

Webinar Question & Answer

Implementación y Configuración de Web Security Gateway v7.5

Webinar Date: July 28, 2010

¿Puedo yo obtener reportes por grupos de usuarios del Active Directory?

Si. Los grupos pueden ser obtenidos por medio de ambas herramientas de reportes, Presentation Reports e Investigative Reports.

¿Cuando se tiene implementación con PBR, es posible detectar o visualizar si efectivamente el WSG recibe tráfico?

Así es... hay varias formas no solo en WCG sino también desde el filtrado de Websense para validar esto. Desde la interfaz grafica podrá ser en: Monitor>My Proxy>Summary y en la sección de Node Details donde mostrara el trafico http recibido, también desde Monitor>Performance>Overview entre otras.

¿Por motivos de configuración en nuestra red, nuestro 6.3 lo actualizamos semanalmente, esto es factible en 7.5? ¿O deja de funcionar?

Si te refieres a respaldar la configuración cada semana, si lo es. Te recomiendo leer el artículo sobre "[WsBackup](#)" en relación a esto:

[Y también como restaurar dicha configuración](#)

[Y aquí más información sobre los archivos que esta utilidad respalda](#)

¿Pasar de la versión 7.1 a 7.5 es una reinstalación total o existe un upgrade?

Es una actualización directa... así que no habrá problema si lo haces desde la misma 7.1.

¿Si un cliente tiene Websense 7.1 con soporte actual tiene derecho a actualizar a 7.5?

Te recuerdo que mientras la suscripción este actual, tienes acceso a las versiones actuales del componente el cual estas pagando.

¿7.5 utiliza también el agente q utiliza 6.3 con el ISA Server?

No. Es necesario actualizar también el plug-in a la versión actual. Si estas en planes de actualizar el ISA a TMG, este solo se instalan en entornos de 64bits así que tendrás que obtener también el instalador para el plug-in del TMG y Websense desde nuestro portal [mywebsense.com](#)

¿Puedo tener tanto el WCG junto con los demás servicios de Websense en el mismo servidor Linux?

Desafortunadamente por lo robusto de ambos no. Dicha instalación no es recomendada y menos soportada por Websense. Te pido contactes a tu canal local o ingeniero de ventas para recomendaciones sobre hardware para ambas plataformas. Información general sobre esto la encontraras en:

Central de Implementaciones para WWS en v7.5: [Deployment Central](#)

¿Cómo funciona SSL decryption bypass, por ejemplo si habilito esta función para la categoría "Financial" de bancos; el usuario al acceder al sitio, debe recibir directamente el certificado del banco? o debe recibir el certificado del WCG?

Así es... si el ByPass está habilitado, el usuario obtendrá el certificado del sitio el cual está pidiendo desde su navegador.

¿La pregunta va orientada a que si la funcionalidad de content stripping aplica para todos los sitios o yo puedo seleccionar que solo aplique a ciertas categorías de sitios como la categoría de adult sites o spyware?

Por el momento esta función es global a todas las categorías incluidas en nuestra base de datos maestra y no hay forma actual de manipular el comportamiento.

¿Cómo maneja la autenticación en el WCG usuarios duplicados en diferentes dominios?

El mismo síntoma ocurre donde el Servicio de Usuarios no tiene la forma de hacer dicha identificación. Entonces aun si el WCG los ve en dos dominios como cualquier otro agente de identificación lo haría (DC Agent, Logon Agent) el mismo problema ocurrirá.

¿Si uno elije autenticación LDAP en el proxy, es necesario especificar credenciales en las aplicaciones que no usen LDAP que pasen por el proxy?

No necesariamente... en la sección de Authentication Realms en WCG podrás agregar diferentes comportamientos para no pedir credenciales a ciertos rangos de IP y así evitar este comportamiento. Así que no es meramente necesario pero tal vez lo necesites por si una política especifica se aplique aunque la misma la podrías hacer por IP.

¿Sigue siendo recomendable la instalación de los servicios en diferentes maquinas? ¿Cuál es la división más recomendable? ¿Esta soportado la virtualizacion en VMWare?

Para una mejor y detallada respuesta, contacta a tu canal local de ventas, Ingeniero de Ventas para dicha recomendación ya que la recomendación va muy especifica a tu entorno.

¿Algunos clientes usan de forma nativa autenticación con Kerberos, cuando WCG soportará esta autenticación de usuarios?

La versión 7.6 está programada para soportar dicha autenticación mas no es algo final. Esta está pactada a salir a mediados del próximo año

¿Pueden convivir la versión 7.5 de todos los componentes con la versión 7.1.6 de Content Gateway (proxy)? ¿Es decir se pueden migrar todos los componentes salvo el proxy? No. Es necesario tener todos los componentes en la misma versión ya que no es una versión menor la cual estarías usando si no una versión mayor completamente diferente.

¿La integración con el Active Directory es a través de LDAP??

Puede ser Mixta o Activa. Te recomiendo ver el Webinar en español sobre Servicios de Directorio en Websense:

[Webinar: Configurando Websense v7 con servicios de Directorio y agentes de identificación transparente](#)

¿En la sección de usuarios para filtrar, solo puedo adicionar desde el Active Directory a los usuarios y grupos? ¿Es posible adicionar una UNIDAD ORGANIZACIONAL completa?

Si es posible. Lo más seguro es que tienes configurado Websense a comunicarse en modo mixto, te recomiendo ver el Webinar en español sobre Servicios de Directorio en Websense:

[Webinar: Configurando Websense v7 con servicios de Directorio y agentes de identificación transparente](#)

¿Por qué se dice que se tiene Triton en WSG cuando no se maneja ambientes híbridos o más de un vector de seguridad? Porque parece que esto solo lo hace el WSGA? Correcto. La interfaz grafica “Websense Manager” ha sido renombrada a Triton, y los servicios se habilitan en base a tu suscripción los cuales son mostrados en la interfaz grafica con el Banner apropiado al inicio de sesión.

Acerca del NTLM en el proxy. ¿La autenticación vía browser aplica a todos los usuario en general o puede aplicar solamente a los equipos que no estén en Dominio e identificar transparentemente a los equipos que si lo estén?

La autenticación proveniente del Proxy es transparente siempre y cuando no haya algún error de configuración. Esta misma podrá ser NTLM o LDAP y seria en base a reglas donde se configuraría diferentes opciones para diferentes rangos de Red como lo muestro (esto desde la sección Configure>Security>Access Control>Authentication Realms:

Rule Type	LDAP	• Specifies the type of authentication profile for how Websense Content Gateway will identify and authenticate users.
Profile Name	Administrativo	• Specifies a descriptive name for the profile (must be unique).
Source IP	172.16.0.1,172.16.0.254	• Specifies sets of single IP addresses or IP ranges to match for this profile (should be entered without any spaces). Example: 10.1.1.1 or 0.0.0.0-255.255.255.255 or 10.1.1.1,20.2.2.3,0.0.0-3.255.255.255
Enabled	<input checked="" type="checkbox"/>	• Specifies if this profile is enabled
LDAP Specifiers		
LDAP Server Name	ad1.midominio.com	• Specifies a single LDAP server. Example: ldap.foo.com
LDAP Server Port	389	• Specifies the LDAP Server Port (Optional - Default 389)
LDAP Base Distinguished Name	dc=users, dc=administrativo, dc=midominio, dc=com	• Specifies the LDAP base distinguished name.
LDAP Server Type	Microsoft AD (sAMAccountName)	• Sets the search filter to "sAMAccountName" for Active Directory, or to "uid" for other directory services.
Bind DN	dn=admin, dc=users, dc=administrativo, dc=midominio, dc=com	• Specifies the LDAP bind account distinguished name.
Bind Password	••••••	• Specifies the LDAP bind account password.
Secure LDAP	<input type="checkbox"/>	• Specifies if proxy will use secure communication with LDAP server. If enabled, set the LDAP port to 636 or 3269 (secure LDAP port).
LDAP Attribute Name (Optional)		• Specifies the LDAP attribute name.
LDAP Attribute Value (Optional)		• Specifies the LDAP attribute value.
NTLM Specifiers		
DC List		• Specifies a list of (1 or more) Domain Controllers
DC Load Balance	<input type="checkbox"/>	• Specifies whether to load balance or just fail over

¿Cuáles son las diferentes alternativas para hacer al proxy WCG transparente?

Las diferentes opciones serian:

- ARM
- L4 Switch
- WCCP
- PBR

¿Con esta nueva versión hay la posibilidad de monitorear vía SNMP los procesos/servicios del V10000?

Es correcto. Para información sobre la configuración por favor ve a nuestro portal e inicia sesión para que obtengas la documentación sobre esta configuración (<http://support.websense.com>) o llámanos para asistirte.

¿Si agrego una SSL bypass, va a funcionar solo para el trafico de este tipo o va a hacer bypass a toda la navegación de esa categoría?

Si el Bypass lo haces desde el WCG, este solo hará para un sitio en específico... si el Bypass es hecho desde el Triton, entonces esto es en base a categorías, criterio que aplicaría a todos los sitios dentro de esa categoría.

¿Autenticación de WCG ante 2008 TS?

Si habilitas algún modo de autenticación transparente o manual esta debería funcionar ya que la información de sesión proviene del navegador... solo verificar que la autenticación a nivel Directorio Activa sea la soportada, por ejemplo que no sea NTLMv2.

¿En la parte de "Incidentes SSL" ya acepta páginas http y https?

Los incidentes solamente son para el protocolo https. El protocolo http no requiere de dicho comportamiento ya que la conexión no es cifrada.

¿Las opciones de túnel que acabas de mencionar podríamos utilizarla para indicar que el tráfico de SMTP de ciertos equipos no sea cifrado?

Esta opción solamente funciona para aplicaciones que van por medio de el protocolo https