Guías de Soluciones del Cliente

Soluciones de Seguridad de Cisco®

Construyendo la Red de Autodefensa de Cisco

Índice de materias

Por qué la seguridad es más importante que nunca

- Reputación
- Cumplimiento normativo
- Limitación de la responsabilidad
- Operaciones comerciales eficientes
- Cuestiones iniciales
- Introducción a la Red de Autodefensa de Cisco (Cisco Self-Defending Network)

Reputación

Los consumidores están preocupados. Si permite que la información personal de sus clientes corra riesgos, sus relaciones con ellos y su reputación, sufren espectacularmente. Además, usted no quiere ser la causa de una infección o de una violación de las políticas de seguridad en las redes de sus clientes.

Cumplimiento normativo

Cada empresa está sujeta a algún tipo de normativa, frecuentemente relacionada con la privacidad y la protección de la información del cliente. El cumplimiento de la normativa exige una seguridad rigurosa y bien planeada.

Limitación de la responsabilidad

Si alguna vez se enfrenta una acción judicial, debe demostrar que ha aplicado la debida diligencia en la protección de sus recursos, incluida la información. Normalmente si se demuestra la debida diligencia, se reduce la responsabilidad.

Operaciones comerciales eficientes

Cualquier empresa puede determinar lo que le cuesta un día de inactividad. Los gusanos, los virus, los piratas informáticos e incluso los empleados, contribuyen a la interrupción de las operaciones empresariales, lo cual cada vez ocurre con mayor frecuencia.

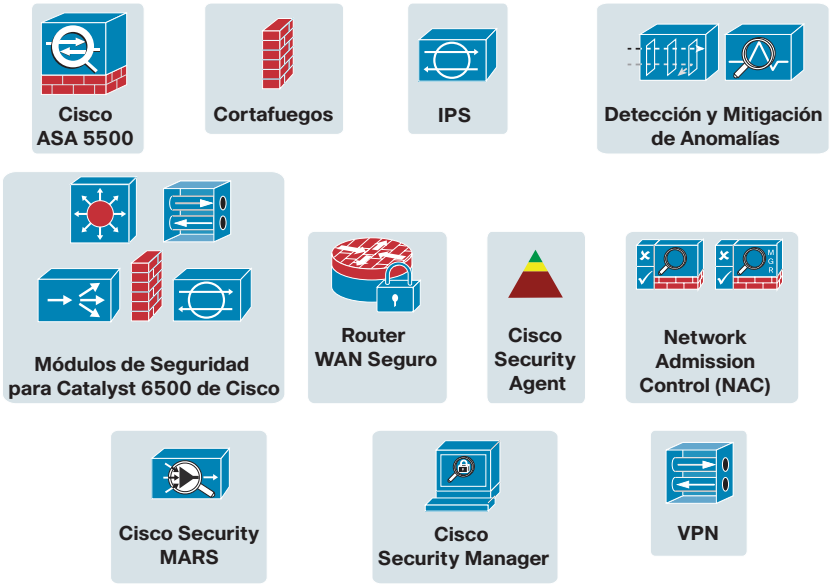
Preguntas iniciales

- ¿Cómo comparte información electrónicamente con sus clientes?
- ¿Cómo almacena datos confidenciales de clientes?
- ¿ Ha sufrido su empresa alguna vez un incidente de seguridad?
- Si sus clientes, reguladores o auditores le pidieran ver su plan de seguridad, ¿qué les mostraría?
- ¿Tiene una política de seguridad documentada que defina claramente la forma en que protege los recursos de su empresa, incluida la información?
- ¿Puede hacer cumplir esta política?
- Cada punto de acceso a su red también es un punto de riesgo. ¿Cuál es su plan para proteger cada punto de entrada en la red?
- ¿Podemos dedicar algún tiempo a discutir cómo Cisco protege la red de un extremo a otro?

Introducción a la Red de Autodefensa de Cisco (Cisco Self-Defending Network)

La Red de Autodefensa de Cisco es una arquitectura o sistema de seguridad que proporciona una defensa de extremo a extremo de la red al mismo tiempo que refuerza el cumplimiento de la política. El sistema garantiza la defensa contra amenazas y el cumplimiento de políticas en cada punto de entrada en la red, por lo que empresas de todos los tamaños pueden mitigar el riesgo significativamente, al mismo tiempo que demuestran una mayor diligencia en la protección de información. Esta arquitectura comprende soluciones desarrolladas por Cisco ® y muchos proveedores de hardware y software de la industria que participan formalmente en esta importante iniciativa de seguridad. La Red de Autodefensa de Cisco es escalable y puede aplicarse a empresas de cualquier tamaño. Actualmente los clientes, reguladores y auditores esperan una defensa completa del sistema, y Cisco está en una posición única para proporcionar esta defensa a través de la amplia cartera de soluciones de Cisco englobadas en la Red de Autodefensa y de la extensa colaboración y soporte de la industria.

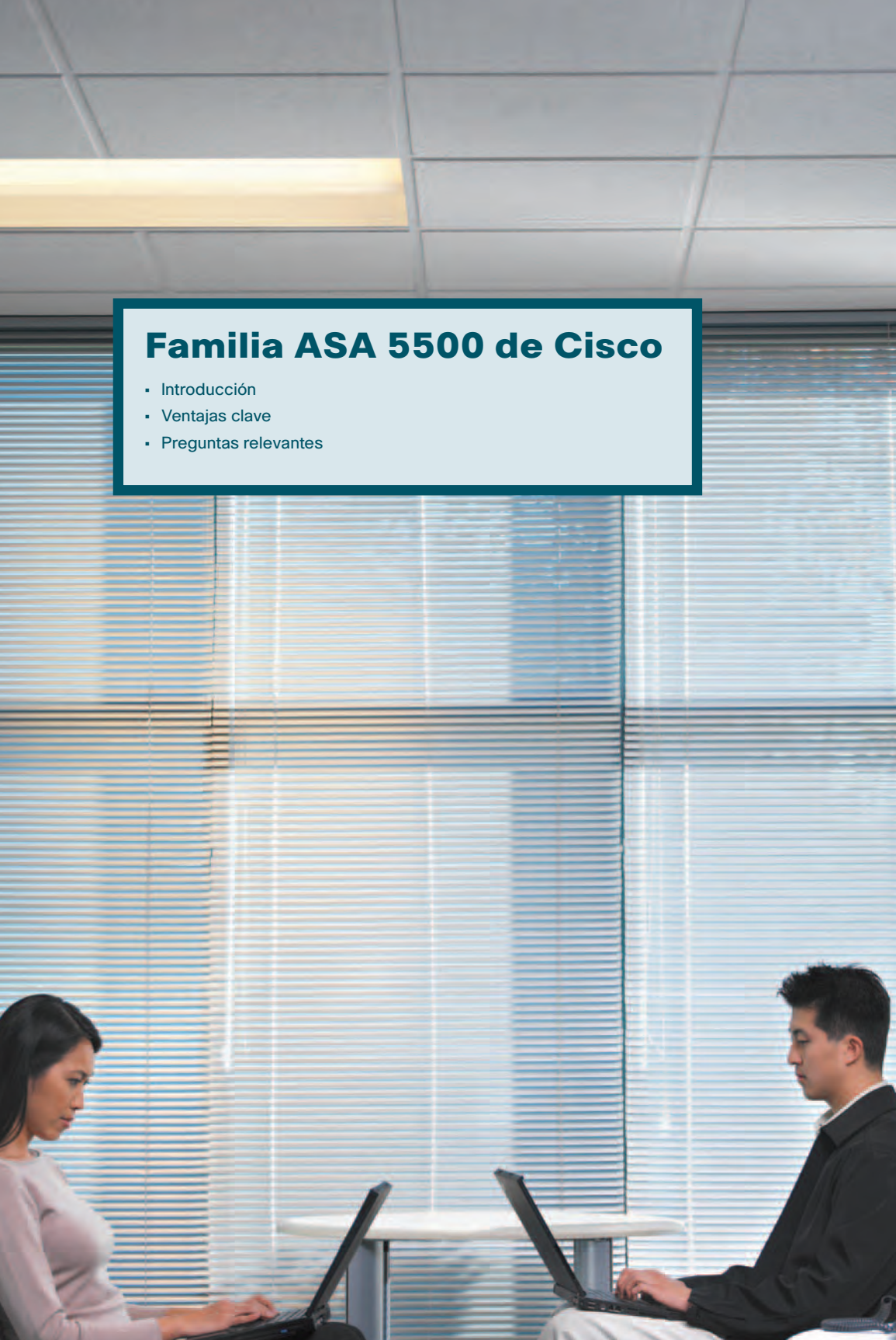
Consulte la Figura 1 para ver las categorías de soluciones de seguridad de Cisco.



"Cualquiera puede construir una señal de stop-o incluso un semáforo-pero para concebir un sistema de control de tráfico para toda una ciudad se requiere un modo de pensar diferente."
–Bruce Schneier, "Beyond Fear"(Más allá del miedo)

Familia ASA 5500 de Cisco

- Introducción
- Ventajas clave
- Preguntas relevantes

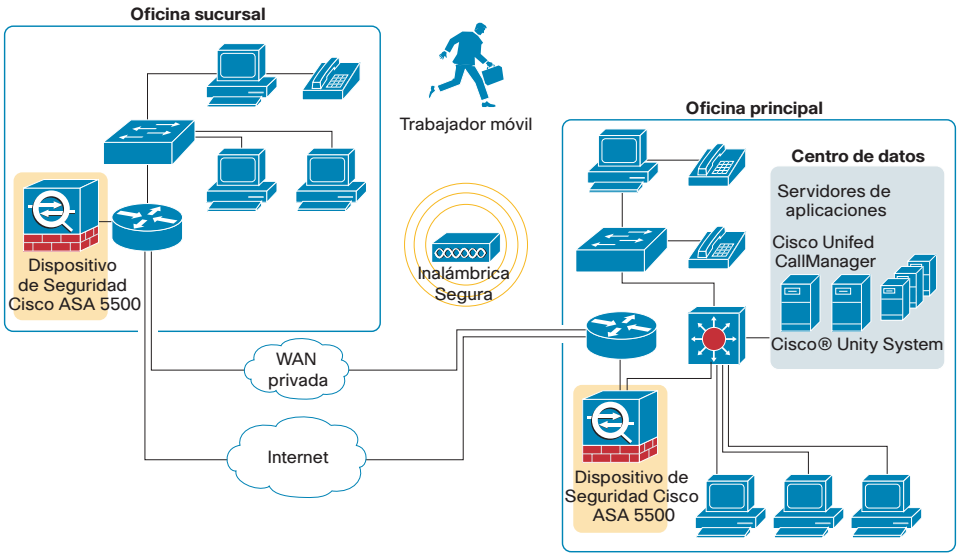


Introducción

- La familia ASA 5500 de Cisco® integra la funcionalidad completa de cortafuegos de alto rendimiento, sistema de prevención de intrusos (intrusion prevention system (IPS)), servicios anti-X, y terminacón de redes virtuales privadas o VPN basadas en IPSecurity y Secure Sockets Layer (IPsec/SSL) en un solo dispositivo de seguridad fácil de utilizar.
- La familia ASA 5500 le proporcionará una robusta solución para su red al mismo tiempo que se reduce el coste y la complejidad de la misma, combinando funciones de seguridad múltiples en un dispositivo de alto rendimiento.
- La familia está formada por distintos modelos y configuraciones de los ASA 5500 y esto facilita su utilización como cortafuegos, dispositivo IPS, núcleo de los servicios anti-X y concentrador VPNs, proporcionando los servicios más apropiados para el lugar idóneo de la empresa. Puden encontrarse también modelos diseñados para empresas pequeñas y medianas con el objetivo de que estas empresas se beneficien de una solución de seguridad completa y robusta que combina la funcionalidad de cortafuegos líder del mercado, los servicios VPN y capacidades anti-X opcionales.

La Figura 2 muestra donde encajan en la red los dispositivos de seguridad ASA 5500 de Cisco.

Figura 2 Donde encaja



Ventajas clave

- Reduce el coste y la complejidad proporcionando servicios de cortafuegos, VPN, prevención de intrusos y defensa anti-X en red
- Suministra servicios de seguridad múltiples con alto rendimiento por el mismo coste que un cortafuegos
- Se adapta a nuevas amenazas a la seguridad
- Los clientes Cisco se familiarizan con el producto rápidamente pues el interfaz de configuración es el mismos que el de los cortafuegos PIX® de Cisco, los concentradores VPN 3000 de Cisco y los sensores IPS de Cisco
- Asegura que no se ponga en riesgo la oficina remota
- En un solo dispositivo, proporciona una solución integrada de protección contra amenazas a la conectividad, tanto si se utilizan VPNs SSL como VPNs IPsec

Preguntas relevantes

- ¿Está buscando formas de reducir el coste y la complejidad de sus despliegues de VPN y seguridad de red?
- ¿Quiere aumentar la productividad y la resiliencia empresarial proporcionando acceso remoto a la red a los empleados, contratistas y socios comerciales?
- ¿Sigue luchando contra amenazas relacionadas con Internet como gusanos, virus, spyware, spam e intentos de phishing?
- ¿Quisiera poder proporcionar servicios de seguridad adicionales para sus oficinas remotas?
- ¿Quiere elevar el nivel de su seguridad existente o añadir seguridad extra a su red?
- ¿Encuentra convincente el concepto de tener cortafuegos, IPS, antivirus de red y VPN remoto en un dispositivo gestionable único?

Cortafuegos (Familia ASA 5500 de Cisco, Cisco PIX, Módulos cortafuegos para Catalyst 6500 de Cisco y software IOS de Cisco)

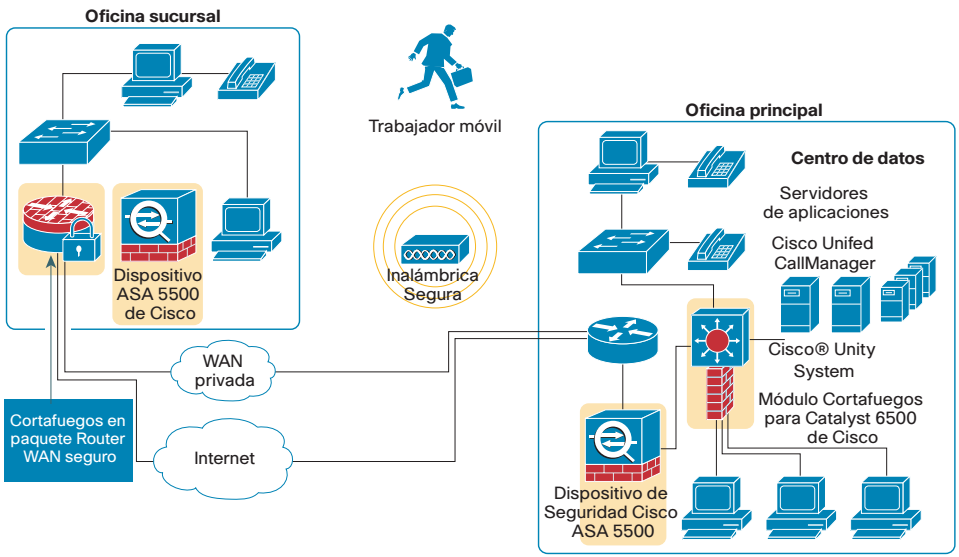
- Introducción
- Ventajas clave
- Preguntas relevantes

Introducción

- El cortafuegos protege los recursos de una red privada contra el acceso no autorizado de usuarios internos o externos a aplicaciones, redes y datos.
- Las soluciones cortafuegos de Cisco® proporcionan servicios de seguridad de red integrados, que incluyen:
  - Inspección de paquetes manteniendo información de estado (Stateful)
  - Inspección de protocolo y nivel de aplicación
  - Prevención de intrusiones en el camino de la transmisión
  - Seguridad de voz y tráfico multimedia en formatos diversos
- Cisco® ofrece soluciones múltiples de cortafuegos, que incluyen:
  - Dispositivos ASA 5500 y Cisco PIX®
  - Módulos cortafuegos para Catalyst® 6500 de Cisco para entornos que necesitan una mayor escalabilidad
  - Cortafuegos basado en software Cisco IOS® en routers de servicio integrados de Cisco

La Figura 3 muestra donde encajan en la red los productos cortafuegos.

Figura 3 Donde encaja

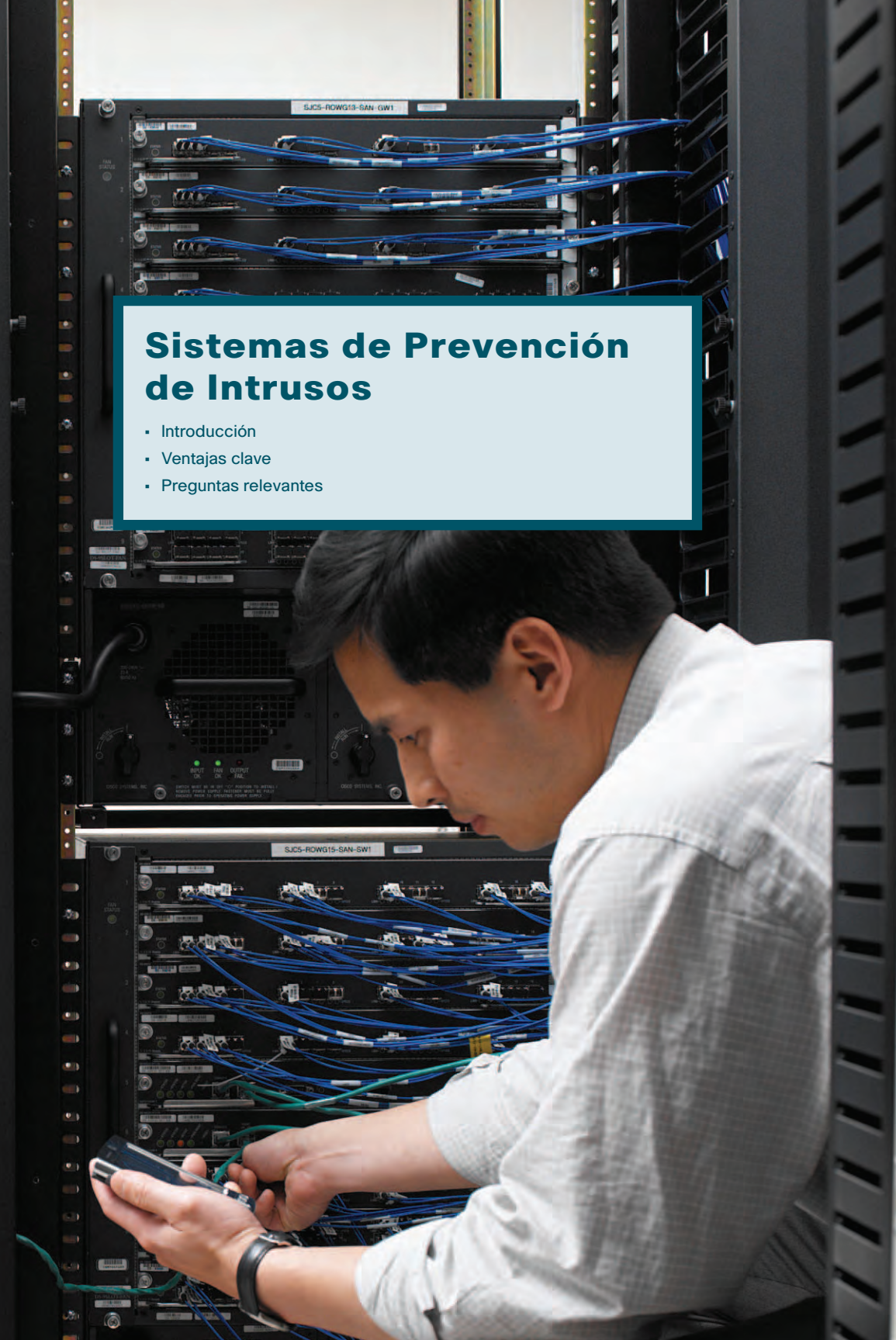


Ventajas clave

- Permite que organizaciones de todos los tamaños protejan su red crítica contra acceso no autorizado
- Ofrece soporte de múltiples protocolos para permitir el enrutamiento dinámico con el fin de mejorar la fiabilidad y el rendimiento
- Facilita la administración y la gestión centralizada de todas las soluciones de cortafuegos utilizando Cisco Security Manager
- Proporciona una infraestructura de seguridad sumamente redundante con capacidades de alta disponibilidad
- Maximiza el tiempo productivo, logrando una mejora de la productividad
- Permite el despliegue seguro de voz sobre IP y aplicaciones multimedia de próxima generación

Preguntas relevantes

- ¿Cree que tiene una estrategia cortafuegos completa basada en sus requisitos empresariales?
- ¿Qué tipo de usuarios finales y aplicaciones necesitan acceder a su red (empleados, proveedores, clientes, voz, video y contenidos)?
- ¿Tiene que utilizar soluciones de gestión múltiples para gestionar su infraestructura de seguridad?
- ¿Se beneficiaría de una familia de soluciones cortafuegos que cubriera desde su oficina sucursal más pequeña hasta el núcleo de su red?
- ¿Le parecen desmesurados los costes de mantenimiento de sus cortafuegos ?



Sistemas de Prevención de Intrusos

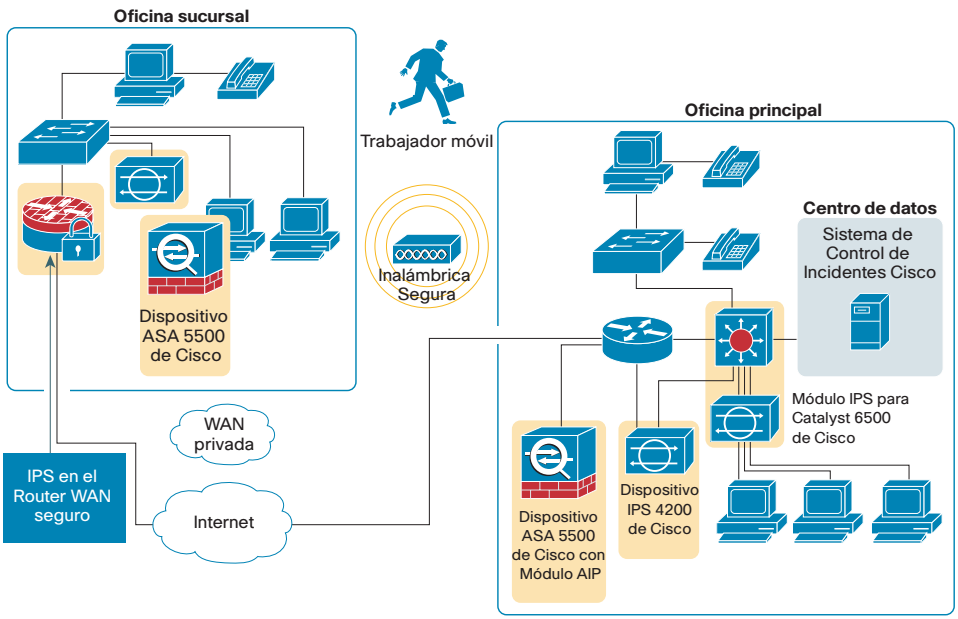
- Introducción
- Ventajas clave
- Preguntas relevantes

Introducción

- Los Sistemas de Prevención de Intrusos de Cisco® (Cisco® Intrusion Prevention System (IPS)) permiten que los administradores de redes y seguridad detecten con rapidez y precisión los intentos no autorizados de acceso a recursos críticos internos. Los IPS de Cisco son una solución basada en inspecciones de paquetes en profundidad con el objetivo de mitigar con efectividad una amplia gama de ataques a la red y proteger los datos y la infraestructura de red.
- Los productos IPS de Cisco ofrecen una prevención eficaz ante intrusos mediante cuatro elementos críticos:
  1. Detección precisa de las amenazas
  2. Investigación inteligente de las amenazas
  3. Facilidad de gestión
  4. Opciones flexibles de despliegue
- El sistema de control de incidencias de Cisco (Cisco Incident Control System (ICS)) aumenta el valor de los productos IPS de Cisco e impide ataques en la red mediante la activación de acciones preventivas a los pocos minutos de la detección de una nueva amenaza.

La Figura 4 muestra donde encajan en la red los productos IPS de Cisco.

Figura 4 Donde encaja



Ventajas clave

- La prevención precisa de amenazas detecta completamente todas las amenazas potenciales.
- La investigación inteligente de amenazas reduce enormemente las alarmas falsas.
- La facilidad de gestión a través de herramientas basadas en navegadores web simplifica la interacción al mismo tiempo que proporciona potentes herramientas analíticas.
- Las opciones flexibles de despliegue incluyen:
  - Familia de dispositivos IPS 4200
  - Módulos integrados de Inspección y prevención avanzada (Advanced Inspection and Prevention (AIP)) para ASA 5500 de Cisco
  -Sistemas integrados de prevención de intrusiones en router (IPS)
  - Módulos de de detección de intrusos (Intrusion Detection System (IDSM-2)) para Catalyst® 6500 de Cisco
- El dispositivo ICS de Cisco configura los IPS, routers y conmutador de la red para detener a la red de la invasión de gusanos y virus de red.

Preguntas relevantes

- ¿Cree que tiene una estrategia completa para detección y correlación de intrusios en red?
- ¿Puede demostrar a sus auditores que tiene un enfoque coherente para defender la red a nivel de toda la empresa?
- ¿Ha experimentado pérdidas económicas causadas por ataques, robos o desfiguración debido que alguien accedió de forma ilícita a sus servidores críticos?
- ¿Considera que el problema del masivo número de alarmas falsas resultan frustrantes en su despliegue actual de IPS?
- ¿Le gustaría poder detener invasiones de gusanos y virus a nivel de red, antes de que lleguen al ordenador?

Soluciones Cisco para la Detección y Mitigación de Anomalías

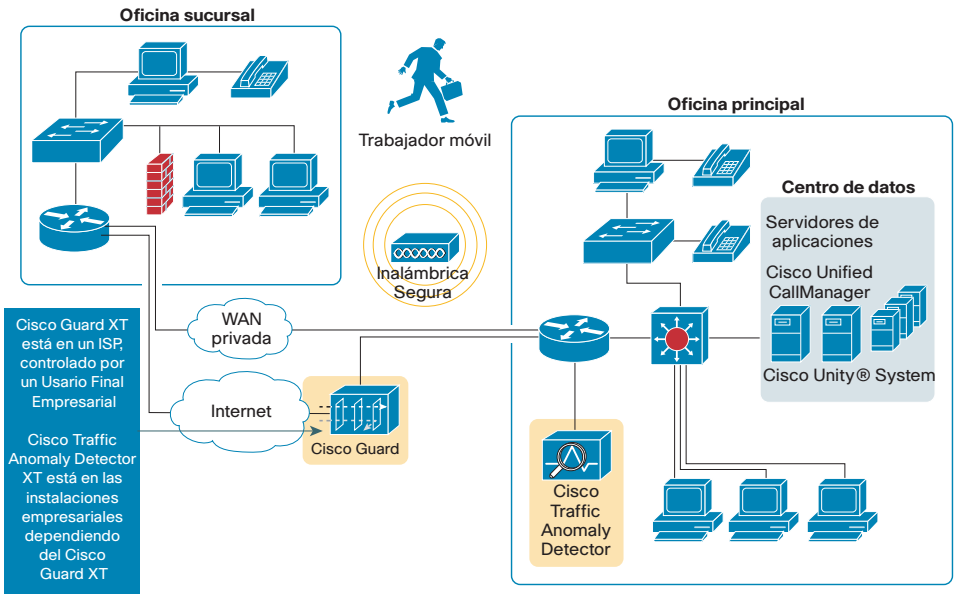
- Introducción
- Ventajas clave
- Preguntas relevantes

Introducción

- La soluciones Cisco® para la Detección y Mitigación de Anomalías no sólo detectan la presencia de un ataque distribuido de denegación de servicio (denial-of-service (DDoS)), sino que además identifican y bloquean tráfico malicioso en tiempo real sin afectar al flujo de las transacciones legítimas de misión crítica.
- Gracias a esto, las operaciones empresariales de las organizaciones objetivo, continúan funcionando, lo que ayuda a asegurar que los recursos corporativos críticos estén siempre protegidos.

La Figura 5 muestra donde encajan en la red las soluciones Cisco para la Detección y Mitigación de Anomalías.

Figura 5 Donde encaja



Ventajas clave

- Tiene en cuenta la necesidad de “asegurar la disponibilidad” de la red y de los recursos del centro de procesamiento de datos
- Impide que un excesivo número de transacciones que parecen legítimas afecten la disponibilidad empresarial
- Refuerza la solución de seguridad general
- Permite que los cortafuegos, la inspección de contenidos y el sistema de prevención de intrusiones (IPS) ejecute funciones complementarias de protección de acceso e integridad de datos
- Opciones de producto:

- Dispositivos dedicados Cisco Guard XT y Traffic Anomaly Detector XT

- Módulos Guard y Traffic Anomaly Detector para Catalyst® 6500 de Cisco

Preguntas relevantes

- ¿Será afectada su empresa si su sitio web es el objetivo de un ataque DoS?
- ¿Está preparada su organización para detectar y mitigar la gama más amplia de ataques DDoS?
- ¿Puede garantizar la continuidad empresarial permitiendo que los usuarios legítimos accedan a su sitio web al mismo tiempo que desvía a usuarios ilegítimos?
- ¿Es consciente de que las soluciones Cisco para la Detección y Mitigación de Anomalías pueden ofrecer una oportunidad de servicios gestionados a clientes que no pueden permitirse gestinar su propia protección contra DDoS?

Módulos de Seguridad para Catalyst 6500 de Cisco

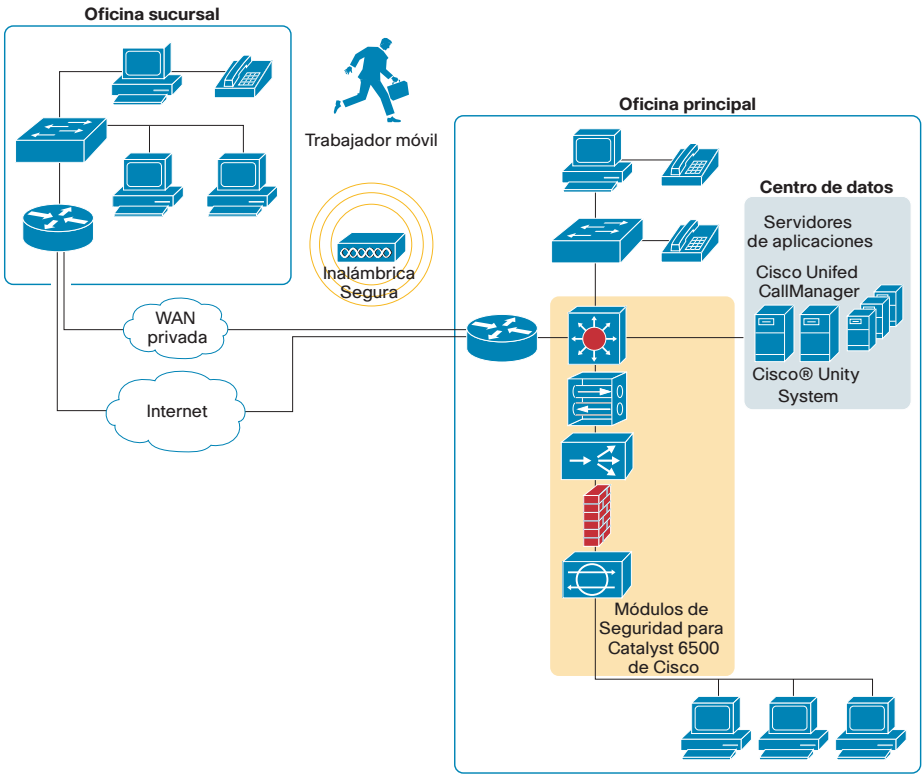
- Introducción
- Ventajas clave
- Preguntas relevantes

Introducción

- Cisco Systems® proporciona seguridad de red integrada por medio de un paquete de módulos de seguridad avanzada en los conmutadores Catalyst® 6500 de Cisco o en los routers 7600, que incluyen módulos cortafuegos, módulos de prevención de intrusos (IPS), módulos de detección de anomalías como los ataques de denegación de servicio en modo distribuido (distributed denial-of-service (DDoS)), modulos para establecimiento de redes privadas virtuales o VPN con IPSec y un módulo de análisis de red con capacidad gigabit
- Estos módulos de seguridad añaden seguridad integrada, adaptiva, escalable y de alta disponibilidad a la conectividad, los servicios y las aplicaciones en red.

La Figura 6 muestra donde encajan en la red los Módulos de Seguridad para Catalyst 6500 de Cisco.

Figura 6 Donde encaja



Ventajas clave

- Capacidad de aprovechar la inversión en conmutadores Cisco Catalyst 6500 o routers 7600
- Soluciones de seguridad a nivel de infraestructura estrechamente integradas con los dispositivos de red
- Soluciones de seguridad de gran rendimiento que ofrecen capacidad multigigabit en un solo conmutador Cisco Catalyst 6500
- Visibilidad de nivel de aplicación en la infraestructura
- Protección de una plataforma crítica para la colaboración de tecnologías emergentes tales como las que permiten el tratamiento de los mensajes entre aplicaciones en los dispositivos de red.

Preguntas relevantes

- Módulo de servicios VPN
  -Teniendo en cuenta la normativa de la industria, ¿cómo planea garantizar el cifrado de alto rendimiento a través de su red?
  -¿Ha considerado utilizar tecnología VPN para proteger su red inalámbrica de forma que el cifrado no afecte al rendimiento de su red inalámbrica?
- Módulo de servicios cortafuegos
  - Las estrategias de seguridad recomendadas consisten en colocar los sistemas de seguridad más cerca de todos los puntos finales y proporcionar más segmentación entre redes. ¿Tiene alguna estrategia de este tipo?
- Módulo de análisis de red
  -¿Cuál es su estrategia para analizar flujos de tráfico cuando está sufriendo un ataque, con el fin de identificar amenazas desconocidas?
- Módulo de sistema de detección de intrusiones
  -¿Cómo planea identificar y bloquear ataques maliciosos que atraviesan el núcleo de su red?

Paquete Router WAN Seguro de Cisco

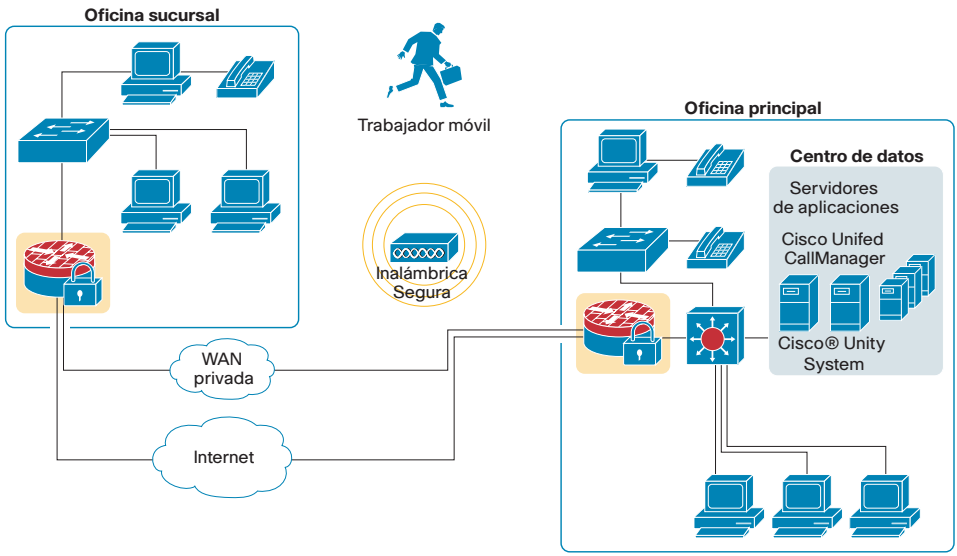
- Introducción
- Ventajas clave
- Preguntas relevantes

Introducción

- El paquete Router WAN Seguro de Cisco® añade una multitud de importantes funciones de seguridad a su router de sucursal por un pequeño coste incremental que proporciona un retorno de la inversión muy alto.
- El paquete añade las capacidades siguientes a su router de sucursal: VPN del sitio web a sitio web, VPN de acceso remoto, cortafuegos que mantienen información de estado, cortafuegos de aplicaciones, filtrado de URLs, prevención de intrusos, control de admisión en red o NAC (Network Admission Control) y gestión segura.
- En la actualidad, la sucursal debe ser tan segura como la sede corporativa. Los paquetes Router WAN Seguro de Cisco® proporcionan un medio persuasivo y económico para aumentar la seguridad, eliminando el gasto del dinero y tiempo requeridos al añadir estas importantes funciones de seguridad en el futuro.
- Los routers de servicios integrados de Cisco pueden habilitar otros servicios como comunicaciones IP (voz y video) y LAN inalámbrica seguras.

La Figura 7 muestra donde encaja en la red el paquete Router WAN Seguro de Cisco.

Figura 7 Donde encaja

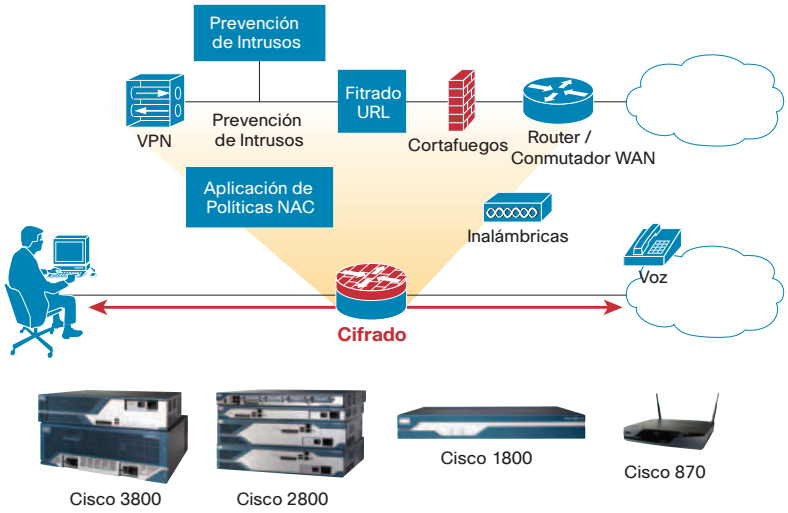


Ventajas clave

- Maximiza el retorno de la inversión al aumentar enormemente el valor del router con servicios de seguridad, que incluyen la terminación de redes virtuales privadas con IP Security (IPsec) y Secure Sockets Layer (SSL), cortafuegos, sistema de prevención de intrusos (IPS), Control de Admisión en red (NAC) y filtrado de URLs
- Permite que las empresas desplieguen con seguridad LANs inalámbricas y servicios de comunicaciones unificados como voz y video
- Ofrece una forma segura, económica, fácil de gestionar y escalable para comunicaciones empresariales de sitio web a sitio web
- Permite cumplir las leyes sobre protección de datos y privacidad como la LOPD o los requisitos del mercado para realizar pagos con tarjetas de crédito a traves de la red
- Simplifica la gestión ya que la seguridad se integra con otros servicios en un solo dispositivo de red

La Figura 8 muestra los numerosos servicios de seguridad disponibles en los routers de servicios integrados de Cisco.

Figura 8 Servicios de seguridad en routers de servicios integrados de Cisco



Preguntas relevantes

- ¿Ha puesto el mismo énfasis en proteger sus sucursales que en proteger su sede central?
- ¿Le gustaría poder aprovechar su inversión en routers Cisco Systems® para proteger su red?
- ¿Le gustaría poder consolidar cajas múltiples y proporcionar enrutamiento, conmutación, conexión inalámbrica, voz y seguridad en una plataforma única?
- Si sigue formulando su estrategia de seguridad, ¿es razonable esperar que usted necesite una de estas funciones de seguridad de WAN en el próximo período de 12 a 18 meses? Si lo es, será mucho más costoso añadir estas capacidades en el futuro, considerando los costes de actualizar cada router y el trastorno de las operaciones normales de router.

Cisco Security Agent

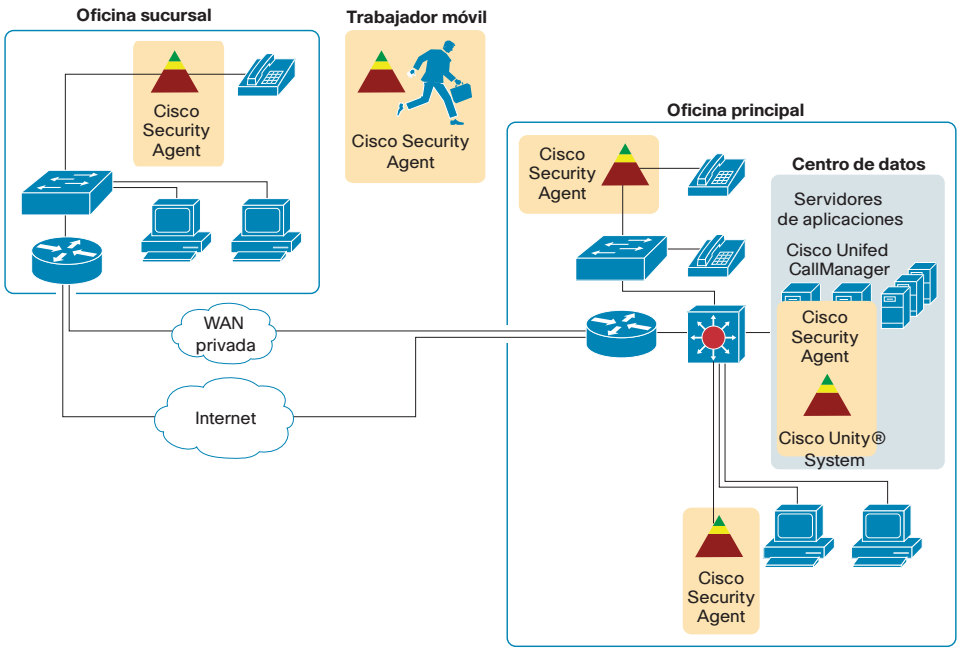
- Introducción
- Ventajas clave
- Preguntas relevantes

Introducción

- Añade y amplía funciones múltiples de seguridad en el extremo de la red (ordenadores o servidores) como la prevención de intrusos, las funciones de cortafuegos distribuido, la protección contra códigos maliciosos, y la garantía de la integridad del sistema operativo, todo dentro de un solo agente
- Protege proactivamente contra categorías completas de ataques, que incluyen spyware, escaneos de puertos, desbordamientos de memoria intermedia, troyanos, paquetes invalidos, solicitudes maliciosas de HTML y gusanos que se transmiten a través del correo electrónico
- Proporciona prevención de actualizaciones de día cero para ataques conocidos y desconocidos; no se requieren parches de emergencia
- Lidera la industria en la protección de servidores y PCs ya que protege contra amenazas conocidas y desconocidas al estar basado en el análisis del comportamiento.
- Proporciona protección específica de aplicaciones para servidores Web y bases de datos
- Incorpora arquitectura escalable a nivel de empresa; hasta 100.000 agentes por gestor

La Figura 9 muestra donde encaja en la red el Cisco Security Agent.

Figura 9 Donde encaja



Ventajas clave

- Proporciona protección para servidores y PCs detectando y previniendo comportamientos maliciosos
- Impide ataques desconocidos sin requerir reconfiguración o actualizaciones; proporciona protección robusta al mismo tiempo que reduce los costes operativos
- Se integra con dispositivos de seguridad de red Cisco® :
  - Control de admisión en red o Network Admission Control (NAC)-Se integra con Cisco NAC ya que proporciona las credenciales que sirven para tomar decisiones sobre el acceso completo o parcial a la red del dispositivo en el que se está ejecutando.
  - Cisco Intrusion Prevention System (IPS)-Se integra con dispositivos Cisco IPS para proporcionar un mejor análisis de puntos finales dentro de la red; suministra información crítica de seguridad de punto final a dispositivos IPS, software IPS en el sitema operativo Cisco IOS®, familia ASA 5500 de Cisco y módulos IPS para Catalyst® 6500 Series/Routers 7600 de Cisco para proporcionar una mayor exactitud en las respuestas de IPS a eventos ocurridos en la red
- Proporciona un control fiable de calidad de servicio (QoS), garantizando que el tráfico de aplicaciones críticas se prioriza, mejorando por tanto el flujo de tráfico de misión crítica en la red
- A través de políticas basadas en normas, controla el acceso a las aplicaciones, las memorias y discos externos (USB) y en general a los recursos críticos de la máquina
- Crea inventarios de aplicaciones y perfiles instalados en puntos finales
- Facilita la gestión de parches proporcionando tiempo para probar nuevos parches antes de su despliegue en la red

Preguntas relevantes

- ¿Le gustaría poder priorizar tráfico de aplicaciones específicas para que estas tengan preferencia en la red en situaciones de congestión o ataque?
- ¿Le gustaría facilitar la exactitud en la operación de sus dispositivos Cisco IPS?
- ¿Le gustaría controlar e imponer políticas que regulen el uso de archivos de datos confidenciales, MP3s, mensajería instantánea, etc. a través de su empresa?
- ¿Encuentra que no puede probar y acreditar adecuadamente nuevos parches de vulnerabilidades de una forma oportuna? ¿Le gustaría reducir el tiempo improductivo dedicado a probar nuevos parches y el volumen de trabajo del departamento de informática asociado a la gestión de parches?
- ¿Cree que si se enfrentara a una acción judicial, podría demostrar con confianza que ha ejercido la debida diligencia al proteger la información crítica y confidencial asi como al controlar el comportamiento de los empleados?

- (Si su cliente tiene una solución de telefonía IP de Cisco) Debido a que la voz es una aplicación crítica para la empresa, Cisco Unified CallManager y el sistema de mensajería Cisco Unity® se entregan con un Cisco Security Agent. ¿Podemos explorar como aprovechar esta capacidad del producto Cisco Security Agent para sacar partido del control de políticas personalizadas y la generación centralizada de informes de eventos?
- En sus servidores que contienen datos privados, ¿le gustaría inhabilitar la capacidad de copiar archivos en soportes físicos como disquetes o unidades de memoria flash USB?
- Tiene desplegados en la actualidad dispositivos Cisco VPN para proporcionar acceso remoto a sus teletrabajadores y empleados móviles? ¿Cómo protege los ordenadores desde los que se conectan?
- ¿Le gustaría controlar la capacidad de los usuarios de copiar archivos confidenciales de servidores corporativos en sus soportes de datos removibles?

Control de Admisión en Red de Cisco

- Introducción
- Ventajas clave
- Preguntas relevantes

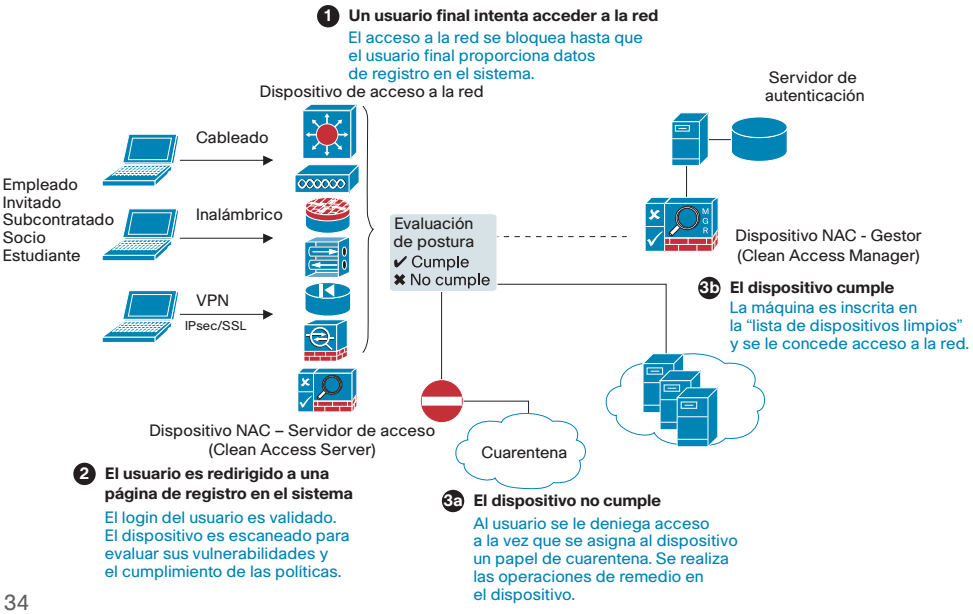
Introducción

- La propuesta de Control de Admisión en Red de Cisco® o Network Admission Control (NAC) es una solución que permite que la red imponga políticas de seguridad en todos los dispositivos que quieren acceder a los recursos informáticos de la red.
- Cisco NAC minimiza los riesgos asociados con dispositivos no acordes a la política de seguridad, independientemente del tipo de sistema, su origen y el método de acceso, lo que produce redes más resistentes y seguras.
- Cisco NAC proporciona una protección proactiva de la infraestructura y mejora enormemente la seguridad de la información en la red.
- Los dispositivos que no cumplen con las políticas se asocian a una red de cuarentena desde la que se podrán realizar las acciones necesarias para que el dispositivo cumpla con todos los criterisos de acceso a la red sin restricciones.

La solución NAC de Cisco es una solución robusta y probada por la industria para el control y el cumplimiento centralizados de políticas y cuenta con dos alternativas: dispositivos NAC o solución de infraestructura NAC. Los dispositivos NAC de Cisco constituyen la solución de control de acceso más utilizada actualmente en el mercado. Los dispositivos NAC suponen una solución eficaz y de fácil despliegue para la gran mayoría de los clientes. Aquellos clientes con necesidades particulares no cubiertas por los dispositivos NAC han de considerar el despliegue de la solución de infraestructura NAC que implica que todos los dispositivos de acceso a la red han de ser Cisco.

La Figura 10 muestra donde encaja en la red Cisco NAC.

Figura 10 Donde encaja



Ventajas clave

- Asegura el cumplimiento de la política
  -Impone la política de seguridad a nivel de red
- Protege proactivamente contra ataques (como virus y gusanos) en la infraestructura de red
  - Controla y reduce ataques de gran escala en la infraestructura de red
  - Reduce los gastos operativos y mantiene una mayor productividad de los empleados
- Impide el acceso no autorizado
  - Controla el acceso a la red basándose en credenciales de usuario y dispositivo para mantener la seguridad y proteger la información confidencial
  - Proporciona controles eficaces para el acceso de huéspedes y conexiones de socios desde máquinas no gestionadas
- Mejora las inversiones existentes
  - Se integra generalmente con programas antivirus y software de seguridad de múltiples proveedores que colaboran con Cisco en este programa
  - Se integra en la infraestructura de red existente
- Forma parte se la Red de Auto-defensa de Cisco
  - Cisco NAC es un elemento estratégico de la Red de Auto-defensa de Cisco
  - Se integra con otros componentes de la Red de Auto-defensa de Cisco como Cisco Security Agent y Cisco Security MARS (Cisco Security Monitoring, Analysis and Response System) para proporcionar identificación, prevención y respuesta precisas a las amenazas

Preguntas relevantes

- ¿Necesita imponer en su empresa políticas de seguridad de forma coherente para todos los recursos, tanto gestionados como no gestionados?
- ¿Ha sufrido en su empresa alguna vez los efectos de un gusano o virus que no podía controlar?
- ¿Necesita su empresa controlar el acceso a la red de personas contratadas, como huéspedes, visitantes, y socios?
- ¿Es importante para su empresa proteger los recursos de la red impidiendo la propagación de infecciones?
- ¿Es importante decrementar las llamadas al servicio de asistencia así como reducir el tiempo y los gastos de actualización de los ordenadores corporativos y resolución de los problemas de los usuarios?
- ¿Es importante para su empresa proporcionar protección proactiva para todos los dispositivos finales, independientemente de cómo entraron en la red (acceso remoto, inalámbrico, WAN o LAN)?

CS-MARS: Sistema de gestión de eventos y mitigación de amenazas

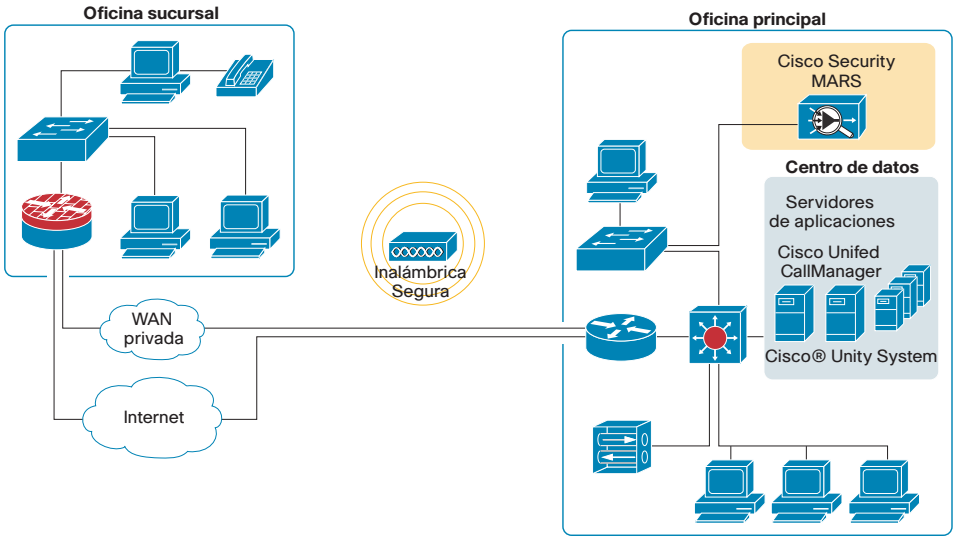
- Introducción
- Ventajas clave
- Preguntas relevantes

Introducción

- CS-MARS (Cisco Security Monitoring, Analysis and Response System) de Cisco® es una familia de dispositivos de alto rendimiento que se instalan en la red para gestionar, monitorizar y mitigar amenazas ayudando a los clientes a conseguir una mayor seguridad y a utilizar de una forma más eficaz los dispositivos de seguridad en la red.
- CS-MARS combina la monitorización tradicional de eventos de seguridad con la inteligencia de red para proporcionar capacidades precisas de mitigación de ataques.

La Figura 11 muestra donde encaja en la red Cisco Security MARS.

Figura 11 Donde encaja



Ventajas clave

- Recoge, analiza y correlaciona eventos procedentes de una diversa gama de dispositivos en la red (de Cisco y de otros fabricantes)
- Muestra la ruta de ataque gráficamente sobre el mapa topológico de la red
- Sugiere acciones específicas sobre los dispositivos de red para conseguir rápidamente la mitigación y contención de amenazas
- Simplifica el despliegue -ya que se basa en un dispositivo de facil instalación en la red
- Proporciona alto rendimiento -Un solo dispositivo de Cisco Security MARS puede manejar hasta 10.000 eventos por segundo.
- Proporciona acceso rápido y fácil a informes de cumplimiento de normativas (muy útil para auditorías)

Preguntas relevantes

- ¿Está contento con la información proporcionada por su sistema de monitorización de seguridad?
  - ¿Tiene un sistema de monitorización de seguridad en su red?
- ¿Puede darse cuenta de cuando se está realizando un ataque en su red ?
- ¿Quiere poder eliminar ataques tanto conocidos como desconocidos en su red, en tiempo real?
- ¿Cuándo fue la última vez que examinó las alarmas de su cortafuegos o sistema de detección de intrusos (IDS)?
- ¿Necesita proporcionar a su equipo directivo informes sobre el cumplimiento de las normas de seguridad en tiempo real?
- ¿Cómo impide que los incidentes trastornen sus operaciones?
- ¿Cómo garantiza el cumplimiento normativo en servidores y servicios críticos?

Cisco Security Manager

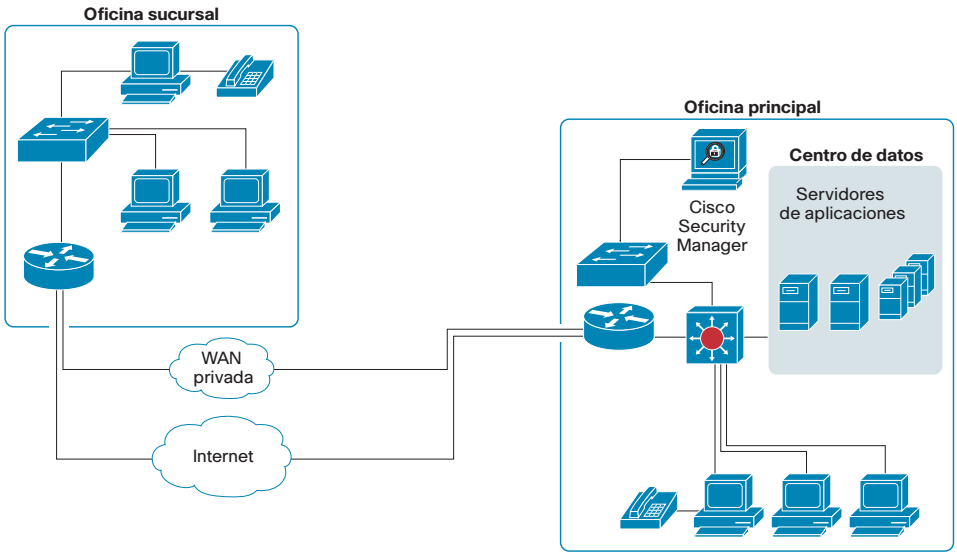
- Introducción
- Ventajas clave
- Preguntas relevantes

Introducción

- Cisco® Security Manager es una solución muy potente y fácil de utilizar para gestionar centralmente todas las políticas de seguridad y las configuraciones de los dispositivos como cortafuegos, concentradores VPNs y sistemas de prevención de intrusos (IPS) de Cisco®.
- Cisco Security Manager proporciona administración de seguridad centralizada, despliegue más rápido y configuración más exacta.
- La solución es eficaz para gestionar desde redes pequeñas consistentes en menos de 10 dispositivos, hasta redes de gran tamaño compuestas por miles de dispositivos.

La Figura 12 muestra donde encaja en la red Cisco Security Manager.

Figura 12 Donde encaja



Ventajas clave

- Responde a las amenazas con más rapidez -Define y asigna nuevas políticas de seguridad a miles de dispositivos en unos cuantos pasos sencillos
- Proporciona una gran facilidad de uso por medio de un interfaz de usuario muy completo
- Incorpora vistas múltiples que proporcionan métodos flexibles de gestionar dispositivos y políticas, incluida la capacidad de gestionar visualmente la red de seguridad mediante un mapa topológico de seguridad
- Asigna tareas específicas a cada administrador durante la implementación de una política, con control y seguimiento formales de cambios; permite que los empleados del grupo de seguridad y del grupo de operaciones de red trabajen juntos como un equipo único con una coordinación eficaz a través de esta aplicación de gestión
- Admite el aprovisionamiento de plataformas de router Cisco que ejecuten una imagen de software de cortafuegos en el sistema operativo IOS® de Cisco, dispositivos ASA 5500 de Cisco, dispositivos de seguridad PIX® de Cisco, sensores IPS 4200 de Cisco y módulos de seguridad para Catalyst® 6500 de Cisco.

Preguntas relevantes

- ¿Puede gestionar sus concentradores VPN, cortafuegos y dispositivos IPS con un solo sistema de gestión?
- ¿Quiere aumentar su eficiencia operativa cuando gestiona su red?
- ¿Quiere un sistema de aprovisionamiento que cree políticas coherentes para todos sus dispositivos?
- ¿Quiere un sistema que compruebe la coherencia y la exactitud de las políticas antes de implementarlas?
- ¿Le gustaría tener vistas múltiples de su red - topológica, global y lógica?
- ¿Le gustaría configurar sus VPNs en menos de cinco pasos?

Redes Privadas Virtuales

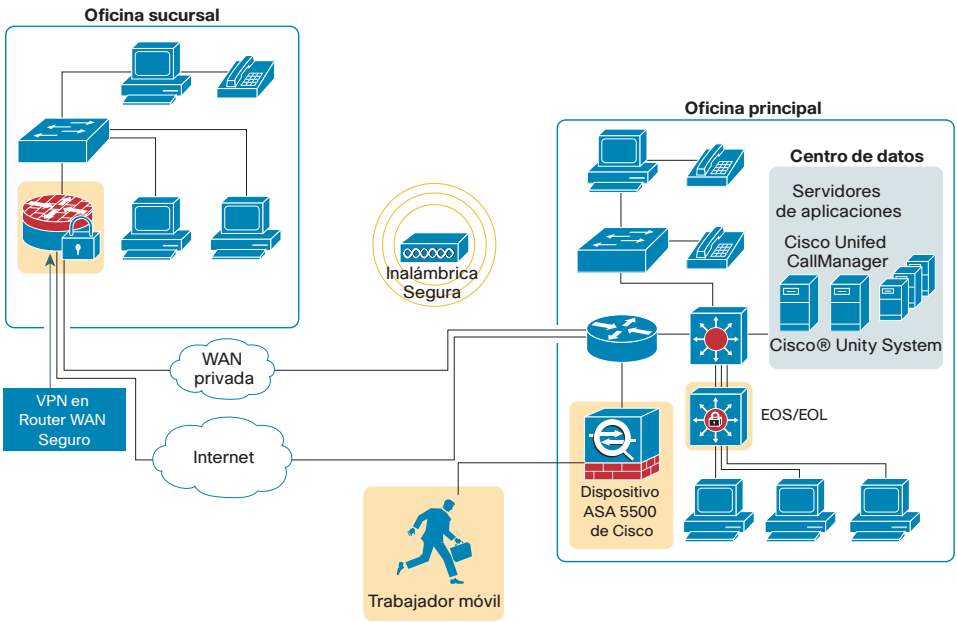
- Introducción
- Ventajas clave
- Preguntas relevantes

Introducción

- Las redes privadas virtuales (VPNs) permiten el despliegue de conectividad rápida, fiable y segura para oficinas remotas, o el acceso remoto a empleados desde su casa, usuarios móviles, empleados subcontratados y socios comerciales. Cisco® ofrece una serie de soluciones VPN basadas en IP Security (IPsec) y Secure Sockets Layer (SSL) que proporcionan conectividad remota económica y muy fácil de gestionar.
- Cisco® ofrece múltiples tecnologías VPN, que incluyen IPsec y SSL, integradas en una sola plataforma, lo que reduce el coste del equipo y la complejidad de la gestión. Colectivamente estas soluciones representan la cartera de VPN más completa y escalable de la industria.
- La soluciones Cisco VPN incluyen:
  - Famila ASA 5500 de Cisco-La solución VPN de acceso remoto más avanzada de Cisco que proporciona escalabilidad de usuario concurrente de 10 a 5000 sesiones más VPN integrado de sitio web a sitio web, cortafuegos, sistema de prevención de intrusos (IPS) y servicios anti-X
  - Routers Cisco -La solución VPN de sitio web a sitio web o acceso remoto integrado, cortafuegos, y servicios IPS
  - Cisco Catalyst® 6500 Serie La plataforma VPN más escalable de Cisco junto con cortafuegos integrado y servicios IPS

La Figura 13 muestra donde encaja en la red las VPNs.

Figura 13 Donde encaja



Ventajas clave

- El acceso remoto aumenta la productividad ofreciendo acceso seguro a la red en cualquier momento y en cualquier lugar a empleados que extienden su día laboral, trabajadores remotos, contratistas y socios comerciales.
- Los VPNs de sitio web a sitio web conectan oficinas y habilitan la conectividad a menor coste que los de servicios WAN tradicionales.
- El soporte de conectividad IPsec (acceso remoto y sitio web a sitio web) y SSL VPN desde una sola plataforma reduce el coste y la complejidad, al mismo tiempo que habilita servicios VPN personalizados para cada despliegue.
- Los VPNs suministran conectividad de alta calidad y fiabilidad a cualquier aplicación (incluso voz y video sensibles a la latencia) y en cualquier lugar.
- Los servicios VPN integrados en el router protegen contra amenazas como virus, spyware y piratas informáticos, sin necesidad de añadir otro equipo de seguridad más.

Preguntas relevantes

- ¿Tiene su organización empleados remotos que requieran acceso a la red corporativa?
- ¿Requiere un método de acceso seguro para empleados subcontrados y socios comerciales?
- ¿Le gustaría reducir sus gastos operativos de WAN o acceso remoto?
- ¿Le gustaría poder soportar redes virtuales privadas IPsec y SSL en una sola plataforma?
- ¿Está su VPN totalmente protegida contra virus, spyware y piratas informáticos?
- ¿Sabía que Gartner informa lo siguiente respecto a las empresas que despliegan VPNs?:
  - El ochenta y cinco por ciento desvela niveles superiores de seguridad de red y conectividad más rápida.
  - Casi el 90 por ciento experimentó reducciones de costes: el rendimiento medio de la inversión es del 54 por ciento a lo largo de 18 meses.
  - Más del 70 por ciento comunica que los VPNs mejoraron las comunicaciones con sus clientes y socios.
  - Más del 75 por ciento informa que los VPNs hacen que el soporte de usuarios remotos por el personal de informática sea más fácil.
  - Los aumentos medios de productividad son de 3 horas semanales por empleado.
- ¿Están pidiendo sus oficinas y usuarios remotos una conectividad más rápida y fiable?

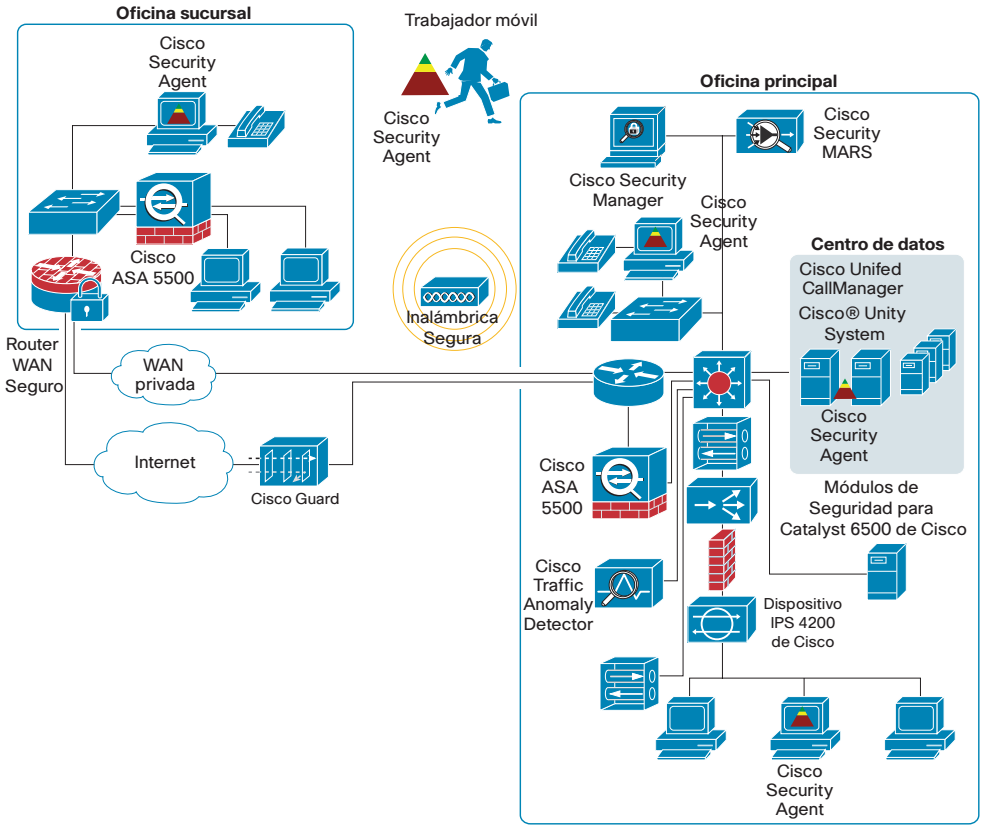
Combinación de todos los elementos

Sólo la Red de Auto-defensa de Cisco® permite la combinación todos los elementos y aporta:

- Integración de la seguridad a través de todos los aspectos de la red
- Colaboración entre los diversos elementos de seguridad y red
- Adaptación a nuevas amenazas a medida que surgen

La Figura 14 muestra donde encajan los productos Cisco en la Red de Auto-defensa de Cisco®.

Figura 14 Donde encaja todo



Sede en América
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
EE.UU.
www.cisco.com
Tel: 408 526-7660
800 553-NETS (6387)
Fax: 408 527-0883

Sede en Asia Pacífico
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Sede en Europa
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
Países Bajos
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Cisco Systems tiene más de 200 oficinas en los siguientes países y regiones. Las direcciones, números de teléfono y de fax se pueden encontrar en el sitio Web Cisco.com en **www.cisco.com/go/offices.**