Especialidad en Redes

Facultad de Informática

Universidad Nacional de La Plata

Trabajo:

“Control de Acceso a Redes”

Alumno: Daniel Omar Esmoris

Director: Ing. Luis Marrone

1 RESUMEN

El presente trabajo trata el tema de la implementación de Control de Acceso a Redes

El trabajo comienza con una breve descripción de las distintas soluciones de diferentes fabricantes y a continuación se detallan las distintas metodologías utilizadas.

2 JUSTIFICACIÓN

En los últimos años se ha producido una necesidad de acceso a las redes corporativas utilizando distintos medios de acceso ya que las empresas tienen cada vez redes mas distribuidas, con oficinas y centros de negocios repartidos en distintas ubicaciones geográficas.

Además, se ha intensificado el uso de aplicaciones multimedia que requieren que la red le garantice condiciones de seguridad y confidencialidad para el tráfico de los datos que intercambian.

3 OBJETIVO

El presente trabajo pretende analizar las distintas alternativas que ofrece el mercado y analizar los accesos a las redes. A esto se asocian diversos productos y tecnologías, y los estándares no están aun definidos en un mercado que es extremadamente difícil de entender. Esta confusión lleva a ideas confusas, mucha gente toma pedazos de información que oyen y forman juicios incorrectos de qué pueden hacer los productos y qué amenazas tratan realmente.

4 ÍNDICE TEMÁTICO DEL TRABAJO

1. Entendiendo el escenario, amenazas dentro y fuera de la red
2. Entendiendo términos y tecnologías
3. NAC de Cisco
4. NAP de Microsoft
5. Esfuerzos por estandarización. TNC .IETF
6. Tecnologías con funcionalidad NAC/NAP : 802.1X, IPSec VPN y SSL VPN
7. Alternativas de Código Abierto
8. Conclusiones

BIBLIOGRAFÍA

- http://www.infoworld.com/article/05/09/05/36FEbattlesecurity_1.html
- Implementing NAP and NAC Security Technologies. Daniel V. Hoffman
- Network Security Technologies and Solutions. Yusuf Bhaiji
- http://www.interop.com/newyork/eventhighlights/interoplabs/
- http://searchnetworking.techtarget.com/generic/0,295582,sid7_gci1228704,00.html
- http://en.wikipedia.org/wiki/Network_Admission_Control
- http://sslvpn.breakawaymg.com/eps/NAC.phpRedes&Telecom, suplemento especial del número 207
- http://en.wikipedia.org/wiki/Access_Control• Cisco NAC
- http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html• Microsoft NAP
- http://www.microsoft.com/technet/network/nap/default.mspxhttp://en.wikipedia.org/wiki/Access_Control• TCG TNC
- http://www.germinus.com/sala_prensa/articulos/SIC73_096-100.pdf
- https://www.trustedcomputinggroup.org/groups/network/
- https://www.trustedcomputinggroup.org/news/events/specs/TNC• 802.1X
- http://en.wikipedia.org/wiki/802.1X
- http://netpass.sourceforge.net/
- http://www.freenac.net/
- http://www.packetfence.org/

1. Entendiendo el escenario, amenazas dentro y fuera de la red

La razones de la importancia del control de acceso a redes pueden encontrarse porque las empresas cada vez tienen redes mas distribuidas, con oficinas y centros de negocios repartidos en distintas ubicaciones geográficas, todos con la necesidad de acceso a la red y sistemas de la compañía utilizando distintos medios de acceso desde tecnologías inalámbricas, Internet, VPN, etc.

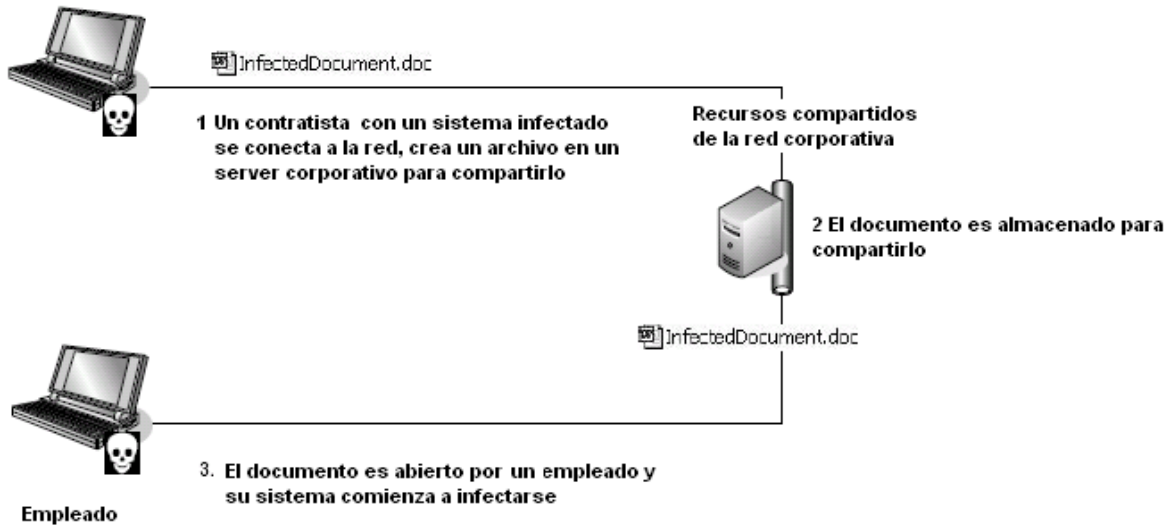
Este entorno de interconexión tan complejo unido a la mayor criticidad de los datos que poseen las empresas y organizaciones, y a la necesidad de acceso a los datos desde cualquier dispositivo y ubicación, todo ello sin comprometer la integridad y confidencialidad de la información, ha provocado la aparición de innumerables y nuevos puntos débiles de acceso. Estas circunstancias implican nuevos riesgos y amenazas ante los cuales las empresas demandan nuevas soluciones para solventarlas

En respuesta a esta demanda surgen iniciativas y tecnologías para resolverlas que se engloban dentro de lo que se conoce como Control de Acceso a la Red.

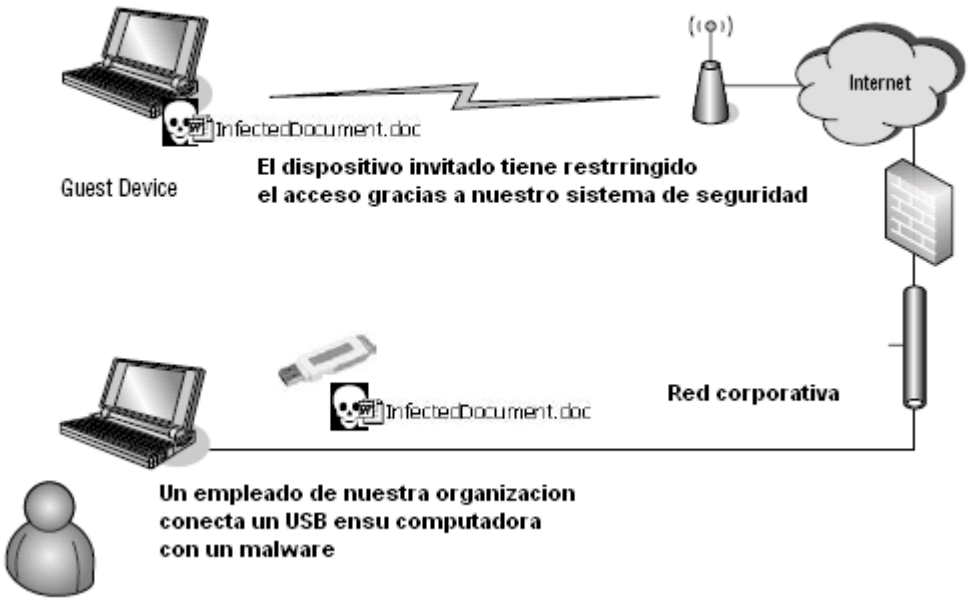
Otro gran problema que puede ofrecer la implementación de una arquitectura NAC es el impacto en la infraestructura donde se implante, debido a que afecta tanto a los elementos de red, como switches, routers y firewalls como a equipos de usuarios y su software, también incrementa la carga de los servidores de autenticación.

Amenazas de seguridad pueden ser causadas por usuarios de una organización sin ninguna intención, por ejemplo:

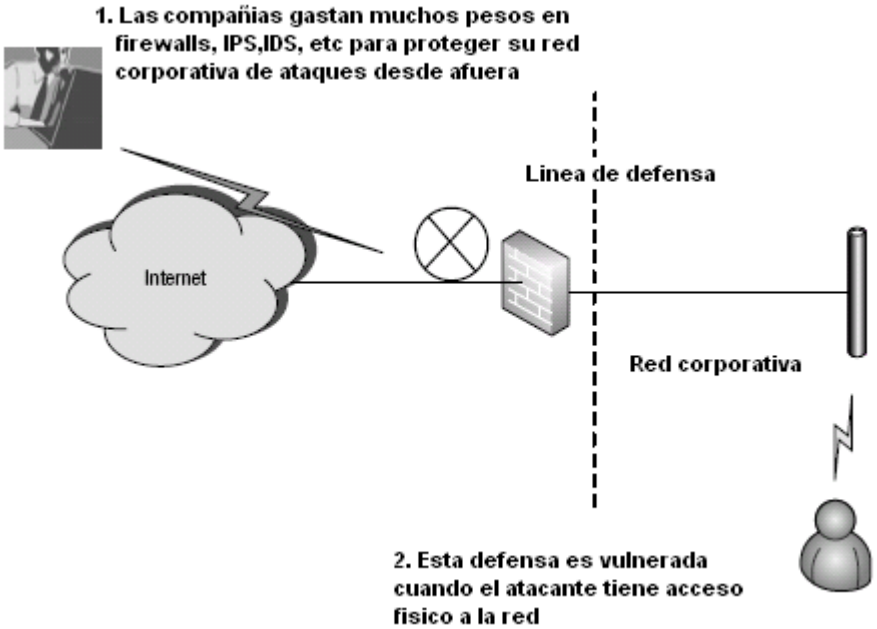
Si no tenemos control de quienes se conectan a nuestra red



O aun teniendo un sistema de seguridad externo, el problema puede ser causado sin intención por un empleado



No solo es importante tener un sistema de seguridad que controle el acceso desde el exterior



Tampoco es suficiente proveer de laptops con todos los sistemas de seguridad corporativas a los empleados

Tenemos un escenario en el que debemos tener protección tanto externa como interna y en la puja por la supremacía de proveer sistemas de acceso seguro nos encontramos con tres tecnologías claramente diferenciadas:

- NAC de Cisco
- NAP de Microsoft
- TNC (del Trusted Computing Group)

2. Entendiendo términos y tecnologías

Las soluciones NAC son diferentes pero pueden ser clasificadas en dos grupos

- **Clienless** no necesita de ningún software instalado en los dispositivos
- **Client-based** un componente de software es preinstalado en los dispositivos para poder asistir al proceso de NAC

Existe un numero de factores para decidir cual tipo de solución es la mas adecuada dependiendo de cómo esta formada la organización, NAC basado en cliente provee mas detalle del dispositivo pero también hay que tener en cuanta que requiere su instalación equipo por equipo

Pre admisión NAC

Determina que un dispositivo cumpla con ciertos criterios predeterminados antes de permitirle el acceso a la red. Si esos criterios no se cumplen, no permite que el dispositivo se conecte a la red, o le asigna un acceso restringido.
La Pre-Admisión en NAC se encuentra en las siguientes soluciones:

- Microsoft NAP
- Cisco NAC
- Mobile NAC
- IPSec VPN
- SSL VPN

Pre-Admission NAC

Estrategias

Existen tres estrategias de implantación de NAC basándonos en dónde se introduce el control de acceso a la red, así que uno debe decidir cuál de las tres se ajusta más a las características y particularidades de la organización.
Estas estrategias son:

• **Control en el perímetro (Edge control**): introduce el control de acceso a la red en el exterior, es decir en el punto donde se conectan los sistemas a ésta, por ejemplo en el switch de una LAN, o en un concentrador VPN.

• **Control central (Core control**): el control de acceso se puede implantar en cualquier punto de acceso a la red, por ejemplo, a través de un dispositivo que se coloca en medio de la red por el que pasa el tráfico de los equipos cuyo acceso se quiere analizar

• **Control en el cliente (Client control):** la implantación de las políticas de seguridad y control de acceso se realiza fundamentalmente en el usuario final, instalando en cada uno de los equipos y sistemas que se quiera gestionar y controlar todas las aplicaciones necesarias para realizar este control, como firewalls personales, aplicaciones de control del acceso inalámbrico, control de dispositivos USB, etc.

Terminología utilizada en cada una de las arquitecturas

Dependiendo de la arquitectura de cada uno de los protagonistas la terminología se resume en el siguiente cuadro:

TERMINOLOGÍA	IETF	TCG TNC	MICROSOFT NAP	CISCO NAC
Colector de estado	Posture Collector	Integrity Measurement Collector	System Health Agent	Posture Plug-in Applications
Agente intermedio	Client Broker	TNC Client	NAP Agent	Cisco Trust Agent
Módulo de peticiones de acceso	Network Access Requestor	Network Access Requestor	NAP Enforcement Client	Cisco Trust Agent
Punto de acceso y aplicación de políticas	Network Enforcement Point	Policy Enforcement Point	NAP Enforcement Server	Network Access Device
Servidor de verificación de estado	Posture Validator	Integrity Measurement Verifier	System Health Validator	Policy Vendor Server
Módulo intermedio	Server Broker	TNC Server	NAP Administration Server	Access Control Server
Servidor de autorización de acceso	Network Access Authority	Network Access Authority	Network Policy Server	Access Control Server

Soluciones existentes y sus características

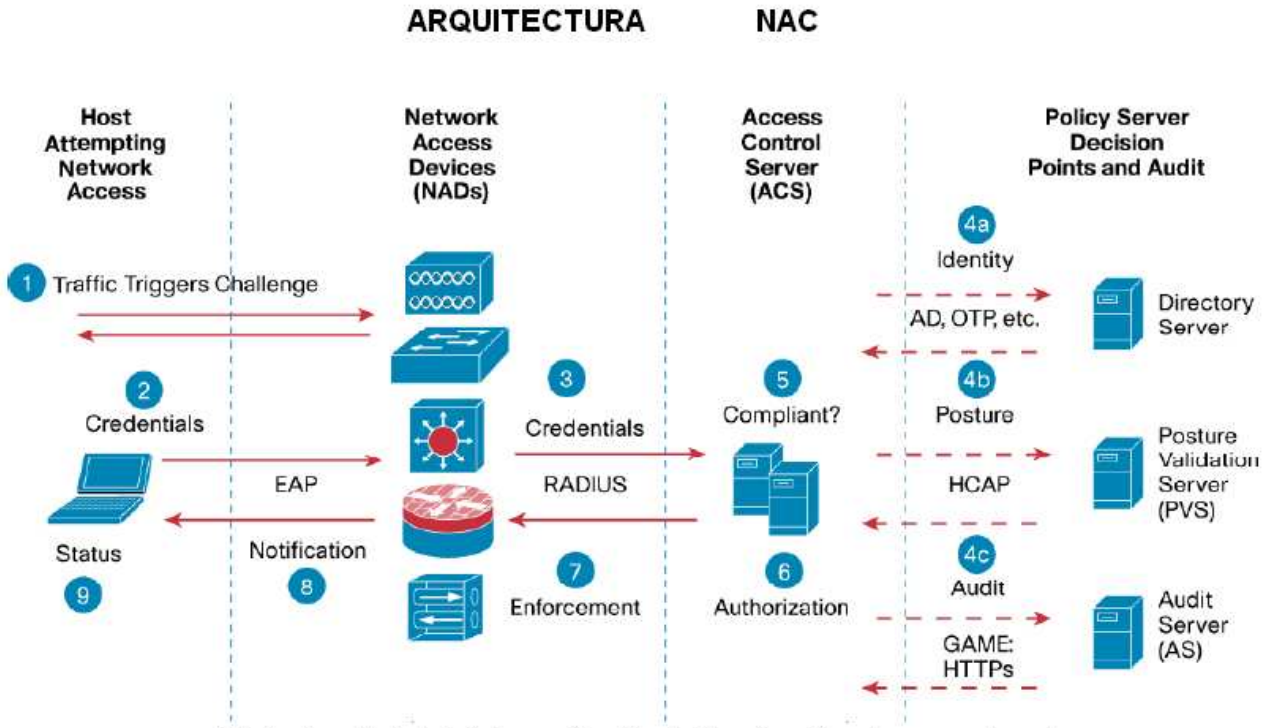
Producto	Descripción de la solución	Tecnología
Cisco NAC Framework	Iniciativa propietaria de Cisco basada en la implantación de control de acceso dentro de la infraestructura de red	Cisco NAC
Cisco NAC Appliance	Equipos Cisco que permiten una rápida implantación de políticas de control de acceso a la red sin realizar cambios en *switches* y *routers*	Cisco NAC
ConSentry LANShield	Solución NAC de alto rendimiento pensada para ser desplegada de forma perimetral. Control de acceso basado en identidad, políticas y datos de usuario	Basada en dispositivos propios, *appliances* creados por ConSentry
Elemental Security Platform	Sistema diseñado para monitorizar dispositivos de red, configuraciones, actividad de los usuarios, implementando políticas de seguridad basadas en roles	Propietaria, basada en un modelo de servidores y software de agentes
ENDFORCE Enterprise	Solución basada en software, diseñada para redes heterogéneas, con la capacidad de extender las funcionalidades ofrecidas por las arquitecturas NAC, NAP y TNC	Basada en estándares, compatible con C-NAC, NAP y TNC
FireEye NAC Appliance	Basada en *appliances* que implanta el control de acceso basándose en la inspección del tráfico de los dispositivos de la red, y por tanto en la detección de tráfico peligroso o dañino	Propietaria, basada en dispositivos propios junto con la tecnología FACT
ForeScout CounterAct	Utiliza *appliances* propios, para realizar un despliegue transparente, no perjudicial para la red donde se realiza, combinando control de acceso que no utiliza clientes con prevención de intrusos para asegurar el correcto cumplimiento de la seguridad en los equipos	Propietaria, basada en dispositivos propios junto con la tecnología FastPass
InfoExpress CyberGatekeeper	La familia CyberGatekeeper ofrece tres productos, uno para implementar en entornos LAN, otro para sistemas remotos y el tercero que focaliza el control de acceso sobre el usuario final	Propietaria, basada en dispositivos servidores y software de agentes y servidores
Insightix NAC	Mantiene un inventario exhaustivo de todos los dispositivos conectados a la red, permitiendo, gracias a su tecnología de bloqueo y cuarentena única, implementar políticas de seguridad y control de acceso para cualquier dispostivo o tráfico	Propietaria
Juniper Networks Unified Access Control (UAC)	El Control de Acceso Unificado 2.0 incluye varios elementos: Infranet Controller, agente UAC y puntos de aplicación de la política de seguridad. Funciona en gran variedad de entornos, incluyendo aquellos con 802.1X	Compatible con la arquitectura TNC
Lockdown Enforcer	Se trata de *appliances* dinámicos de control de acceso a la red, que autentica de forma simultánea a usuarios y dispositivos y los analiza de forma periódica y también en caso de solicitud puntual, comprobando que cumplen las políticas de seguridad	Propietaria, basada en *appliances*
Microsoft NAP	Iniciativa propietaria de Microsoft	Microsoft NAC
Mirage Networks NAC	Familia de productos NAC, en la que las decisiones sobre qué política aplicar a los usuarios se toman en dispositivos diferentes a los que finalmente aplican la política, basada en escaneos de dispositivos y prevencion de intrusos	Propietaria, compatible con arquitecturas TNC y NAP
Nevis Networks LANenforcer	Esta solución se implementa sobre *switches* que son los que realizan el control de acceso de los usuarios, cada uno de los cuales se ubica en una DMZ personal donde se le protege de amenazas, y a la vez se protege a la red de las amenazas que pueda provocar dicho usuario	Propietaria, basada en el uso de dispositivos propios (*switches*)
Nortel Secure Network Access	Solución de control de acceso a redes basada en la implementación del control en los *switches* LAN, *routers* y *gateways* SSL VPN de Nortel	Propietaria
Senforce NAC & Endpoint Security Suite	Solución que integra la comprobación de que los usuarios finales están libres de amenazas, con la seguridad inalámbrica y el control de acceso a la red	Compatible con la arquitectura Cisco NAC
StillSecure SafeAccess	Solución muy flexible, que ofrece cinco opciones de aplicación de políticas en diferentes entornos, por lo que se adapta muy bien a redes complejas y heterogéneas	Compatible con la arquitectura Cisco NAC
Symantec Network Access Control	Ofrece una solución que permite aplicar control de acceso para dispositivos que se conecten a través de SSL VPNs, *switches* inalámbricos, aplicaciones basadas en Web, usando 802.1X, y casi cualquier infraestructura LAN o inalámbrica	Compatible con la arquitectura Cisco NAC
Vernier EdgeWall	*Appliances* NAC, que validan a los usuarios mediante una mezcla de política de confianza y chequeo de vulnerabilidades	Propietaria
Enterasys Secure Networks	Arquitectura basada en redes inteligentes, capaces de gestionar de forma individualizada cada usuario o dispositivo, permitiendo un control granular de usuarios, dispositivos y aplicaciones, ofreciendo una respuesta dinámica a intrusiones	Basada en estándares, no propietaria
HP Procurve Networking Adaptative EDGE	Arquitectura que permite construir redes con inteligencia perimetral, que pone la inteligencia en el punto de conexión del usuario, permitiendo realizar en ese punto funciones como la priorización de tráfico, autenticación, reserva de ancho de banda y aplicación de políticas	Arquitectura propietaria

3. NAC de Cisco

NAC Network Admisión Control

Se trata de la solución de control de acceso a redes de Cisco. Es una arquitectura propietaria, que en el lado del cliente se compone de un agente denominado Cisco Trust Agent software gratuito descargable desde la página del fabricante y cuya función es la de recibir la información del estado de la seguridad del equipo a conectar a la red proporcionando toda la información recogida, para recopilar esta información pueden usarse aplicaciones de distintos fabricantes o una propietaria de Cisco, el Cisco Secure Access. Para el Trust Agent Cisco ha desarrollado un protocolo propietario el EAP, en dos versiones: una sobre UDP y otra sobre 802.1X. La diferencia entre ambas es que sobre UDP se hace solo validación y en 802.1X se hace validación y autenticación. Además no todos los equipos Cisco soportan todos los escenarios posibles a través del protocolo EAP, muchos switches y routers requieren de una actualización. En cuanto a servidores Cisco la implementa en base al Access Control Server que ha desarrollado para tal fin, completando con interfaces de verificación, auditoria y autenticación de otros fabricantes. Cisco también ofrece una solución basada en appliances permitiendo una más rápida implementación

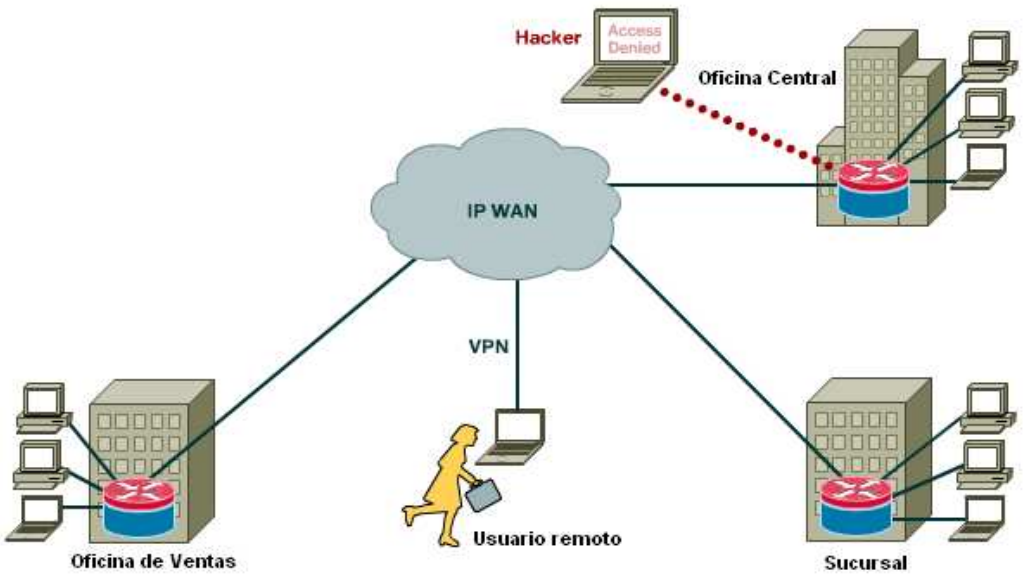
Cisco define a NAC como: El control de la admisión de la red de Cisco (NAC) es una solución que utiliza la infraestructura en red para hacer cumplir políticas de seguridad en todos los dispositivos que intentan tener acceso a recursos de computación de la red… NAC ayuda a asegurar que todos los hosts cumplan con las últimas políticas de seguridad corporativa, tales como antivirus, software de la seguridad, y patch (remiendo) del sistema operativo, antes de obtener el acceso de red normal.



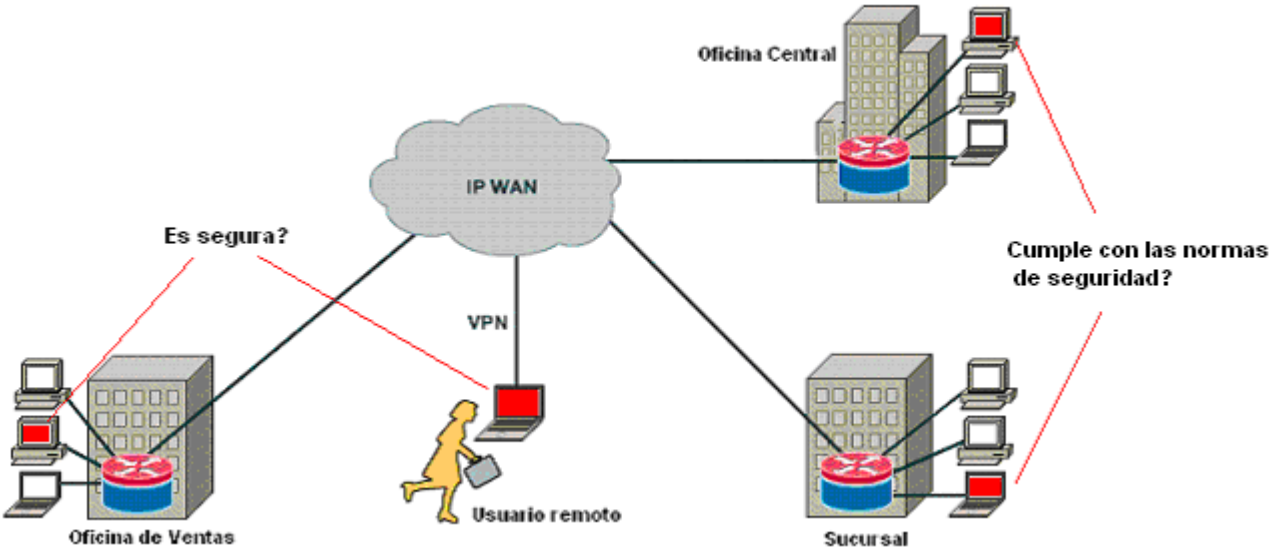
Estado el resultado de la interrogaciòn al host determina el tipo de acceso a la red: acceso full, acceso limitado, sin acceso , en cuarentena

1. La validación de postura ocurre cuando un dispositivo de acceso a la red detecta que un host se quiere conectar o usar los recursos de la red
2. una vez detectado el nuevo dispositivo el NAD (dispositivo de acceso a la red) habilita una conexión entre el AAA server)servidor de autorización autenticación y auditoria y el access control server ACS o server de control de acceso, una vez establecida el Server AAA requiere las credenciales de postura al host desde uno o mas plugins de posturas
3. el host responde a la petición con sus credenciales de postura desde los software compatibles con NAC
4. el server AAA valida la información de las posturas localmente, o puede delegar esta decisión a otros servers de validación de posturas
5. el server AAA agrega los resultados individuales de la postura, o símbolo (tokens)de postura, de todos los servers para determinar la conformidad total del host, o del símbolo de postura del sistema
6. la autenticación de identidad y el token de postura del sistema son luego chequeadas por una red de autorización , que puede consistir en : server Radius, asignación de VLANs o listas de acceso descargables
7. Estas cualidades del Radius se envían al NAD para la aplicación en el host
8. El CTA en el host envía el estado de su postura para notificar los plugins respectivos de su postura individual del uso así como la postura entera del sistema
9. se puede enviar opcionalmente un mensaje al usuario final usando el diálogo de la notificación de CTA's notificando el estado actual del anfitrión en la red.

Firewall, IPS e IDS previenen de ataques de hackers.



Pero que pasa con nuestra red, con nuestros dispositivos. Muchas compañías no tienen un control de sus propias pc`s, laptops del personal que accede desde afuera, oficinas remotas de la organización.

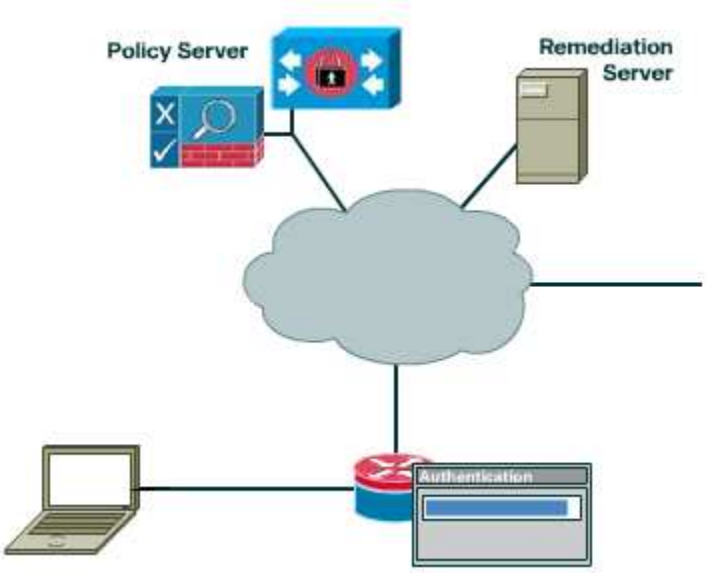


No sabemos si todos ellos cumplen con las políticas de seguridad en todos los puntos de acceso ala red, quizás en un primer momento en su implementación pero hace falta una política global para todos aquellos que usan nuestra red, esto es una política de control de admisión de acceso
¿Qué y quien se conecta y por cuanto tiempo?
¿Cuáles son los requerimientos para garantizar un acceso seguro a la red?
¿Que pasos se deben seguir para conseguir que se cumpla este acceso seguro?
¿Cuales son los requerimientos creados y cuales modificaremos?
Cisco introduce el concepto de NAC o Control de Admisión a la red
NAC securiza la entera relación entre los puntos finales y la red
Una verdadera solución de NAC debe:

- Autenticar e identificar accesos
- Hacer cumplir la política de accesos, impidiendo aquellos no permitidos
- Identificar e impedir el acceso a usuarios que no cumplan con la política de seguridad establecida
- Eliminar o en su defecto mitigar la vulnerabilidades

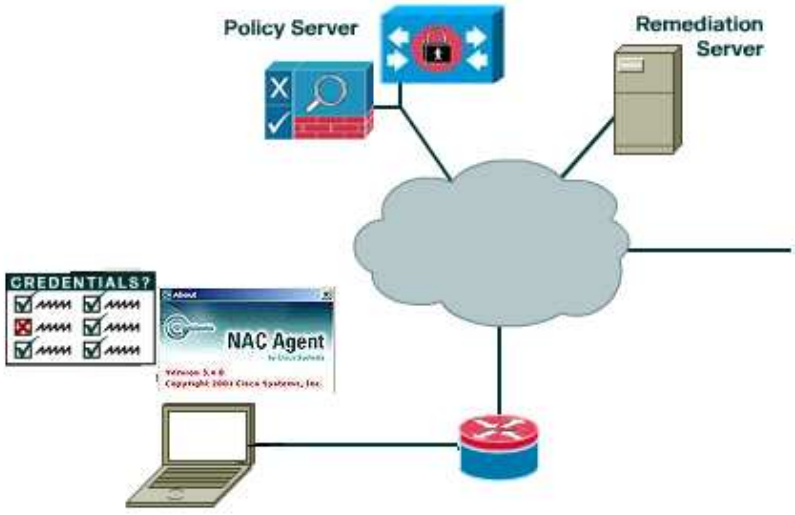
El control de acceso a la red se define como una tecnología o arquitectura que permite controlar el acceso de los usuarios a la red en un punto de acceso verificando además de su identidad el cumplimiento de todas las políticas se seguridad establecidas por la organización, es decir que el equipo que trate de conectarse este actualizado, tenga todas las herramientas de seguridad exigidas por la empresa, etc. se incluye además el control sobre lo que pueden hacer, a que contenidos e información pueden acceder estos usuarios y que sistemas o recursos son accesibles una vez admitidos en la red

Un usuario se conecta a la red corporativa con su laptop, pero su sistema operativo es vulnerable

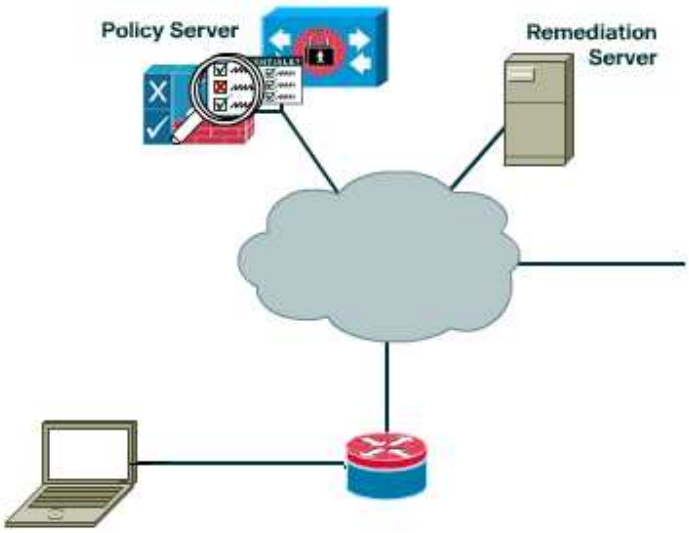


Su autenticación es validada

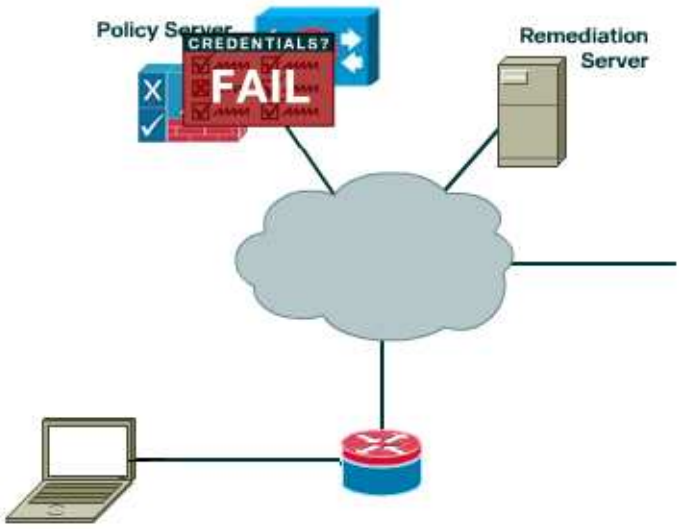
El sistema de control de admisión a la red scanea el dispositivo que se quiere conectar y encuentra que el sistema operativo de esa laptop es vulnerable a un nuevo gusano que acaba de aparecer



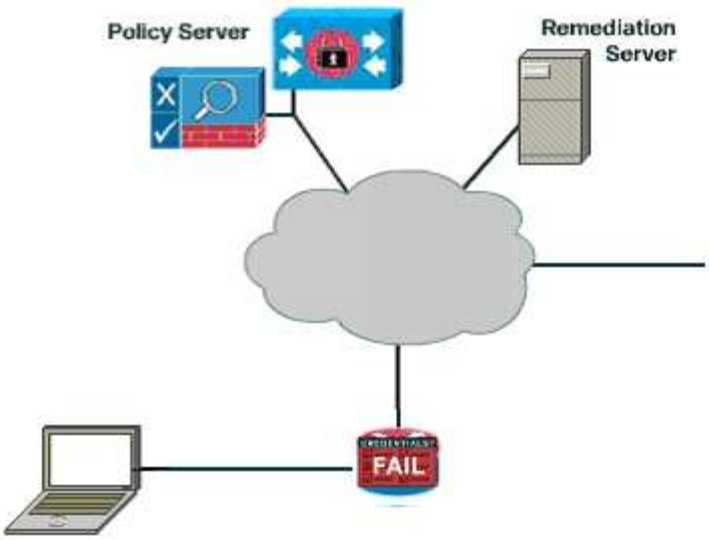
Esta vulnerabilidad es chequeada por el o los servers de políticas de validación



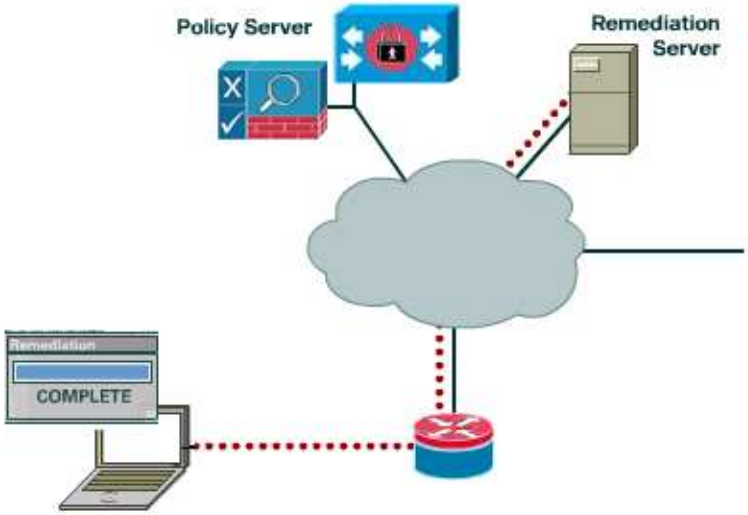
Si no cumple con lo estipulado sus credenciales no son aceptadas



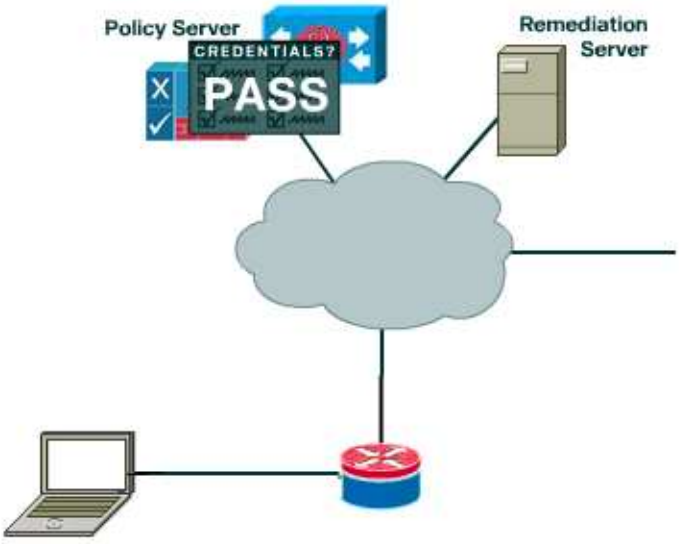
Por tal motivo su acceso no es otorgado



El sistema redirecciona la conexión a un server llamado server de remediación, el cual actualiza el sistema operativo con los últimos fixes haciendo que el dispositivo cumpla con las normas de seguridad establecidas por la organización.



El dispositivo es nuevamente chequeado y ya remediado se le otorgan las credenciales de acceso



4. NAP de Microsoft

Soluciones de Microsoft NAP (Network Access Protection)

Microsoft ofrece una variedad de tecnologías

- Microsoft Network Protection (NAP)
- 802.1X vía Microsoft
- Microsoft Network Access Quarantine Control (NAQC)

NAP (Network Access Protection) es la solución propietaria de Microsoft. Consta de una plataforma de aplicación pensada para ser soportada por el sistema operativo de Windows Vista y el servidor Windows Longhorn, requiere servers corriendo Windows Server 2008 y clientes corriendo Windows Vista o Windows XP service pack 3
NAP protege las redes y dispositivos que componen la red aplicando políticas de confianza basadas en requerimientos de salud que deben cumplir los dispositivos al componer una red.
La mayor diferencia que presenta esta solución es que al no ser fabricante de equipos de networking Microsoft basa su despliegue de agentes y aplicaciones en el lado del cliente y en el uso de distinto tipo de servidores en el lado de la red tanto para la verificación como para la admisión.
Microsoft define NAP como sigue: La protección del acceso de red (Network Access Protection NAP) es una plataforma que proporciona componentes para la aplicación de políticas para ayudar a asegurarse que las computadoras conectadas o a conectarse en una red cumplan con los requisitos para la salud del sistema

Plataforma NAP.
Los siguientes son los componentes de Microsoft NAP:

- NAP Agente-Este mantiene el estado de la salud basado en entrada de las comunicaciones del SHA (sistema agente de salud) con el Enforcement CLient Component (cliente de la aplicación componentes). Este agente crea el SOH (declaraciones de la salud) basándose sobre esta información.
- System Health Agent (SHA) agente de salud del sistema - éste es un componente para cada tipo de requisito de salud. Por ejemplo, podía haber SHA para el antivirus y otros para las actualizaciones del sistema operativo. (Éstos son similares a los plugins de postura de NAC de Cisco.)
- SHA Aplication Programming Interface (API) interfaz de programación de aplicación - éste permite que los vendedores creen e instalen SHAs a medida o por encargo.
- Enforcement Client Components (EC) componentes del cliente de la aplicación - éstas piden el tipo de acceso a la red, pasan el estado de salud de la computadora a un punto de la aplicación NAP que esté proporcionando el acceso de red, e indican el estado limitado o ilimitado del acceso de red del cliente NAP a otros componentes de la arquitectura
- .NAP EC API-Esta permite que los vendedores creen y que instalen ECs adicionales.

Los componentes del server son:

- NAP Enforcement Server servidor de la aplicación NAP(ES) - éste permite un nivel de acceso o de comunicación de red. Pasa estado de salud del cliente a un servidor de la política sanitaria y, basado sobre esa regeneración, puede controlar el acceso de red. Es el punto de la aplicación para la solución NAP

- NAP Administration Server. Servidor de Administración -Esta obtiene el SoH del NAP ES con el servicio de NPS. Distribuye el SoHs en la declaración del sistema de la salud (SSoH) al System Health Validators del sistema. Él recoge la declaración de las respuestas de la salud (SoHRs) de la salud Validators del sistema y la pasa al servicio de NPS para la evaluación.
- Newtwork Policy Servers Servidores de la política de la red (NPS) - la puesta en práctica de un servidor Radius y un proxy server Windows 2008. Esto proporciona la configuración de la política sanitaria y la evaluación centralizadas del estado de la salud del cliente NAP.
- System HealthValidator Validator de la salud del sistema (SHV) - éste recibe un SoH del servidor de la administración y compara la información del estado de salud del sistema en el SoH con el estado requerido de la salud del sistema.

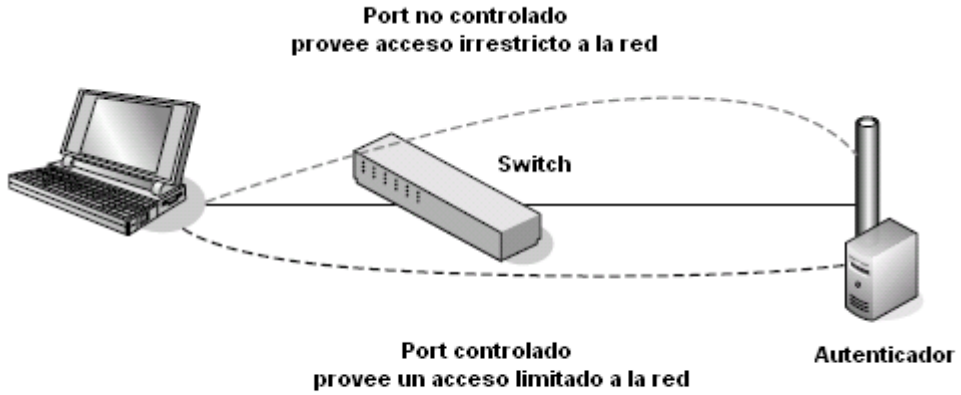
Microsoft NAP trabajará con infraestructura basada en Windows existente tal como el Acvtive Directory, Policy Group, Microsoft Systems Management Server (SMS), los servicios de actualización de Windows, y el servidor Microsoft Internet Security and Aceleration (ISA). Además, algunos componentes pueden ser proporcionados por otros vendedores. Microsoft ofrece dos APIs para que los vendors provean la integración de sus productos.

Microsoft 802.1X

802.1X es una autenticación basada en el port que puede aplicarse tanto para redes alámbricas como inalámbricas, la autenticación comienza en el port de acceso y tiene dos componentes primarios:

- **Suplicante** – requiere el acceso a la red
- **Autenticador**- autentica suplicantes y decide o no darle acceso a red.

Para entender mejor 802.1X podemos hablar de ports controlados y ports no controlados.
Un port controlado es aquel que nos habilita a ciertas direcciones de red. Un port no controlado nos permite un acceso irrestricto a la red.



Ports controlados y no controlados

Teniendo todos los ports de la LAN con ports controlados el acceso a la red el dado por el Autenticador. Microsoft ofrece soluciones 802.1X desde Windows 2000, Windows Server 2003, Windows XP y ediciones superiores.

NAQC (Microsoft Network Access Quarantine Control)

El control de la cuarentena del acceso de red (NAQC) es una herramienta de la inspección del acceso remoto que viene con el servidor 2003 de Windows. El propósito de esta tecnología era determinar que dispositivos pueden intentar conectividad remota a una LAN corporativa.

Microsoft no quiere ninguna confusión entre NAQC y NAP.
Microsoft indica específicamente lo siguiente:

NAQC proporciona solamente protección agregada para las conexiones de acceso remoto. NAP proporciona la protección agregada para las conexiones virtuales (VPN), Configuración del protocolo de configuración de anfitrión dinámico (DHCP), y comunicaciones basadas en IPsec. .

NAQC tiene los siguientes componentes:

- **Quarantine Compatible Remote Access Client**—sistemas operativos que soportan esta función, tal como Windows Xp, edición de Windows Millennium, y superiores

- **Remote Access Server**— corriendo sobre el servicio Routing and Remote Access

- **Remote Access Policy—** corriendo sobre el Remote Access Server

NAQC utiliza los scripts custom-written para analizar un sistema. Una vez que el script corre con éxito, la información se pasa a un componente notificador, que entonces se comunica con un servicio oyente en el servidor del acceso remoto. Si todo está bien, el servidor del acceso remoto lanza el requerimineto en la conexión. NAQC que viene con un número de componentes, incluyendo un componente del notificador rqc.exe y un servicio oyente remoto del agente de la cuarentena del acceso (Rqs.exe). , se puede crear un par de servicio oyente notificador usando las herramientas del kit del recurso del servidor de Windows 2003.

5. Esfuerzos por estandarización TNC. IETF

Confusión, complejidad y falta de interoperatividad

Las actuales tecnologías de control de accesos (NAC-Network Access Control) desaparecerán a medida que las empresas vayan adoptando sistemas de autenticación que operen en el extremo de las redes, de acuerdo con una reciente investigación de Forrester Research.

Según la consultora, la complejidad y falta de interoperatividad multimarca de estas tecnologías creará oportunidades de mercado a otros tipos de soluciones de autenticación y control de accesos más fáciles de implementar y gestionar.

Para Forrester, el mercado NAC se encuentra actualmente sumido en una gran confusión, debido en gran parte al amplio conjunto de soluciones y herramientas que engloba, que van desde sistemas de extremo a extremo sumamente complejos a aplicaciones de autenticación mucho más simples. Esta gran diversidad se ve reflejada también en los propios suministradores activos en este negocio, cuyos perfiles van desde las típicas firmas de seguridad a los grandes fabricantes de infraestructura de red, como Cisco Systems y Juniper Networks, sin olvidar a Microsoft, que se está haciendo un hueco en este negocio. Y todos ellos siguen un enfoque NAC diferente, creando un entorno operativo y funcional heterogéneo que complica la elección de los usuarios.

Uno de los mayores problemas de los sistemas NAC actuales es que obligan a crear varias políticas para controlar los mismos procesos. En el estudio se asegura que, por ejemplo, no es infrecuente que clientes de tecnologías de acceso inalámbrico y remoto de Symantec utilicen productos de Cisco para acceso de usuario local, lo que da lugar a políticas dispares que impiden que el usuario disfrute de una experiencia consistente cuando intenta acceder desde la oficina o en remoto.

Asimismo, el informe mantiene que muchos de los productos NAC actuales son “meramente preventivos”, limitándose a avisar a los usuarios de que sus ordenadores y dispositivos no cumplen las políticas de seguridad corporativas pero sin ofrecerles una solución efectiva para resolver el problema. Una incapacidad que, para la consultora, representa una de las mayores carencias de estas tecnologías. Incluso la funcionalidad de puesta en “cuarentena” de los dispositivos que no cumplen las normas de seguridad –un segmento de red donde quedan bloqueados los sistemas clientes hasta que logran cumplir las políticas de la empresa – queda en entredicho en el estudio. Según Forrester, esto podría perjudicar la productividad de usuarios autorizados pero que son enviados a la zona de cuarentena, impidiendo así su acceso a contenidos de su interés. Un inconveniente que favorecerá la adopción de aplicaciones NAC basadas en dispositivo o directamente en el extremo, donde residirá la inteligencia de seguridad, en lugar de en la propia red. “En muchos casos, las empresas ya disponen de la infraestructura de gestión y seguridad capaz de tratar esta función; sólo se trata de mejorar lo que ya está instalado”. Esta tendencia provocará un proceso de consolidación en la industria de seguridad de extremo y de autenticación de red, puesto que los principales fabricantes tratarán de disponer de todas las piezas necesarias para crear productos que puedan trabajar de tal manera.

TNC (Trusted Network Connect)

TNC es una arquitectura abierta desarrollada por Trusted Computing Group Se trata de una iniciativa que pretende ser una alternativa a las soluciones NAC propietarias, cuyo propósito principal es posibilitar que cualquier organización pueda implementar políticas de integridad y control de acceso en todas sus redes y conexiones, además de ofrecer interoperabilidad entre los dispositivos finales de red de los distintos fabricantes Por lo tanto, se trata de una iniciativa para ofrecer un estándar a todos los fabricantes y organizaciones que deseen acogerse a ella que les permita crear productos de control de acceso a la red compatibles unos con otros, y compatibles con las tecnologías y entornos ya existentes. Está especialmente diseñada para trabajar con el protocolo de control de acceso, autenticación y autorización 802.1X, aunque TNC no se ha limitado a este entorno y está desarrollando estándares para el resto de métodos de acceso y control como por ejemplo VPN. La meta de TNC es permitir que cualquier solución NAC/NAP pueda interactuar libremente
El gran problema es conseguir el consentimiento de todos los involucrados.
En Mayo del 2007 Microsoft y TCG anunciaron interoperabilidad en el evento Interop de Las Vegas. Básicamente, significa que los dispositivos que funcionan con el agente NAP de Microsoft se pueden utilizar en infraestructuras de NAP y de TNC. De hecho, este agente será incluido en le sistema operativo de Microsoft en las versiones siguientes: Windows Vista
Servidor 2008 de Windows
Versiones futuras de Windows Xp
En la lista de compañías que han anunciado compatibilidad con el estándar TNC o que tiene intención de hacerlo están:

- Microsoft
- Juniper
- Sygate
- Symantec

Por su parte Cisco lanza un programa para que terceras partes tengan interoperabilidad con su solución NAC.
Hay una gran diferencia entre TNC y este programa de Cisco. Mientras TNC pretende ser un Standard la intención de Cisco es que distintas compañías se acoplen a su solución NAC

IETF (Internet Engineering Task Force)

El gran problema de las soluciones NAC hoy disponibles es la falta de estándares que las haga interoperativos. Una carencia que trata de suplir el IETF, que formó el grupo de trabajo Network Endpoint Assessment (NEA) para estandarizar los protocolos comunes de las actuales arquitecturas NAC.

Inicialmente, la prioridad está siendo la normalización de los protocolos encargados de transportar la información sobre el estado de seguridad de los sistemas que intentan acceder –lo que NEA llama "posture attributes"– entre los "collectors" situados en dichos clientes y los "validators" que corren en los servidores de políticas.
NEA creó un subgrupo que definió un primer borrador del documento donde se recogen la terminología propuestas, diversos escenarios de uso y un modelo de referencia que incluye los recolectores de información de estado ("posture collector") y los "validators" de dicho estado respecto de componentes específicos de la política, como los antivirus, por ejemplo.

NEA propone estandarizar el protocolo PA (Posture Attibute), que pasa los atributos de estado del sistema cliente sobre un determinado componente de la política entre los "collectors" y los "validators", y el protocolo PB (Posture Broker), encargado de transportar los mensajes de PA agregados de extremo a extremo. Además, estipula los requerimientos que deberían cumplir los protocolos encargados de pasar la información de estado de los mensajes PB entre el cliente NEA y el servidor NEA.

Es de resaltar que otras capacidades y protocolos que podrían afectar a la interoperatividad son obviados concientemente de los objetivos actuales de NEA, especialmente los relacionados con la solución de problemas cuando el cliente no cumple las normas de seguridad de la empresa y el reforzamiento de políticas. Además, sólo se propone estandarizar los protocolos NAC que afectan a la infraestructura, mientras que existen fabricantes que se apartan de este modelo, como por ejemplo, los que siguen el reforzamiento IPSec, que utilizan certificados de clave pública X.509. Estos certificados se obtienen de un servidor que actúa como autoridad de registro sobre el estado de seguridad y los utiliza posteriormente para establecer relaciones con otros servidores que actúan como iguales del primario.

Elegir una determinada arquitectura NAC depende de los objetivos que se persigan y de la estrategia global de seguridad de cada empresa. Si una organización se mueve en un entorno Cisco actualizado, lo mejor será adoptar la arquitectura de este fabricante, tan completa como cualquier otra. Para aquellos interesados en soluciones basadas en estándares, TNC es la única opción real, a pesar de sus riesgos. El enfoque de Microsoft, finalmente, resulta el más apropiado para redes más pequeñas donde se quiera controlar los PC de la empresa y la principal preocupación sean los virus y no tanto la autenticación y el control de accesos.

6. Tecnologías con funcionalidad NAC/NAP : 802.1X, IPSec VPN y SSL VPN

Existen distintas tecnologías que componen todo el entramado de las soluciones NAC, entre las que se puede destacar la autenticación en el acceso a un punto ¨vivo¨ en la red tecnología estándar 802.1X. A pesar de ser un estándar ya consolidado que data del año 2001 al contrario de lo que ocurre con la mayoría de que componen el control de acceso a la red, hay problemas con la integración con algunos sistemas operativos.

La **IEEE 802.1X** es una norma del IEEE para el control de admisión de red basada en puertos. Es parte del grupo de protocolos IEEE 802 (IEEE 802.1). Permite la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto previniendo el acceso por ese puerto si la autenticación falla. Es utilizado en algunos puntos de acceso inalámbricos cerrados y se basa en el protocolo de autenticación extensible (EAP– RFC 2284). El RFC 2284 ha sido declarado obsoleto en favor del RFC 3748.

802.1X está disponible en ciertos switches de red y puede configurarse para autenticar nodos que están equipados con un software *suplicante*. Esto elimina el acceso no autorizado a la red al nivel de la capa de enlace de datos.

Algunos proveedores están implementando 802.1X en puntos de acceso inalámbricos que pueden utilizarse en ciertas situaciones en las cuales el punto de acceso necesita operarse como un punto de acceso cerrado, corrigiendo fallas de seguridad de WEP. Esta autenticación es realizada normalmente por un tercero, tal como un servidor de RADIUS. Esto permite la autenticación sólo del cliente o, más apropiadamente, una autenticación mutua fuerte utilizando protocolos como EAP-TLS.

Windows.XP y Windows Vista soportan 802.1X para todas las conexiones de red por defecto. Windows 2000 lo soporta con el último service pack. El Windows Mobile 2003 y sistemas operativos más últimos también vienen con un cliente nativo 802.1X.
Un proyecto para Linux conocido como Open1X produce a cliente abierto de la fuente, Xsupplicant.
El wpa_supplicant más general se puede utilizar para 802.11 en wireless y en redes cableadas.
Ambos apoyan una gama muy amplia de EAP. MAC OS X ha ofrecido la ayuda nativa desde 10.3 mientras que iPhone y el iPod Touch lo soportarán en junio 2008

Para algunas compañías, la ejecución de una verdadera solución NAC/NAP no esta en sus planes inmediatos. Al mismo tiempo, pueden reconocer que los sistemas móviles plantean una amenaza grave a su LAN y quisieran aprovecharse de una tecnología para asistir con este problema. Este es un ejemplo perfecto en donde usar tecnologías existentes tales como dispositivos VPN que puede ayudar a agregar funcionalidad NAC.

Funcionalidad NAC en IPSec VPN

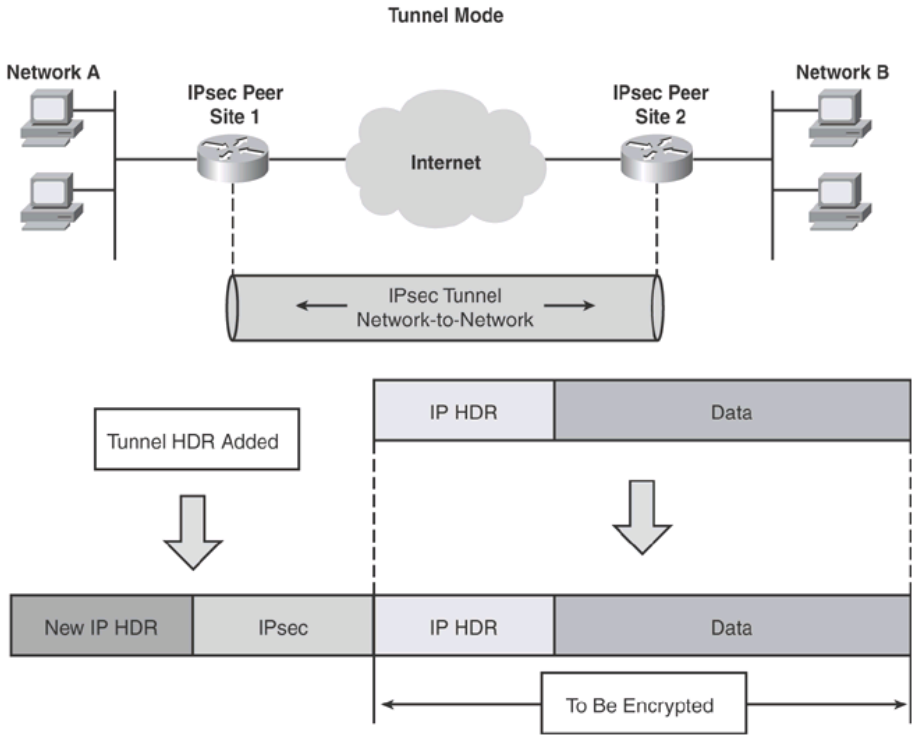
IPsec (Protocolo de Seguridad de Internet) es un set de estándares abiertos desarrollados por el IETF. IPsec es ejecutado por un sistema de los protocolos criptográficos para asegurar tráfico IP.
El marco de IPsec asegura el funcionamiento del tráfico IP en la capa 3 (capa de red) del modelo de OSI, así asegurando todos los usos de la red y las comunicaciones que utilizan la red del IP. Usando combinaciones de hashing, de llave simétrica, y de algoritmos criptográficos asimétricos, IPsec ofrece los servicios siguientes de seguridad:

- Peer Authentication Autentificación del par
- Data confidentiality Secreto de los datos
- Data integrity Integridad de datos
- Data origin Authentication Autentificación del origen de datos
- Replay detection Detección de la respuesta
- Access control Control de acceso
- Traffic flow confidentiality Secreto de circulación

IPsec Request for Comments (RFCs)

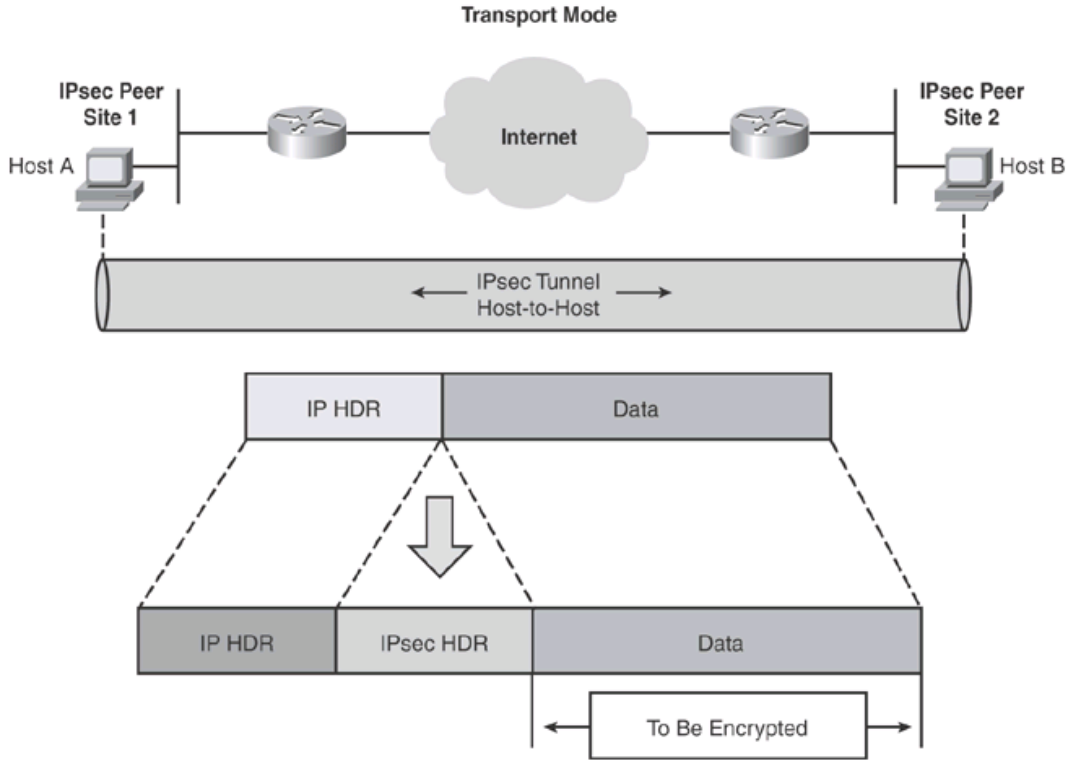
IPsec es un sistema de estándares abiertos que se documenta en varios RFCs. Originalmente, IPsec fue definido en una serie de RFCs 1825-1829, publicado en 1995. Mientras que la tecnología se desarrolló, éstos fueron puestos al día por más nuevas revisiones e hicieron obsoleto por RFCs 2401-2412 publicado en 1998. En 2005, una tercera generación de RFCs 4301-4309 (de 2401-2412) fue producido para incluir otros adelantos en este tema. IPsec tiene dos métodos para propagar los datos a través de una red:

Modo túnel: Protege datos en red-a-red o sitio-a-sitio Por ejemplo, la red A en el Site1 se conecta con la red B en Site2. En modo del túnel, IPsec protege datos a nombre de la otra red entidad-que es, cifra tráfico a través de los pares de IPsec. El modo del túnel encapsula y protege la carga útil entera del paquete IP incluyendo el header original de IP y agrega un nuevo header IP. El header de IPsec se agrega según muestra el siguiente dibujo

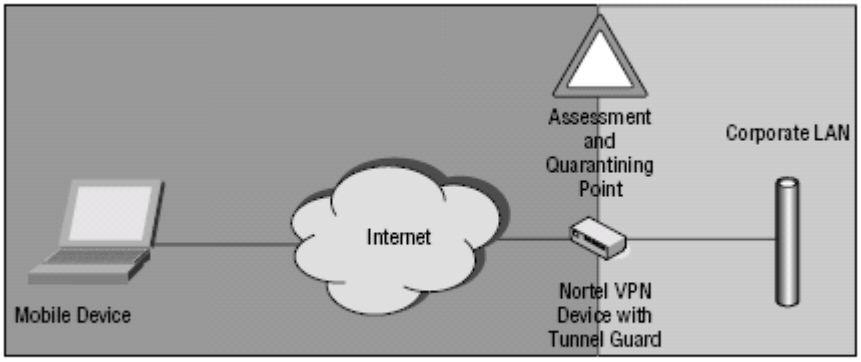


IPSec modo transparente

Protege datos en host –a-host o end to end Por ejemplo, el host A en el Site1 se conecta con el host B en Site2. En modo transparente, IPsec protege datos peer to peer., agrega un nuevo header IP entre el payload y el header original según muestra el siguiente dibujo



Cuando los sistemas remotos intentan crear un VPN a la red corporativa con sus clientes de IPSec VPN, hay ventajas en la seguridad porque se determina el acceso para esos clientes antes de que se les permita acceso completo. Mientras que muchos dispositivos de IPSec VPN pueden realizar esta funcionalidad, centrémonos en la solución de VPN de Nortel.
Nortel introdujo la funcionalidad de Tunnel Guard (protector del túnel) a sus dispositivos de VPN. El protector del túnel es una aplicación relacionada con el cliente de IPSec VPN que comprueba si los componentes de seguridad requeridos están instalados y activos en la máquina del usuario remoto. Este chequeo ocurre mientras que el usuario intenta conectarse con el VPN.



Nortel VPN Tunnel Guard topology

El Túnel Guard debe buscar cuando el usuario se conecta las reglas predeterminadas de requisito de software (SRS). Si el dispositivo pasa estas reglas, entonces el acceso es proporcionado a la red según lo definido en su política del grupo. Si falla, su acceso puede ser limitado, o el túnel de VPN puede ser desconectado. El protector de túnel tiene en cuenta diversos elementos de seguridad para analizar en un sistema que intenta el acceso, incluyendo lo siguiente:

- Ejecutables
- archivos de .dll
- Archivos de configuración

El protector del túnel también tiene en cuenta la integración con los chequeos predefinidos de software de otros vendors lo que le permite una fácil integración

Funcionalidad de NAC en SSL VPN

Secure Sockets Layer -Protocolo de Capa de Conexión Segura-
Muchos dispositivos VPN pueden actuar tanto como IPSec VPN y SSL VPN,
Con SSL VPN no es necesaria la instalación de un cliente
El estándar primario en el espacio de VPN era IPSec, aunque algunos fabricantes utilizaran otros métodos, incluyendo el protocolo Layer 2 Tunneling (L2TP), y el Point-to-Point Tunneling Protocol (PPTP). SSL VPNs usa una diversa metodología de transportar datos confidenciales a través de Internet En vez de la confianza en el usuario final para tener un cliente configurado en una laptop de la compañía, SSL VPNs usa HTTPS que está disponible en todos los browsers Web como mecanismo de transporte seguro, sin la necesidad del software adicional. Con SSL VPN, la conexión entre el usuario móvil y el recurso interno sucede vía una conexión Web en la capa de aplicación, en comparación con el "túnel abierto" de IPSec VPNs en la capa de red.
El uso del SSL es ideal para el usuario móvil porque:

- SSL VPN no requiere software previamente instalado n el dispositivo que es utilizado para tener acceso a recursos corporativos.

- SSL VPN no necesita ser configurado en la máquina remota por un usuario o un administrador.

- SSL VPN está disponible de cualquier Web browser estándar, así que los usuarios no necesitan una laptop de la compañía.

Comparación entre IPSec VPN y SSL VPN.

IPsec y SSL VPN Comparación		
	IPsec VPN	**SSL VPN**
Opciones de usuarios	Habilita acceso desde desktops propias de la organización	Habilita acceso desde desktops propias de la organización, desktops de terceros desde Internet cybercafé
Método de acceso	Requiere usar un cliente VPN de softwarte	Se inicializa a través de un web browser.
Requerimientos de Software	Requiere preinstalar un cliente software propietario	No requieres un especial cliente de software VPN; solo es requerido un web browser
Software Updates	Puede hacer update automáticos , pero es mas intrusivo y requiere la operación del usuario	No requiere software instalado; no requiere updates. El acceso es provisto por software instalado dinámicamente y el usuario no tiene que hacer updates
Configuración del acceso de los usuarios	Ofrece políticas de acceso granular pero no portales web	Ofrece políticas de acceso granular, y portales web.

La empresa Juniper es la que mayor desarrollo ha logrado en esta tecnología y ofrece una amplia gama de productos

7. Alternativas de Código Abierto

Las comunidades NAC de código abierto aportan dos ventajas clave comunes a todas las comunidades de software libre:

a. la capacidad para encontrar fallas de seguridad rápidamente gracias al espíritu de colaboración con el que trabajan

b. la ampliación progresiva de características y funcionalidades a medida que crece la demanda.

Existe bastante oferta de de código abierto para NAC. Ciertamente, el "libre" los productos no viene sin ninguna dificultad, el software de código abierto en general es propenso a la falta de apoyo técnico del creador, la falta de actualizaciones y la grave falta de interoperabilidad. Si uno llama a un soporte de Microsoft para recibir soporte y le dice que estaba en ejecución NAC de código abierto no obtendrá ningún tipo de soporte.

El potencial de la falta de apoyo técnico a su vez tiende a muchos usuarios de software de código abierto a invertir mucho tiempo tratando de solucionar temas de compatibilidad.

En la lista de proveedores de código abierto NAC podemos encontrar:

1. PacketFence Zero Effort NAC (ZEN),
2. FreeNAC
3. Netpass

PacketFence Zero Effort NAC (ZEN)

Es un appliance virtual que consta de una imagen de sistema operativo que corre sobre Linux o Windows y realiza chequeos de políticas de dispositivos según acceden a la red. Su software autentica a los usuarios mediante cualquiera de los métodos soportados por los servidores Web Apache de fuente abierta y realiza análisis de vulnerabilidades, desviando a los sistemas que no cumplan las políticas a una zona preparada para solucionar su situación. Puede aislar dispositivos mediante cambios por DHCP y manipulando caches ARP Address Resolution Protocol. PacketFence ZEN no es más que la última innovación entre alrededor de una docena de paquetes NAC basados en software libre, la mayoría de ellos creados en reacción a los mismos problemas de seguridad, como los gusanos Sasser y Blaster, que empujan a las firmas comerciales a desarrollar sus soluciones. Y como sucede con el resto de software libre, precio e independencia de fabricantes son las principales razones por la que algunos usuarios se inclinan por este tipo de soluciones.

PacketFence ZEN es compatible con cualquier switch con soporte de SNMP, es decir, prácticamente la totalidad de los switches.

FreeNAC

Desarrollado por Swisscom, el operador dominante de Suiza. Su versión comercial incorpora algunas características no disponibles en la versión de código abierto que se pueden conseguir por una tasa de suscripción que incluye instalación y soporte. El servicio se dirigía inicialmente a empresas con infraestructuras heterogéneas sin actualizar, como switches sin soporte de autenticación de puerto 802.1x, una exigencia de muchos productos NAC convencionales. Sin embargo, FreeNAC, que, como otras herramientas de código libre, comenzó utilizando VMPS de Cisco para reforzar políticas, ahora también soporta 802.1X cubriendo así, además, entornos mixtos en proceso de actualización a soluciones comerciales.

FreeNAC proporciona fácil uso de VLANS, control de acceso de LAN para todo tipo de dispositivos de red (tales como servidores, estaciones de trabajo, impresoras, teléfonos IP, cámaras web ...), y gestión de la documentación. Permite revisión de cableado.

La solución FreeNAC Desde el punto de vista de seguridad, detecta los dispositivos ajenos a la red que están intentando obtener acceso a través de un conector de red Ethernet y, a continuación, niega el acceso (y registra el evento). Conocidos y registrados se habilitan a la LAN que se les atribuyen. Los visitantes (los dispositivos desconocidos), opcionalmente pueden tener acceso a una zona llamada VLAN de default / guest VLAN. Esto puede ser útil, por ejemplo, para las organizaciones que deseen permitir acceso a los visitantes Web / VPN de acceso por Internet, pero que no tienen acceso a las redes internas.

Funcionamiento

Un switch detecta una nueva PC y pide la autorización de FreeNAC, que comprueba su base de datos y se niega o concede el acceso a la red basado en la dirección MAC. FreeNAC es una versión muy mejorada de "OpenVMPS" y directamente puede sustituir a otras soluciones VMPS con importantes mejoras en la facilidad de uso.

Las principales características de FreeNAC son:

- asignación dinámica de VLAN, es decir, se asignan VLAN basada en la dirección MAC del dispositivo, no se basa en el puerto Switch, los dispositivos pueden moverse y seguir perteneciendo a la misma VLAN asignado
- Una interfaz de usuario amigable para la gestión
- Se puede vincular con bases de datos externas
- Documentación de cableado y presentación de informes
- El uso de una base de datos MySQL proporciona escalabilidad, flexibilidad, facilidad de integración y permite hacer consultas de inventario de red.

Beneficios:

- No se necesita software de los dispositivos finales
- código abierto y extensible
- se ejecuta en hardware estándar y los sistemas operativos (Linux / Unix)
- mejor utilización de los puertos de switch (eficiencia, ahorro de costes)
- puede ser configurado por el apoyo de nivel 1 de Helpdesk
- cambiar la configuración más sencilla, ya que los puertos son "dinámicas"
- menor número de cambios en el cableado durante reorganizaciones

La arquitectura FreeNAC se compone de un servidor con la base de datos master y programas de control.
Opcionalmente, uno o varios servidores esclavos para redundancia y distribución de la carga

Netpass

Trabaja asignando los puertos de un switch en una de dos VLANs

El valor por defecto es asignar el puerto en la VLAN de cuarentena. En este estado, todo el tráfico desde el cliente se dirige al Server Validación NetPass (NPVS). El NPVS intercepta el tráfico, realiza el control, facilita la auto-reparación y mueve el puerto del cliente a la VLAN de no cuarentena una vez que se garantice el cumplimiento. La auto-reparación se logra con la corrección específica de las reglas para el cumplimiento de las mismas. Una vez que estos pasos se realizan se vuelve a chequear el cumplimiento

NetPass está construido para ofrecer módulos de identificación. Cualquier parte de la infraestructura existente se puede utilizar para activar una cuarentena de un cliente. Por ejemplo, su servidor de correo podría detectar un cliente en particular envío un correo electrónico con la carga de un virus - señal segura de que el cliente está infectado. Ese mismo mailserver puede encargarse de pasar a ese usuario a la VLAN de cuarentena. Como parte de esa transacción, el servidor de correo le dirá la razón por la que el cliente está en cuarentena al NVPS . Esta información se utilizará para ayudar al cliente en el proceso de auto-reparación.

NetPass incluye módulos para comprobar el cumplimiento de Snort y Nessus, además de un API para la integración de otros sistemas de identificación. NetPass también incluye una interfaz web para fines administrativos - que le permite cuarentena manualmente anfitriones cuando sea necesario.

NetPass presta atención al estado de los puertos del switch y de los dispositivos adscritos a cada puerto. Si un cliente en cuarentena se mueve a otro puerto se mantendrá en cuarentena. Si un cliente en cuarentena se conecta a otro switch en una VLAN de no cuarentena será automáticamente conectado a la VLAN de cuarentena. NetPass soporta múltiples fabricantes de switches

NetPass está diseñado para ser flexible y ofrece varias opciones de implementación - lo que le permite decidir cuan estricto se desea ser con un dispositivo en cuarentena

Cuarentena: una vez que el cliente es identificado como fuera de las normas de cumplimiento, está en cuarentena. Esto se logra mediante el cambio de la pertenencia a la VLAN de los puertos del switch donde el cliente esté conectado. NetPass proporciona subredes de cuarentena, en lugar de una gran VLAN de cuarentena. Esto permite una serie de estados de cuarentena, algunas de carácter temporal

Mientras que un dispositivo está en cuarentena mantiene su dirección IP. No se le asigna una dirección IP distinta. NetPass no se basa en el protocolo DHCP para trabajar

Remediación: El cliente utiliza su normal servidor DNS, no necesita de otros servidores DNS. El cliente tiene acceso a la Web a sitios Web aprobados (que usted puede controlar) a los efectos de la descarga de parches, archivos de definición de virus y utilidades para ayudar al cliente a la remediación. Esto ayuda, en muchos casos, a reducir la cantidad de personal de TI que se requiere para regularizar el host. Esto permite corregir el problema y salir de cuarentena lo antes posible.

Una vez que el cliente ha terminado la remediación NetPass chequea una vez más los controles para asegurar el cumplimiento. Si alguno de los pasos a de remediación no fue hecho con éxito vuelve a cuarentena. Este proceso continúa hasta que el host cumpla con las normas establecidas

NetPass tiene flexibilidad, permitiendo que el administrador de NetPass pueda pasar a un cliente a un estado por la fuerza si es necesario. Un cliente puede estar en cuarentena o no de forma permanente.

8. Conclusiones

Escenario actual:
TNC esta trabajando para consolidar un estándar y hasta ahora cuenta con el apoyo de importantes empresas como: Microsoft, Juniper Networks, Sygate y Symantec.

Mientras que Cisco sigue con su Programa de Alianza con sus partners y los ha dividido en dos grupos: los que están activamente adhiriendo a Cisco NAC y los que están desarrollando productos para trabajar junto con Cisco NAC.

En el primer grupo se encuentran las empresas:
AhnLab, Belarc, BigFix, Computer Associates, Core, Emaze Networks, Endforce, F-Secure, GreatBay Software, GriSoft, Sauri, IBM, InfoExpress, Intel, IPass, Kaspersky, LANDesk, Lockdown Networks, McAfee, Norman, Panda Software, PatchLink, Phoenix Technologies, Qualys, Safend, SecureAxis, Secure Elements, Senforce, Shavlik, Sophos, StillSecure, Sumitomo Electric Field Systems CO, LTD., TrendMicro, TriGeo Network Security, Websense.

En el segundo grupo:
Applied Identity, AppSense, Aranda Software, Beijing Beixnyuan Tech Co, LTD., Cambia, CounterStorm, Credant Technologies, Criston, Dimension Data, EagleEyeOS, Ecutel, eEye Digital Security, Envoy solutions, ESET, Fiberlink, GuardedNet, HP, INCA, Kace, Kingsoft, Lancote, Mi5 Networks, nCircle, netForensics, Nevis,, NRI-Secure, NTT, OPSWAT, Pino, Promisec, Rising Tech, ScanAlert, SignaCert, SkyRecon, SmartLine, Softrun,Inc., Telus, Tenegril, Trust Digital, VMWare ACE, Webroot.

Independientemente de que se logre un estándar o no, es absolutamente importante adoptar un criterio para proteger las redes corporativas tanto desde adentro como desde accesos remotos y, analizando las distintas propuestas todas ellas tienen como premisa seguir los siguientes criterios para analizar los dispositivos que se van a conectarse la red.

- ¿Está el antivirus instalado y corriendo?
- ¿Es el antivirus que tiene instalado aceptablemente actualizado (por ejemplo no necesariamente tiene que estar instalado la última versión de antivirus, generalmente se acepta como valido tener una o dos versiones anteriores a la ultima
- ¿Está el antispyware (programa anti espía) instalado y ejecutándose?
- ¿Está el antispyre aceptablemnet actualizado) se siguen los mismos criterios que para el antivirus
- ¿Está el firewall personal instalado y ejecutándose?
- ¿Tiene el dispositivo los últimos patches de Microsoft?
- ¿El dispositivo tiene los patches requeridos para otros componentes de software? (Los programas de Microsoft no son los únicos usos de la empresa que requieren remiendos/actualizaciones de la seguridad.)
- ¿Están instalados y corriendo programas prohibidos como LimeWare, Kazaa, por ejemplo?
- ¿Es el dispositivo un activo de la empresa? (Esto es a menudo establecido para comprobar el seteo de la regestry, o la existencia de archivos específicos u otras seteos que existen solamente en activos corporativos.)
- ¿El software de encripción del archivo está instalado y en funcionamiento?
- ¿Otros aplicaciones específicas de seguridad de la empresa están instalados y funcionamiento?

Por lo expuesto la empresa Cisco tiene mucho poder y está empeñada en seguir con su programa sin importarle trabajar para un estándar, y a mi criterio apuesta a que su solución sea en el futuro un estándar de facto
Un estándar de facto es aquel patrón o norma que se caracteriza por no haber sido consensuada ni legitimada por un organismo de estandarización al efecto. Por el contrario, se trata de una norma generalmente aceptada y ampliamente utilizada por iniciativa propia de un gran número de interesados, Además cuenta con el viejo adagio: ¨*Ninguna organización ha despedido jamás a un empleado por haber elegido comprar equipos Cisco*¨.

La elección de una alternativa de código abierto es una solución que en general no tiene buena aceptación por lo menos en las grandes empresas privadas argentinas, ya que prefieren adoptar tecnologías provistas por sus partners tecnológicos y no tener que lidiar con soluciones en las que tengan que invertir horas de sus equipos de desarrollo. Además, la adopción de un código abierto es mucho más complicada, ya que de una u otra manera forman parte o tiene estrechas relaciones con las grandes multinacionales y están atadas a seguir los lineamientos que dictan sus casas matrices.

En Europa, las organizaciones gubernamentales (expresamente en Alemania) adoptan alternativas de código abierto, porque la relación que tienen con sus universidades es muy estrecha y el soporte que reciben de ellas es el que se requeriría de un departamento de desarrollo si se tratase de una empresa.

Independientemente de ello cada organización tiene que tener conciencia de que es imprescindible contar con un Control de Acceso a Red tanto externa como internamente.