**VPN**

Las vpn de este tipo ofrecen tres beneficios básicos:

**Autenticación:**  esto se puede lograr mediante el uso de nombres de usuario y contraseñas, claves compartidas (PSK), contraseñas de un solo uso (OTP) o tokens, infraestructura de clave publica (PKI)

**Integridad:** proporciona un medio para garantizar que los datos no hayan sido manipulados a lo largo de la ruta entre el origen y el destino (si un atacante intenta realizar un ataque de intermediario).

**Anti reproducción:** el dispositivo de envío puede agregar números de secuencia a cada paquete enviado.

**Ejemplos:**

* Acceso remoto Ipsec (IKEv1)
* Cliente y servidor Easy VPN Remote (IKEv1)
* Cliente de hardware Easy VPN Remote (solo ASA 5505)
* Acceso remoto SSL sin cliente
* Acceso remoto AnyConnect SSL (SSL/TLS)
* Acceso remoto AnyConnect IKEv2 (SSL/TLS y seguridad de la capa de transporte de datagrama [DTLS]).
* Ipsec de sitio a sitio (IKEv1 e IKEv2) (ASA 8.4 permite túneles de LAN a LAN [L2L] utilizando IKEv1 e IKEv2)

**Tipos de VPN:**

Según las capas del modelo OSI, las VPN se pudeen dividir en las siguientes tres ctegorias principales:

VPN de enlace de datos

VPN de capa de red

VPN de capa de aplicación

**VPN de capa de enlace de datos**

Con las VPN de capa de enlace de datos, se conectan dos redes privadas en la capa 2 del modelo OSI mediante un protocolo como Frame Realy o ATM.

Aunque estos mecanismos proporcionan una forma adecuada de crear VPN, a menudo son costosos, porque requieren la creación de rutas.

**VPN de capa de red**

Las VPN de capa de red se crean utilizando técnicas de tunelización y/o encriptación de capa3. Un ejemplo es el uso del protocolo de encriptación y tunelización Ipsec para crear VPN. Otros ejemplos son los protocolos…

**VPN de capa de aplicación**

Las VON de la capa de aplicación se crear para funcionar específicamente con determinadas aplicaciones.

Un muy buen ejemplo de este tiempo de VPN son las VPN basadas en SSL. SSL proporciona cifrado entre los navegadores web y los servidores que ejecutan SSL.

Uno de los principales inconvenientes de las VPN de la capa de aplicación es que a menudo no son perfectas. El usuario debe realizar una acción para habilitar los dispositivos finales para crear…

**Protocolos**

**Ipsec**

El protocolo de seguridad de internet (IPSec) es una estructura genérica iniciada y mantenida por un grupo de trabajo del grupo de trabajo de ingenieria de internet (IETF) para proporcionar varios servicios de seguridad para el Procotolo de Internet (IP), tanto para IPv4 como para IPv6 (el próximo).

IPSec fue diseñado para admitir dos modos de cifrado.

El modo de transporte protege solo la porción de carga útil de cada paquete, mientras que el modo de túnel ecnripta tanto el encabezado como la carga útil.

Para que IPSec funcione como se espera, todos los dispositivos deben compartir una clave común.

Aunque los protocolos utilizados para cifrar los datos son muy importantes para el éxito general del sistema, se ha dedicado una gran cantidad de trabajo a la autenticación e inercambio de claves por parte del remitente y el receptor.

Esto se logra en gran cantidad…

**ESP (carga útil de seguridad encapsulada)**

La unidad fundamental de trasmision en internet es el paquete IP (protocolo de Internet), del que dpenden la mayoría de las comunicaciones WAN y LAN.

IPSec maneja el cifrado a nivel de datagrama IP usando un nuevo protocolo, el encapsulating security protocol (ESP).

ESP fue diseñado para soportar casi cualquier tipo de cifrado simétrico, como DES o DES triple, ESP se basa mínimamente en DES de 56 bits.

**AH (encabezado de autenticación)**

Donde ESP asegura los datos mediante cifrado, el protocolo de encabezado de autenticación AH …

**Intercambio de claves de internet, ISAMKP/Oakley**

**Tener soloESP y AH no completa la imagen de un sistema IPSec.**

Para una comunicación segura, ambas partes deben poder negociar claves para su uso mientras se realiza la comunicación. Además, ambas partes deben poder decidir que algoritmos de autenticación y cifrado utilizar.

El protocolo de intercambio de claves de internet (IKE) anteriormente conocido como ISAKMP/Oakley) proporciona autenticación de todos los pares, maneja las políticas de seguridad que cada uno puede realizar y controla el intercambio de claves.

**ISO X.509 v.3 (certificados digitales)**

El sistema X.509 es importante porque proporciona un nivek de control de acceso con un alcance mas amplio.

Debido a que los sistemas de certificados X.509 se utulizan…

**PPTP (point-to-point Tunneling Protocol)**

**El protocolo de túnel punto a punto (PPTP) es una extensión del protocolo estándar PPP (punto a punto).**