseña de cuenta**.
4. Vuelva a ingresar la contraseña en el campo **Confirmar contraseña**.
5. Haga clic en **Aceptar**.
6. Haga clic en el icono **Guardar** para guardar la configuración.

Vínculos relacionados

Restablecimiento de la contraseña en la página 87

Capítulo 13: Apéndice A: ejemplo del Asistente de configuración rápida de AVG

Para iniciar el asistente, abra una nueva imagen de AVG. En la consola, cuando aparezca el aviso `localhost login:`, inicie sesión con el usuario “admin” y la contraseña “admin”. Se abre el menú del asistente. Seleccione `new` y siga las instrucciones.

Configurar las interfaces de AVG

```
localhost login: admin
Password:
Alteon iSD SSL
Hardware platform: 3050-VM
Software version: 10.0.1.0

------------------------------------------------------------
[Setup Menu]
      join        - Join an existing cluster
      new         - Initialize host as a new installation
      boot        - Boot menu
      info        - Information menu
      exit        - Exit  [global command, always available]

>> Setup# new

Setup will guide you through the initial configuration.
```

```
Enter port number for the management interface [1-4]: 1
Enter IP address for this machine (on management interface): 172.16.1.5
Enter network mask [255.255.255.0]:
Enter VLAN tag id (or zero for no VLAN) [0]:
Setup a two armed configuration (yes/no) [yes]:
Enter port number for the traffic interface [1-4]: 2
Enter IP address for this machine (on traffic interface): 10.136.66.195
Enter network mask [255.255.255.0]:
Enter VLAN tag id (or zero for no VLAN) [0]:
Enter default gateway IP address (on the traffic interface): 10.136.66.1
Enter the Management IP (MIP) address: 172.16.1.6
Making sure the MIP does not exist...ok
Trying to contact gateway...ok
```

Configurar el certificado autofirmado

```
Enter a timezone or 'UTC' or 'select' [select]: UTC
Enter the current date (YYYY-MM-DD) [2014-11-20]:
Enter the current time (HH:MM:SS) [23:54:18]:
Enter NTP server address (or blank to skip):
Enter DNS server address: 198.152.7.12
   Enabled SSH (allow CLI access).
Enter a password for the "admin" user:
Re-enter to confirm:
Run VPN quick setup wizard [yes]:
Enter VPN Portal IP address: 10.136.66.196
   Using VPN device without an Alteon switch.
   Using empty DNS search list.
   Creating HTTP to HTTPS redirect server.
   Enabling HTTPS BBI on port 443.
Use self-signed certificate (yes/no) [yes]:
!!!The combined length of the following parameters may not exceed 225 bytes!!!
Country Name (2 letter code): ca
State or Province Name (full name): on
Locality Name (eg, city): ottawa
Organization Name (eg, company): smec
Organizational Unit Name (eg, section):
Common Name (eg, your name or your server's hostname): testavg
Email Address:
Subject alternative name (blank or comma separated list of
URI:<uri>, DNS:<fqdn>, IP:<ip-address>, otherName:<string>, email:<email-address
>):
Valid for days [2556 (7 years)]:
Key size (512/1024/2048/4096) [2048]:
```

Opción 1: configurar el grupo de direcciones IP local

```
Use RADIUS authentication server (yes/no) [yes]: no
   Using LOCAL authentication.
Enter Lower IP address in pool range: 172.30.0.1
Enter Upper IP address in pool range: 172.30.255.254
Enter Network mask for the pool range [255.255.255.0]: 255.255.0.0
```

Opción 2: configurar el servidor RADIUS

```
Use RADIUS authentication server (yes/no) [yes]:
Use generic RADIUS server configuration parameters (yes/no) [yes]:
Enter RADIUS server IP address: 172.16.1.2
Enter shared secret:
Re-enter to confirm:
```

Configurar la subred del agente de servicio

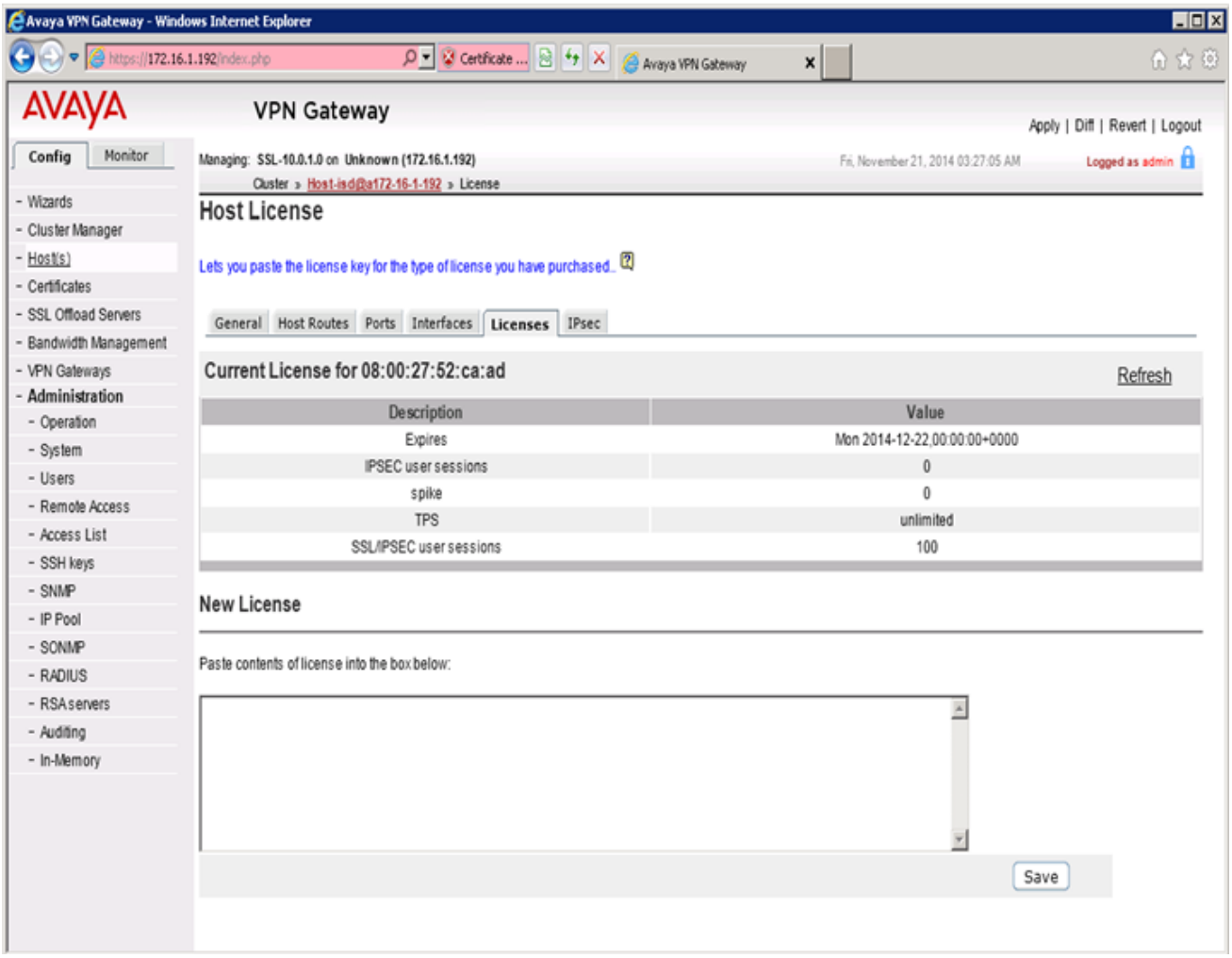
Nota:

Si la subred del agente de servicio se encuentra en la misma subred que la interfaz de host de AVG, por ejemplo, 172.16.1.0, máscara de red 255.255.255.0, recibirá un aviso de la puerta de enlace, aun cuando no esté configurada o no se utilice. Si la subred de la interfaz de host tiene una puerta de enlace predeterminada disponible, utilice la dirección IP de la puerta de enlace (por ej., 172.16.1.1). De lo contrario, introduzca la dirección de la subred nuevamente (por ej., 172.16.1.0).

```
Enter intranet network address: 172.17.1.0
Enter intranet network mask [255.255.255.0]:
Enter intranet gateway: 172.16.1.1
   Enabling network attributes.
   Enabling NetDirect.
   Enabling Split Tunnel Mode.
   Set splittun based on intranet network.
   Added a static route with intranet network.
   Creating empty portal linkset 'base-links'.
   Creating group 'trusted' with secure access.
   Creating network access rule to allow only intranet network for group 'truste
d'.
   Asigning portal linkset 'base-links' to group 'trusted'.
   Creating group 'ipoffice' with secure access.
   Creating network access rule to allow only intranet network for group 'ipoffi
ce'.
   Asigning portal linkset 'base-links' to group 'ipoffice'.
Initializing system.....
```

Agregar la licencia de VPN SSL

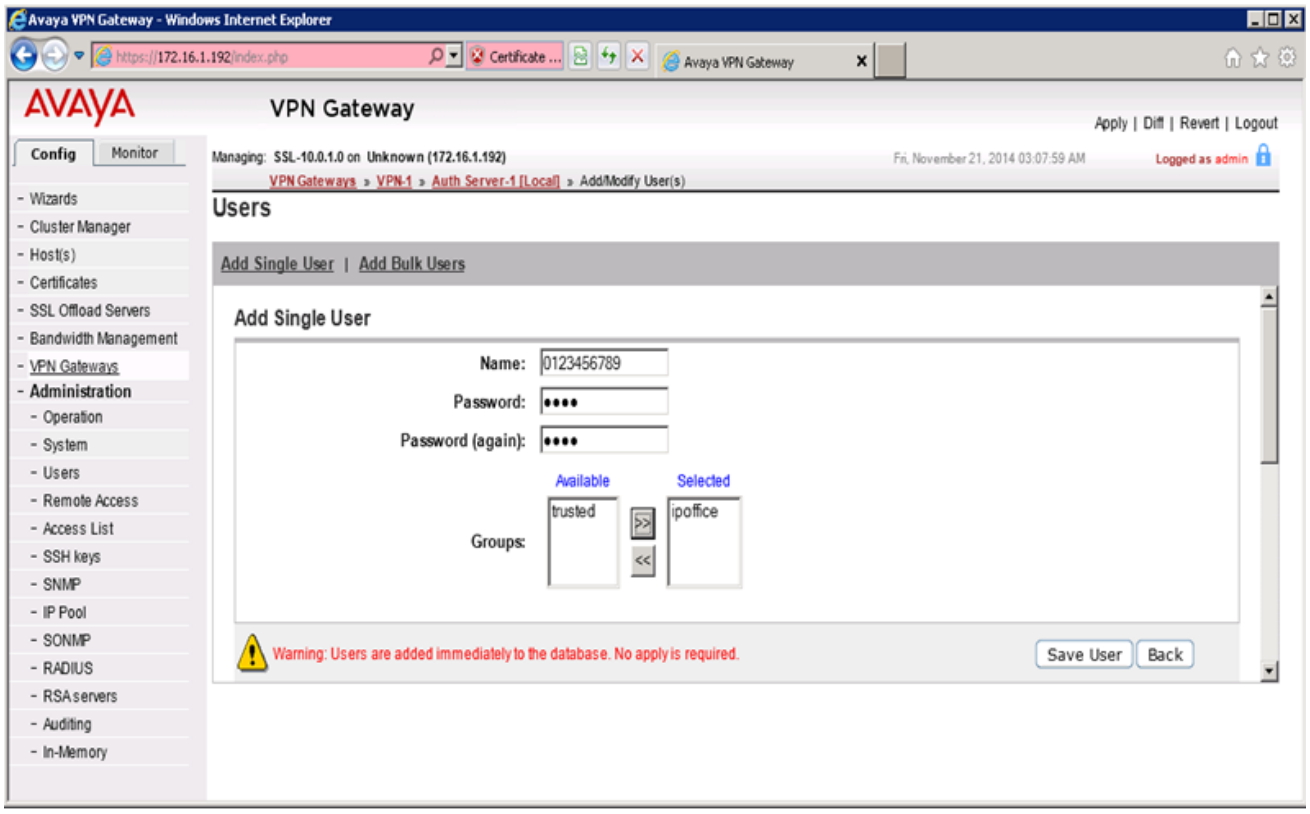
Inicie sesión en la interfaz de AVG para agregar una licencia.



Agregar un usuario

La configuración se completó.

Si utilizó la opción 1, configurar el grupo de direcciones IP local, ahora puede agregar usuarios en la base de datos de AVG local. Los usuarios deben formar parte del grupo **ipoffice**.



Capítulo 14: Apéndice B: modificación del AVG predeterminado para VPN SSL (con pantallas)

Después de ejecutar los asistentes de configuración Configuración rápida y Net Direct, la configuración predeterminada debe modificarse para respaldar una conexión VPN SSL con un sistema IP Office.

Realice este procedimiento utilizando la interfaz basada en el explorador de AVG. Consulte la *Guía de la aplicación Avaya VPN Gateway*.

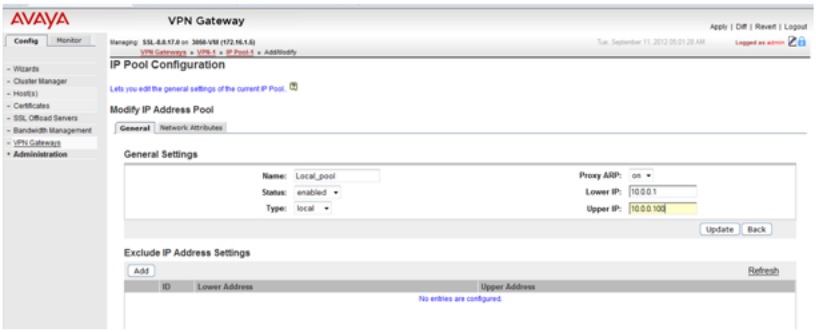
Antes de empezar

Asegúrese de que la puerta de enlace predeterminada configurada en AVG responda a las solicitudes ICMP. Si la puerta de enlace predeterminada no responde a las solicitudes de ICMP, el AVG no puede proporcionar los servicios VPN.

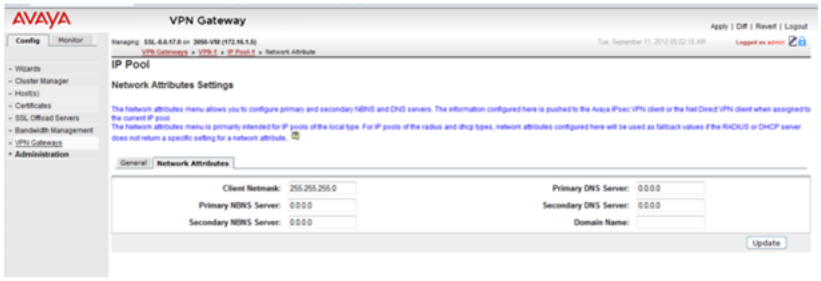
Procedimiento

1. Inicie sesión en el BBI de AVG como administrador.
2. En el panel de navegación de la izquierda, seleccione la ficha **Config** y luego **VPN Gateway** > **VPN1** > **Grupo de IP**.
3. Es posible que el VPN predeterminado de la configuración básica de AVG ya tenga un grupo local. Si no es así, debe agregar un grupo local al VPN predeterminado. En la página **Agregar nuevo grupo de dirección IP**, agregue un grupo local al VPN predeterminado.

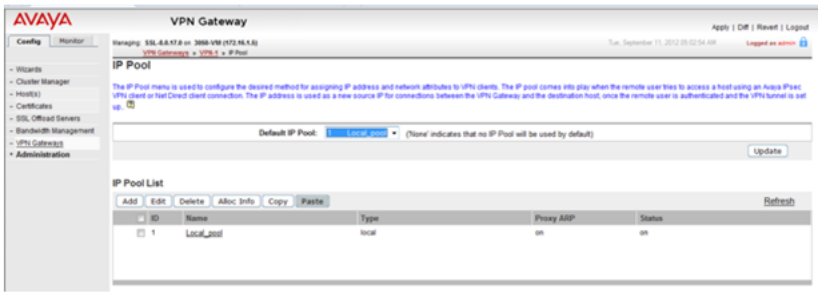
4. En la página **Modificar grupo de dirección IP**, verifique que los valores de los campos **IP inferior** e **IP posterior** coincidan con los valores establecidos utilizando el asistente Configuración de Net Direct.



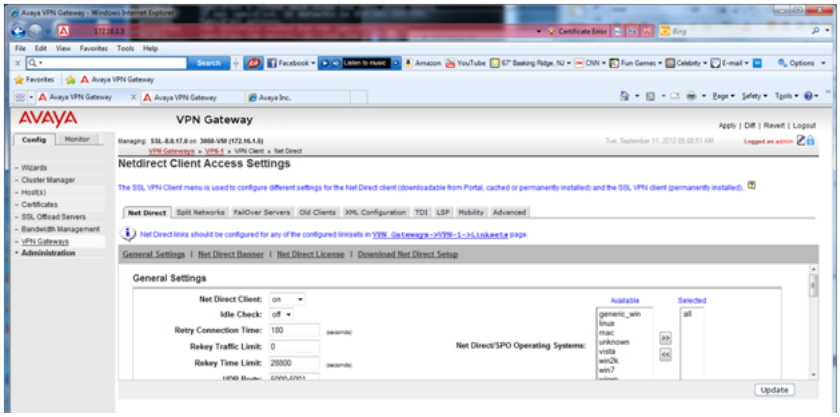
5. En la página **Grupo IP** > **Configuración de atributos de red**, seleccione la ficha **Atributos de red** e ingrese los valores de su red.



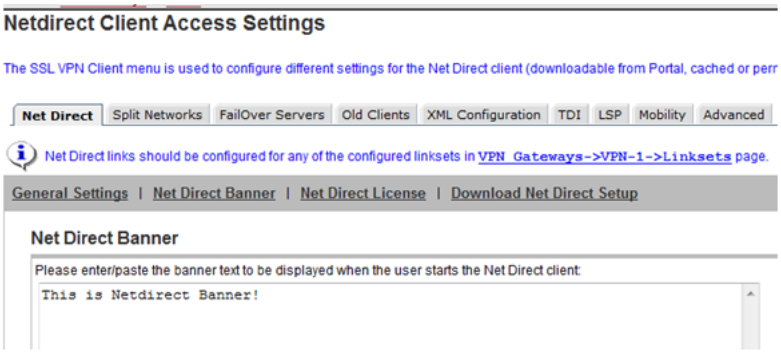
6. En la página **Grupo IP**, configure el **Grupo IP predeterminado** en el grupo local creado en el paso 3.



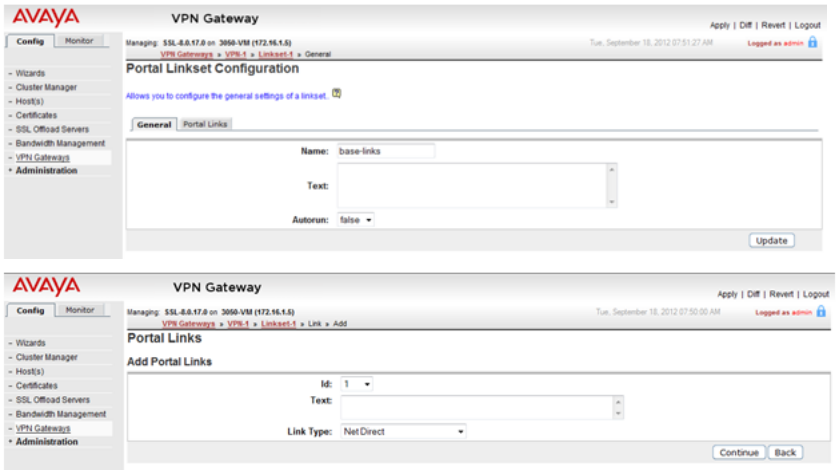
7. En la página **Configuración de acceso de cliente Net Direct**, verifique las configuraciones creadas por el asistente Configuración de Net Direct.
    a. Asegúrese de que **Verificación de sesión inactiva** esté configurado en **desactivado**.



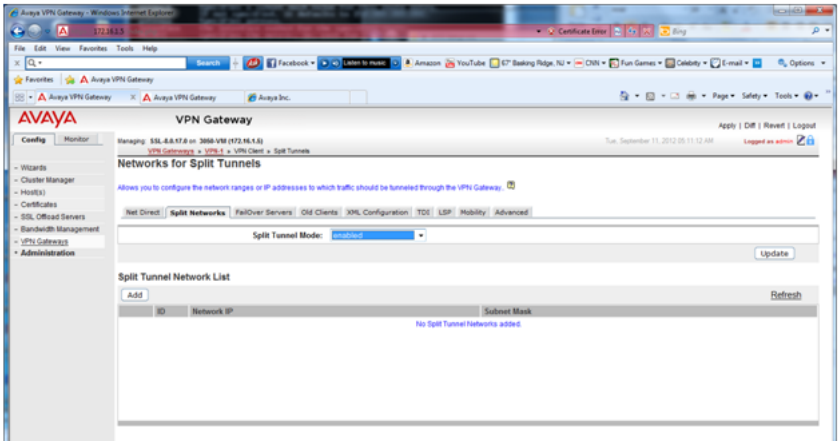
b. Asegúrese de que el encabezado de Net Direct esté configurado.



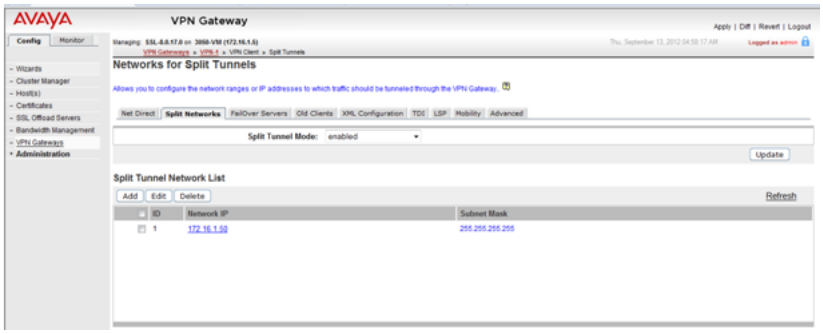
8. Defina el enlace del portal para iniciar el cliente de Net Direct. En la página **Configuración de conjunto de enlace de portal**, seleccione la ficha **Enlace de portal**. En el campo **Tipo de enlace**, seleccione **Net Direct**.



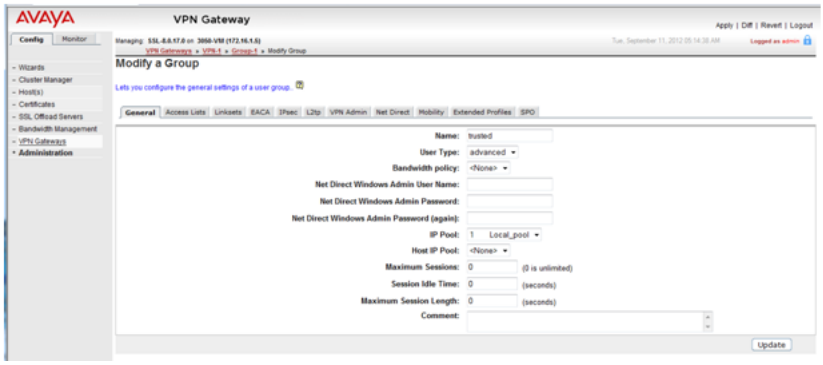
9. En la página **Redes para tunelización dividida**:
   a. Configure **Dividir modo de túnel** en **habilitado.**



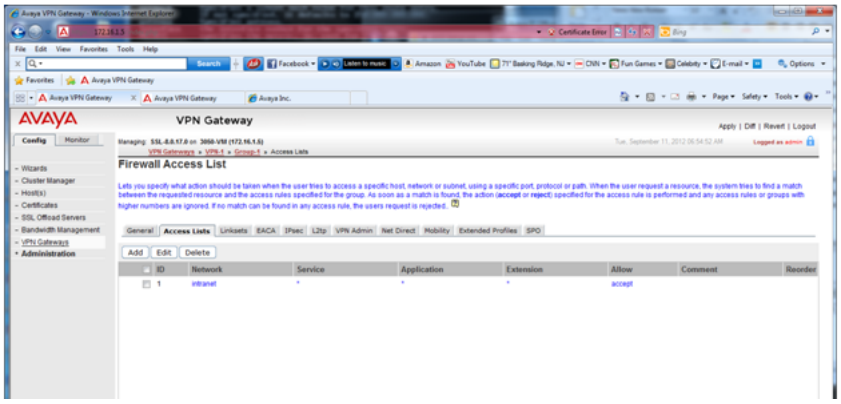
b. Configure las rutas de tunelización divididas para alcanzar al agente de servicio en la red privada.



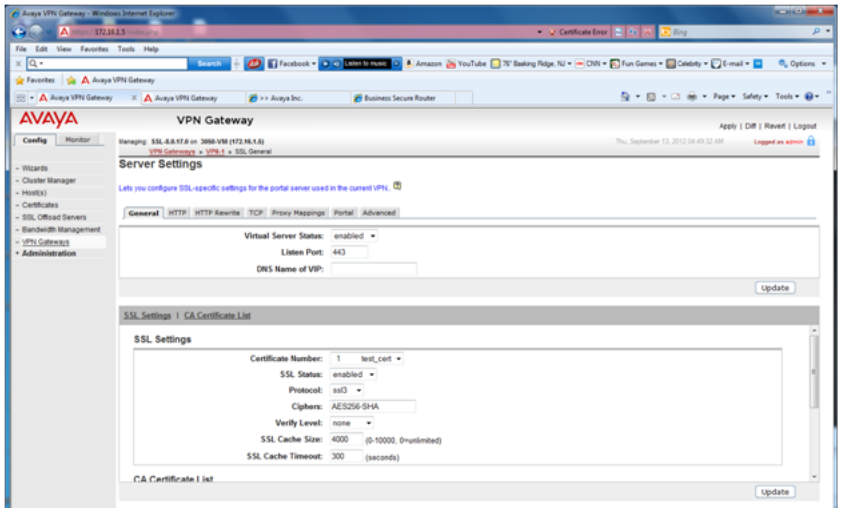
10. Para VPN1, vaya a la página de grupos y seleccione **Grupo1**. En la página **Modificar un grupo**, configure el Grupo IP en el grupo local creado en el paso 3.



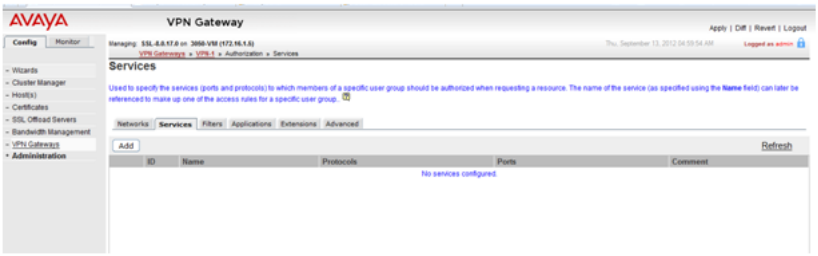
11. Vaya a la página **VPN1** > **Grupo1** > **Listas de acceso**. En la página **Lista de acceso de firewall**, cree una regla de acceso si no se creó de manera predeterminada.



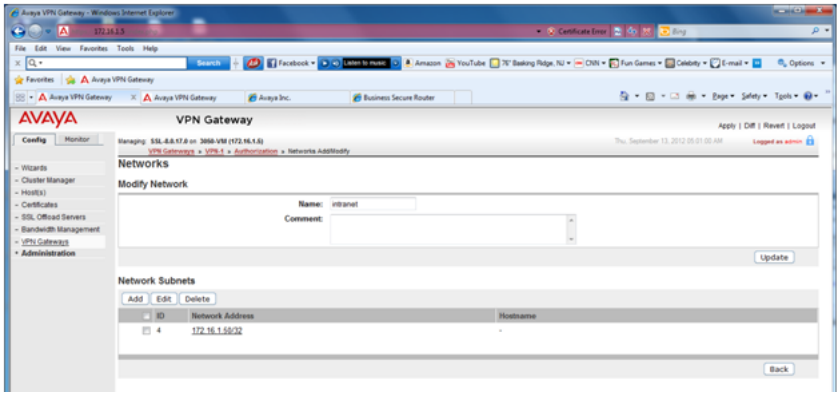
12. Vaya a la página **VPN1** > **SSL**. En la página **Configuración de servidor**, en **Configuración de SSL** configure **Cifrados** en **AES256-SHA** para un cifrado sólido.



13. Vaya a la página **VPN1** > **Autorización** > **Servicios**. Elimine todos los servicios configurados en la configuración predeterminada ya que no son requeridos por VPN SSL.



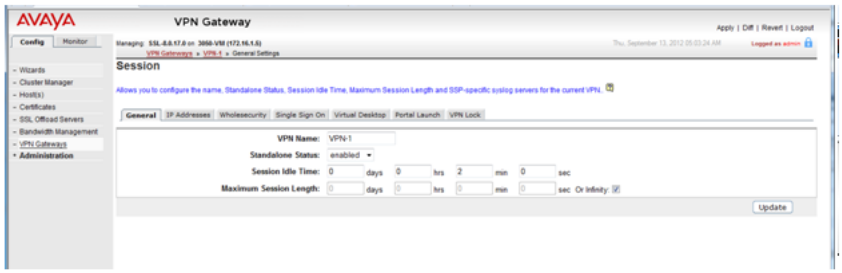
14. Vaya a la página **VPN1** > **Autorización** > **Redes**. Configure el subgrupo de redes de autorización al que se hace referencia en una de las reglas de acceso que está configurado en **VPN1** > **Grupo1** > **Listas de acceso**.



Nota:

Esta opción controla la comunicación interna en el túnel de la VPN SSL. La comunicación se habilita únicamente cuando se especifica una lista de redes “intranet” permitidas. La comunicación con clientes dentro de la VPN se bloquea de manera predeterminada.

15. Vaya a la página **VPN1** > **Configuración general** > **Sesión**. Configure **Tiempo de inactividad de sesión** en dos minutos.



Capítulo 15: Apéndice C: configuración de autenticación de RADIUS (con pantallas)

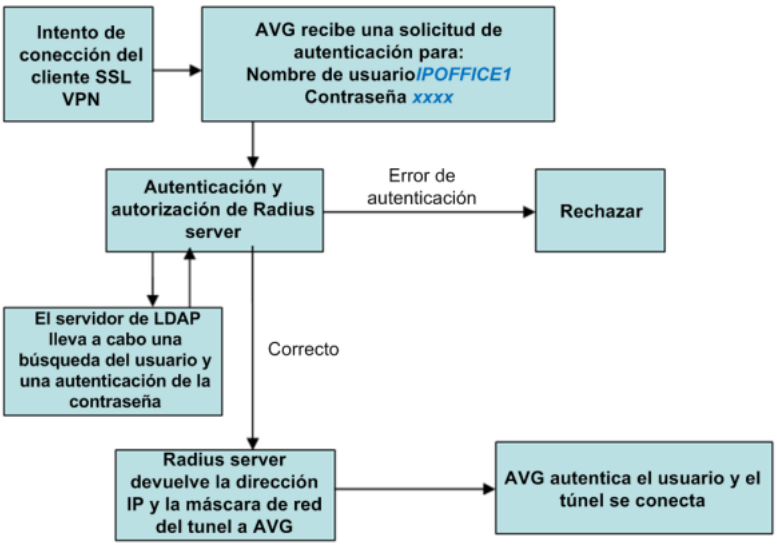
El beneficio clave de la autenticación de RADIUS es que el servicio de VPN SSL siempre está asignado a la misma dirección IP de túnel.

Para configurar la autenticación de RADIUS, debe instalar un servidor de RADIUS. Avaya recomienda Avaya Identity Engine para un servidor de Radius. Para obtener información y la descarga del software, vaya a http://support.avaya.com.

La información de autenticación del protocolo de RADIUS como la información de cuenta del usuario así como la información de túnel de VPN SSL como la dirección IP y la máscara de red deben almacenarse en la base de datos. Hay dos opciones posibles:

- Use la base de datos local de Identity Engine para almacenar la información de usuario y ofrecer tanto búsqueda y autenticación como servicios de autorización. La opción se puede usar para un pequeño número de usuarios. Identity Engine tiene un límite estricto de usuarios. Consulte la documentación para conocer el valor exacto.
- Use un servidor LDAP para almacenar las credenciales de usuarios y la información de túnel de VPN SSL tanto para servicio de búsqueda como de autenticación. Esta opción se adapta a situaciones de implementación para un gran número de usuarios.

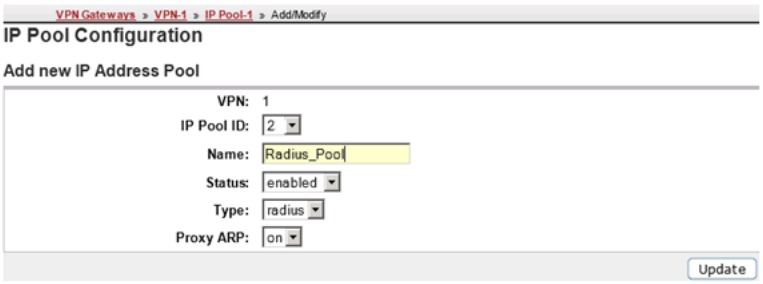
Para la instalación del servidor LDAP, la documentación de Avaya Identity Engine Radius Server contiene opciones de configuración para servidores de LDAP de distintos proveedores. La autenticación de RADIUS con un servidor LDAP se ilustra en la figura a continuación. Tenga en cuenta que esta configuración del servidor de RADIUS en este procedimiento no requiere un servidor LDAP.



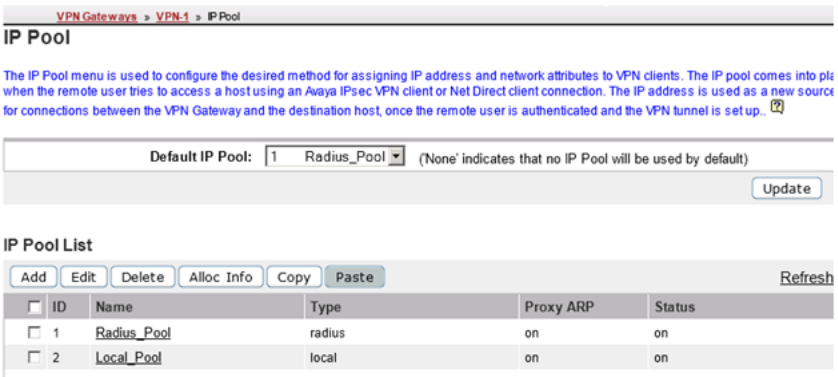
Este procedimiento cubre los pasos del manual para configurar la autenticación de RADIUS. También puede configurar la autenticación utilizando el asistente de autenticación de AVG.

Procedimiento

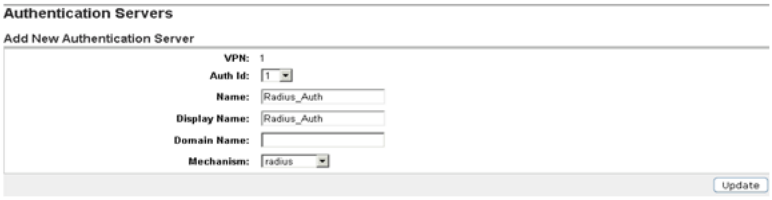
1. Inicie sesión en el BBI de AVG como administrador.
2. En la página **Configuración del grupo de IP**, agregue un nuevo grupo de dirección IP para la autenticación de RADIUS.



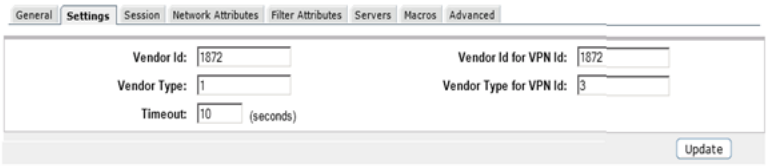
3. En la página **Grupo de IP**, configure el **Grupo de IP predeterminado** en el grupo de dirección IP de autenticación de RADIUS que creó en el paso 2.



4. Modifique el VPN. En la página **Servidores de autenticación** > **Agregar nuevo servidor de autenticación**, complete los campos del servidor RADIUS.

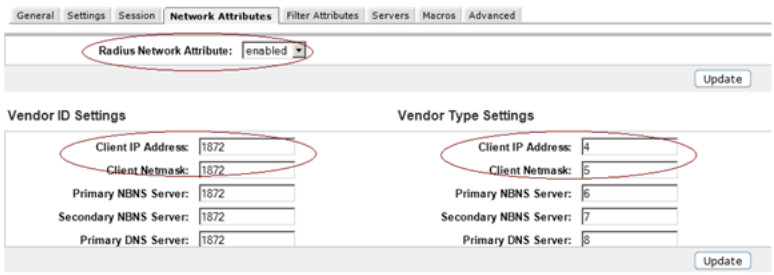


5. Configure los ajustes del servidor de autenticación RADIUS. Tenga en cuenta que la ID de proveedor 1872 está asociada al proveedor Alteon e identifica a AVG. Seleccione la ficha **Configuración** y complete los siguientes campos.
   - **ID de proveedor: 1872**
   - **Tipo de proveedor: 1**
   - **Tiempo de espera: 10**
   - **ID de proveedor para ID de VPN: 1872**
   - **Tipo de proveedor para ID de VPN: 3**

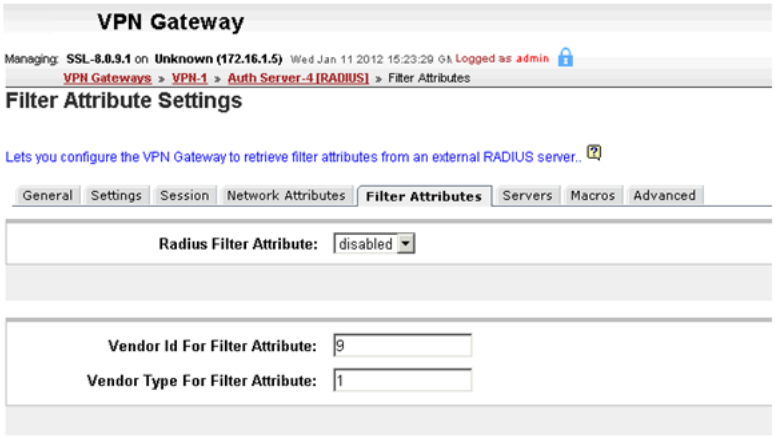


6. Configure los atributos de red de RADIUS. Seleccione la ficha **Atributos de red** y complete los siguientes campos.

Configuración de ID de proveedor	Configuración de tipo de proveedor
Dirección IP del cliente: 1872	Dirección IP del cliente: 4
Máscara de red del cliente: 1872	Máscara de red del cliente: 5
Servidor NBNS primario: 1872	Servidor NBNS primario: 6
Servidor NBNS secundario: 1872	Servidor NBNS secundario: 7
Servidor DNS primario: 1872	Servidor DNS primario: 8



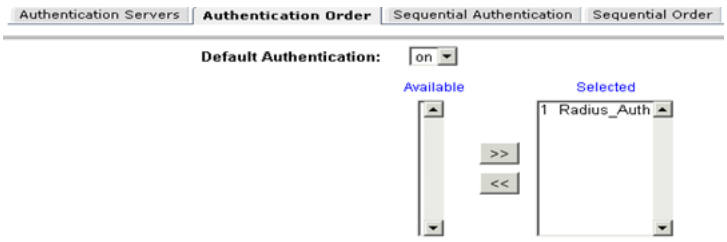
7. Configure los atributos del filtro. Seleccione la ficha Atributos de filtro y complete los siguientes campos>.
   - **Atributo de filtro de Radius: desactivado**
   - **ID de proveedor para atributo de filtro: 9**
   - **Tipo de proveedor para atributo de filtro: 1**



8. Especifique la dirección del servidor Radius. Seleccione la ficha **Servidores** en la página **Servidores RADIUS**.

9. Haga clic en **Agregar** y en la página **Modificar servidor RADIUS**, ingrese la dirección IP del servidor RADIUS y el secreto compartido.

10. Seleccione la ficha **Orden de autenticación** y especifique el orden preferido para los métodos de autenticación.


Authentication Servers
Authentication Order
Sequential Authentication
Sequential Order
Default Authentication:
on
Available
Selected
1 Radius_Auth
>>
<<

Capítulo 16: Apéndice D: ajustes de la configuración de AVG

```
[Main Menu]       info       - Information menu       stats      -
Statistics menu       cfg        - Configuration menu       boot
     - Boot menu       maint      - Maintenance menu       diff
    - Show pending config changes   [global command]       apply
    - Apply pending config changes  [global command]       revert
    - Revert pending config changes [global command]       paste
    - Restore saved config with key [global command]       help
    - Show command help             [global command]       exit
    - Exit  [global command, always available]

>> Main# cfg

------------------------------------------------------------
[Configuration Menu]
      ssl        - SSL offload menu
      cert       - Certificate menu
      vpn        - VPN menu
      test       - Create test vpn, portal and certificate
      quick      - Quick vpn setup wizard
      sys        - System-wide parameter menu
      lang       - Language support
      bwm        - Bandwidth management menu
      log        - logging system menu
      ptcfg      - Backup configuration to TFTP/FTP/SCP/SFTP server
      gtcfg      - Restore configuration from TFTP/FTP/SCP/SFTP server
      dump       - Dump configuration on screen for copy-and-paste

>> Configuration# dump
Dump private/secret keys (yes/no) [no]:
Collecting data, please wait...
/*
/*
/* Alteon iSD SSL
/* Configuration dump taken Tue Sep 18 08:40:50 EDT 2012
/* Hardware Platform: 3050-VM
/* Software Version: 8.0.17.0
/* Uptime:  8 days 3 hours 59 minutes
/* IP Address: 172.16.1.4
/* Hardware Address: 00:0c:29:e0:d8:73
/* Disk space:   config         10110  386513  3 %
  user_content   32832  6015488  1 %

/*
/*
/cfg/.
/cfg/ssl/.
/cfg/ssl/server 1/.
        name "Redirect to VPN 1"
        vips 216.13.56.91
```

```
        standalone off
        port "80 (http)"
        rip 0.0.0.0
        rport 81
        type http
        proxy on
        loopback on
        fastfin off
        ena enabled
/cfg/ssl/server 1/trace/.
/cfg/ssl/server 1/ssl/.
        cert 1
        cachesize 4000
        cachettl 5m
        renegotiate legacy
        protocol ssl3
        verify none
        log none
        verifylog none
        ciphers ALL:-EXPORT:-LOW!ADH
        ena disabled
/cfg/ssl/server 1/tcp/.
        cwrite 15m
        ckeep 15m
        swrite 15m
        sconnect 30s
        csendbuf auto
        crecbuf auto
        ssendbuf auto
        srecbuf 6000
/cfg/ssl/server 1/http/.
        httpsredir on
        redirect on
        downstatus unavailable
        securecookie off
        certcard off
        cookieonce off
        sslheader on
        sslxheader off
        sslsidheader off
        addxfor off
        addvia on
        addxisd off
        addfront off
        addbeassl off
        addbeacli off
        addclicert off
        addnostore off
        nocachehdr off
        compress off
        cmsie on
        rhost off
        maxrcount 40
        maxline 16384
        urlobscure off
        sessionhdr off
/cfg/ssl/server 1/http/redirmap/.
/cfg/ssl/server 1/http/dynheader/.
/cfg/ssl/server 1/http/rewrite/.
        paramtag none
        urldeferattr on
        rewrite off
        ciphers HIGH:MEDIUM
        response iSD
        URI "/cgi-bin/weakcipher"
```

```
/cfg/ssl/server 1/http/auth/.
        mode basic
        realm Xnet
        proxy off
        ena disabled
/cfg/ssl/server 1/dns/.
/cfg/ssl/server 1/adv/.
/cfg/ssl/server 1/adv/pool/.
        timeout 15s
        ena disabled
/cfg/ssl/server 1/adv/traflog/.
        protocol bsd
        sysloghost 0.0.0.0
        udpport 514
        priority info
        facility local4
        ena disabled
/cfg/ssl/server 1/adv/loadbalancing/.
        type all
        persistence none
        metric hash
        health auto
        interval 10s
        grace on
        ena disabled
/cfg/ssl/server 1/adv/loadbalancing/script/.
/cfg/ssl/server 1/adv/loadbalancing/remotessl/.
        protocol ssl3
        ciphers ALL
/cfg/ssl/server 1/adv/loadbalancing/remotessl/verify/.
        verify none
/cfg/ssl/server 1/adv/sslconnect/.
        protocol ssl3
        cachemode on
        ciphers EXP-RC4-MD5:ALL!DH
        ena disabled
/cfg/ssl/server 1/adv/sslconnect/verify/.
        verify none
/cfg/cert 1/.
        name test_cert
        cert
-----BEGIN CERTIFICATE-----
MIIEejCCA+OgAwIBAgIJAODDyCE7V9E3MA0GCSqGSIb3DQEBBAUAMIG/MQswCQYD
VQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTEQMA4GA1UEBxMHVGVzdGluZzEo
MCYGA1UEChMfVGVzdCBJbmMuIDEgMDQ6Mzc6MjEgMjAxMi0wOS0xMDESMBAGA1UE
CxMJdGVzdCBkZXB0MSAwHgYDVQQDExd3d3cuZHVtbXlzc2x0ZXN0aW5nLmNvbTEp
MCcGCSqGSIb3DQEJARYadGVzdGVyQGR1bW15c3NsdGVzdGluZy5jb20wHhcNMTIw
OTEwMDgzNzIyWhcNMTMwOTEwMDgzNzIyWjCBvzELMAkGA1UEBhMCVVMxEzARBgNV
BAgTCkNhbGlmb3JuaWExEDAOBgNVBAcTB1Rlc3RpbmcxKDAmBgNVBAoTH1Rlc3Qg
SW5jLiAxIDA0OjM3OjIxIDIwMTItMDktMTAxEjAQBgNVBAsTCXRlc3QgZGVwdDEg
MB4GA1UEAxMXd3d3LmR1bW15c3NsdGVzdGluZy5jb20xKTAnBgkqhkiG9w0BCQEW
GnRlc3RlckBkdW1teXNzbHRlc3RpbmcuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GN
ADCBiQKBgQCyw80A6VzNwFRpizR9iWJnvZziAgwJZBmI7V2QjtQD+7tMwZA1mNZf
JohYRRS24WGOerGJd3YtAkQHv3yWSo6NiQ5X0Ng8ou4wvg7nlhsqSjeReSn7RUPV
Jl7L45MySiLI5iKWH2j+i1NxLfLbtkqO7+RVAlM3lL4T0Lsjg4RiswIDAQABo4IB
ejCCAXYwDAYDVR0TBAUwAwEB/zARBglghkgBhvhCAQEEBAMCAkQwMgYJYIZIAYb4
QgENBCUWI0FsdGVvbi9Ob3J0ZWwgR2VuZXJhdGVkIENlcnRpZmljYXRlMB0GA1Ud
DgQWBBSGR0w74d4NpcyEeYyLayjiBtRc9DCB9AYDVR0jBIHsMIHpgBSGR0w74d4N
pcyEeYyLayjiBtRc9KGBxaSBwjCBvzELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNh
bGlmb3JuaWExEDAOBgNVBAcTB1Rlc3RpbmcxKDAmBgNVBAoTH1Rlc3QgSW5jLiAx
IDA0OjM3OjIxIDIwMTItMDktMTAxEjAQBgNVBAsTCXRlc3QgZGVwdDEgMB4GA1UE
AxMXd3d3LmR1bW15c3NsdGVzdGluZy5jb20xKTAnBgkqhkiG9w0BCQEWGnRlc3Rl
ckBkdW1teXNzbHRlc3RpbmcuY29tggkA4MPIITtX0TcwCQYDVR0SBAIwADANBgkq
hkiG9w0BAQQFAAOBgQAMw7vnW4aWgwQZEpjWEYxzRkbAD1+vWYbtdNix9kPtHzWu
e5Fr9c4iuzSHW6cC8natTQc+8iAUNjokBpZ2PT62mENRsNjfj2Ov3/OzXuUYtwkt
```

```
OtOCddd5gM1DL6ovxM4k59VLkDYdn5p0kwknSAGHJyoUjQ3g7XWGAOffJy+Wbw==
-----END CERTIFICATE-----
...
/cfg/cert 1/revoke/.
/cfg/cert 1/revoke/automatic/.
        anonymous false
        interval 1d
        verify off
        ena disabled
/cfg/vpn 1/.
        name VPN-1
        ips 216.13.56.91
        standalone on
        hostippool false
/cfg/vpn 1/aaa/.
        idlettl 2m
        sessionttl infinity
        authorder 1
        defauth on
        defippool 1
/cfg/vpn 1/aaa/tg/.
        ena disabled
        recheck 15m
        action teardown
        details on
        runonce off
        logmode off
        loglevel info
        bypass off
/cfg/vpn 1/aaa/tg/agent/.
        timeout 2s
        minver 0.0.0.0
/cfg/vpn 1/aaa/nap/.
        autorem false
/cfg/vpn 1/aaa/nap/probation/.
        ena false
/cfg/vpn 1/aaa/nap/servers/.
/cfg/vpn 1/aaa/nap/shvs/.
        add 311 128 wshv
        add 40082 0 nshv
/cfg/vpn 1/aaa/nap/wshv/.
        firewall on
        autoupdate on
/cfg/vpn 1/aaa/nap/wshv/virus/.
        enabled false
/cfg/vpn 1/aaa/nap/wshv/spyware/.
        enabled false
/cfg/vpn 1/aaa/nap/wshv/secupdates/.
        enabled false
/cfg/vpn 1/aaa/wholesec/.
        ena false
/cfg/vpn 1/aaa/auth 1/.
        type local
        name local
/cfg/vpn 1/aaa/auth 1/local/.
        pwdage 0
        expirewarn 15
/cfg/vpn 1/aaa/auth 1/adv/.
/cfg/vpn 1/aaa/seqauth/.
        ena false
        copyuser off
        usesecond off
        retries 3
/cfg/vpn 1/aaa/network 1/.
        name intranet
```

```
/cfg/vpn 1/aaa/network 1/subnet 4/.
        net 172.16.1.50
        mask 255.255.255.255
/cfg/vpn 1/aaa/group 1/.
        name trusted
        restrict 0
        usertype advanced
        idlettl 0
        sessionttl 0
        ippool 1
/cfg/vpn 1/aaa/group 1/access 1/.
        network intranet
        service *
        appspec *
        extspec *
        action accept
/cfg/vpn 1/aaa/group 1/linkset/.
        add base-links
/cfg/vpn 1/aaa/group 1/l2tp/.
/cfg/vpn 1/aaa/group 1/ipsec/.
/cfg/vpn 1/aaa/ssodomains/.
/cfg/vpn 1/aaa/ssoheaders/.
/cfg/vpn 1/aaa/radacct/.
        ena false
/cfg/vpn 1/aaa/radacct/servers/.
/cfg/vpn 1/aaa/radacct/vpnattribute/.
        vendorid "1872 (alteon)"
        vendortype 3
/cfg/vpn 1/aaa/adv/.
/cfg/vpn 1/aaa/adv/unmatchgrp/.
        ena disabled
/cfg/vpn 1/server/.
        port "443 (https)"
        loopback on
        fastfin off
        ena enabled
/cfg/vpn 1/server/trace/.
/cfg/vpn 1/server/ssl/.
        cert 1
        cachesize 4000
        cachettl 5m
        renegotiate legacy
        protocol ssl3
        log none
        verifylog none
        ciphers AES256-SHA
        verify none
        ena enabled
/cfg/vpn 1/server/tcp/.
        cwrite 15m
        ckeep 15m
        skeep 2m
        sinterval 1m
        swrite 15m
        sconnect 30s
        csendbuf auto
        crecbuf auto
        ssendbuf auto
        srecbuf 6000
/cfg/vpn 1/server/http/.
        downstatus unavailable
        securecookie on
        certcard off
        cookieonce off
        sslheader off
```

```
        sslxheader off
        sslsidheader off
        addxfor off
        addvia on
        addxisd off
        addclicert off
        addnostore on
        nocachehdr off
        compress off
        allowimage on
        allowdoc off
        allowscript off
        allowica on
        cmsie on
        maxrcount 40
        maxline 16384
        urlobscure off
        sessionhdr off
/cfg/vpn 1/server/http/rewrite/.
        paramtag none
        urldeferattr on
        rewrite off
        ciphers HIGH:MEDIUM
        response iSD
        URI "/cgi-bin/weakcipher"
/cfg/vpn 1/server/proxymap/.
/cfg/vpn 1/server/portal/.
        wipecookies on
        cookiedb on
        resetcookie off
        persistent off
/cfg/vpn 1/server/portal/urlrewrite/.
        rewrite on
        jrewrite on
        cssrewrite on
        gziprewrite on
        ena enabled
/cfg/vpn 1/server/adv/.
/cfg/vpn 1/server/adv/traflog/.
        protocol bsd
        sysloghost 0.0.0.0
        udpport 514
        priority info
        facility local4
        ena disabled
/cfg/vpn 1/server/adv/sslconnect/.
        protocol ssl23
        cachemode on
        ciphers EXP-RC4-MD5:ALL!DH
/cfg/vpn 1/server/adv/sslconnect/verify/.
        verify none
/cfg/vpn 1/l2tp/.
        ena disabled
        cert unset
        authorder mschapv2,pap
        groupmatch true
/cfg/vpn 1/ipsec/.
        ena disabled
        cert unset
        groupmatch true
        groupbind off
/cfg/vpn 1/ipsec/sys/.
/cfg/vpn 1/ipsec/sys/failover/.
        primary 0.0.0.0
        secondary 0.0.0.0
```

```
        tertiary 0.0.0.0
/cfg/vpn 1/ipsec/sys/nat-t/.
        udpport 10001
        portswitch off
        ena false
/cfg/vpn 1/ippool 1/.
        type local
        name Local_pool
        lowerip 10.0.0.1
        upperip 10.0.0.100
        proxyarp on
        ena enabled
/cfg/vpn 1/ippool 1/exclude/.
/cfg/vpn 1/ippool 1/netattr/.
        netmask 255.255.255.0
        primnbns 0.0.0.0
        secnbns 0.0.0.0
        primdns 0.0.0.0
        secdns 0.0.0.0
/cfg/vpn 1/portal/.
        logintext
This is a configurable text.
...
        seclogtext
This is a configurable text.
...
        iconmode fancy
        linktext

...
        linkurl on
        punblock off
        linkcols 2
        linkwidth 100%
        companyname "Avaya Inc."
        smbworkgrp WORKGROUP
        autojre on
        applet on
        wiper on
        rsaauto off
        ieclear on
        citrix off
        clientauth off
        trustsite off
/cfg/vpn 1/portal/colors/.
        color1 #ececec
        color2 #ececec
        color3 #cc0000
        color4 #cc0000
/cfg/vpn 1/portal/content/.
        ena disabled
/cfg/vpn 1/portal/faccess/.
        ena disabled
        ipsecmode native
        contip 0.0.0.0
        portalmsg
From this page you can gain full network access. This
requires that Net Direct is enabled or
that you have either Avaya's IPSEC client (version 4.89 or better)
and/or SSL-VPN (TDI version 1.1 or better) client installed. If the Net Direct
installable client is installed it will be used if Net Direct is enabled.
Note: Your browser must support Java. If not download SUN's
J2SE JRE from
class="white_link" href="javascript:download_jre()">www.java.com.
Remember: You can only access resources on the network as defined by
```

```
your access rights. Contact your network operator if you are
dissatisfied with your current access rights.
...
appletmsg
The quest for full network access has started._The outcome of the quest will be indicated
in the progress bar and console window below.
...
/cfg/vpn 1/portal/lang/.
        setlang en
/cfg/vpn 1/portal/lang/beconv/.
/cfg/vpn 1/portal/whitelist/.
        ena disabled
/cfg/vpn 1/portal/whitelist/domains/.
/cfg/vpn 1/portal/blacklist/.
        ena disabled
/cfg/vpn 1/portal/blacklist/domains/.
/cfg/vpn 1/portal/usertype/.
/cfg/vpn 1/portal/usertype/novice/.
        sysinfo off
/cfg/vpn 1/linkset 1/.
        name base-links
        autorun false
/cfg/vpn 1/linkset 1/link 1/.
        href <netdirect>
        NetdirectFlag off
        type netdirect
/cfg/vpn 1/linkset 1/link 1/netdirect/.
/cfg/vpn 1/vdesktop/.
        ena off
        prelogon off
        always off
        force off
        switch off
        secure off
        persist off
        filesep off
        remdisk off
        print off
        netshare off
        cryptlevel 128
        timeout 5
        conncntrl off
/cfg/vpn 1/vdesktop/mcd/.
        ena disabled
        keylogger off
        scrscrap off
        acntcreate off
/cfg/vpn 1/vdesktop/mcd/vkeyboard/.
        ena disabled
/cfg/vpn 1/sslclient/.
        ippool off
        netdirect on
        caching off
        ndbanner
This is Netdirect Banner!
...
ndlicense
END USER LICENSE AGREEMENT
FOR AVAYA VPN CLIENT
This Software License Agreement ('Agreement') is between you, ('User') and Avaya
Corporation and its subsidiaries and affiliates ('Avaya').  PLEASE READ THE FOLLOWING
CAREFULLY.
BY CLICKING ON THE 'YES' BUTTON OR USING THIS SOFTWARE, YOU ('USER') ARE CONSENTING TO BE
BOUND BY THIS AGREEMENT BETWEEN YOURSELF AND AVAYA.  IF YOU DO NOT AGREE TO BE BOUND BY
THIS AGREEMENT, CLICK 'NO' AND DO NOT USE THIS SOFTWARE.
```

```
LICENSE GRANT: This Agreement shall govern the licensing of Avaya and Avaya licensor's
software and the accompanying user manuals, on line help services, Avaya Web Site and
other instructions (collectively, the 'Software') provided or made available to User.
The Software includes client software, which resides on the computers of User, to access
Sublicensor's networks (the 'Client Software').  The Software provided under this License
is proprietary to Avaya and to third parties from whom Avaya has acquired license
rights.  This Software was licensed in conjunction with the purchase of a 'Avaya VPN
Gateway' or other Avaya VPN device, that will give the User access to the Sublicensor's
purchaser's network and may only be used for this purpose by you.  User is hereby granted
a nonexclusive object code only license to use the Software under the following terms:
- User shall use the Software only in conjunction with the Avaya VPN Gateway or other
Avaya VPN device with which the Software was distributed.
- User may make one copy of the Software only for safekeeping (archives) or backup
purposes.
- User may not modify, translate, adapt, decompile, disassemble, decrypt, extract,
or otherwise reverse engineer or attempt to discover the source code and techniques
incorporated in the Software.  User may not create derivative works based on the Software
or any trade secret or proprietary information of Avaya.
- Title to Software shall not pass to User.
- User shall not provide, or otherwise make available, any Software, in whole or in part,
in any form, to any third party, nor shall User sublicense, rent or lease the Software.
- Upon termination or breach of this Agreement, or in the event that the Avaya device
with which it was distributed is no longer in use, User will immediately cease use of
and destroy all copies of the Software and  return the Software to Avaya or certify as
to such destruction to Avaya that is has been destroyed. Avaya and Third-party owners
from whom Avaya has acquired license rights to material that is incorporated into the
Software shall have the right to enforce the provisions of this Agreement against User.
IN NO EVENT SHALL AVAYA OR ITS  AGENTS, SUPPLIERS, MANUFACTURERS OR DISTRIBUTORS BE
LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF
BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION OR DATA, DAMAGES
BASED ON ANY THIRD PARTY CLAIM,  OR, OR ANY OTHER PECUNIARY LOSS ARISING OUT OF THE USE
OR INABILITY TO USE THE SOFTWARE, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY
OF SUCH DAMAGES.  SOME JURISDICTIONS DO NOT ALLOW THESE LIMITATIONS OR EXCLUSIONS AND IN
SUCH EVENT THEY MAY NOT APPLY.
User agrees to comply with all export restrictions regarding the Software, and shall not
export, directly or indirectly, any Software or related technical data or information
without first obtaining any required export licenses or other governmental approvals. THE
SOFTWARE IS PROVIDED 'AS IS' WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS
OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. THE ENTIRE RISK ARISING OUT OF
USE OR PERFORMANCE OF THE SOFTWARE REMAINS WITH USER.  Avaya is not obligated to User
to provide support of any kind for the Software, and in the event it chooses to do
so, such support is subject to the terms of this Agreement.  Some jurisdictions do not
allow exclusion of implied warranties and, in such event, the above exclusions may not
apply. If User is the United States Government, the following paragraph shall apply:
All Software provided hereunder is commercial computer software and commercial computer
software documentation, as applicable, and in the event Software is licensed for or
on behalf of the United States Government, the respective rights to the Software is
governed by Avaya standard commercial license in accordance with U.S. Federal Regulations
at 48 C.F.R. Sections 12.212 (for non-DoD entities) and  48 C.F.R. 227.7202 (for DoD
entities). Software contains trade secrets and copyrighted material and User agrees to
treat the Software as confidential information using a reasonable standard of care.  User
shall not remove or obscure any copyright, patent, trademark, trade secret, or similar
intellectual property or restricted rights notice within or affixed to any Software and
shall reproduce and affix such notices on any backup copy of software. User may terminate
this Agreement at any time.  Avaya may terminate this Agreement if User fails to comply
with any of its terms.  This Agreement is the complete and exclusive agreement between
the parties hereto regarding its subject matter, and shall be governed solely by the laws
of the state of New York, without regard to its rules governing conflicts of law.
...
          oslist all
        udpports 5000-5001
        rekeytraf 0
        rekeytime 8h
        portalbind on
```

```
        idlecheck off
        keepalive 0
        recncttime 3m
        clampmss on
        splittun enabled
        tdiclient off
        lspclient off
        oldclients false
/cfg/vp
```

Index

O

P

R

S

T

V