

SISTEMAS DE CONTROL DE ACCESO Y FIREWALL

Perspectivas para una red más segura.

Ansel Serie 9500

Si usted es un profesional de la seguridad informática, probablemente ya haya escuchado de los términos TAP (Total Access Protección), NAP (Network Access Protección) ó NAC (Network Admisión Control/Network Access Control). Este último término es el más utilizado de los tres, todos ellos describen sistemas de control de acceso a una red que proveen una serie de determinadas funcionalidades enfocadas en integrar la autenticación de un usuario, la administración de la “salud” de los equipos, la protección contra código maligno y el control de acceso basado en políticas de las redes de determinada organización.

Cisco y Microsoft han sido los creadores en los últimos años de el concepto de estos equipos y en determinada forma, han dictado los lineamientos para el desarrollo de los mismos, sin embargo esta tecnología ha ganado espacios cuando Cisco a través de una iniciativa liderada por la compañía, publico el producto NAC, desde entonces las compañías han adoptado al NAC para administrar el acceso a su información y evitar así la propagación de “malware”, incrementando así el control de acceso a sus recursos de red y la seguridad de la información que pasa a través de ella.

Los productos o sistemas NAC garantizan que computadoras y laptops conectadas a la red estén en estricto cumplimiento con las políticas de la organización y aíslan o evitan el acceso a la misma a los dispositivos que requieran revisión aislándolos hasta que sean “limpiados” o reparados. El NAC no solo realiza la verificación del uso de las computadoras por los empleados, verifica también la “salud” de los equipos visitantes, y en general de todos aquellos equipos que se conecte a la red de la organización.

Un NAC puede ser dividido en tres fases funcionales: evaluación, aislamiento y reparación. Cuando un equipo se conecta a la red, este pasa al menos, por la etapa de evaluación la cual se compone por funciones de autenticación, autorización y validación. Las otras fases (aislamiento y reparación) son ejecutadas de acuerdo a las políticas creadas en el NAC y solo si el equipo lo requiere. Resumiendo, las funciones realizadas durante el proceso en un NAC son autenticación, autorización, validación, aislamiento, reparación e inspección. La autenticación y autorización son intrínsecas y corresponden a la fase inicial del proceso, cuando el dispositivo es identificado en la red y el acceso se le permite o deniega. La identificación y control de acceso es ejecutado a través de mecanismos que usan el estándar 802.1x y servicios de DHCP. Posteriormente que el dispositivo es detectado, este debe pasar la validación, en la cual se verifica si el equipo cumple con las políticas básicas establecidas por el departamento de seguridad de la compañía, de igual forma se verifica la existencia de elementos de seguridad como parches de actualización y seguridad, firmas de antivirus, servicios y aplicaciones activas, opciones especiales, para permitir inicialmente tener acceso a la red. En caso de que el dispositivo no cumpla con las políticas previas establecidas, este es automáticamente “aislado” o puesto en “cuarentena” y el acceso a la red le es bloqueado, El sistema de acceso puede ser mas robusto aún, este dispositivo puede ser diseccionado a un Server de “cuarentena” en el cual se podrán realizar labores de reparación que dependiendo también de ciertos criterios y políticas, podría actualizar parches o antivirus, detectar y desactivar

“malware” del dispositivo, desactivar servicios innecesarios, etc. Exactamente después de las etapas de identificación y validación en la red, se realizarán análisis de tráfico al dispositivo. Esta inspección es una de las funciones principales de la arquitectura de un NAC, estas funciones funcionan de servicios de prevención de intrusos (IDS/IPS).

Los NAC pueden ser clasificados en tres categorías que se caracterizan por la forma en que estos son integrados a la infraestructura de la red.

- **Appliances NAC**
Están divididos en equipos “in-line” y “out-of-band” es integrado de forma básica por un equipo hardware que incluye todo el sistema NAC de forma ínter construido
- **Soluciones NAC**
Generalmente se componen por software instalado en toda la plataforma de la red que en conjunto realiza las funciones de NAC, estas soluciones pueden integrar distintas tecnología e incluso dispositivos como switch y routers.
- **Seguridad para Equipos**
Las soluciones de seguridad para equipos existentes se extienden a la variedad de antivirus, anti-spyware, etc. Y en general a todo aquel programa instalado de forma individual que fortalezca la integridad y seguridad de una computadora personal.

Los appliances NAC pueden operar “in-line” o bien “out-of-band”. Las soluciones “in-line” monitoréan todo el tráfico, desde las funciones de autenticación hasta la inspección, permitiendo un enorme control sobre lo que es transmitido en la red, appliances de este tipo son recomendados incluso para redes inalámbricas. Actualmente las soluciones que operan “out-of-band” solo monitoréan el acceso del dispositivo a la red (la “entrada”), no existiendo la capacidad de visualización de tráfico transmitido después de las fases iniciales. La ventaja de este tipo de solución es que las políticas pueden ser aplicadas en el equipo existente, lo cual hace su implementación más sencilla

Los “iniciadores” de estas tecnologías, Microsoft y Cisco, tienen sin embargo, estándares independientes e incompatibles entre sí al 100%, para facilitar la integración entre productos y soluciones NAC, fue creado el “Trusted Computing Group” el cual ha definido un estándar para productos NAC llamado “Trusted Network Connect” (TNC) una alternativa abierta a las iniciativas propietarias de NAC. Esta tiene el objetivo de proveer seguridad a los puntos finales de cualquier conexión en la red, permitiendo la interoperabilidad entre equipo de diferente fabricante.

Soluciones Ansel De Control De Acceso Ansel NAC-Firewall Serie 9500

Los sistemas de control de acceso de Ansel están basados en las especificaciones TNC (Trusted Network Connect) revisión 1.1 publicadas por el TNG en mayo del 2006.

Ansel provee su solución firewall clase enterprise y un NAC en un formato “appliance” conformado por un equipo de alto rendimiento para trabajo en red, alta disponibilidad y redundancia. El tipo de appliance es “in-line” lo que proporciona el máximo de funcionalidades que una solución Firewall o NAC cubre por definición; por cubrir las especificaciones TNC el Ansel 9500 es compatible con equipos y soluciones similares, así como con dispositivos de acceso ala red tales como Switch y routers, servidores Radius y DHCP comerciales.

Al contrario de soluciones propietarias que solo funcionan en ambientes específicos o arquitecturas particulares, El Ansel 9500 es una solución completa TNC (NAC) que no exige a utilizar costosas infraestructuras de red o actualizaciones de las mismas. El Ansel 9500 trabaja en su ambiente sin importar el proveedor de equipo de red o modelo de su infraestructura.

La solución Ansel 9500 provee cinco opciones de refuerzo para equipos en cuarentena. Esto habilita al Ansel 9500 para reforzar las políticas de compatibilidad aun en redes complejas y heterogéneas

Las opciones de refuerzo incluyen:

- Seguridad basada en 802.1x
- Seguridad basada en DHCP
- Seguridad basada en destino
- Seguridad en línea para conexiones VPN y RAS
- Seguridad basada en Cisco NAC

Las opciones de refuerzo de seguridad pueden ser mezcladas y administradas a través del sistema de administración del ANSEL 9500 y de su consola WEB. Adicionalmente, el ANSEL 9500 ofrece tres opciones de prueba para los puntos finales (computadoras cliente)

- Pruebas libres-de-Agente
- Pruebas agente-ActiveX
- Pruebas basadas-en-Agente

La figura siguiente muestra como la combinación de estas poderosas y flexibles opciones de refuerzo permiten a los puntos finales, incluyendo a usuarios que se conecten a la red inclusive por medios remotos, incluyendo también, visitantes, usuarios gíreles, etc.. Todos ellos serán revisados minuciosamente antes de proporcionarles simple acceso a la red.



El Ansel 9500 es un Firewall clase enterprise con TCN (NAC) dedicado, su máquina de análisis y búsqueda propietaria provee un profundo análisis en todos los puntos destino, generando una mínima transacción de datos por sesión, y probando los dispositivos rápidamente de forma totalmente transparente para los usuarios cuyos dispositivos cumplen completamente las políticas.

A diferencia de otros mal llamados “soluciones NAC” que se ejecutan sobre aplicaciones vulnerables a scanner, firewalls personales, soluciones IDS/IPS, el Ansel 9500 no puede ser “pasado” por alto por otros procesos o procedimientos o bien, limitado en cuanto a sus capacidades de análisis. Adicionalmente (a diferencia de estos otros productos) el Ansel 9500 es una verdadera solución “pre-conexión” que elimina riesgos, probando dispositivos y equipos incluso antes de conectarse físicamente a la red.

Ventajas de la maquina NAC-Firewall del Ansel 9500

- Velocidad de Prueba: 3 – 5 segundos por equipo
- mínima transferencia de datos por sesión: 35K en promedio
- Impacto mínimo en el usuario final.
- Pruebas intensivas especificas para riesgos determinados
- Verdadera protección pre-conexión
- No vulnerable a problemas de licenciamiento (soluciones basadas en Nessus pueden serlo!!)

Conjunto de pruebas básicas

El TNC Ansel 9500 incluye cientos de pruebas que proporcionaran una adecuada certificación de seguridad para los clientes o conexiones que requieran acceso a la red.

Las categorías de pruebas que incluye son:

- Verificación de service packs y parches de seguridad al sistema Operativo
- Configuraciones de seguridad en sistema operativo y navegador WEB
- Antivirus, instalación y actualizaciones
- Firewall personal, instalación y actualizaciones
- Anti-Spyware, instalación y actualizaciones
- Presencia de spy-ware, malware, etc.
- Presencia de aplicaciones peer-to-peer
- Presencia de “gusanos”, virus y troyanos
- Software requerido por el administrador
- Software prohibido por el administrador

El listado completo de las pruebas de seguridad realizadas por el Ansel 9500 se muestra a continuación, pruebas múltiples son combinadas dentro de políticas de acceso, las cuales son aplicadas a dispositivos que se conecten a la red. Las pruebas y diagnósticos nuevos son implementados automáticamente a los dispositivos en cuanto estas estén definidas dentro del rango de pruebas a efectuar por determinada política, las pruebas, diagnósticos son desarrolladas, controladas en calidad y proveídas por Ansel de México y el equipo de desarrollo de seguridad de la empresa.

PRUEBAS DE SEGURIDAD REALIZADAS POR EL ANSEL 9500

<p>Sistemas Operativos</p> <ul style="list-style-type: none"> •Service Packs •Rogue WAP Connection •Windows 2000 hotfixes •Windows Server 2003 SP1 hotfixes •Windows Server 2003 hotfixes •Windows XP SP2 hotfixes •Windows XP hotfixes •Windows automatic updates <p>políticas de seguridad en Navegadores</p> <ul style="list-style-type: none"> •IE Internet security zone •IE local intranet security zone •IE restricted site security zone •IE trusted site security zone •IE version <p>Pruebas de version Ms-Office</p> <ul style="list-style-type: none"> •Microsoft Office XP •Microsoft Office 2003 •Microsoft Office 2000 <p>Configuraciones de Seguridad</p> <ul style="list-style-type: none"> •MS Excel macros •MS Outlook macros •MS Word macros •Services not allowed •Services required •Windows Bridge Network Connection •Windows security policy •Windows startup registry entries allowed <p>Anti-spyware</p> <ul style="list-style-type: none"> •Ad-Aware SE Personal •Ad-Aware Plus •Ad-Aware Professional •CounterSpy •McAfee AntiSpyware •Pest Patrol •Spyware Eliminator 	<p>P2P y mensajería instantánea</p> <ul style="list-style-type: none"> •Altnet •AOL instant messenger •BitTorrent •Chainsaw •Chatbot •DICE •dIRC •Gator •Hotline Connect Client •IceChat IRC client •ICQ Pro •IRCXpro •Kazaa •Kazaa Lite K++ •leafChat •Metasquarer •mIRC •Morpheus •MyNapster •MyWay •NetIRC •NexIRC •Not Only Two •P2PNet.net •PerfectNav •savIRC •Trillian •Turbo IRC •Visual IRC •XFire •Yahoo! Messenger <p>Firewall Personales</p> <ul style="list-style-type: none"> •AOL Security Edition •Black ICE Firewall •Computer Associates EZ Firewall •Internet Connection Firewall (Pre XP SP2) •McAfee Personal Firewall •Panda Internet Security 	<p>Spyware, Gusanos, virus, y Troyanos</p> <ul style="list-style-type: none"> •CME-24 •Keylogger.Stawin •Trojan.Mitglieder.C •VBS.Shania •W32.Beagle.A •W32.Beagle.AB •W32.Beagle.AG •W32.Beagle.AO •W32.Beagle.AZ •W32.Beagle.B •W32.Beagle.E •W32.Beagle.J •W32.Beagle.K •W32.Beagle.M •W32.Beagle.U •W32.Blaster.K.Worm •W32.Blaster.Worm •W32.Doomhunter •W32.Dumaru.AD •W32.Dumaru.AH •W32.Esbot.A.1 •W32.Esbot.A.2 •W32.Esbot.A.3 •W32.Galil.F •W32.HLLW.Anig •W32.HLLW.Cult.M •W32.HLLW.Deadhat •W32.HLLW.Deadhat.B •W32.HLLW.Doomjuice •W32.HLLW.Doomjuice.B •W32.HLLW.Lovgate •W32.Hiton •W32.IRCBot.C •W32.Kifer •W32.Klez.H •W32.Klez.gen •W32.Korgo.G •W32.Mimail.Q
--	---	---

<ul style="list-style-type: none"> •Webroot Spy Sweeper •Windows Defender <p>Anti-virus</p> <ul style="list-style-type: none"> •NOD32 AntiVirus •AVG AntiVirus Free Ed •Computer Associates eTrust AntiVirus •Computer Associates eTrust EZ AntiVirus •F-Secure AntiVirus •Kaspersky AntiVirus for FileServers •Kaspersky AntiVirus for Workstations •McAfee VirusScan •McAfee Managed VirusScan •McAfee Enterprise VirusScan •McAfee Internet Security Suite 8.0 •Norton Internet Security •Trend Micro AntiVirus •Trend Micro OfficeScan Corporate Edition •Sophos AntiVirus •Panda Internet Security •Symantec Corporate AntiVirus 	<ul style="list-style-type: none"> •F-Secure Personal Firewall •Norton Personal Firewall / Internet Security •Sygate Personal Firewall •Symantec Client Firewall •Tiny Personal Firewall •Trend Micro Personal Firewall •ZoneAlarm Personal Firewall •Senforce Advanced Firewall •Windows Firewall <p>Software no permitido</p> <ul style="list-style-type: none"> •Administrator defined <p>Software requerido</p> <ul style="list-style-type: none"> •Administrator definid 	<ul style="list-style-type: none"> •W32.Mimail.S •W32.Mimail.T •W32.Mydoom.A •W32.Mydoom.AX-1 •W32.Mydoom.AX •W32.Mydoom.B •W32.Mydoom.M •W32.Mydoom.Q •W32.Netsky.B •W32.Netsky.C •W32.Netsky.D •W32.Netsky.K •W32.Netsky.P •W32.Rusty@m •W32.Sasser.B •W32.Sasser.E •W32.Sasser.Worm •W32.Sircam.Worm •W32.Sober.O •W32.Sober.Z •W32.Welchia.Worm •W32.Zotob.E <p>Software de alto riesgo</p> <ul style="list-style-type: none"> •Google Desktop
--	--	---

Pruebas individuales son combinadas dentro de las políticas de acceso. Ansel 9500 se distribuye con políticas de acceso predefinidas (Alto, medio y bajo riesgo), y los administradores pueden crear políticas personalizadas para adecuarlas a las necesidades específicas de sus negocios (por ejemplo., políticas específicas para visitantes, usuarios locales, oficinas remotas,laptops, oficinas globales,etc).

Funcionalidades Firewall de la serie 9500

- filtrado por puerto, destino, proocolo o tipo de trafico
- Realizacion de reglas basadas en roles de destino u origen
- Capacidad de filtrado transparente para capa 2
- Seguimiento y establecimiento de reglas por huella de SO
- Agrupacion y establecimiento de ALIAS para grupos de direcciones IP, puertos, orígenes y destinos
- Tamaño de tabla de estado ajustable hasta 20000 entradas

- Reglas de limitación por cliente, por origen, por destino, por host, por red o por familia de protocolo
- Manejos de estado: keep-state, modulate-state, synproxy-state, none
- Optimización de manejo de estado : normal, highlatency, aggressive, conservative.
- Soporta NAT, DNAT, SNAT 1-1NAT y UpnP
- Nat-reflection y portforward
- Redundancia CARP y RSYNC
- soporte de 802.1q

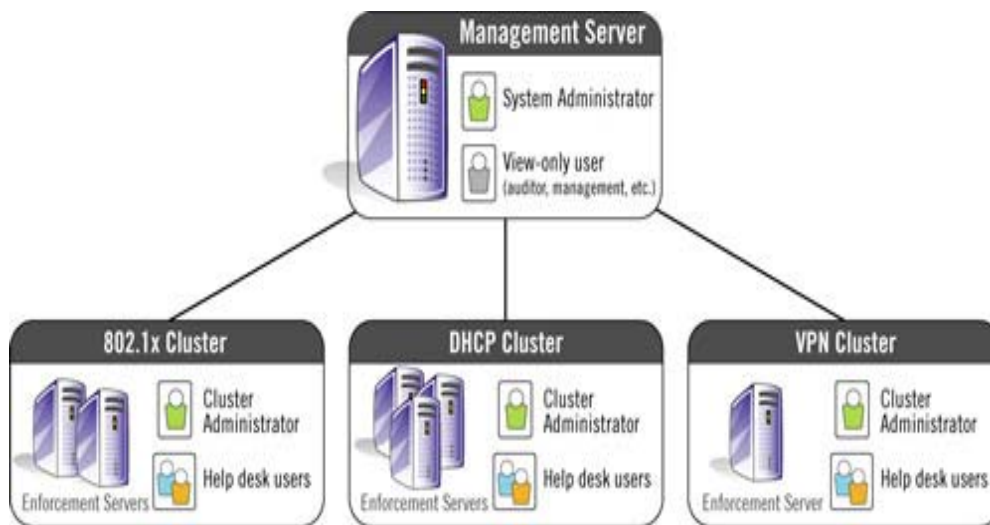
Funciones de filtrado de contenido de la serie 9500

- Restricciones de acceso basadas en autenticación por proxy, transparente y sistemas LDAP
- Restricciones de acceso basadas en roles administrativos.
- Restricciones basadas en listas negras, listas blancas y listas grises de más de 30 proveedores de bases de datos.
- Definición de políticas basadas en roles, horarios, fechas y autenticación de la redundancia
- Definición de políticas basadas en dirección IP, nombre de host o red de origen.
- Acceso a sistemas de mensajería instantánea solo a clientes específicos basados en reglas particulares.
- Acceso a transferencias y sistemas p2p a usuarios o clientes según establecimiento de roles.
- Categorización de políticas hasta en 60 niveles distintos
- Personalización de filtrado basado en URL, IP, dominio, frase, o arreglo asociativo.
- Filtrado por tipo de archivo MIME
- Filtrado por tipo de aplicación o tipo de cliente-destino
- Bloqueo por puerto o IP
- Establecimiento de políticas para usuarios y visitantes
- autenticación de usuarios basados en LDAP
- Asignación de excepciones por usuario o grupo
- Políticas de alerta mediante mensaje WEB o SMS
- Monitoreo de tráfico interno y externo
- Asignación de horarios y calendarización de filtros o bloqueos.

- Bloqueo de descargas por sitio o usuario
- Bloqueo de spyware y troyanos
- Actualización de políticas automatizadas cada 30 min.
- Detección y bloqueo de tráfico interno de tipo Spyware o virus.
- Protección antivirus en contenido y tráfico Spyware/troyanos

Manejo Y Administración Grado Enterprise

El Ansel 9500 está desarrollada pensando en ambientes enterprise donde decenas, cientos o miles de puntos de contacto (usuarios) requieren ser controlados. Independientemente del tamaño o complejidad de la red, la solución Ansel 9500 consolida centralmente la administración de todas las pruebas y actividades de diagnóstico, proveyendo un simple punto de acceso a la seguridad de todos los puntos de entrada a la red. Un equipo Ansel 9500 puede controlar múltiples servers de apoyo y configuración conectados en cluster, tal y como se ilustra en la siguiente imagen.



A través del Server de Administración, pruebas personalizadas y políticas de acceso podrían ser distribuidas a todos los Server de apoyo por medio de una simple operación. Esta arquitectura provee a los administradores del sistema acceso inmediato a todo el rango de información sobre los temas de seguridad, desde información general hasta detalles de un simple cliente o punto de acceso a la red.

Alta Disponibilidad Y Balanceo De Carga.

Una implementación de soluciones Ansel 9500 provee soporte mutuo simultáneo, esto es, cuando uno de los equipos llegase a fallar otros sistemas Ansel 9500 automáticamente cubrirían al segmento de red afectado, proporcionando los servicios que el equipo que ha fallado dejó de proveer. Al igual que esto, los picos de actividad

o procesos de pruebas dirigidos a un simple Server Ansel 9500 serían balaceados en carga a través de todo el cluster.

Acceso Multi-Usuario Basado En Roles.

Los accesos administrativos a los sistemas son estrictamente controlados haciendo uso de roles de usuario y asignaciones del cluster, el sistema Ansel 9500 se distribuye con 4 roles básicos de administración:

- Administrador del Sistema
- Administrador de Cluster
- Usuario de Help-desk
- Usuario de Monitoreo

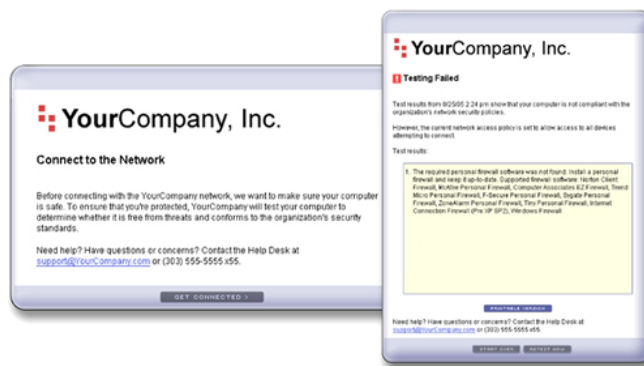
Los administradores del sistema pueden crear roles adicionales usando permisos específicos del sistema principal, Por ejemplo, un administrador de cluster podría solo ver datos de los equipos conectados dentro de su propio cluster. El Ansel 9500 puede integrarse a su sistema usando AD/LDAP para importar información referente a sus cuentas de usuario.

Integración Con Ambientes IT

El Ansel 9500 incluye un ambiente de integración transparente y de arquitectura abierta que permite la importación/exportación de datos de y hacia el Ansel 9500. Esta integración permite a sistemas de otros proveedores controlar funciones de prueba y cuarentena del mismo Ansel 9500, por consiguiente, esto permite al Ansel 9500 compartir la seguridad de los puntos de acceso con otros sistemas de IT como match-managers, sistemas de detección de intrusos IDS / IPS , administradores de vulnerabilidades, administradores de información de seguridad, trouble-ticketing, herramientas de reporte, etc.

Impacto En Clientes, Limpieza Y Certificación.

Los administradores tienen un completo control sobre la profundidad y frecuencia con la cual los usuarios finales son informados de las actividades de prueba y sus resultados. La comunicación puede ser configurada para ser visible o invisible según sea necesario, los usuarios o clientes pueden ser notificados de las pruebas a los dispositivos, de los resultados de estas y los pasos necesarios para en su caso, cumplir con determinada certificación. Un ejemplo es mostrado en la imagen siguiente:



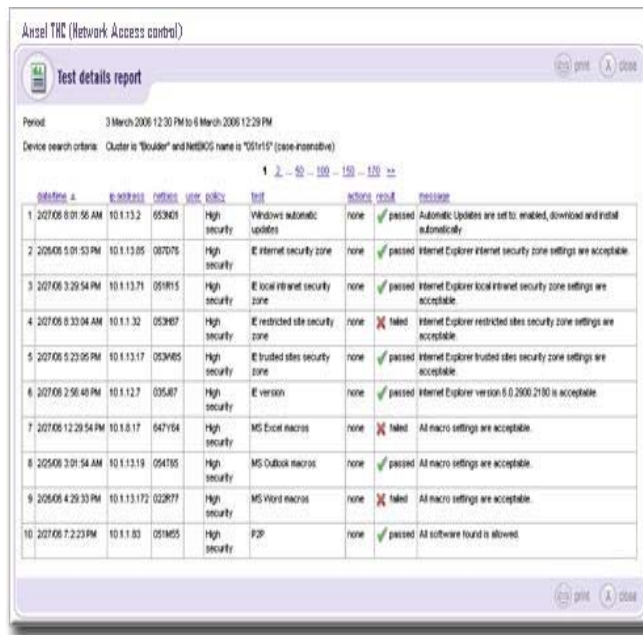
Reparación De Clientes Manual Y Automática

El Ansel 9500 asegura una solución total de seguridad al facilitar una variedad de opciones de remediación en clientes que no aprobaran las pruebas de compatibilidad y certificación:

- **Remediación Automática** – La integración con BigFix®, Microsoft@SMS y Citadle Hercules soportados nativamente proporcionan estas herramientas de corrección, adicionalmente pueden desarrollarse integraciones con otras soluciones previa solicitud
- **Auto remediación** – Los usuarios son notificados acerca de las deficiencias en sus equipos y se les provee de instrucciones para su remediación.
- **Acceso con periodo de gracia** - Provee una ventana de tiempo definida por el administrador (pe. 3 días) durante el cual equipos que no cumplan con determinadas especificaciones, podrán tener acceso a la red mientras corrigen su situación

Reportes Para Administración Y Auditorias

El Ansel 9500 cuenta con robustas opciones de reporte las cuales permiten adecuarse a las necesidades del cliente, auditores, administradores y staff IT. Los reportes proveen estados concisos sobre la seguridad, información de cumplimientos y certificaciones de clientes, actividad de acceso, listado de dispositivos, acciones tomadas, resultados de pruebas, resultados por dispositivo, resultados por usuario resultados por IP y mas.



Test details report

Period: 3 March 2008 12:30 PM to 6 March 2008 12:29 PM

Device search criteria: Cluster is "Boulder" and NetBIOS name is "S01r1P" (case-insensitive)

id	datetime	ip	hostname	user	policy	test	action	result	message
1	20768 8:01:56 AM	10.1.13.2	053401		High security	Windows automatic updates	none	passed	Automatic Updates are set to: enabled, download and install automatically.
2	20808 5:01:53 PM	10.1.13.05	007076		High security	IE internet security zone	none	passed	Internet Explorer internet security zone settings are acceptable.
3	20768 3:29:54 PM	10.1.13.71	091915		High security	IE local intranet security zone	none	passed	Internet Explorer local intranet security zone settings are acceptable.
4	20768 8:33:04 AM	10.1.1.32	053487		High security	IE restricted site security zone	none	failed	Internet Explorer restricted sites security zone settings are acceptable.
5	20768 6:23:05 PM	10.1.13.17	053485		High security	IE trusted sites security zone	none	passed	Internet Explorer trusted sites security zone settings are acceptable.
6	20768 2:50:48 PM	10.1.12.7	035487		High security	IE version	none	passed	Internet Explorer version 6.0.2900.2100 is acceptable.
7	20768 12:29:54 PM	10.1.8.17	047164		High security	MS Excel macros	none	failed	All macro settings are acceptable.
8	20568 3:01:54 AM	10.1.13.19	094105		High security	MS Outlook macros	none	passed	All macro settings are acceptable.
9	20808 4:29:33 PM	10.1.13.172	022877		High security	MS Word macros	none	failed	All macro settings are acceptable.
10	20768 7:2:23 PM	10.1.1.03	051455		High security	P2P	none	passed	All software found is allowed.