www.DarFe.es

"Charlas sobre Ciberseguridad"

*(módulo: cursos On-Line Ciberseguridad **moodle.darFe.es**)*

TEMA 5

Ciberseguridad: Plataformas / infraestructuras de Seguridad en Red

(Jueves 03 de agosto de 2017)

Cursos en: http://moodle.darfe.es

Índice

1. INTRODUCCIÓN

Esta es la quinta de nuestras charlas. Trataremos este aspecto fundamental para nuestra empresa, que se relaciona al hardware y software que debemos tener en cuenta para nuestra tarea de "ciberdefensa".

2. OBJETIVO

Fomentar el empleo de las plataformas o infraestructuras básicas desde el punto de vista de Ciberseguridad, ofreciendo aspectos de interés sobre buenas y malas prácticas en la gestión de las mismas.

3. TEMARIO Y FECHAS DE TODO EL CICLO 2017

A continuación se presentan la totalidad de las charlas que conforman este ciclo durante el año 2017.

Temario y fechas

Nº	Tema de la charla	Fecha
1	**Presentación, conceptos y situación de Ciberseguridad. *¿De quién nos defendemos?***	**Jueves 30 de marzo**
2	**Estrategias de Ciberseguridad en grandes redes (*Seguir y perseguir - proteger y proceder*)**	**Jueves 27 de abril**
3	**Ciberdefensa en profundidad y en altura (*la conquista de las cumbres*)**	**Jueves 25 de mayo**
4	**Ciberseguridad: La importancia de los procesos.**	**Jueves 29 de junio**

5	**Ciberseguridad: Plataformas / infraestructuras de Seguridad en Red**	27 de Julio (trasladada a **03 de agosto**)
6	**Ciberseguridad: Cómo son las entrañas de esta gran red mundial**	**Jueves 31 de agosto**
7	**Ciberseguridad: empleo de SOC y NOC**	**Jueves 28 de setiembre**
8	**Ciberseguridad: la importancia de saber gestionar "Logs"**	**Jueves 26 de octubre**

4. PRESENTACIÓN DEL TEMA DE HOY

Hasta ahora hemos venido desarrollado conceptos, definiciones, y procesos. En este charla presentamos una serie de despliegues que son de utilidad en el trabajo de Ciberseguridad de nuestras redes. Muchos de estos despliegues pueden ser considerados como plataformas, infraestructuras, appliances, desarrollos de software e inclusive como un conjunto de medidas de seguridad. Nuestra intención de presentarlas en este Webinar es que una vez que ya hemos comprendido los niveles más importantes de una red (Enlace, red y transporte) ahora podamos aplicar diferentes productos u ofertas del mercado para ampliar nuestro trabajo de Ciberseguridad, por esa razón es que los hemos incluido en este ciclo de charlas.

Aunque es cierto que algunos de ellos no respondan estrictamente al título de "Plataforma" o "Infraestructura", presentaremos a continuación una clasificación de las mismas intentando clasificarlas por su función principal:

- Autenticación y control de Accesos
  - Plataformas de Autenticación
  - Plataformas de Control de Accesos
  - Empleo de máquinas de salto.
  - Centralización y explotación de Logs.
- Virtualización
  - host
  - redes

- Filtrado
  - Firewalls.
  - ACLs en routers.
- Gestión y Supervisión
  - Supervisión / Monitorización / Alarmas.
  - Infraestructuras para la resolución de nombres.
  - Balanceo de carga.
  - Plataformas de sincronización de tiempo.
  - Herramientas de gestión de Routers.
  - Herramientas de gestión de Firewalls.
- Detección / Prevención / Mitigación.
  - IDSs/IPSs (Sistemas de Detección / Prevención de intrusiones).
  - Plataformas AntiDDoS

5. RESUMEN TEMAS DE LOS MESES ANTERIORES.

Hemos ido avanzando en conceptos , definiciones, ideas, opiniones de empresas líderes del mercado, analizando niveles de intrusos, predicciones para este año: Organizaciones mafiosas, análisis internacional de grandes empresas, "Resiliencia". Presentamos dos estrategias que nos ofrece la **RFC 1244**: *Proteger y Proceder - Seguir y Perseguir.* Nuestra propuesta fue, invitaros a que seáis "audaces" y preparéis vuestras infraestructuras paso a paso para enfrentar la segunda de ellas, dejando de lado el viejo concepto estático de la defensa, para poder plantear vuestra seguridad por medio del concepto militar de "**Acción Retardante**" y avanzamos sobre esta operación.

Continuamos nuestro ciclo, haciendo una analogía entre el "**combate de montaña**" y cómo podemos pensar en alturas de nuestras redes y un análisis del reglamento militar.

Quedó la reflexión sobre las alturas dominantes.

- Planos de altura (*Niveles TCP/IP*).
- Planos de Segmentación (*redes de Gestión y de Servicio*).

En la última charla nos centramos en los procesos que creemos fundamentales en nuestras infraestructuras:

- Entrada en producción
- Gestión de cambios
- Gestión de accesos
- Configuraciones e inventario
- Gestión de Backup
- Gestión de Incidencias
- Supervisión y Monitorización
- Gestión de Logs
- Gestión de actualizaciones

6. DEBATE SOBRE TAREAS PARA EL HOGAR

Antes de avanzar sobre el tema de hoy, retomemos lo que os invité a tratar durante todo este mes:

1. ¿Cómo está nuestro nivel de procedimientos de seguridad?
2. ¿Se están aplicando adecuadamente?
3. El nivel de cada uno de ellos ¿es el adecuado? (*es decir aplica al área, función o persona idónea para su cumplimiento*).
4. ¿Sobre cuál de ellos debo incrementar la atención?
5. ¿Creo necesario incluir alguno más?, ¿Cuál?
6. ¿Qué tipo de herramientas o aplicaciones puedo emplear para dar cumplimiento a estos procedimientos?

7. PLANTEO INICIAL

Dentro del universo de plataformas e infraestructuras de seguridad, que sería infinito de resumir en estas páginas, en textos anteriores y también en Internet hay varios de estos temas que son bastante conocidos o que podemos encontrar información en abundancia.

En los aspectos de Filtrado (*Firewalls y ACLs en routers*), sabemos bien que lo importante es tener un buen conocimiento de nuestras redes y hosts, en particular sobre sus sistemas operativos (y actualizaciones), su direccionamiento IP y los puertos que nos dan acceso a las aplicaciones.

Si partimos de esta base, es relativamente sencillo abrir o cerrar las reglas necesarias para permitir o negar el ingreso o salida de cada uno de ellos.

No merece la pena detenernos en esta función.

Si hablamos de:

- Gestión y Supervisión
  - Supervisión / Monitorización / Alarmas.
  - Infraestructuras para la resolución de nombres.
  - Balanceo de carga.
  - Plataformas de sincronización de tiempo.
  - Herramientas de gestión de Routers.
  - Herramientas de gestión de Firewalls.

Podríamos presentar varios fabricantes de estos productos, sistemas de ticketing, de **OSS** (*Operations Support System*), **BSS** (*Business Support System*), metodologías de empleo del protocolo **NTP** (*Network Time Protocol*) y también qué parámetros nos sirven para determinar cómo puedo repartir el tráfico para que el servicio sea más eficiente.

Otro componente de este rubro que hemos querido destacar es la **resolución de nombres, que en todo Internet se sustenta con el protocolo DNS** (*Domain Name System*), desde el punto de vista de seguridad siempre nos ha traído dolores de cabeza. La realidad es que la masa de los productos comerciales se basan en nuestro viejo y querido **BIND** (*Berkeley Internet Name Domain*) de Unix, que sabiéndolo operar adecuadamente es inmejorable.

Pero como tenemos un par de puntos sobre los que deseamos centrar la atención en estos pocos minutos, también dejaremos de lado estas infraestructuras.

8. UNOS BREVES MINUTOS

Sólo nos detendremos unos minutos a tratar el tema de:

- Detección / Prevención / Mitigación.
  - IDSs/IPSs (Sistemas de Detección / Prevención de intrusiones).
  - Plataformas AntiDDoS.

Pues creemos necesario hacer hincapié únicamente en un par de ideas fuerza:

- **IDSs/IPSs** (Sistemas de Detección / Prevención de intrusiones).

  Como punto de partida: "Cuidado" con las medidas de prevención de intrusiones.

Los IDSs, llevan años en producción. A principios de este milenio, tuve la suerte de poder hacer un trabajo de evaluación de estas nacientes tecnologías. El resultado fue un artículo muy conocido "**Nivel de inmadurez de los NIDS**". En este trabajo, se montó un laboratorio con los cuatro mayores fabricantes de IDS a nivel mundial, generamos todo tipo de tráfico, y lo llamativo de sus resultados fue que cada uno de ellos respondía de forma diferente; algunos detectaban ciertos patrones y protocolos, otros no, los umbrales eran muy diferentes y los falsos positivos y negativos aparecían más que los datos ciertos.

Hoy, quince años después, el panorama no ha cambiado mucho si intentamos emplear estas herramientas sin un adecuado ajuste o personalización y actualización constante. Los IDSs siguen siendo herramientas que necesitan mucho trabajo y recursos dedicados. Los considero **fundamentales** e **imprescindibles** en toda gran infraestructura de red, pero "**sí, y solo sí**" le dedicamos los recursos suficientes, sino no merece la pena gastar tiempo ni dinero, pues no sirven para nada.

Es decir, en primer lugar, los IDSs son buenísimos si los tomamos en serio (*es decir con dedicación*), por lo tanto, si pensamos en "prevenir" intrusiones el tiempo de personalización es aún mayor, sino estaremos gastando del doble de tiempo y dinero y, a su vez, incrementando el riesgo de nuestra empresa, pues como siempre me gusta afirmar, por mi parte "apuesto por el humano". Es el ejemplo que pongo siempre del prisionero que mira a su cárcel durante horas, días, meses, años… hasta que encuentra la vía de escape, la cual, como no existe fortaleza invulnerable, tarde o temprano la hallará.

Con los IPSs es algo similar, si los millones de intrusos comienzan a analizar las respuestas de nuestras redes a sus actividades, poco a poco podrán ver de qué forma "automática" se cierran puertos, conexiones, accesos, etc… y a través de los mismos, ya hemos conocido grandes ataques de negación de servicio que han logrado aislar redes en virtud de la reacción de los IPSs.

Para cerrar este tema, no dejo de insistir en que tenemos a nuestro alcance una herramienta fabulosa como es "**Snort**" (https://www.snort.org) que invito a que la instaléis y pongáis a prueba, seguramente nos enseñará muchísimo y si la ponemos en producción (*y le dedicamos los recursos suficientes*) tendremos un pilar fundamental para nuestra seguridad.

- Plataformas **AntiDDoS**.

  Para esta plataforma pondremos por ejemplo la que ofrece **Arbor**

Networks y el paquete comprende dos herramientas diferentes:

- **Peakflow**
- **TMS**: Threat Management System

Algunas empresas, sólo poseen PeakFlow como una herramienta de supervisión y monitorización de tráfico, es cierto que desde la misma manualmente se pueden configurar medidas para minimizar ciertos patrones de tráfico, pero el concepto de "Mitigación" efectivo pasa por medio de TMS. Su lógica la podemos describir mejor a través de las imágenes que presentaremos más abajo.

Para entender bien el concepto, debemos considerar que un ataque bien lanzado de DDoS, en general, busca dejar inactivo un servicio concreto, por ejemplo una página Web, un servidor de correo, una aplicación, etc. Por lo tanto si se bloquea todo el tráfico hacia el mismo, lo que estamos logrando es exactamente el ejemplo que acabamos de presentar con los IPSs. Alguien que se dedique a analizar en qué momento se bloquea este tráfico, puede lograr dejar fuera de servicio intencionadamente al mismo. Por lo tanto, no es una medida eficiente el bloqueo de todo el tráfico. Tampoco es sencillo lograr la "granularidad" suficiente como para que en "tiempo real" podamos analizar "en línea" la totalidad del tráfico que pasa por un gran router. Hemos remarcado con comillas estas tres palabras, pues estamos hablando de un tráfico de varios cientos de gigas o hasta tera bits por segundo, este inmenso caudal no es sencillo de procesar, de hecho es uno de los grandes problemas de colocar Firewalls en las interfaces de acceso a Internet por parte de los **ISP** (Internet Service Provider) pues al día de hoy, siguen sin existir FWs en capacidad de desarmar este altísimo volumen de tramas y procesarlas, sin causar una baja de rendimiento considerable.

Para dar solución seria a este problema el protocolo BGP introdujo el concepto de "**BGP flow spec**", que si bien no desarrollaremos en estas líneas, al menos presentaremos algunas breves ideas.

La BGP flow Spec es una nueva herramienta que puede utilizarse para ayudar en la mitigación de DDOS de una manera dinámica, aprovechando BGP, permitiendo una mayor granularidad para construir instrucciones de ruteo que coincidan con un flujo particular considerando: origen, destino y parámetros de nivel cuatro, como así también especificaciones de paquetes como longitud, fragmento, etc.

A través del empleo de BGP Flow Spec se pueden definir acciones concretas en los rotuers de frontera para:

- Descartar el tráfico
- Inyectarlo en un **vrf** (virtual routing forwarding) diferente para

su análisis.

- Permitirlo, pero de acuerdo a una política o tasa de tráfico definida y específica.

Para resumirlo y comprender estos conceptos, presentamos a continuación tres imágenes, que como bien se sabe, valdrán más que miles de palabras:

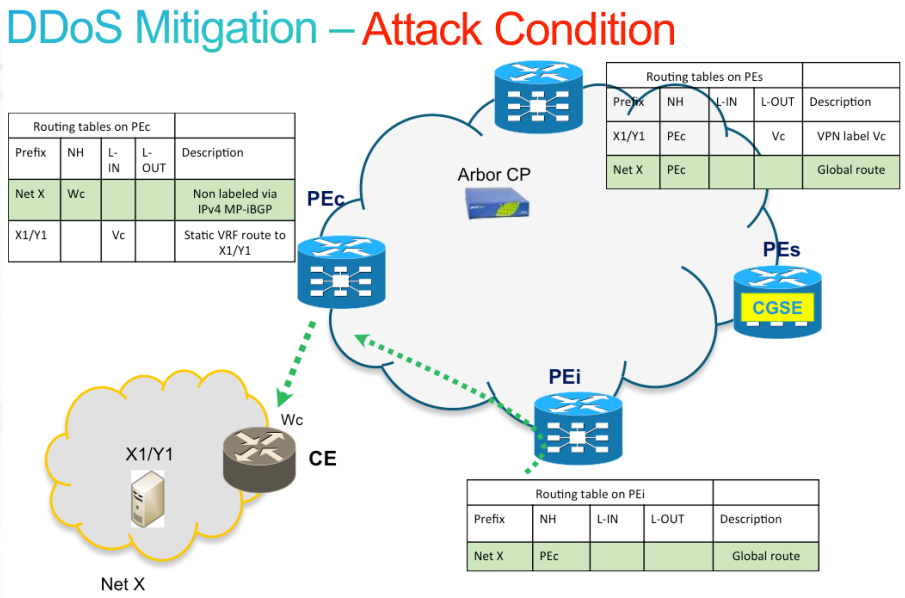


Imagen 1 (tráfico normal – tablas de rutas BGP iniciales)

* **CGSE**:Cisco Carrier Grade Services Engine

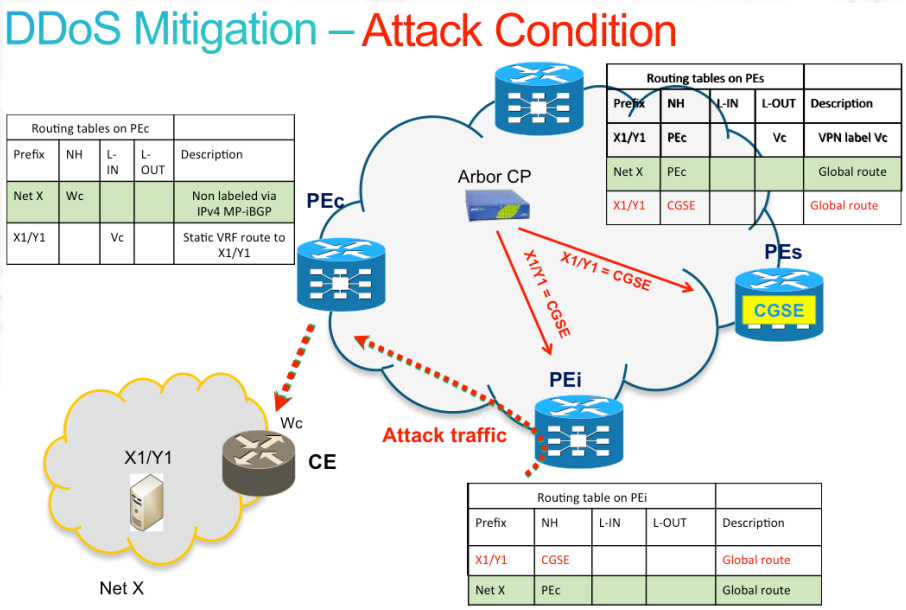


Imagen 2 (ataque – inserción de nuevas rutas BGP)

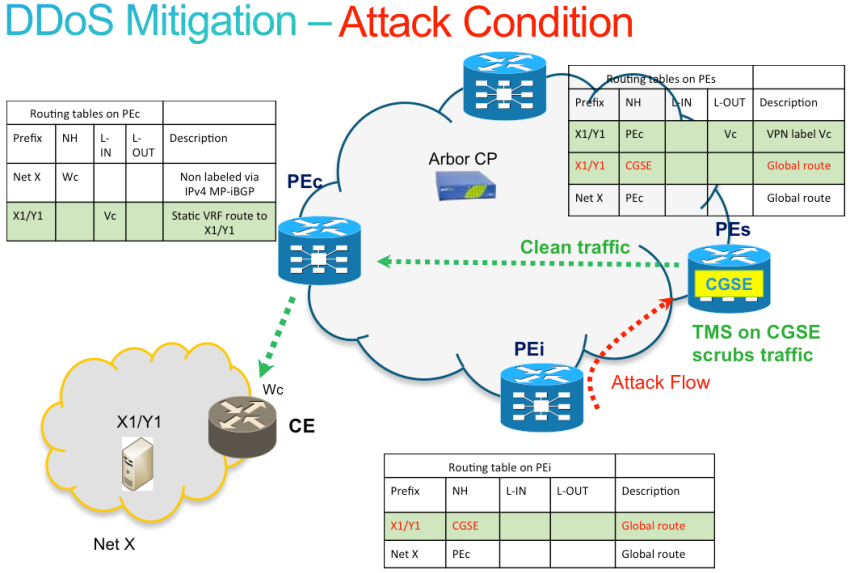


*Imagen 3 (cambio rutas BGP sólo para **X1/Y1** – flujo limpio)*

Hemos intentado resumir este importante concepto en tres imágenes que representan una metodología que creemos, a día de hoy, es la más importante que se puede implementar para hacer frente a ataques de DDoS. Existen otro tipo de soluciones, pero a nuestro juicio, el empleo de Flow Spec, es tal vez la única que permite hacer frente a este problema en gran escala, sin causar afección al resto de los servicios (ni siquiera al atacado), pero desde diferentes direcciones y patrones que los del origen del ataque.

Invitamos a que profundicéis más sobre este tema, pues es uno de los más grandes que se están presentando a nivel ciberseguridad.

9. TEMA BASE DE HOY

Habiendo desarrollado brevemente los conceptos anteriores, queremos centrarnos un poco más en los temas que siguen, para hacer referencia a algunos estándares y normas que seguramente nos serán de interés en el día de hoy.

Los temas que nos quedan son los siguientes:

- Autenticación y control de Accesos
  - Plataformas de Autenticación
  - Plataformas de Control de Accesos

- Empleo de máquinas de salto.
- Centralización y explotación de Logs.

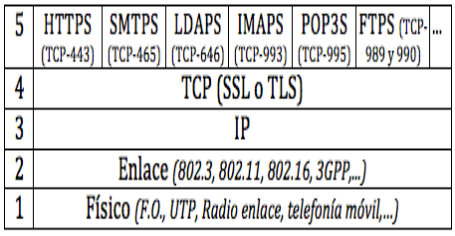
- Virtualización
  - host
  - redes

Teniendo en cuenta que la "movilidad" hoy en día es uno de los aspectos clave de las infraestructuras de red, se hace necesario poder acceder a nuestros servicios y aplicativos desde diferentes ubicaciones y zonas geográficas. Para poder ofrecer esta posibilidad sin dejar de lado la seguridad que nos ofrecen nuestras LANs (Local Área Networks)

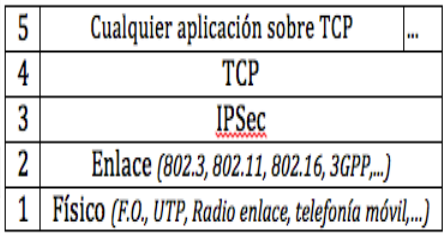
En referencia a los mismos, a continuación vamos a presentar, en primer lugar los tipos de VPNs:

a. VPNs Basadas en **SSL**
b. VPNs basadas en **IPSec**
c. VPNs basadas en **SSH**

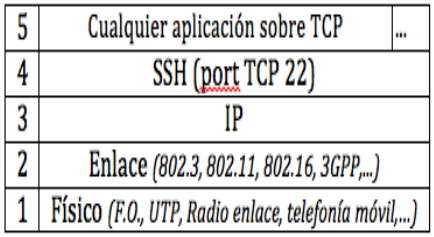
Si los analizamos como modelo de capas TCP/IP, los podemos representar de la siguiente forma:



VPNs Basadas en SSL



VPNs basadas en IPSec



VPNs basadas en SSH

a. VPNs Basadas en **SSL** (*Secure Sockets Layer*)

El protocolo SSL nace como propietario de la empresa Netsacpe y luego se estandariza como **TLS** (*Transport Layer Security*) que se identifica como SSL v3.1, aunque entre ambos tienen algunas diferencias):

Las características de cualquiera de ellos son:

- Protege una sesión entre cliente y servidor.
- Requiere protocolo de transporte orientado a la conexión (*típicamente TCP*)
- Autenticación
  - del servidor hacia el cliente

– opcionalmente, del cliente hacia el servidor. (mediante certificados)

Una comunicación a través de SSL implica tres fases:

- Establecimiento de la conexión y negociación de los algoritmos criptográficos que van a usarse en la comunicación.
- Intercambio de claves.
- Cifrado simétrico del tráfico.

Una opción para poner a prueba esta metodología es **OpenVPN**, que presenta las siguientes características:

- Busca implementar VPNs de forma mas sencilla que IPSEC.
- No requiere de la complejidad del protocolo **IKE** (*Internet Key Exchange*).
- Puede trabajar en modo bridging o en modo routing.
- Utiliza la implementación de **openssl**.
- www.openvpn.net (*Ver también: www.openssl.org*)

NOTA: Una recomendación adicional es hacer todas las pruebas que estén a nuestro alcance con **OpenSSL** (generar claves, firmarlas, generar certificados, instalar una Autoridad de certificación, una de revocación, probar el cifrado con certificados, generar conexiones SSH con el empleo de certificados, emplear los certificados para firma electrónica, etc.)

b. VPNs basadas en **IPSec**

Sobre el protocolo IPSec no entraremos en mayores detalles pues lo hemos desarrollado al completo en el libro "Seguridad por Niveles", sólo mencionamos a continuación los requerimientos que hacen falta para implementar estas VPNs:

Se basan en el empleo de los protocolos: AH (*Authentication Header*), ESP (*Encapsulation Security Payload*) e IKE (*Internet Key Exchange*).

Para el empleo de **IKE** puede hacerse por medio de:

- *Preshared-keys*
- *Pares de claves (firma digital)*
- *Certificados Digitales.*

AH: ofrece verificación de la fuente, integridad de paquetes y anti-replay, **ESP** ofrece Confidencialidad.

c. VPNs basadas en **SSH** *(Secure SHell)*

Esta tecnología se basa en empleo de túneles SSH y la redirección de puertos (*Port forwarding*) que ofrece este protocolo. Este protocolo es nativo en todos los sistemas Unix/Linux, por lo que no requiere ningún tipo de configuración previa y recursos adicionales. Con ProxiSocks se pueden emplear túneles dinámicos que nos permiten acceder a diferentes direcciones IP.

Para profundizar en estos túneles, puede verse el Webinar "**SSH Forwarding**" en la siguiente URL:

https://www.youtube.com/watch?v=dYK1blKK3xc&t=82s

También pueden consultarse una serie de ejercicios que están en el punto 9.3. del libro "**Seguridad en Redes**".

El empleo de este tipo de VPNs es de suma utilidad en la implantación de "máquinas de salto", pues es una solución muy sencilla y práctica y eficiente de crear accesos seguros a redes o segmentos de red sobre los que se desea tener un control más estricto.

Por último debemos mencionar que dentro de nuestras propias LANs, también podemos virtualizar redes. Esto ya lo hemos comentado en charlas previas, pero sobre la base de la familia de protocolos IEEE-802.x, existe uno en particular que es 802.1Q, que justamente introduce el concepto de VLAN (Virtual LAN) y que lo podemos emplear para diferenciar el tráfico de las áreas de nuestra LAN, creando para cada una de ellas su propia VLAN. Esta configuración se realiza en cada uno de los switchs y en grandes líneas lo que se realiza es un encabezado adicional en el campo "Ethertype" del protocolo Ethernet que, cuando contiene el valor **81-00** identifica que se trata de una VLAN específica y en ese nuevo encabezado se incluye toda la información de la misma.

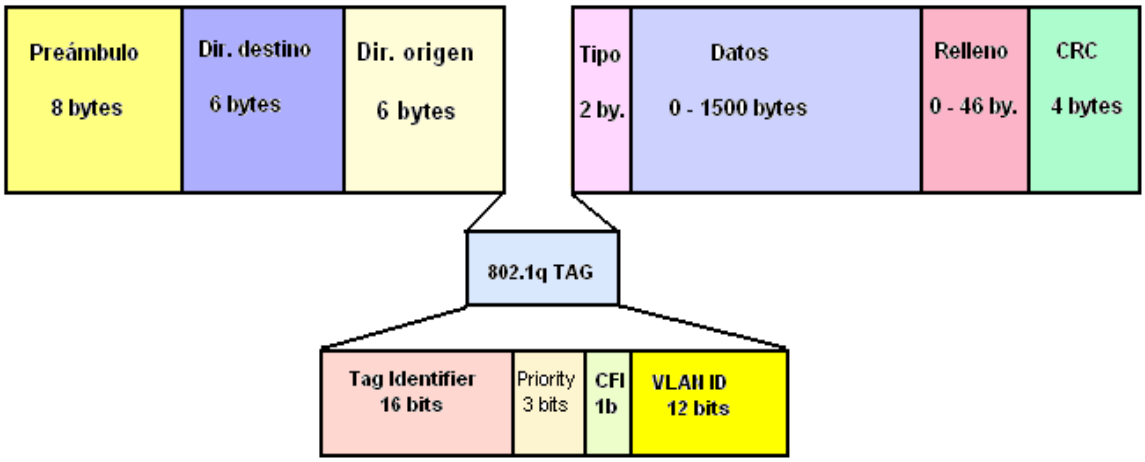


Imagen 4 (Formato de una trama 802.1q)

Todo el detalle sobre este protocolo, podemos encontrarlo en el punto 4.2.3. 802.1Q (Virtual LAN), del libro "**Seguridad en Redes**".

Un punto adicional que dejo como tarea de estudio (y merece la pena comenzar a evaluar) es el protocolo **802.1ae** Media Access Control (MAC) Security, publicado en 2006 y cuya última enmienda es del 2013: **802.1AEbw**)

Conocido como **MACSec** ofrece confidencialidad, integridad y autenticación de origen. Introduce nuevos campos a la trama Ethernet (SecTag, ICV)

Asociaciones seguras de conectividad (grupos de estaciones conectadas por medio de canales seguros con su propia llave SAK).

Al igual que 802.1Q, en este protocolo también se agrega un nuevo encabezado a la trama Ethernet, cuando el campo Ethertype posee el valor Ethertype: **88-E5**. A continuación presentamos la imagen que ofrece en el contenido de la norma:

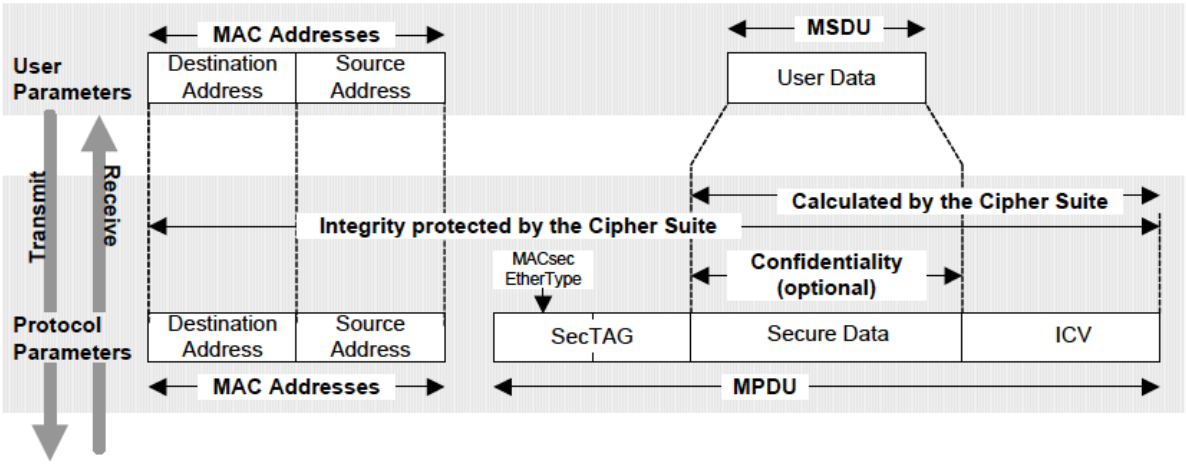


Figure 8-1—MACsec

Imagen 5 (Formato de una trama 802.1ae)

Toda esta información adicional es de suma importancia, ahora que ya estamos comenzando a comprender el tema de Ciberseguridad en su conjunto, pues a medida que vamos incrementando las medidas es cuando nuestras infraestructuras se hacen más sólidas. Por ello como reflexión final, presentamos la secuencia, que en esta caso ofrece Cisco, en el que podemos ver cómo se van integrando los diferentes protocolos de capa dos (enlace) para ofrecer un paquete robusto de autenticación y control de acceso basado en esta serie de protocolos de la familia IEEE-802.x que venimos desarrollando desde hace tiempo en nuestros textos.

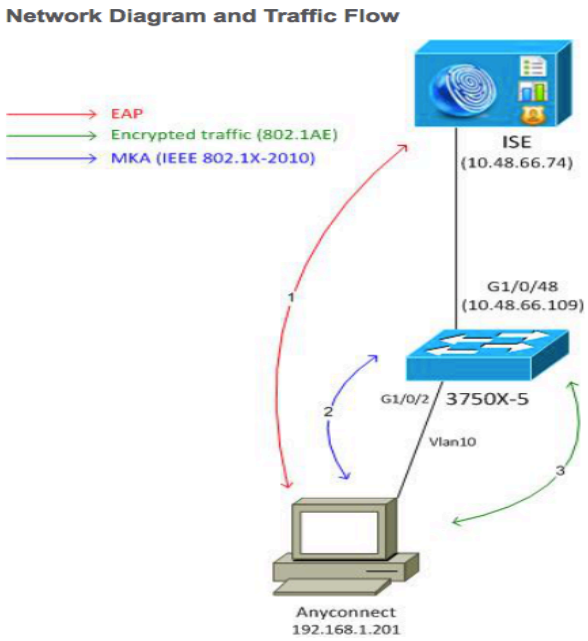


Imagen 6 (Combinación de 802.1x con 802.1ae)

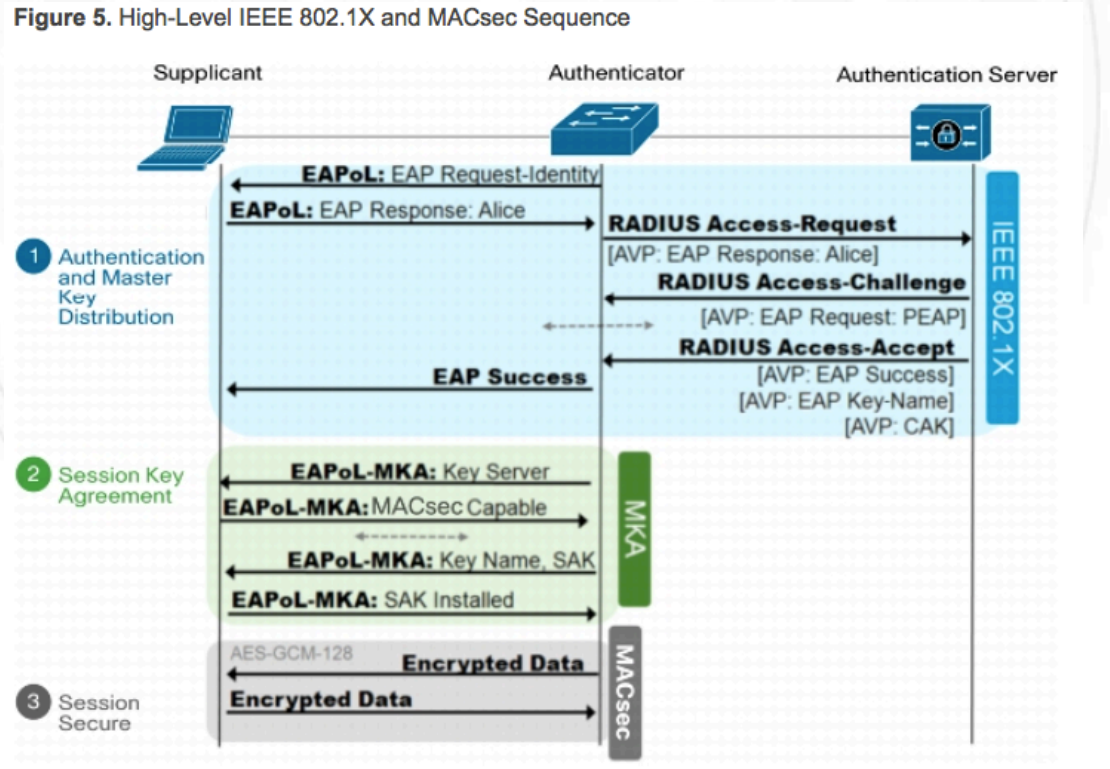


Imagen 6 (Secuencia de 802.1x con 802.1ae)

Ambas figuras están tomadas de:

http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-services/deploy_guide_c17-663760.html

10. TAREAS PARA EL HOGAR (deberes).

Una vez más en esta charla os propongo llevarnos a casa algunas actividades o líneas de reflexión para que comencemos el mes que viene con orto breve debate sobre los mismos.

Os dejo las siguientes "**tareas para el hogar"**:

1. ¿Profundicé con SNORT?, ¿Como funciona su motor?, ¿pude implementas local rules?
2. ¿Necesito implantar sistemas AntiDDoS.
3. ¿Hice pruebas de IPS con respuestas automáticas?
4. Realizar pruebas de túneles SSH y el empleo de redirección de puertos.
5. ¿Pude instalar una máquina de salto?
6. ¿Qué opinión me merece el empleo de IEEE-802.1ae?

Nos vemos dentro de un mes con las tareas hechas (*no quiero suspender a nadie….*). Muchas gracias por todas vuestra atención e interés.

Un afectuoso saludo.

Madrid, 03 de agosto de 2017.

Alejandro Corletti Estrada

acorletti@darFe.es