
GAMAKER

Due to the lapse in appropriations, Department of Justice websites will not be regularly updated. Please refer to the Department of Justice's contingency plan for more information.

FBI

MOST WANTED

Ten Most Wanted | Fugitives | Terrorism | Kidnappings/Missing Persons | Seeking Info | Parental Kidnappings | Bank Robbers | ECAP | VICAP
Crimes Against Children | Murder | Additional Violent Crimes | Cyber | White Collar Crimes | Counterintelligence | CEI | Human Trafficking

Cyber's Most Wanted

Select the images of suspects to display more information.

Search for: Search for... Filter by: Year Filter

Sort by: Newest

Results: 63 Items


APT 10 GROUP


ZHANG SHILONG


ZHU HUA


SAMSAM SUBJECTS


GRU HACKING TO UNDERMINE ANTI-DOPING EFFORTS


ALEKSEI SERGEYEVICH MORENETS


EVGENII MIKHAYLOVICH SEREBRIAKOV


ALEXEY VALEREVICH MININ


OLEG MIKHAYLOVICH SOTNIKOV


DMITRIY SERGEYEVICH BADIN


ARTEM ANDREYEVICH MALYSHEV

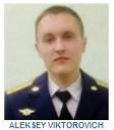

IVAN SERGEYEVICH YERMAKOV


RUSSIAN INTERFERENCE IN 2016 U.S. ELECTIONS


BORIS ALEKSEYEVICH ANTONOV


ANATOLIY SERGEYEVICH KOVALEV


NIKOLAY YURYEVICH KOZACHEK


ALEKSEY VIKTOROVICH LUKASHEV


SERGEY ALEKSANDROVICH MORGACHEV


ALEKSANDR VLADIMIROVICH OSADCHUK


ALEKSEY ALEKSANDROVICH POTEMKIN

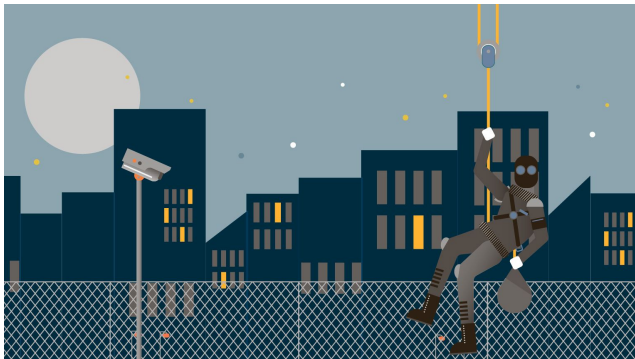

PAVEL VYACHESLAVOVICH YERSHOV


PARK JIN HYOK


IRANIAN MABNA HACKERS


GHOLAMREZA RAFATNEJAD


EHSAN MOHAMMADI



Ciberseguridad en el mundo actual:

https://www.fbi.gov/wanted/cyber

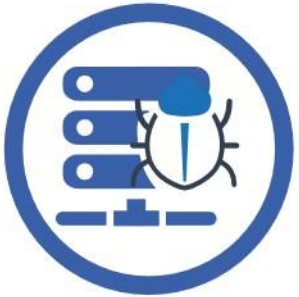

HERRAMIENTAS DE LA CIBERGUERRA
Diplomacia y acciones de inteligencia tradicional
Actos subversivos y de sabotaje
Influencia política y económica
Instrumentalización del crimen organizado
Operaciones psicológicas
Propaganda y desinformación
Ciberataques

OBTENCIÓN DE BENEFICIOS ECONÓMICOS

En 2017 también se llevaron a cabo ataques con el objetivo de obtener rendimiento económico. Para ello, se emplearon distintos métodos.

FRAUDE AL CEO

Los delincuentes intentan que el departamento financiero de una empresa realice transacciones económicas utilizando nombres de dominio similares al de la organización en cuestión.



MALWARE COBALT[2]

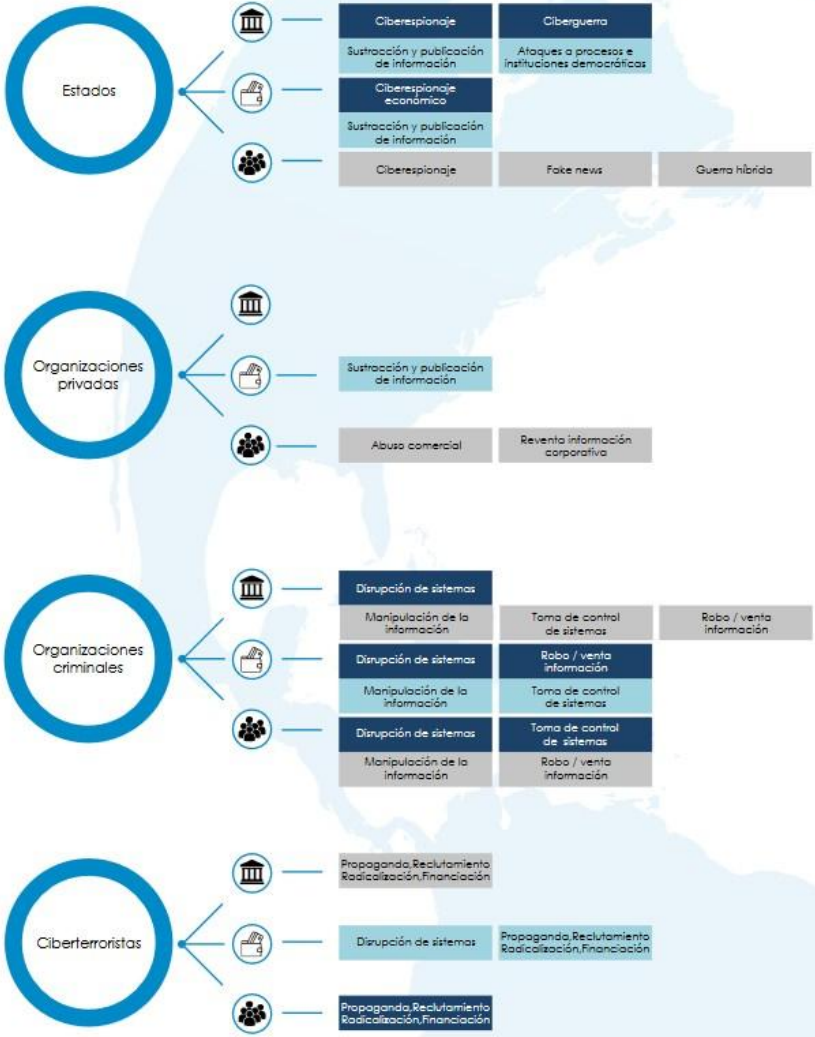
Envío de correos electrónicos a empleados de bancos con un archivo adjunto malicioso que permitía tener acceso a la red bancaria interna e infectar los servidores que controlan los cajeros automáticos.

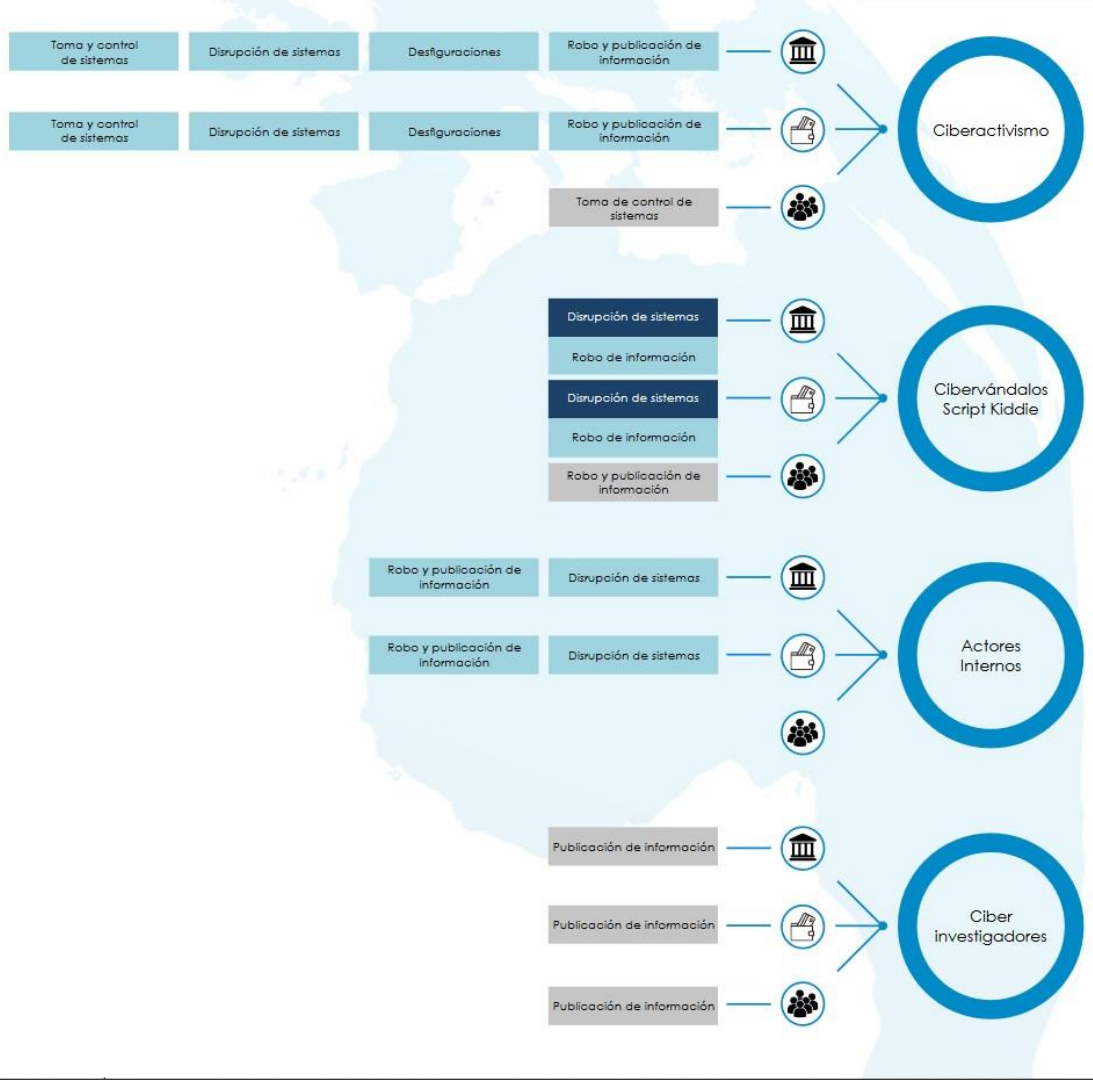
CIBERPIRATERÍA

En Italia, la policía detuvo en 2017 a dos individuos sospechosos de ciberpiratería, que habrían realizado inversiones basándose en información robada.

ORGANIZACIONES PRIVADAS

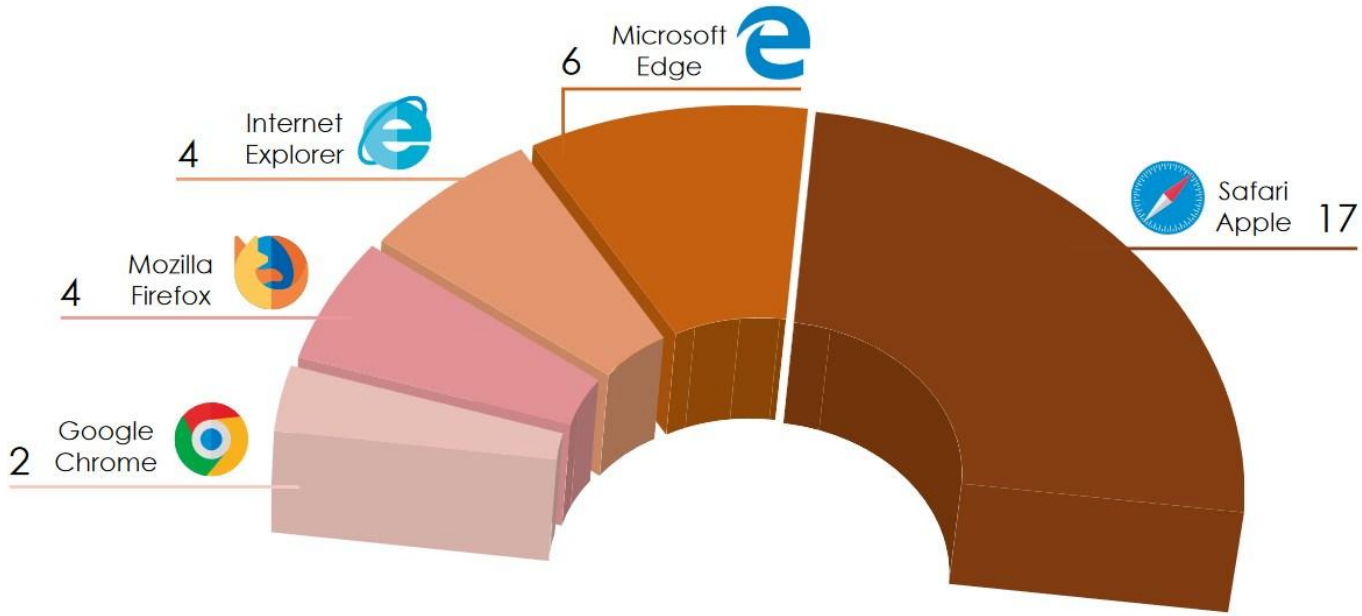
Como se muestra en el siguiente gráfico, las características y, correlativamente, los motivos de los ciberataques desarrollados por organizaciones privadas pueden ser de distintos tipos.

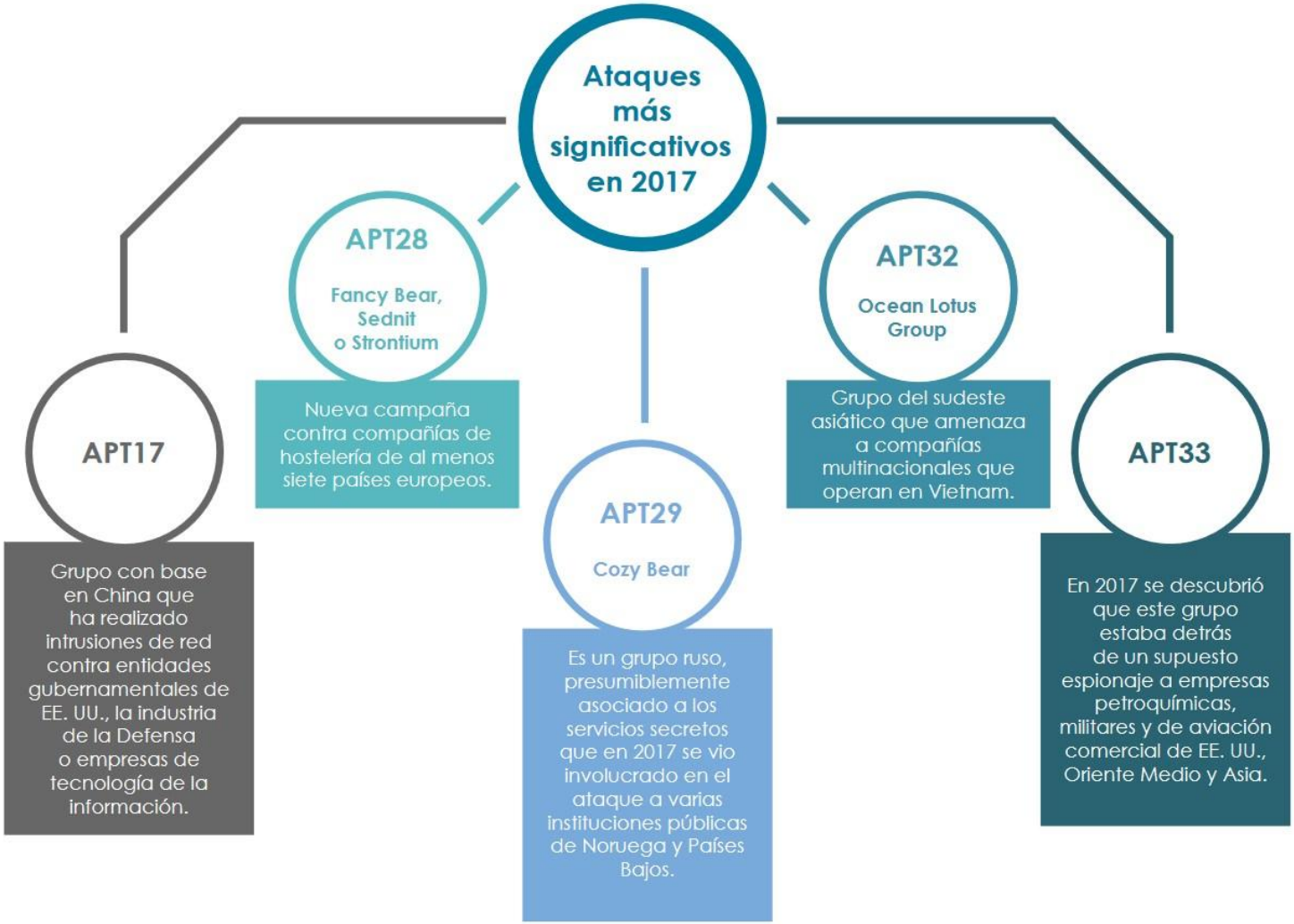

Estados
Ciberespionaje
Sustracción y publicación de información
Ciberguerra
Ataques a procesos e instituciones democráticas
Ciberespionaje económico
Sustracción y publicación de información
Ciberespionaje
Fake news
Guerra híbrida
Organizaciones privadas
Sustracción y publicación de información
Abuso comercial
Reventa información corporativa
Organizaciones criminales
Disrupción de sistemas
Manipulación de la información
Toma de control de sistemas
Robo / venta información
Disrupción de sistemas
Manipulación de la información
Robo / venta información
Toma de control de sistemas
Disrupción de sistemas
Manipulación de la información
Toma de control de sistemas
Robo / venta información
Ciberterroristas
Propaganda,Reclutamiento Radicalización,Financiación
Disrupción de sistemas
Propaganda,Reclutamiento Radicalización,Financiación
Propaganda,Reclutamiento Radicalización,Financiación


Toma y control de sistemas
Disrupción de sistemas
Desfiguraciones
Robo y publicación de información
Toma y control de sistemas
Disrupción de sistemas
Desfiguraciones
Robo y publicación de información
Toma de control de sistemas
Ciberactivismo
Disrupción de sistemas
Robo de información
Disrupción de sistemas
Robo de información
Robo y publicación de información
Cibervándalos Script Kiddie
Robo y publicación de información
Disrupción de sistemas
Robo y publicación de información
Disrupción de sistemas
Actores Internos
Publicación de información
Publicación de información
Publicación de información
Ciber investigadores

NAVEGADORES E INFRAESTRUCTURAS WEB

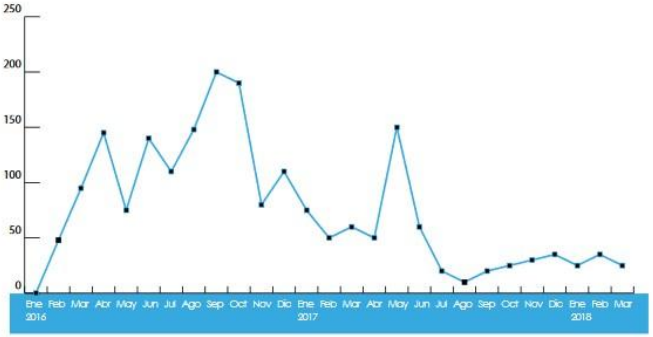
En un reciente informe del Google *Proyect Zero*, se muestra que todos los navegadores de escritorio conocidos tienen **vulnerabilidades de seguridad** asociadas.




Ataques más significativos en 2017
APT17
Grupo con base en China que ha realizado intrusiones de red contra entidades gubernamentales de EE. UU., la industria de la Defensa o empresas de tecnología de la información.
APT28
Fancy Bear, Sednit o Strontium
Nueva campaña contra compañías de hostelería de al menos siete países europeos.
APT29
Cozy Bear
Es un grupo ruso, presumiblemente asociado a los servicios secretos que en 2017 se vio involucrado en el ataque a varias instituciones públicas de Noruega y Países Bajos.
APT32
Ocean Lotus Group
Grupo del sudeste asiático que amenaza a compañías multinacionales que operan en Vietnam.
APT33
En 2017 se descubrió que este grupo estaba detrás de un supuesto espionaje a empresas petroquímicas, militares y de aviación comercial de EE. UU., Oriente Medio y Asia.

RANSOMWARE

A pesar de que el ransomware ha proseguido su sofisticación en los últimos años, se ha apreciado un **descenso en el número de ataques.**



En el siguiente diagrama se muestran algunas de **las modalidades de infección mediante ransomware** empleadas en 2017.

Remote Desktop Protocol

Nueva forma de infectar con ransomware los equipos. Permite el acceso al sistema, que posteriormente será infectado.

Dispositivos móviles

El volumen de ransomware móvil creció más de tres veces durante los primeros meses de 2017, detectándose 218.625 muestras en el primer trimestre.

Correo electrónico

Es el medio más utilizado para distribuir ransomware al no existir un método adecuado que garantice su protección.

Exploits[12]

Empleados para infectar los servidores. Ejemplo de ello es lo sucedido en bases de datos mal protegidas, como los ataques a Mongo DB.

Televisiones

Se ha apreciado en 2017 casos de ransomware en la infección de televisores convencionales, resultado de la sofisticación de estos ataques.

Medjack

Secuestro de dispositivos médicos, resultado de la integración de las TIC tradicionales y la tecnología sanitaria.

Durante 2017 se han detectado evidencias de que **el sector sanitario es el más frecuentemente atacado por esta amenaza.**

PHISHING Y SPAMMING

En 2017, **las campañas de phishing[13] aumentaron tanto en volumen como en sofisticación.** Este método constituye el vector de infección más exitoso, tanto en ataques dirigidos (ciberespionaje) como innominados (ransomware). En la actualidad, los ataques buscan objetivos concretos, convirtiéndose así en ataques más específicos.

Spear phishing	Método adaptado al objetivo que se emplea para atacar a una entidad concreta. Es difícil determinar su naturaleza dañina puesto que generalmente utiliza una recopilación de todo tipo de información pública.
Nuevo método de ataque que se contrata a cibercriminales y que permite obtener contraseñas de las víctimas simulando páginas web de servicio al usuario como Gmail, Facebook o Yahoo.	**Phishing as a service**
BEC / Whalling[14]	Ataques de spear-phishing contra ejecutivos de alto nivel, generalmente con el objetivo de sustraer dinero de sus organizaciones o de sus víctimas. También puede ser empleado para realizar ciberespionaje.

El spam[15], por su parte, ha ganado en calidad, aunque el número de ataques a través de este tipo de mensajes parece haber descendido. No obstante, sigue siendo el principal medio para la **entrega innominada de código dañino** a través de archivos adjuntos y URL[16] dañinas.

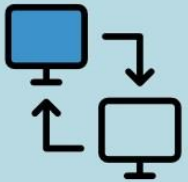
ATAQUES DE DENEGACIÓN DE SERVICIOS (DDoS)

Según el estudio realizado por Kaspersky, **un 33% de las organizaciones se enfrentaron en 2017 a un ataque DDoS,** un 16% de empresas más que en 2016. Estos datos evidencian que estos ataques, además de haber aumentado con respecto al año anterior, también han incrementado su tamaño (*a finales de 2017, la botnet Mirai fue protagonista del mayor ataque DDoS de la historia por ancho de banda, más de 1 Tbps*).

TIPOLOGÍA DE LOS ATAQUES

DISPOSITIVOS IOT

El número de dispositivos IoT vulnerables ha contribuido al aumento del tamaño de los ataques DDoS.



DDoS AS A SERVICE

En desarrollo debido a la reducción del coste de las herramientas precisas para perpetrarlos.

DDoS BASADOS EN DNS

En aumento en 2017, tras las acciones contra el servicio DNS[18] del la empresa DYN.

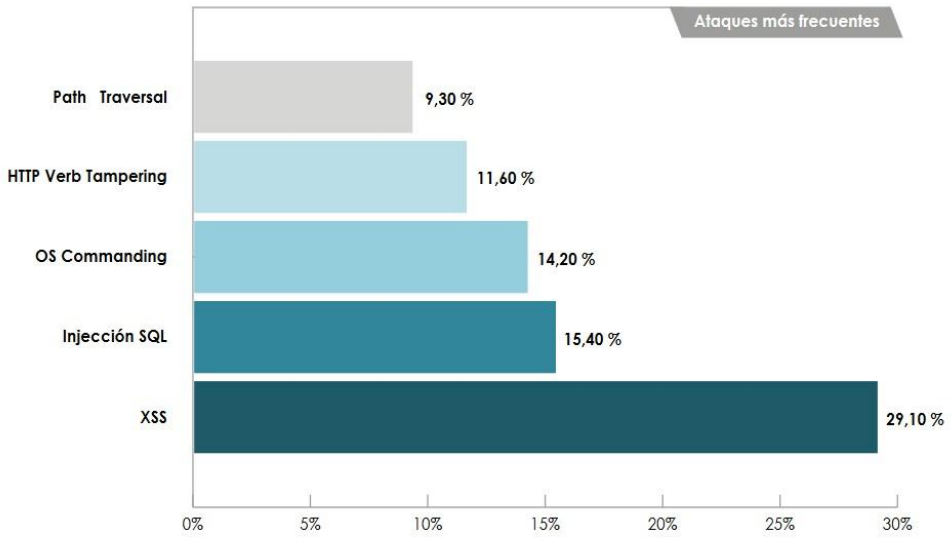
EXTORSIÓN

Acciones de extorsión bajo amenaza de ataques DDoS o de interrupción de servicios en línea.

ATAQUES WEB

El 40% de los ataques web están dirigidos a la **obtención de información,** siendo las aplicaciones web patrocinadas por el sector público y el financiero las que mayor número de ataques han reportado en 2017. Los vectores de agresión más significativos durante el 2017 fueron, según la empresa Positive Technologies, el Cross Site Scripting (XSS) y la inyección SQL.

Asimismo, los ataques basados en web, que hacen uso de sus sistemas y servicios habilitados, han sido en 2017 una de las amenazas más importantes y que perdurará en los próximos años.



Datos del 4º trimestre de 2017
Fuente: Positive Technologies

MENSAJES SMS

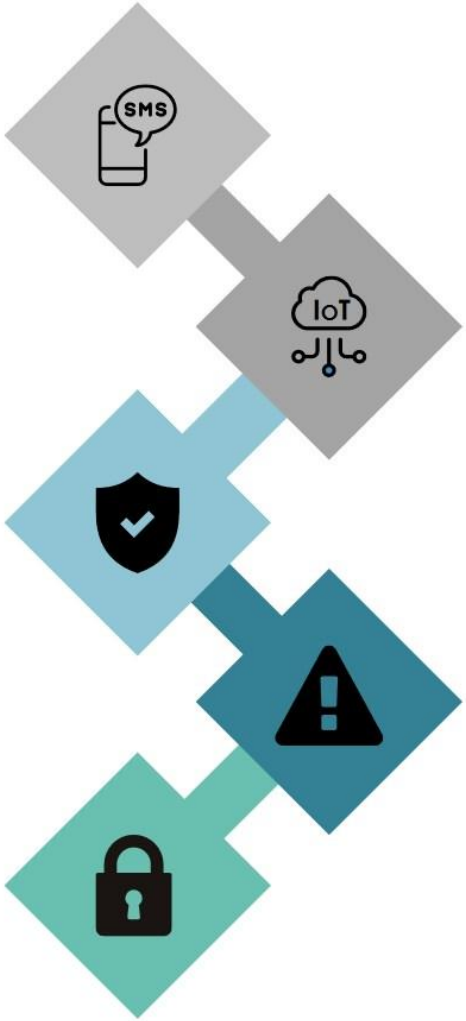
Los dispositivos Android e iOS son susceptibles de sufrir ciberataques que permiten acceder a los mensajes SMS recibidos a través del ordenador del destinatario. Por tanto, el empleo de SMS representa una amenaza para la autenticación de dos factores.

SEGURIDAD DE LOS PRODUCTOS

El CCN publicó en 2017 un Catálogo de Productos de Seguridad TIC que recoge en un listado aquellos productos que cuentan con las certificaciones indicadas para ser empleados en sistemas que demanden altos niveles de seguridad.

LA NECESIDAD DEL CIFRADO

Estados europeos, como los Países Bajos, han hecho obligatorio el uso de HTTPS en los sitios web gubernamentales. Además, esta necesidad se ha extendido a las aplicaciones de mensajería instantánea, como Telegram o WhatsApp, que ya emplean el cifrado de extremo a extremo.



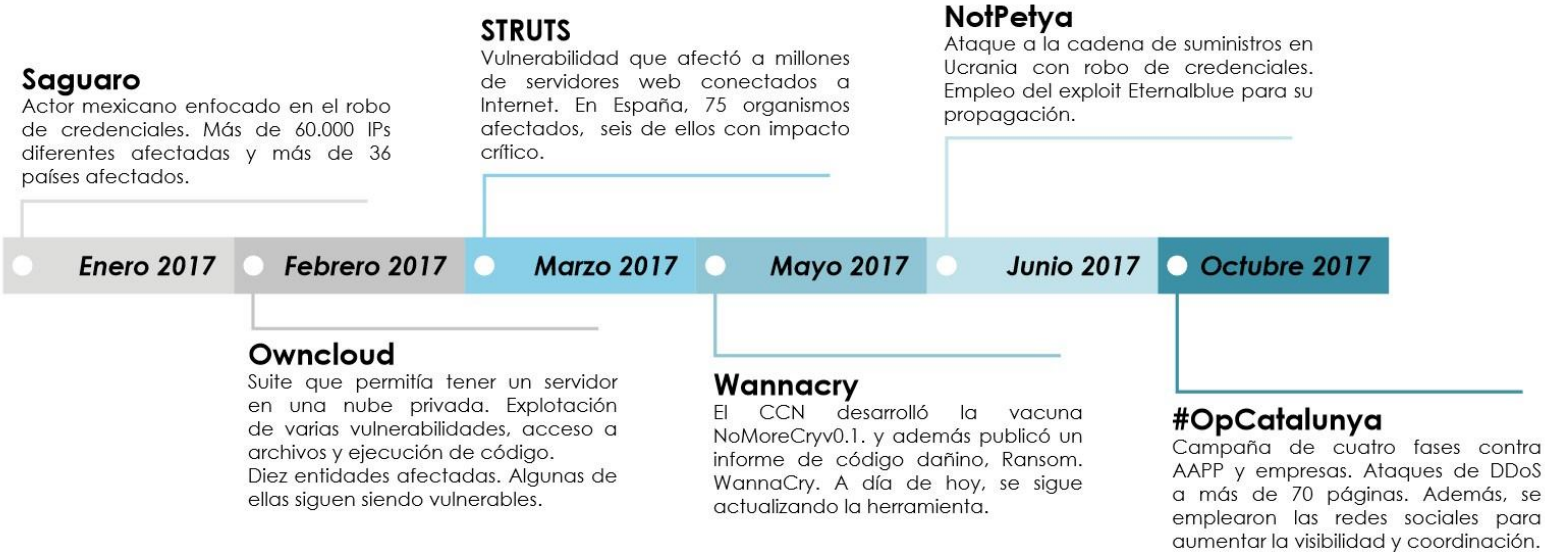
THE INTERNET OF THINGS

Todavía no hay una solución clara para los efectos secundarios no deseados de Internet of Things. La falta de sostenibilidad TIC seguirá siendo un problema si el sector no puede regularse a sí mismo.

VULNERABILIDADES ESENCIALES

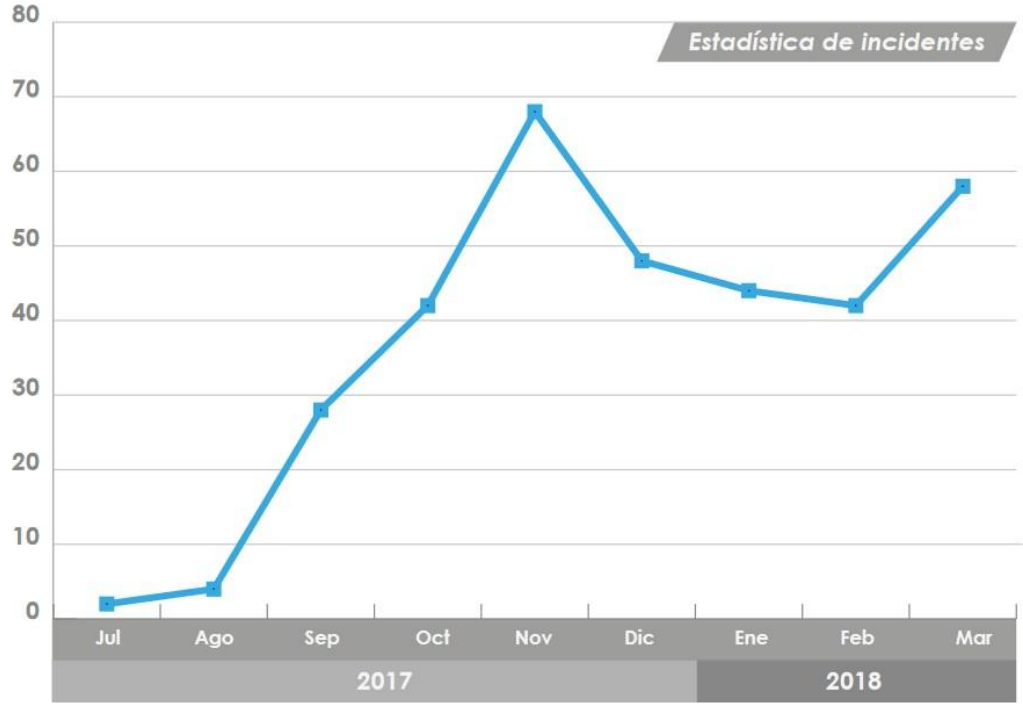
En 2017 se han publicado diferentes estudios referidos a la explotación de vulnerabilidades ligadas al software, como *Dedup Est Machina*, que explota la duplicación de memoria para tomar el control de un navegador.

RESPUESTA A CIBERATAQUES



CRIPTOMINING

Se prevé que este proceso de generación de criptomonedas continúe creciendo a lo largo de 2018, debido a que cada vez más **familias de malware** incluyen funcionalidades de minería en su arsenal de ataque. Asimismo, la tendencia actual apunta también al **empleo de los navegadores** para el minado de monedas, siendo **JavaScript** la tecnología más usada.




Count
1 – 2,218.6
2,218.6 – 4,436.2
4,436.2 – 6,653.8
6,653.8 – 8,871.4
8,871.4 – 11,089

Software Meant to Fight Crime Is Used to Spy on Dissidents

Thor Swift for The New York Times

Morgan Marquis-Boire, left, and Bill Marczak have been looking at the use of computer espionage software by governments.

The 'Million Dollar Dissident' Is a Magnet for Government Spyware

Everything We Know About NSO Group: The Professional Spies Who Hacked iPhones With A Single Text

Thomas Fox-Brewster, FORBES STAFF

I cover crime, privacy and security in digital and physical forms. FULL BIO

Omri Lavie, co-founder of NSO Group, which has just been caught exploiting iPhones with its Pegasus malware. Image from Lavie's Google Plus account.

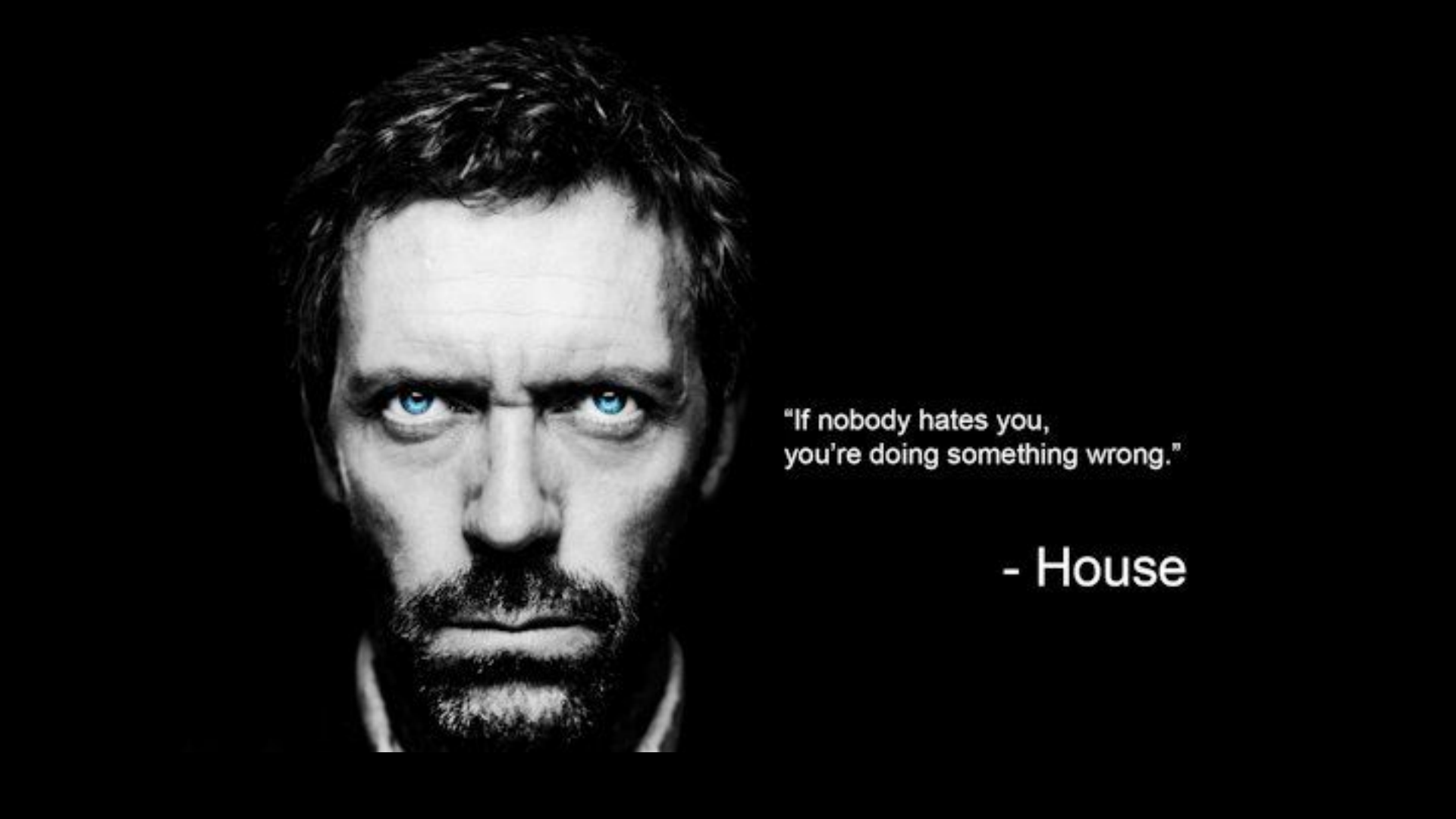
NSO's mission is to help make the world a safer place, by providing authorized governments with technology that helps them combat terror and crime.

The company sells only to authorized governmental agencies, and fully complies with strict export control laws and regulations. Moreover, the company does NOT operate any of its systems; it is strictly a technology company.

The agreements signed with the company's customers require that the company's products only be used in a lawful manner. Specifically, the products may only be used for the prevention and investigation of crimes.

The company has no knowledge of and cannot confirm the specific cases mentioned in your inquiry.


¿Y ese es bueno o es malo?
UH, BUENO, BUENO.
Pues tiene aspecto de malo.
VAYA, PUES ES DE LOS BUENOS.
Dibuja más chicos buenos.


"If nobody hates you,
you're doing something wrong."
- House


"Si conoces a los demás y te conoces a ti mismo, ni en cien batallas correrás peligro", Sun Tzu

BIBLIOTECA INGENIOS

EL ARTE DE LA GUERRA

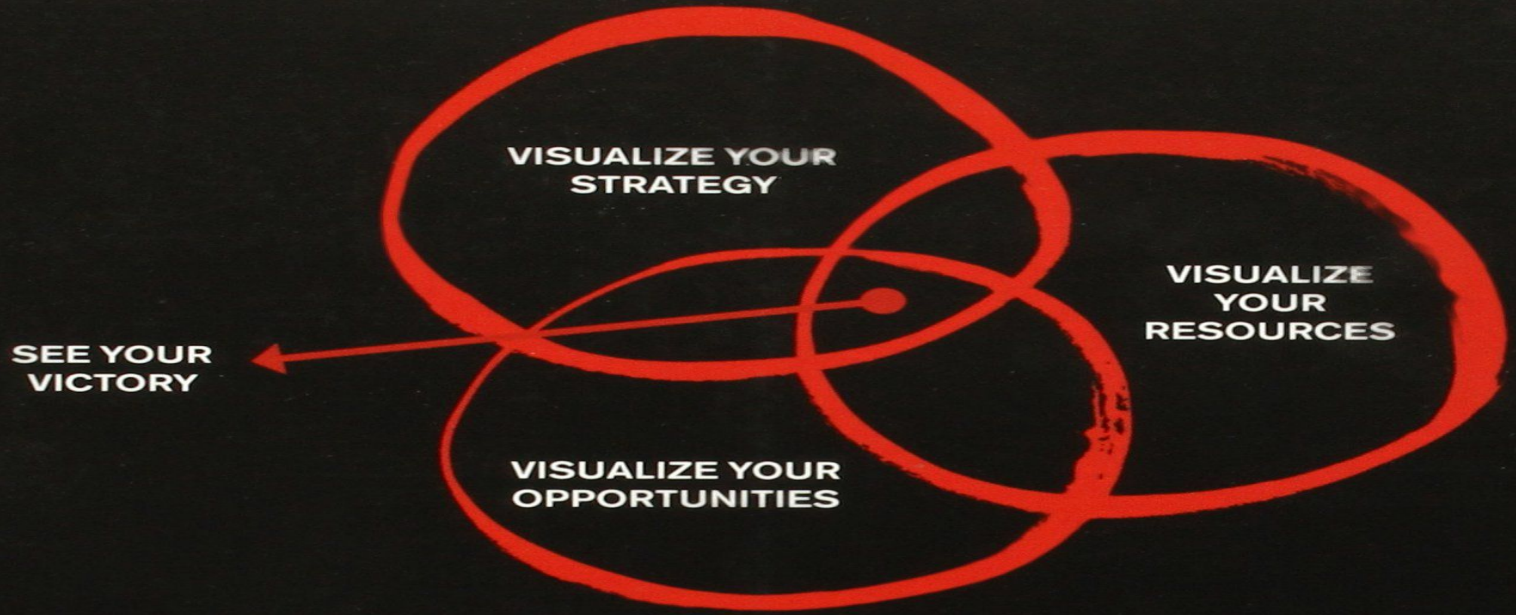
SUN TZU

LAS VICTORIAS DE LOS BUENOS GUERREROS NO SE DEBEN A LA SUERTE, SINO A HABERSE SITUADO PREVIAMENTE EN POSICIÓN DE GANAR CON SEGURIDAD, IMPONIÉNDOSE SOBRE LOS QUE YA HAN PERDIDO DE ANTEMANO.

SUN TZU

EL ARTE DE LA GUERRA

Biblok



THE ART OF WAR has been a game plan to success for more than 800 years. THE ART OF WAR VISUALIZED is its total transformation for the 21st century. Use it whenever there's something worth fighting for.

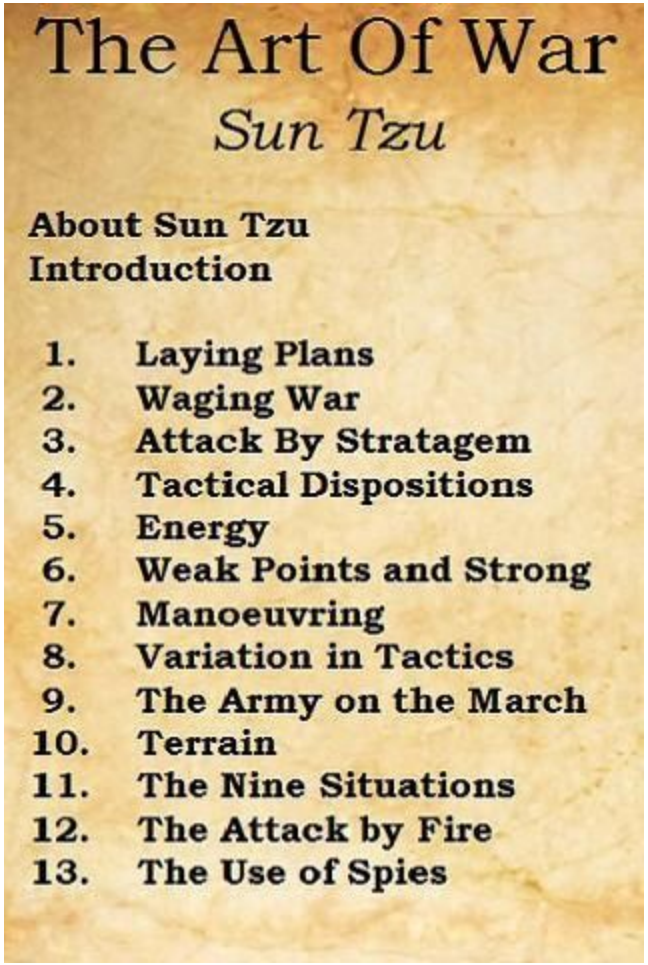
WORKMAN PUBLISHING, NEW YORK
WORKMAN.COM

$14.95 U.S. ISBN 978-0-7611-8238-2

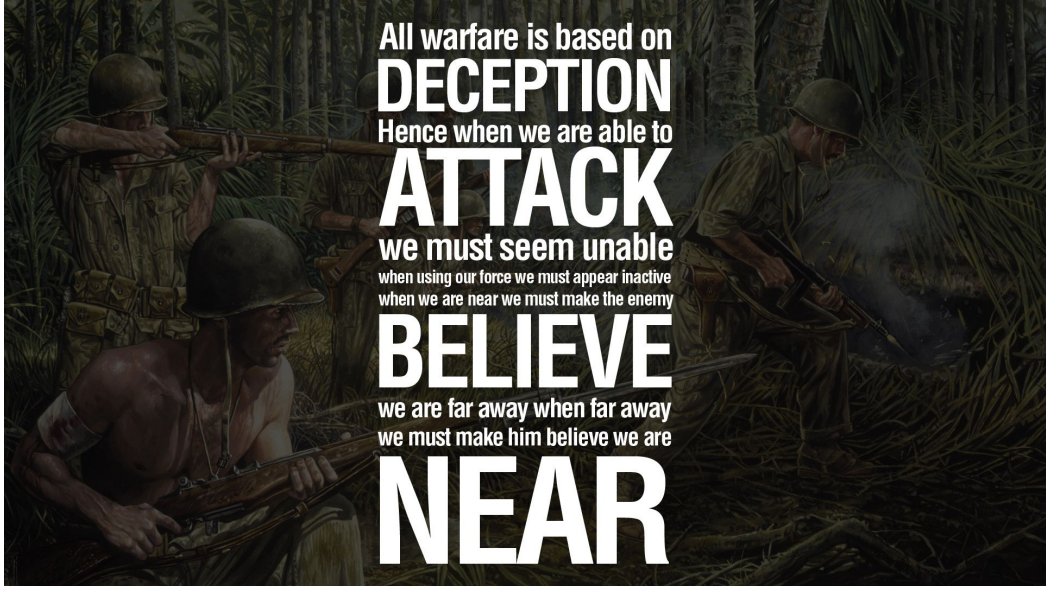
The Art Of War...

¿Por qué?:

- Para detectar sitios influyentes.
- Para averiguar tendencias de consumo.
  - Nuevas demandas o necesidades de los clientes.
- Para obtener ventaja frente a la competencia.
- Detectar amenazas.
  - Nuevos competidores/productos, cambios legislativos.
- Para innovar productos o servicios.
- Para encontrar nuevos nichos de mercado.



The Art Of War...

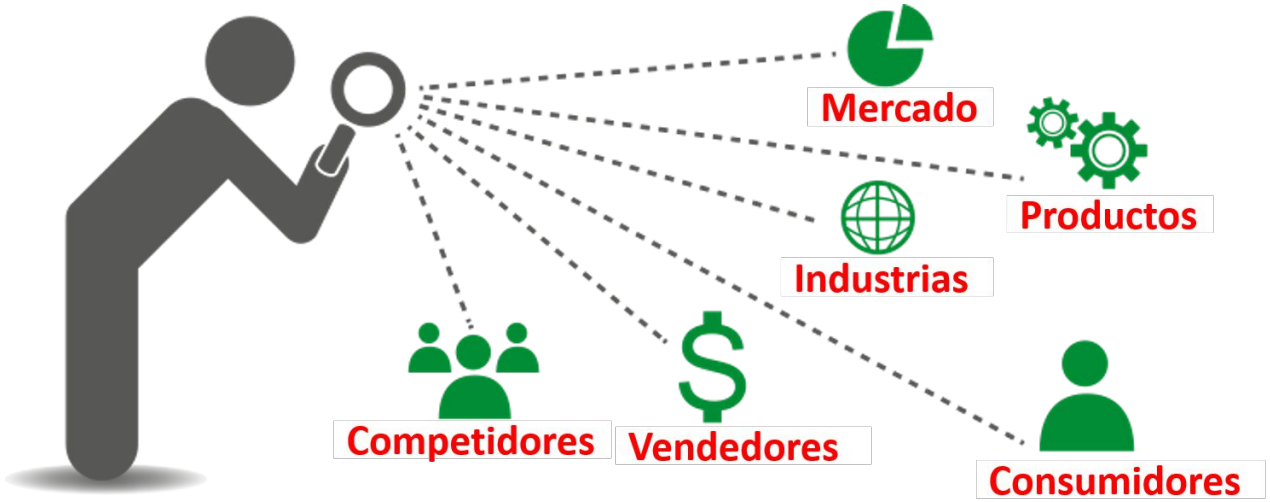


Objetivos clave:

- ¿Cuál es el objetivo?.
- ¿Qué hay que vigilar? ¿Qué informaciones buscar?.
- ¿Dónde localizarlas?.
- ¿Cómo organizar y tratar la información?.
- ¿A quién comunicar la información en la empresa?.
- ¿Qué recursos vamos a destinar?.

Vigilancia competitiva… Factores:

- Tecnologías
- Mercados
- Clientes
- Proveedores
- Entorno
- Productos
- Competidores



Vigilancia competitiva… Tecnologías:

- Maquinaria y tecnología industrial.
- Avances técnicos en el sector.
- Maquinaria y tecnología de la competencia.
- Patentes de la tecnología y del diseño.

Vigilancia competitiva… Clientes:

- Necesidades reales y potenciales.
- Demandas reales y potenciales.
- Hábitos de consumo y comportamiento.
- Perfiles de los consumidores y clientes.

Vigilancia competitiva… Productos:

- Líneas de producto existentes en el mercado:
  - ¿qué productos/servicios pueden ser los más adecuados para comercializar en un mercado concreto?
- Productos de la competencia y su impacto en el mercado:
  - ¿Qué competencia existe?
- Investigación y desarrollo de nuevos productos.

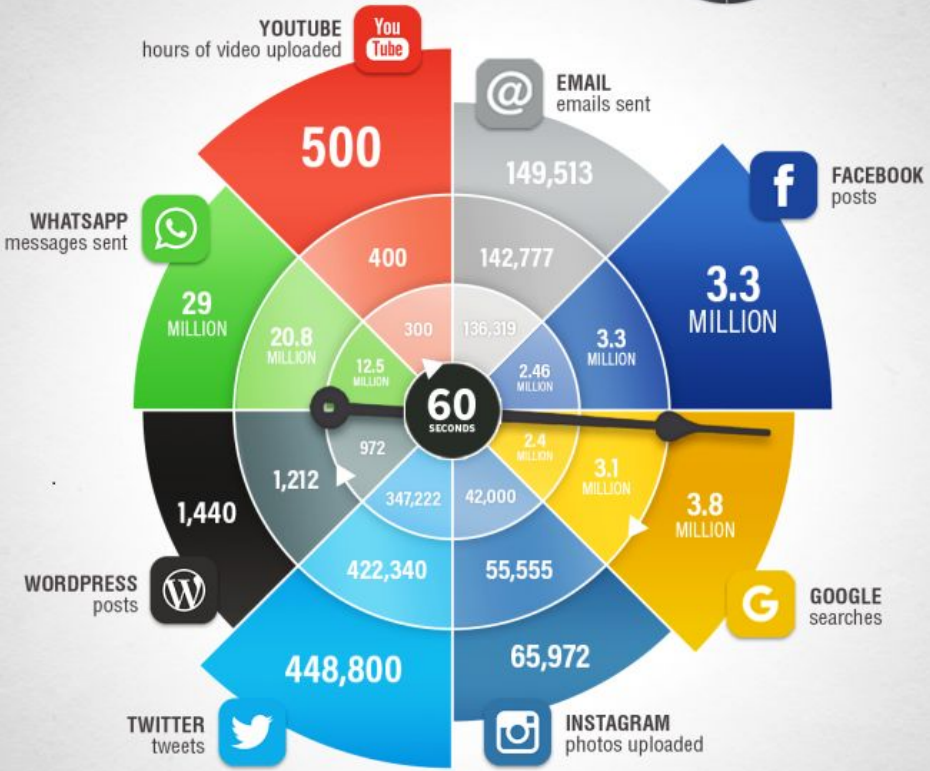
Vigilancia **estratégica**:

- Tecnológica.
- Competitiva.
- Comercial.
- Socio-económica.

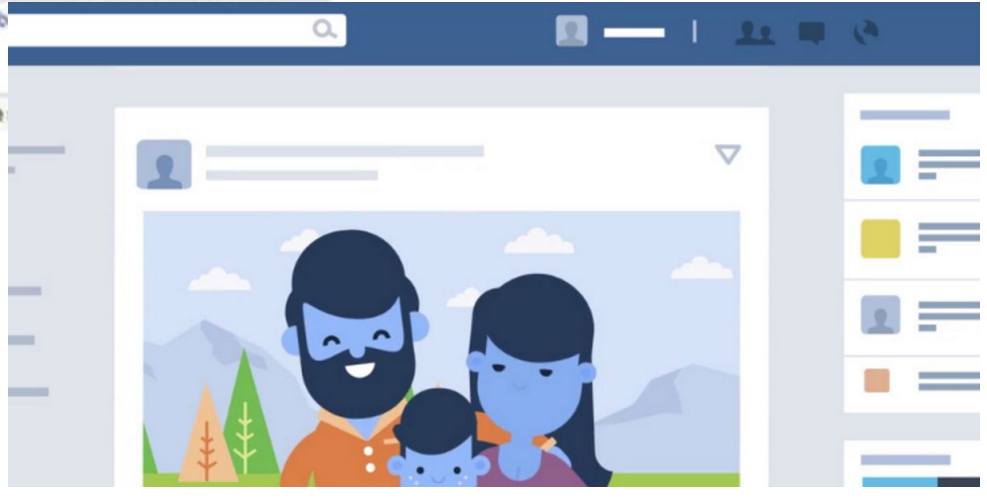

Microphone Recording
Emails
Photos & Screenshots
SMS
Instant Messaging
Location Tracking
File Retrieval
Network Details
Target
Calendar Records
Device Settings
Phone Calls
Browsing History
Social Networks
Contact Details

What Happens Online in 60 Seconds?

Managing Content Shock in 2017




facebook
Profile edit Friends Networks Inbox
home account privacy logout
Search find friends
Applications edit
Photos
Groups
Events
Marketplace
Trips
more
Caroline
Profile
Networks: Trinity School '07
Harvard '11
New York, NY
Sex: Female
Interested In: Men
Relationship Status: Single
Looking For: Friendship
Random play
Whatever I can get
Birthday:
Political Views: Liberal
Mini-Feed
Displaying 10 stories.
See All
Today
August 2
View Photos of Caroline (207)
Send Caroline a Message
Poke Her!
Add Caroline as a Friend



YAHOO! ESPAÑA

Tu progreso | ¿Qué se te ha olvidado? | Verifica tu identidad

Contesta la pregunta secreta

¡Muy bien, ya casi hemos terminado!

Pregunta 1 de 2

¿Dónde pasaste tu luna de miel?

Añadido 11 agosto 2009

Cerrar asistente


Ni tanto...
...ni tan calvo.
¿PERO CÓMO QUE NECESITAN MI SEGUNDO APELLIDO PARA VENDERME UN BILLETE DE TREN? ¡ESO ES UNA INTROMISIÓN EN MI INTIMIDAD PERSONAL!
ESTO DE FACEBOOK ES SENSACIONAL: ESTOY INTRODUCIENDO EN MI PERFIL DE MANERA COMPLETAMENTE VOLUNTARIA Y CON ACCESO PÚBLICO A TODO CRISTO LOS INSTITUTOS Y UNIVERSIDADES DONDE HE ESTUDIADO, MI ÁRBOL GENEALÓGICO, LOS CURROS QUE HE TENIDO, LA COMIDA QUE ME GUSTA, TODAS LAS CIUDADES QUE HE VISITADO EN MI VIDA, LOS TÍTULOS DE MIS LIBROS PREFERIDOS, TODAS LAS NOVIAS QUE HE TENIDO...


That’s just, like, your opinion, man.

1.750€

¿CUÁNTO VALES en Internet?

700€

Cuánto dinero puedes perder

7€
Lo que te cobrarán de media en tu factura si un hacker logra enviar varios SMS a teléfonos de tarificación especial desde un smartphone infectado

18€
Es el dinero que pierdes si secuestran tu Skype junto con el dinero de tu cuenta

540€
La suma robada de tu cuenta bancaria si dispones de 7.200 euros de media (7,5% de media)

72€
El coste de restaurar tus datos tras ser cifrados por el troyano Gpcode

21,50€
La cantidad media de dinero que te pueden llegar a quitar si tu monedero electrónico resulta intervenido con dinero virtual dentro

36€
El coste del antivirus rogue que, además, no hace nada por protegerte

A pesar de la bajada de precios de los proveedores de ancho de banda, el coste del uso de Internet puede ser excesivo para los usuarios que no están correctamente protegidos frente al cibercrimen y nuevas amenazas. Los expertos de Kaspersky Lab afirman que la Red puede resultar un lugar 'caro' para aquellos que no adoptan un enfoque correcto frente a los problemas de seguridad. Tras analizar las estadísticas de infección de malware de las estafas online más extendidas, los analistas han calculado el coste medio de algunas de estas actividades:

1.050€

Beneficios que aportas a los cibercriminales

18€
El beneficio que les genera un pasaporte robado escaneado

2,10€
Infectar un PC con un troyano y vincularlo a una botnet

7€
Por conseguir los datos de una tarjeta de crédito

44€
Datos de acceso a un sitio de una red social

718€
Un nuevo pasaporte donado

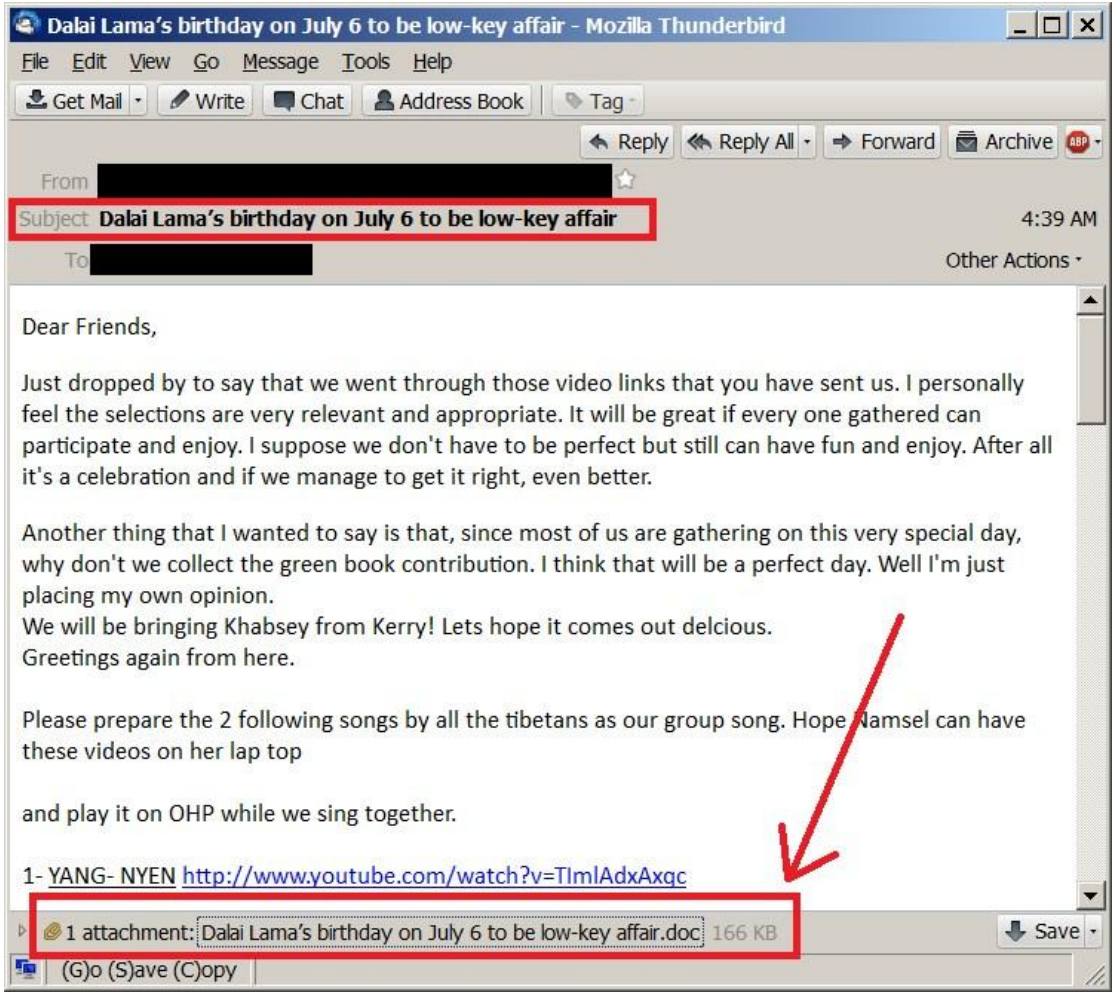
14,50€
Acceder de forma no autorizada a un correo electrónico

7€
El acceso a una cuenta en un servicio de alojamiento como Rapidshare

108€
El robo de un personaje virtual en un juego online

10€
Claves de acceso a un servicio de mensajería instantánea como ICQ, QIP, etc.

KASPERSKY


Dalai Lama's birthday on July 6 to be low-key affair - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Mail Write Chat Address Book Tag
Reply Reply All Forward Archive
From [redacted]
Subject Dalai Lama's birthday on July 6 to be low-key affair
4:39 AM
To [redacted]
Other Actions
Dear Friends,
Just dropped by to say that we went through those video links that you have sent us. I personally feel the selections are very relevant and appropriate. It will be great if every one gathered can participate and enjoy. I suppose we don't have to be perfect but still can have fun and enjoy. After all it's a celebration and if we manage to get it right, even better.
Another thing that I wanted to say is that, since most of us are gathering on this very special day, why don't we collect the green book contribution. I think that will be a perfect day. Well I'm just placing my own opinion.
We will be bringing Khabsey from Kerry! Lets hope it comes out delcious.
Greetings again from here.
Please prepare the 2 following songs by all the tibetans as our group song. Hope Namsel can have these videos on her lap top
and play it on OHP while we sing together.
1- YANG- NYEN http://www.youtube.com/watch?v=TImlAdxAxqc
1 attachment: Dalai Lama's birthday on July 6 to be low-key affair.doc 166 KB
Save
(G)o (S)ave (C)opy

130 Years Of Trust | Calendar | The Tribune ONLINE EDITION | Weather

Lalit Mohan
Tribune News Service

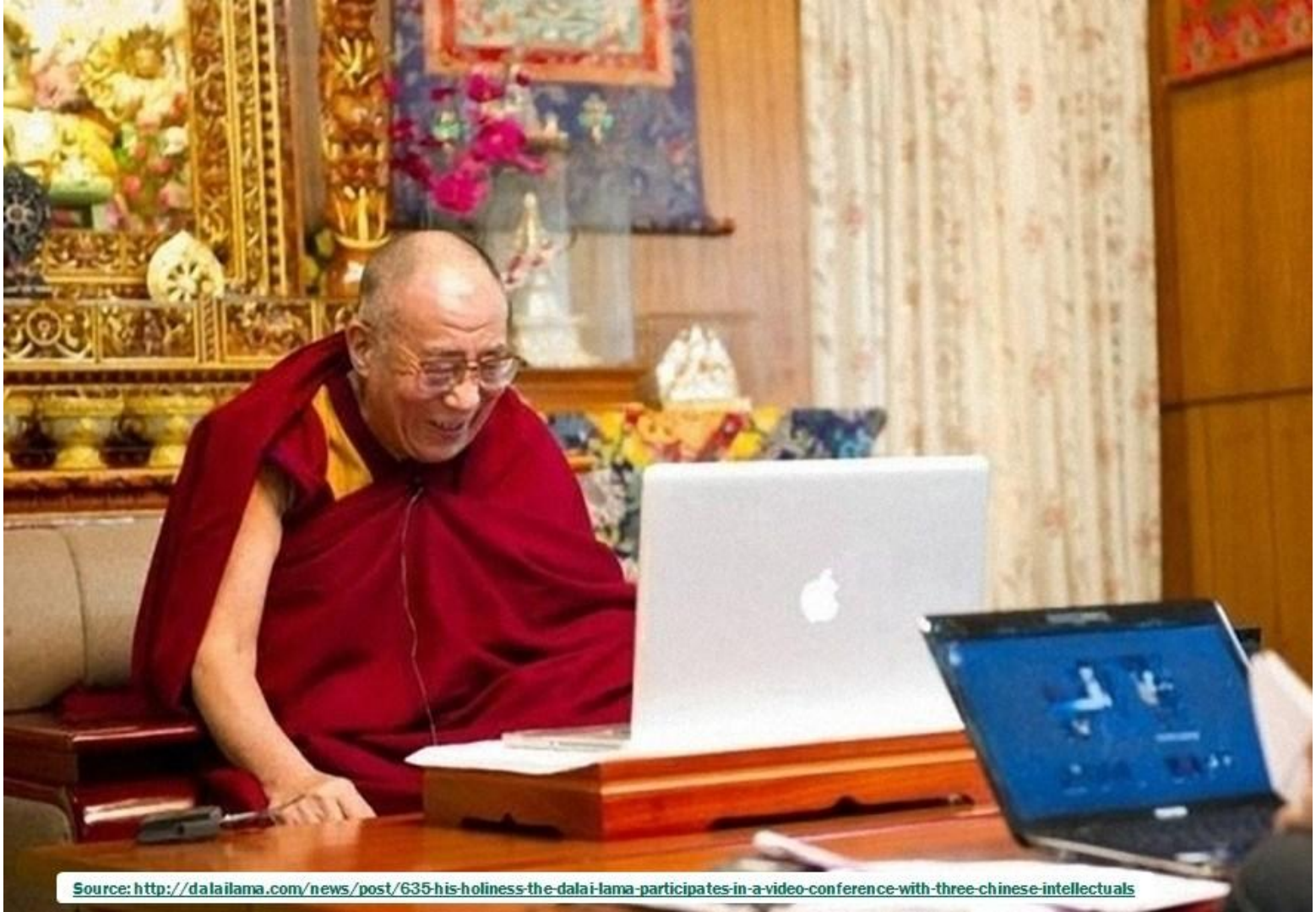
Dharamsala, July 1
The Dalai Lama will turn 77 on July 6. Even after staying in exile for about 52 years, the septuagenarian leader of Tibetans commands huge respect among Tibetans living in Tibet and other parts of the world and is the pivotal force behind the Tibetan movement. He is still the leader for even those young Tibetans who have not seen him in person, since they were born after he fled into exile to India in 1959.

The Dalai Lama's birthday used to be a major event for the Tibetans living in exile, especially in Dharamsala, the headquarters of the Tibetan government-in-exile. On the day, Tibetans used to host events to highlight the Tibet issue from their own perspective. However, sources said the Dalai Lama's birthday was likely to be a low-key affair this year.

No foreign leader or dignitary was likely to visit the Dalai Lama on the day. The Central Tibetan Administration (CTA) had sent an invitation to the Chief Minister of Himachal to attend a function to be organised on the occasion. The programme was yet to be finalised. CTA officials have maintained that they will concentrate on local participation during the event.

As per the schedule being worked out by the CTA, the birthday will be celebrated in two different shifts - morning and evening. Cultural items will be presented by the Tibetan Institute of Performing Arts, while monks and nuns will hold prayers for the long life of the Dalai Lama.

Source: http://dalailama.com/news/post/635-his-holiness-the-dalai-lama-participates-in-a-video-conference-with-three-chinese-intellectuals



Source: http://dalailama.com/news/post/635-his-holiness-the-dalai-lama-participates-in-a-video-conference-with-three-chinese-intellectuals

Operación de falsa bandera:

Operaciones encubiertas llevadas a cabo por gobiernos, corporaciones y otras organizaciones, diseñadas para aparentar como si fueran llevadas a cabo por otras entidades.

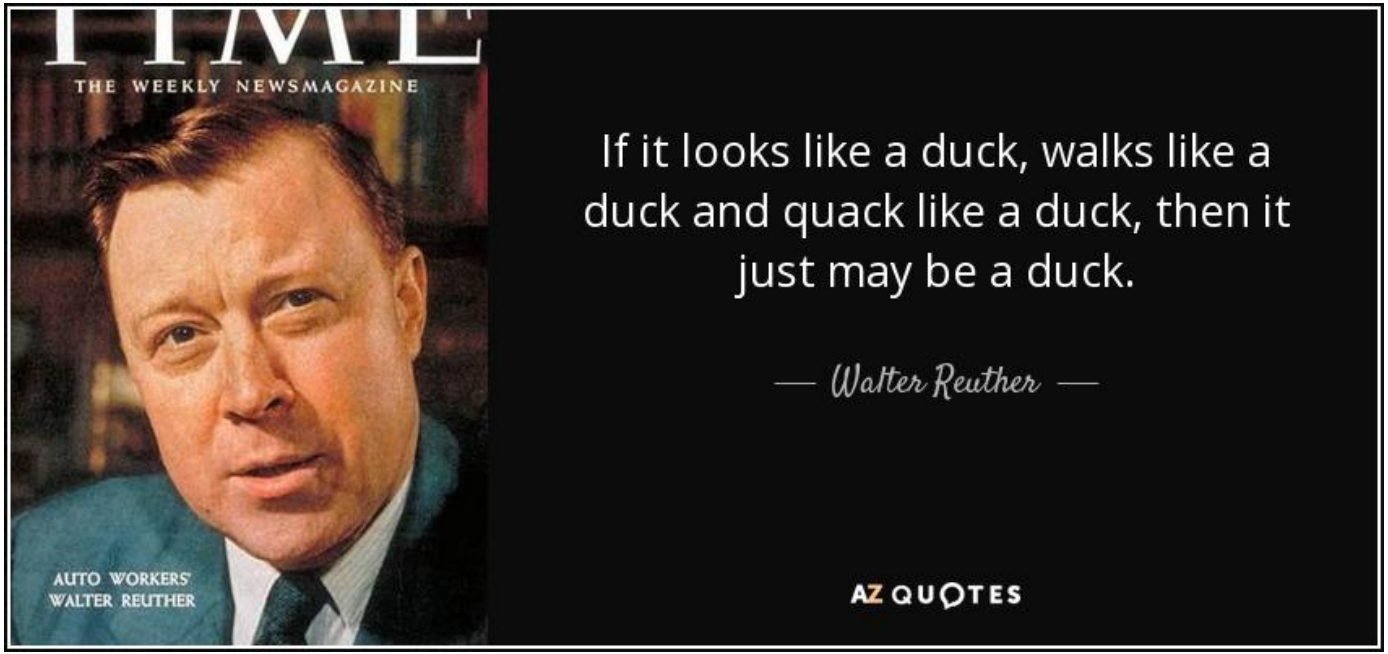
El nombre deriva del concepto militar de izar colores falsos, esto quiere decir: una bandera diferente a la propia.

Operación de falsa bandera... A tener en cuenta:

- Fallos de OPSEC: ¿intencionados o inadvertidos?
- Mala compartimentación de operaciones.
- Tensiones geo-políticas.
- Eventos de relevancia.
- TTPs – fácil reutilización.
- Es necesario mezclar HUMINT + aspectos técnicos y operativos en el mundo "ciber".
- Sólo al alcance de LEAs, militares y servicios de inteligencia.

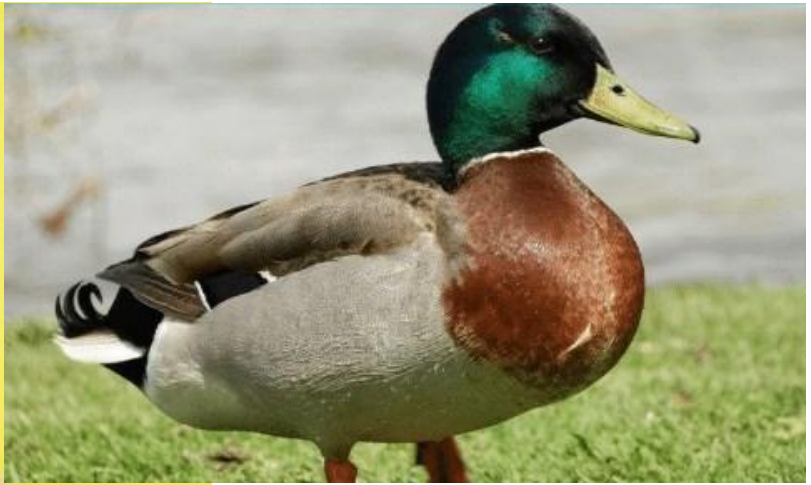
Ciberseguridad en el mundo actual:

- ***It's a duck...***

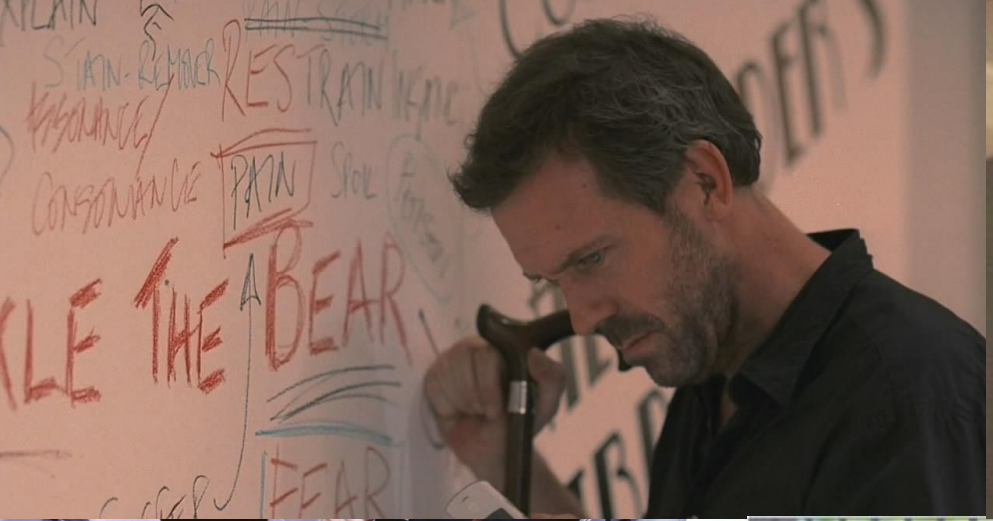


Ciberseguridad en el mundo actual:

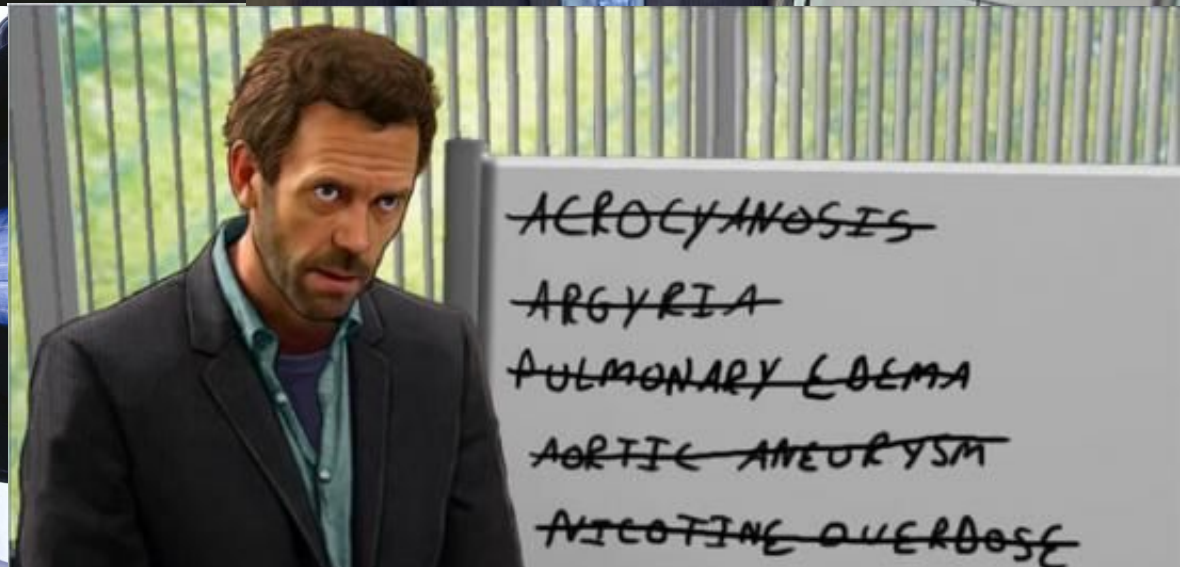
- *… or not.*




- No lo sé Rick, parece falso...


RESTRAIN
PAIN
THE
BEAR


"DEAD MAN DYING"
SYMPTOMS
CAUSES


ACROCYANOSIS
ARGYRIA
PULMONARY EDEMA
AORTIC ANEURYSM
NICOTINE OVERDOSE

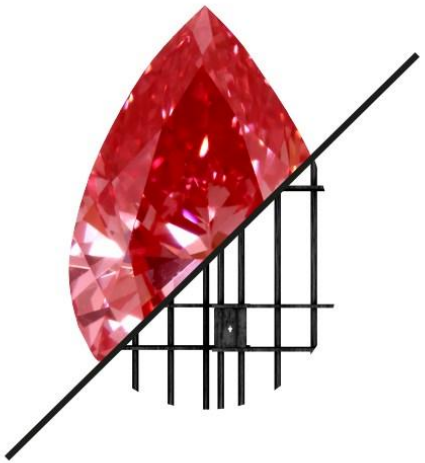
Operación de falsa bandera... Elementos de **atribución**:

- Infraestructura: dominios, direcciones IP, correos, localización, etc.
- Cadenas de texto en el binario cliente / servidor.
- Metadatos de los binarios: lenguaje, fecha compilación, directorios, etc.
- Afectados: sector, país, etc.
- Operaciones: horarios, coincidencias con eventos políticos, religiosos, nacionales, etc.
- Reutilización de código.

They are determined, you have Intelligent Deception

Use **CounterCraft's Cyber Deception Platform** to detect targeted attacks with real-time active response. Turn a passive IT security posture into active defence.

REGISTER FOR A TRIAL

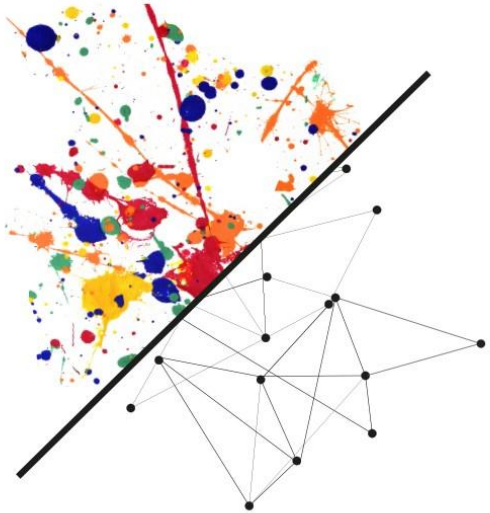


A distributed Deception Platform for the digital realm

Run automated **counterintelligence campaigns** and use cyber deception for active defence. Prevent intruders' espionage and intelligence operations and **reduce costs by 95%.**

REGISTER FOR A TRIAL

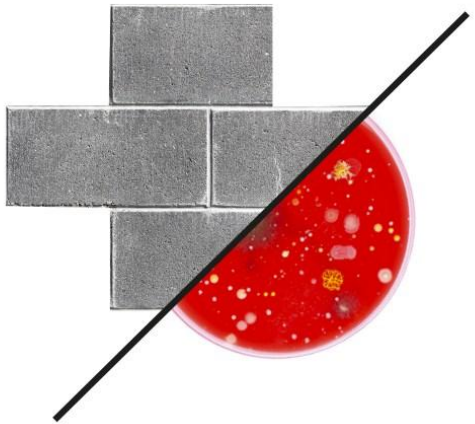
Deception artistry – detect, study and manipulate your adversaries



Our Cyber Deception Platform covers a wide range of deceits at the identity, data and network levels. Orchestrate your campaigns and craft artful deceptions and **complex active responses.**

DISCOVER OUR APPROACH

Changing scenarios require a new paradigm in cybersecurity



We propose something new: don't stop attacks. Let them take place in controlled environments. Deception technology will be a **$3 billion market** over the next 3 years.

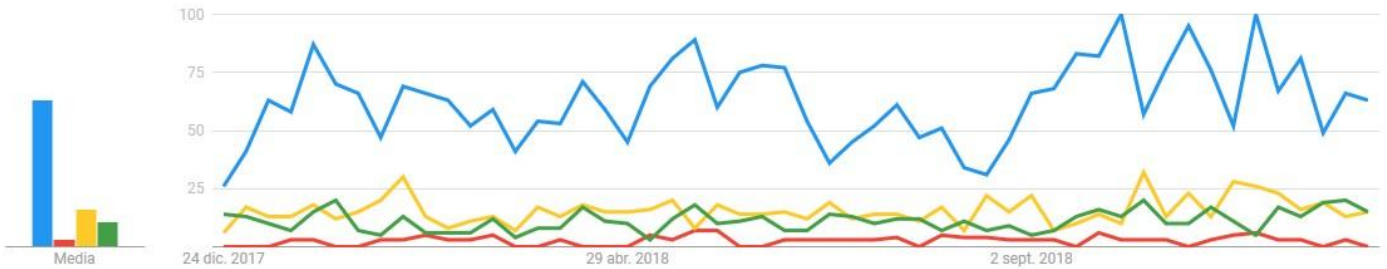
BECOME OUR PARTNER NOW

Google Trends | Comparar

- ciberseguridad — Término de búsqueda
- ciber seguridad — Término de búsqueda
- cybersecurity — Término de búsqueda
- cyber security — Término de búsqueda

España | Últimos 12 meses | Todas las categorías | Búsqueda web

Interés a lo largo del tiempo

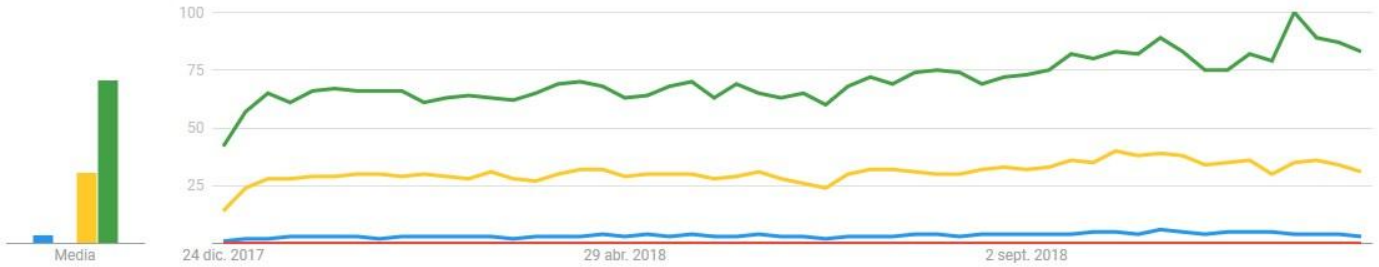


Google Trends | Comparar

ciberseguridad	ciber seguridad	cybersecurity	cyber security	+
Término de búsqueda	Término de búsqueda	Término de búsqueda	Término de búsqueda	

Todo el mundo | Últimos 12 meses | Todas las categorías | Búsqueda web

Interés a lo largo del tiempo



Panorámica de la Ciberseguridad:

- Estado del arte
- Objetivos principales
- Entidades y organismos implicadas

Panorámica de la Ciberseguridad… Estado del arte

Tendencia hacia la interconectividad e interoperabilidad de redes, máquinas y aplicaciones.

La seguridad abarca todo el **ciclo de vida** de los productos:

- Diseño.
- Desarrollo.
- Integración.
- Operación.
- Administración.
- Actualización.

La seguridad de los sistemas de información es una disciplina en continua evolución.

Panorámica de la Ciberseguridad… Estado del arte

- Todo sistema infectado ya no es confiable.

- Ninguna empresa está libre de sufrir un ataque.

Según Kaspersky Lab y Avast, 7 de cada 10 ciberataques están dirigido a pequeñas empresas, de las que el 60% desaparece seis meses después.
En consecuencia, el presupuesto destinado a ciberseguridad no debe ser entendido como un gasto, sino planificado como una inversión en prevención y ciber-resiliencia; pues el hecho de no hacer nada ocasionará costes.

- Atacar es mucho más fácil que defender.
- Un atacante solo necesita una vulnerabilidad para ganar.

Panorámica de la Ciberseguridad… Estado del arte

¿Cuál es el objetivo de la seguridad informática?

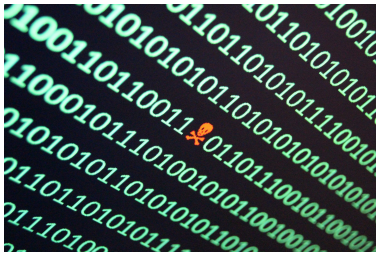
- Proteger el **principal activo** de cualquier organización.

La información


El proceso productivo

Infraestructuras críticas

Panorámica de la Ciberseguridad… Estado del arte



La información es el activo más valioso dentro de las organizaciones.

Su almacenamiento, transmisión y procesado (incluyendo su destrucción y borrado seguro) deben garantizar la **seguridad de la información** de negocio y datos personales, protegiendo así su **integridad, disponibilidad y confidencialidad**.

La seguridad de la información es un **proceso dinámico de mejora continua**, el cual debe gestionarse de forma eficaz y proactiva para identificar los riesgos y protegerse del impacto de nuevas vulnerabilidades y amenazas en constante evolución dentro del entorno operativo de arquitectura empresarial.

Para mejorar el control y detección en la **respuesta a las amenazas** se requiere un enfoque de seguridad basado en inteligencia, facilitando toda la información disponible para detectar amenazas ocultas y predecir amenazas futuras, tanto de fuentes internas como externas; permitiendo al personal ejecutivo y de dirección la toma de decisiones estratégicas que apoyen la continuidad de las operaciones de negocio.

Data Loss Prevention

Metashield Protector

Soluciones preventivas contra la fuga de información sensible

Metashield *Protector* protege los entornos documentales mediante el análisis, filtrado y tratamiento de metadatos proporcionando a las organizaciones el máximo control sobre su información.

Descargar hoja de producto

Contratar

Un conjunto de herramientas que ofrecen una respuesta integral en la aplicación de políticas de prevención sobre la gestión documental de una organización.

Metashield Protector ofrece soluciones de prevención en todos los entornos documentales: estaciones de trabajo o equipos cliente, servidor y servicio online; permitiendo a las organizaciones la aplicación de políticas corporativas de seguridad homogéneas en el tratamiento de metadatos.

Metashield Discovery Solutions

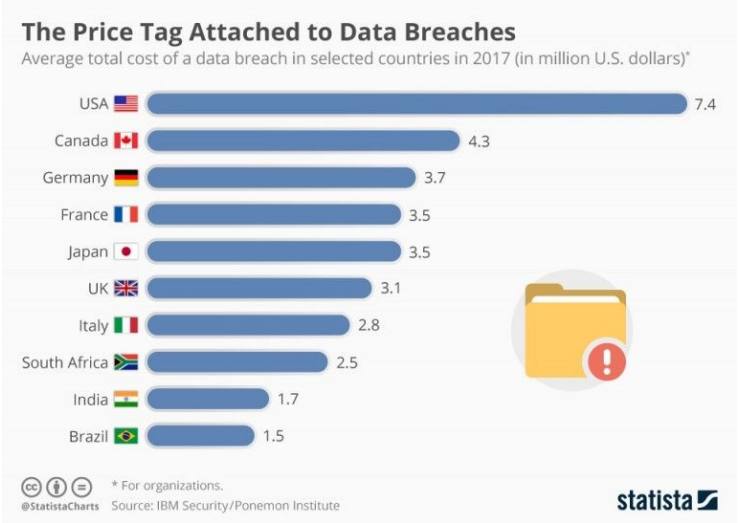
Metashield File Solutions

Panorámica de la Ciberseguridad…

Mitigar la fuga de información:

- Políticas de acceso a la información:
  - Sólo se debe accede a lo estrictamente necesario.
- Cifrado.

Panorámica de la Ciberseguridad… Mitigar la **fuga de información**:



Causas:

- Organizativas:
  - Falta de información.
  - Ausencia de procedimientos.
  - Falta de acuerdos de confidencialidad.
- Técnicas:
  - Malware.
  - Acceso no autorizado a los sistemas o infraestructura:
    - Servicios en la nube para almacenamiento:
      - El eslabón más ***débil/fuerte*** son los usuarios y sus contraseñas.
    - Tecnologías móviles:
      - Pérdida de dispositivos sin cifrado.

SECURITY BREACHES CONTINUE TO PLAGUE FINANCIAL SERVICES

125

Average number of security breaches each year

... FINANCIAL SERVICES IS SLIGHTLY BETTER THAN GLOBAL PEERS

130

Average number of security breaches each year

... AND THE COST OF BREACHES CONTINUES TO RISE

$18.28MM

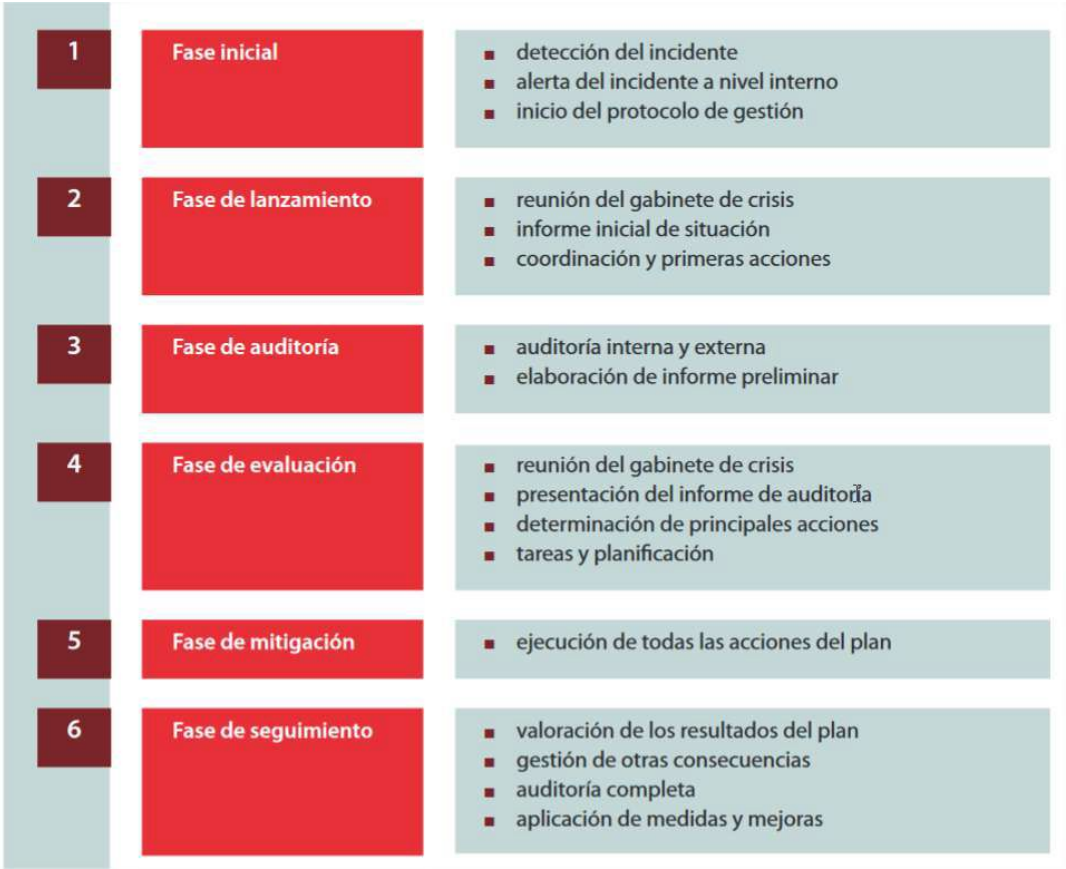
Average annualized cost of cyber crime (USD)

+9.6%

Increase in the last year

Source: Cost of Cyber Crime 2017, Accenture and the Ponemon Institute, September 2017

Panorámica de la Ciberseguridad… Mitigar la **fuga de información**:



Panorámica de la Ciberseguridad… Estado del arte

Todo el personal relacionado con la organización en el flujo de información es responsable en la ciberseguridad y la fuga de datos (**DLP**).
Es necesario crear conciencia así en todas las personas involucradas; desde los miembros en plantilla hasta el personal subcontratado (incluyendo a servicios externos y proveedores) quienes deberán firmar **acuerdos de confidencialidad** que garanticen los cumplimientos requeridos (RGPD, LSSI, COBIT, etc).

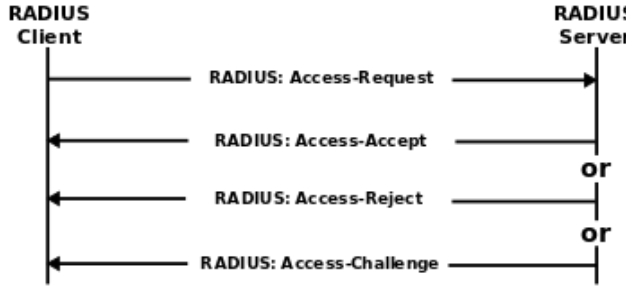
El control de acceso a la información a través de la red corporativa debe ser filtrado y registrado a través de políticas de grupo y (**ACL**) **listas de control de acceso** para autenticación del (**UAC**) **control de cuentas de usuario**, con sus respectivos (timestamp) sellos de tiempo para garantizar la trazabilidad forense.

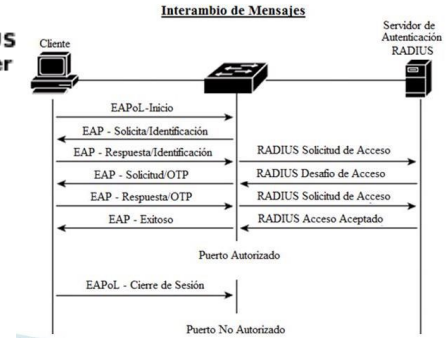
Las comunicaciones requieren de sistemas seguros dotados con cifrado robusto de datos y dispositivos, basados en certificados digitales de confianza. Aplicar criptografía en datos y comunicaciones.

Panorámica de la Ciberseguridad… Protocolos de **Autenticación**

KDC: Centro de distribución de claves fiables.

TACACS+ y **RADIUS**





- TACACS+ (RFC1492) y RADIUS (RFC2138) son ejemplos de centros de distribución de claves o también conocidos como servidores de control de acceso.
- TACACS+ y RADIUS son protocolos para descentralizar el control del acceso.
- Estos servidores se utilizan generalmente como apoyo a los routers de acceso remoto
- Otros servidores de acceso son los servicios **ACTIVE DIRECTORY** de los Controladores de Dominio Microsoft desde w2000 y Zentyal Server http://www.zentyal.com/es/

zentyal
Active Exchange

Panorámica de la Ciberseguridad… Protocolos de **Autenticación**

Kerberos

KDC diseñado por el MIT para:

- autenticar la identidad de los usuarios de una red digital insegura.
- distribuir las claves secretas de sesión transitorias que permitan a los usuarios de la red establecer comunicaciones seguras.

Es centralizado (y no distribuido) en una red, lo cual si falla se compromete toda la red, además las claves almacenadas son privadas y no públicas.

- En ningún momento los passwords viajan por la red ni son guardados en memoria, sólo las credenciales.

Kerberos actúa como un árbitro en quien los usuarios confían, utilizando con cada usuario una clave secreta diferente, intercambiada con Kerberos a través de un canal seguro.

Panorámica de la Ciberseguridad… Protocolos de **Autenticación**

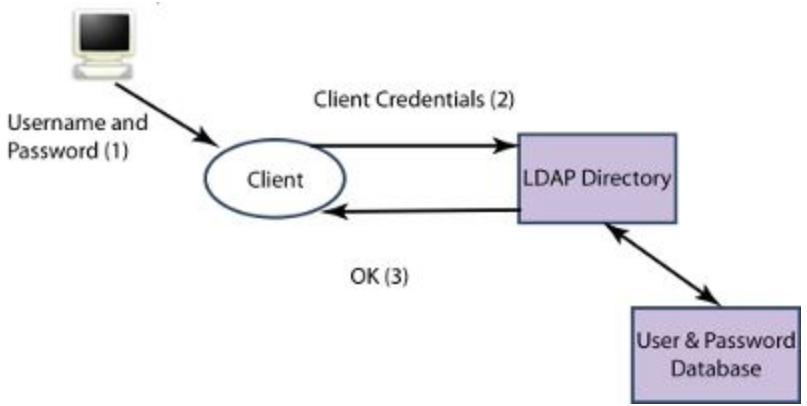
LDAP (Lightweight Directory Access Protocol) y Servicio de Directorio.

Es un protocolo de aplicación. http://www.openldap.org/

Permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.

Es utilizado para autenticarse aunque es posible almacenar otra información:

- datos de contacto del usuario
- ubicación de diversos recursos de la red
- permisos
- certificados...

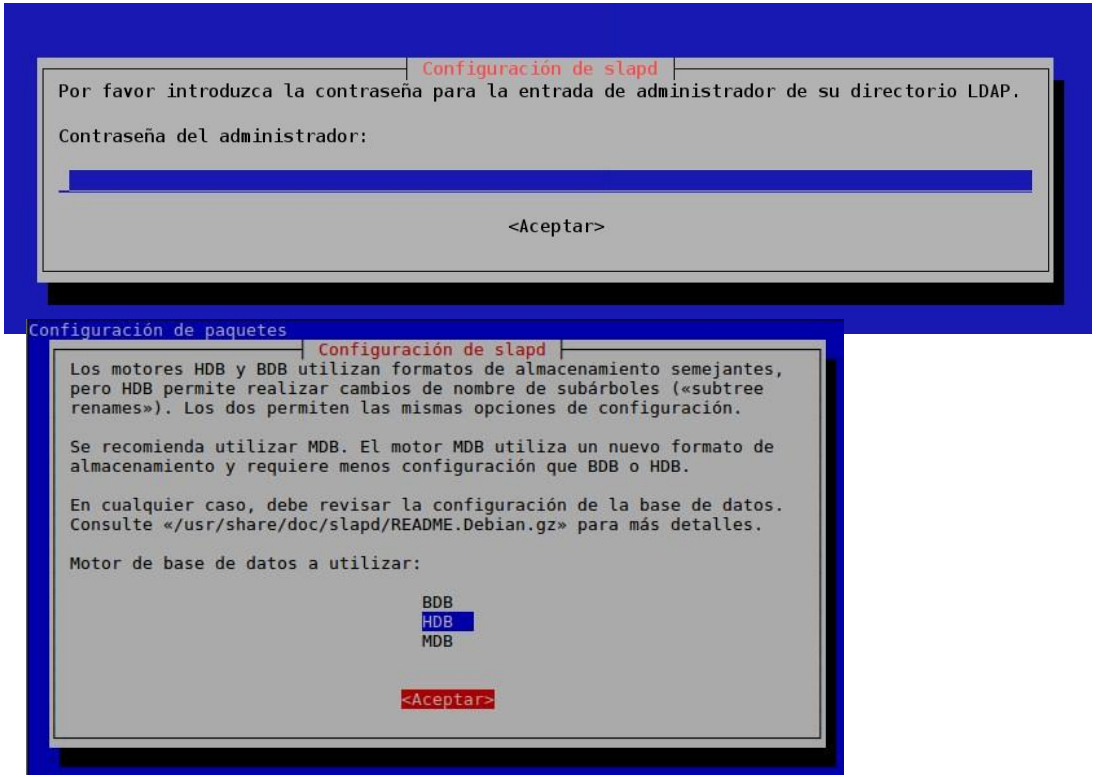


Panorámica de la Ciberseguridad… Protocolos de **Autenticación**

LDAP

Ejemplos de atributos en directorios

- CN Nombre habitual o canonical name
- O Organización
- OU Departamento
- C País
- MAIL Dirección de correo electrónico
- PHONE Número de teléfono
- DC Componente de dominio
- DN Nombre Distinguido



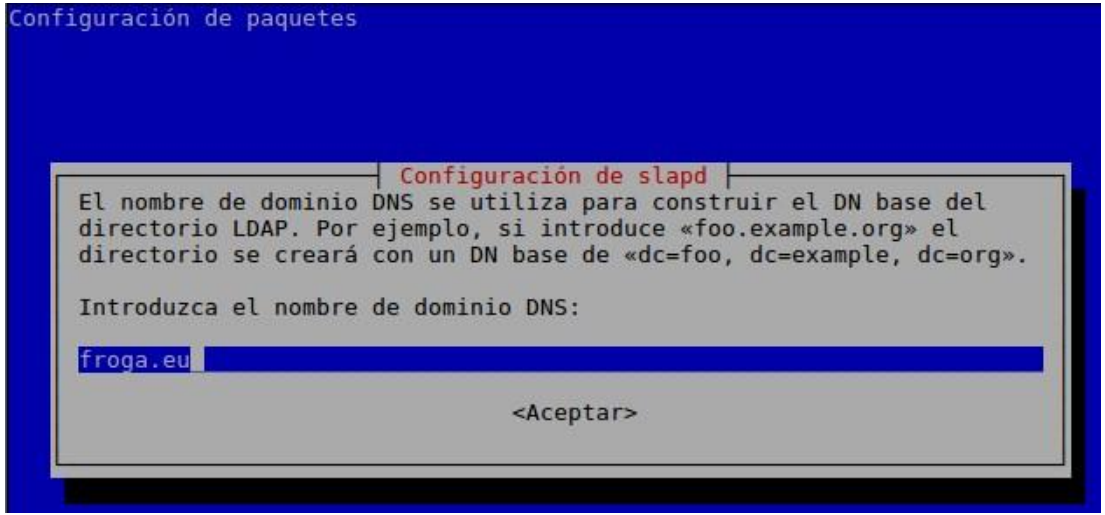
Panorámica de la Ciberseguridad… Protocolos de **Autenticación**

LDAP

paquete SLAPD (Standalone LDAP Daemon)

```
sudo apt-get install slapd ldap-utils
```

```
sudo dpkg-reconfigure slapd
```



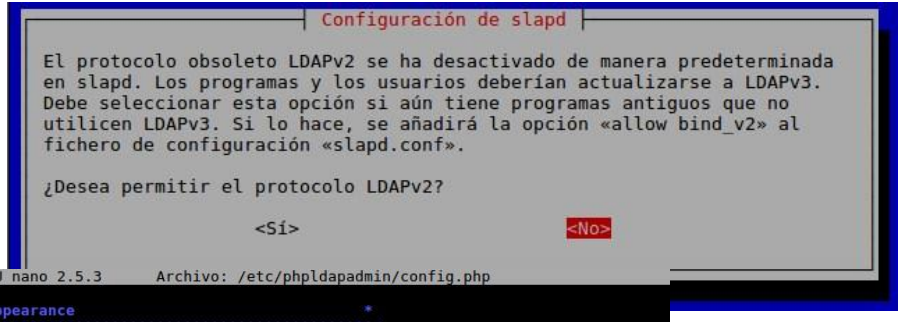
Panorámica de la Ciberseguridad… Protocolos de **Autenticación**

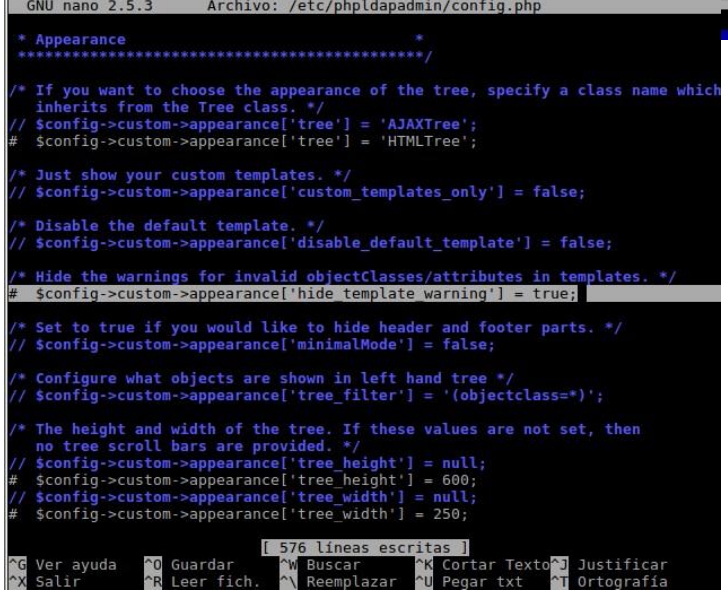
LDAP

paquete phpldapadmin para la administración web.

```
sudo apt-get install phpldapadmin
```

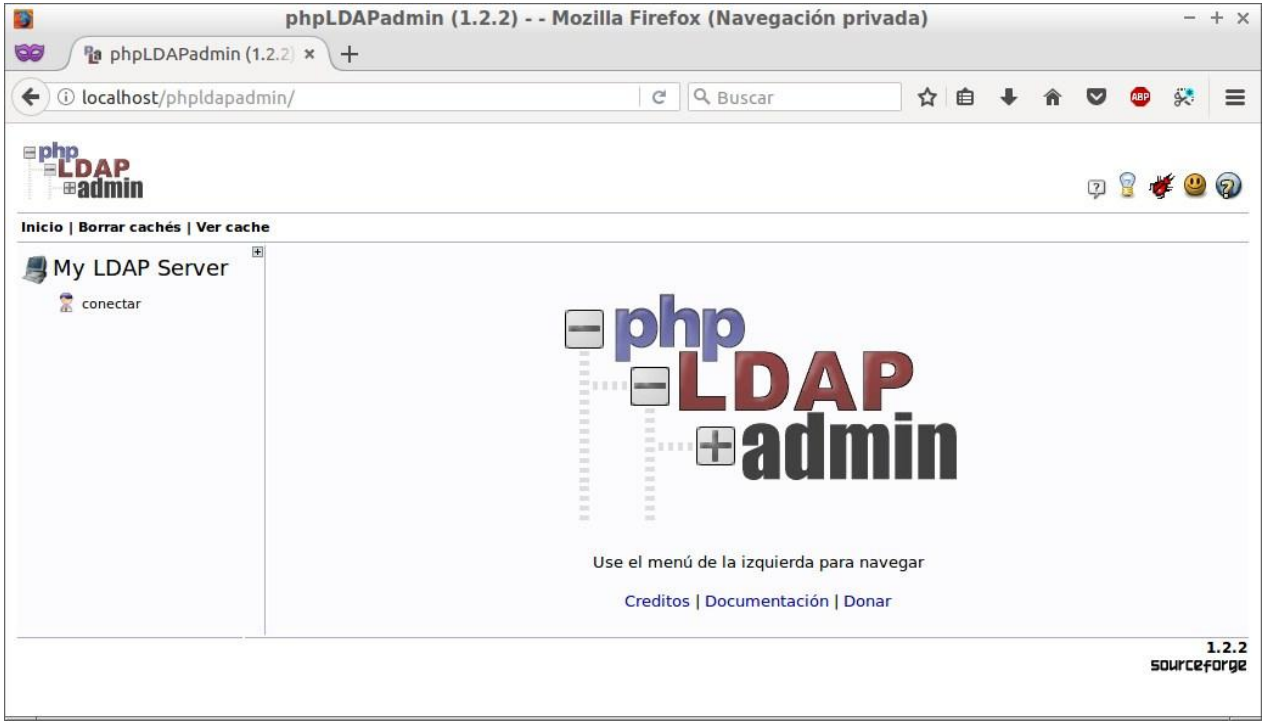
```
sudo nano /etc/phpldapadmin/config.php
```

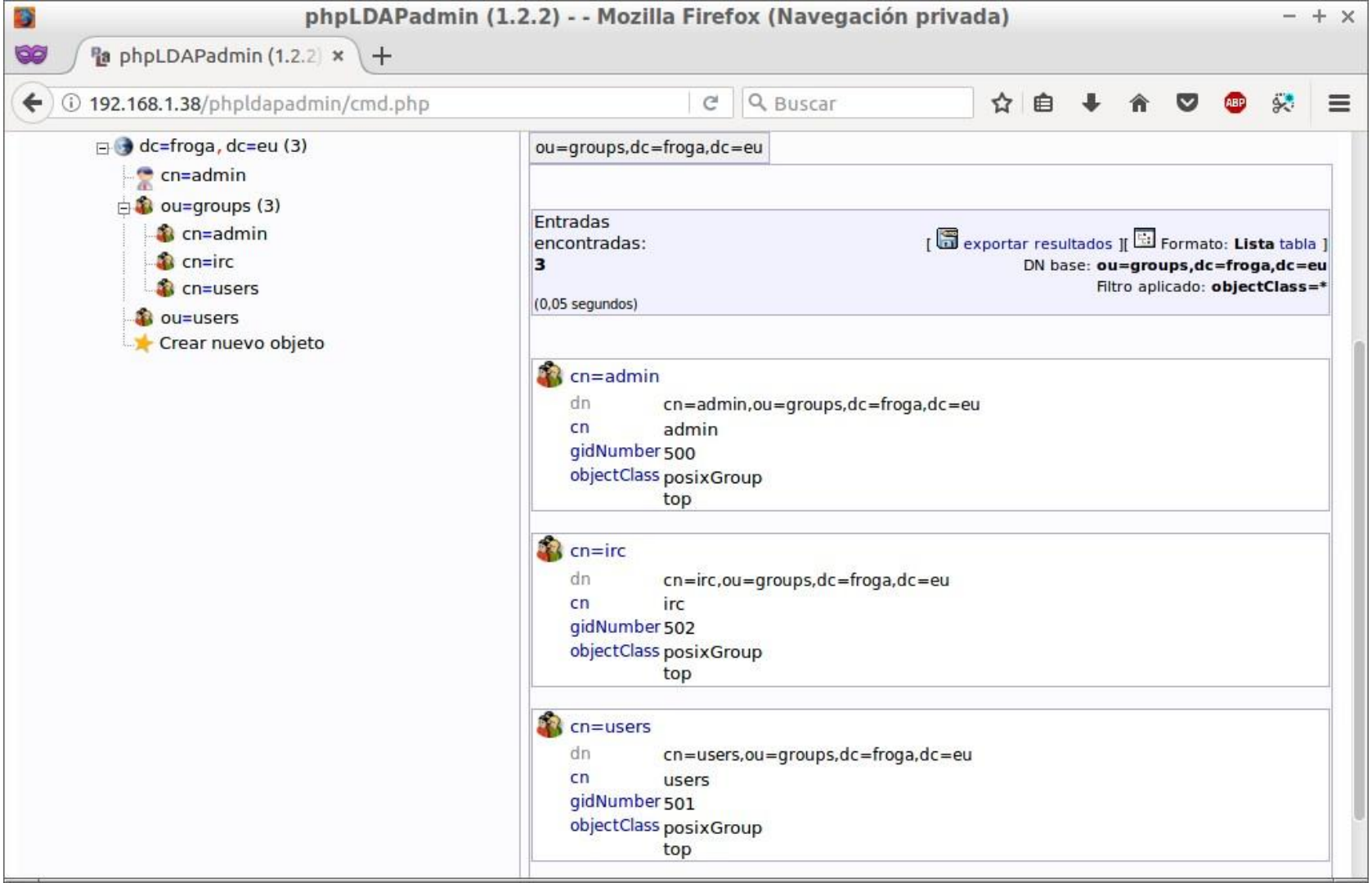




Panorámica de la Ciberseguridad… Protocolos de **Autenticación**

LDAP cn=admin,dc=froga,dc=eu




phpLDAPadmin (1.2.2) - - Mozilla Firefox (Navegación privada)
phpLDAPadmin (1.2.2)
192.168.1.38/phpldapadmin/cmd.php
Buscar
dc=froga, dc=eu (3)
cn=admin
ou=groups (3)
cn=admin
cn=irc
cn=users
ou=users
Crear nuevo objeto
ou=groups,dc=froga,dc=eu
Entradas encontradas: 3
(0,05 segundos)
[exportar resultados][Formato: Lista tabla]
DN base: ou=groups,dc=froga,dc=eu
Filtro aplicado: objectClass=*
cn=admin
dn cn=admin,ou=groups,dc=froga,dc=eu
cn admin
gidNumber 500
objectClass posixGroup
top
cn=irc
dn cn=irc,ou=groups,dc=froga,dc=eu
cn irc
gidNumber 502
objectClass posixGroup
top
cn=users
dn cn=users,ou=groups,dc=froga,dc=eu
cn users
gidNumber 501
objectClass posixGroup
top

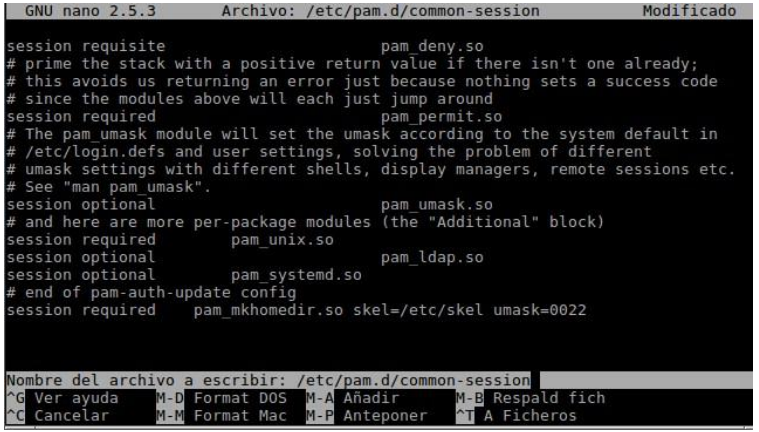
Panorámica de la Ciberseguridad… Protocolos de **Autenticación**

Cliente de **LDAP**

Paquetes **libpam-ldap** y **nscd**

```
sudo apt-get update
sudo apt-get install libpam-ldap nscd
sudo dpkg-reconfigure ldap-auth-config
sudo nano /etc/nsswitch.conf
```

Panorámica de la Ciberseguridad… Protocolos de **Autenticación**



Cliente de **LDAP**

Editamos el archivo /etc/pam.d/common-session:

```
sudo nano /etc/pam.d/common-session
```

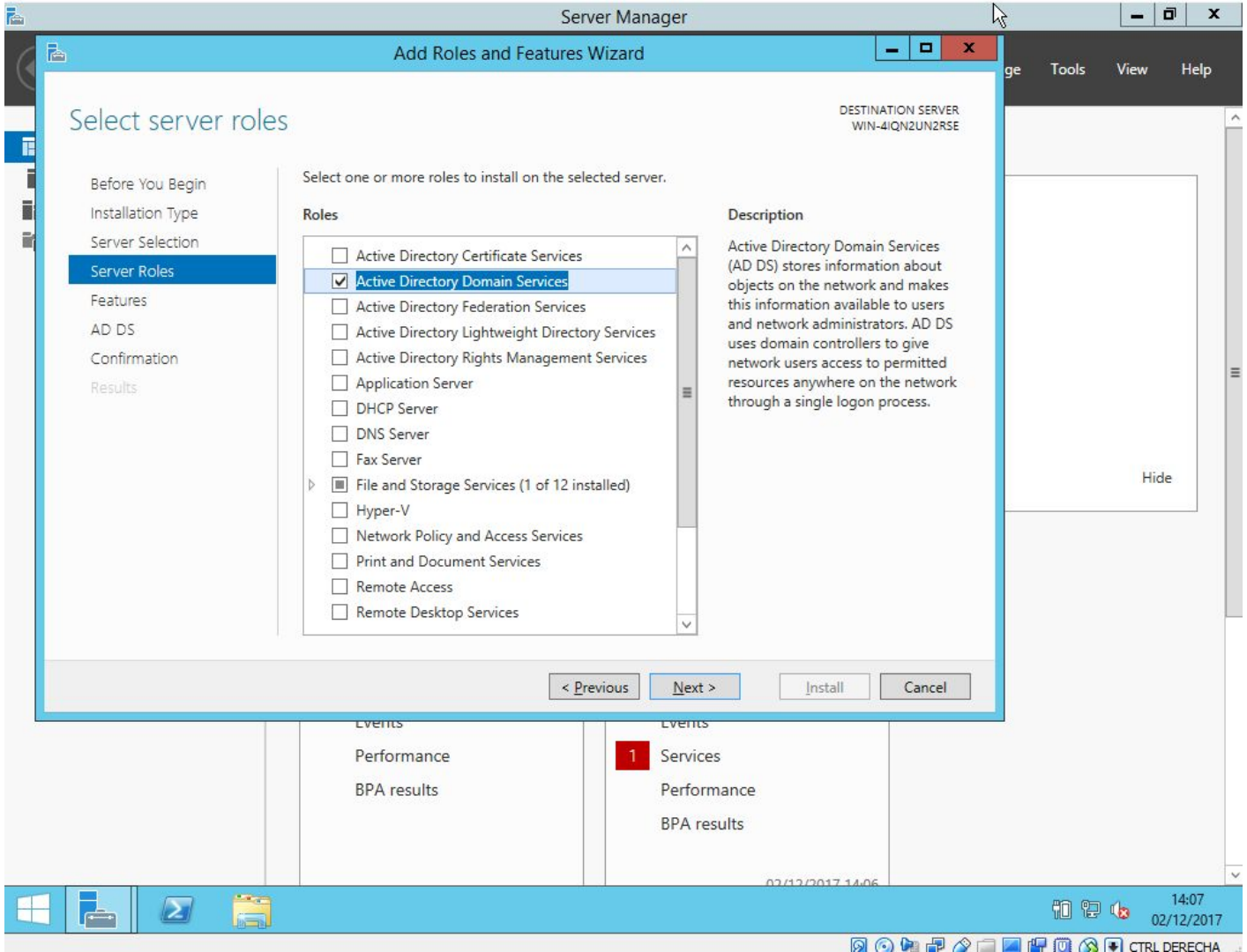
Y añadimos la siguiente línea al final del archivo:

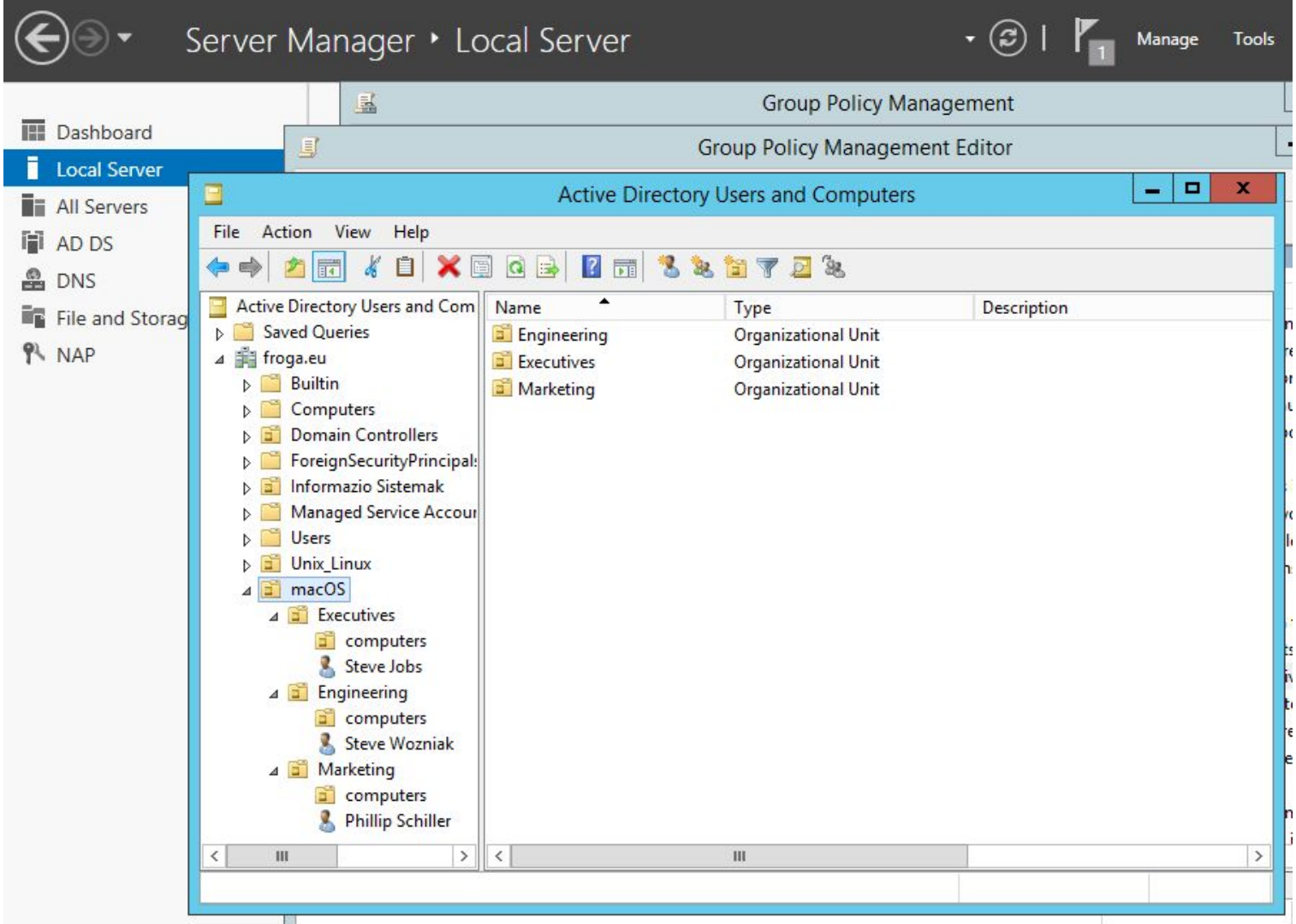
```
session required pam_mkhomedir.so skel=/etc/skel umask=0022
```

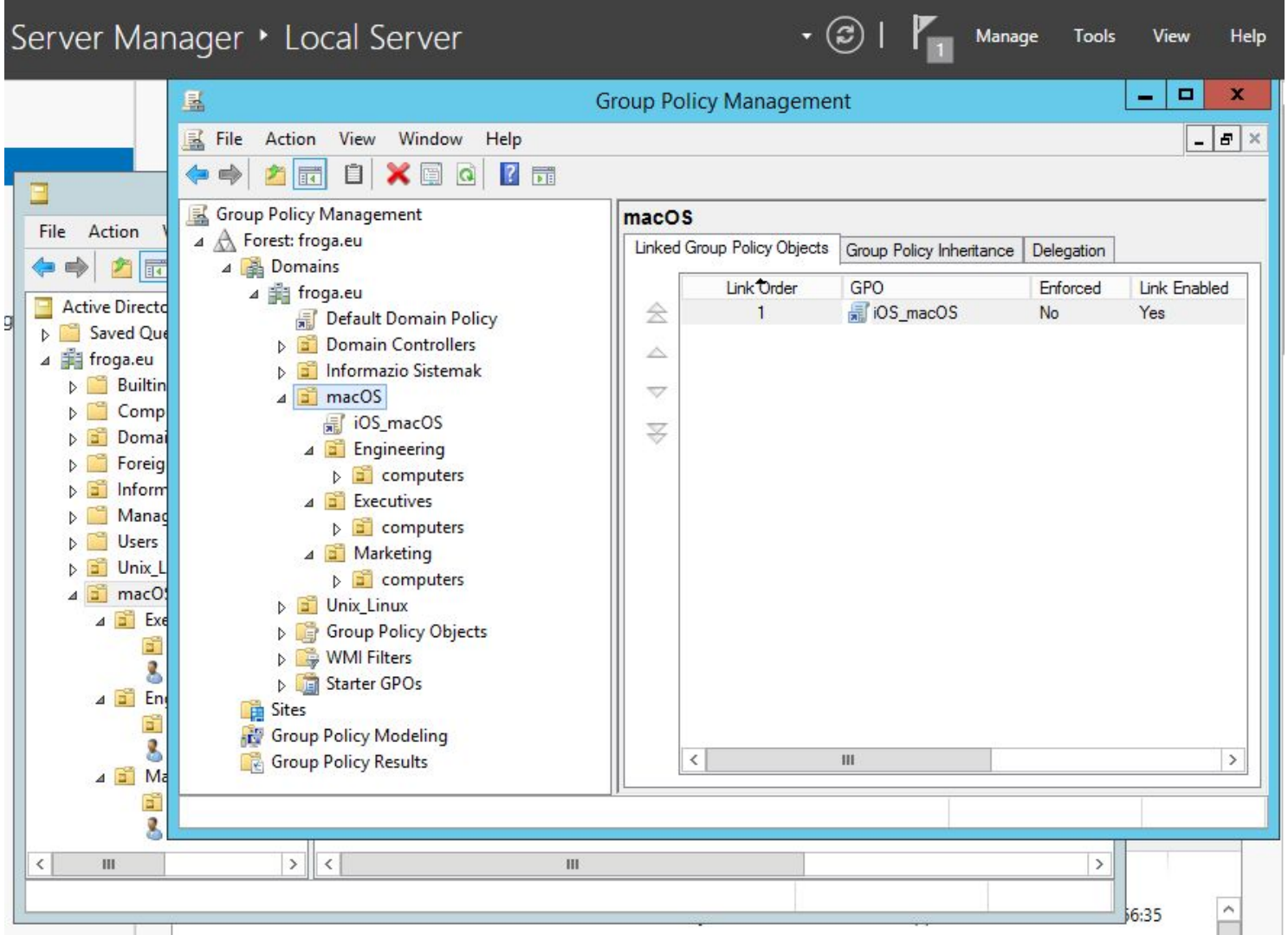
```
sudo /etc/init.d/nscd restart
```

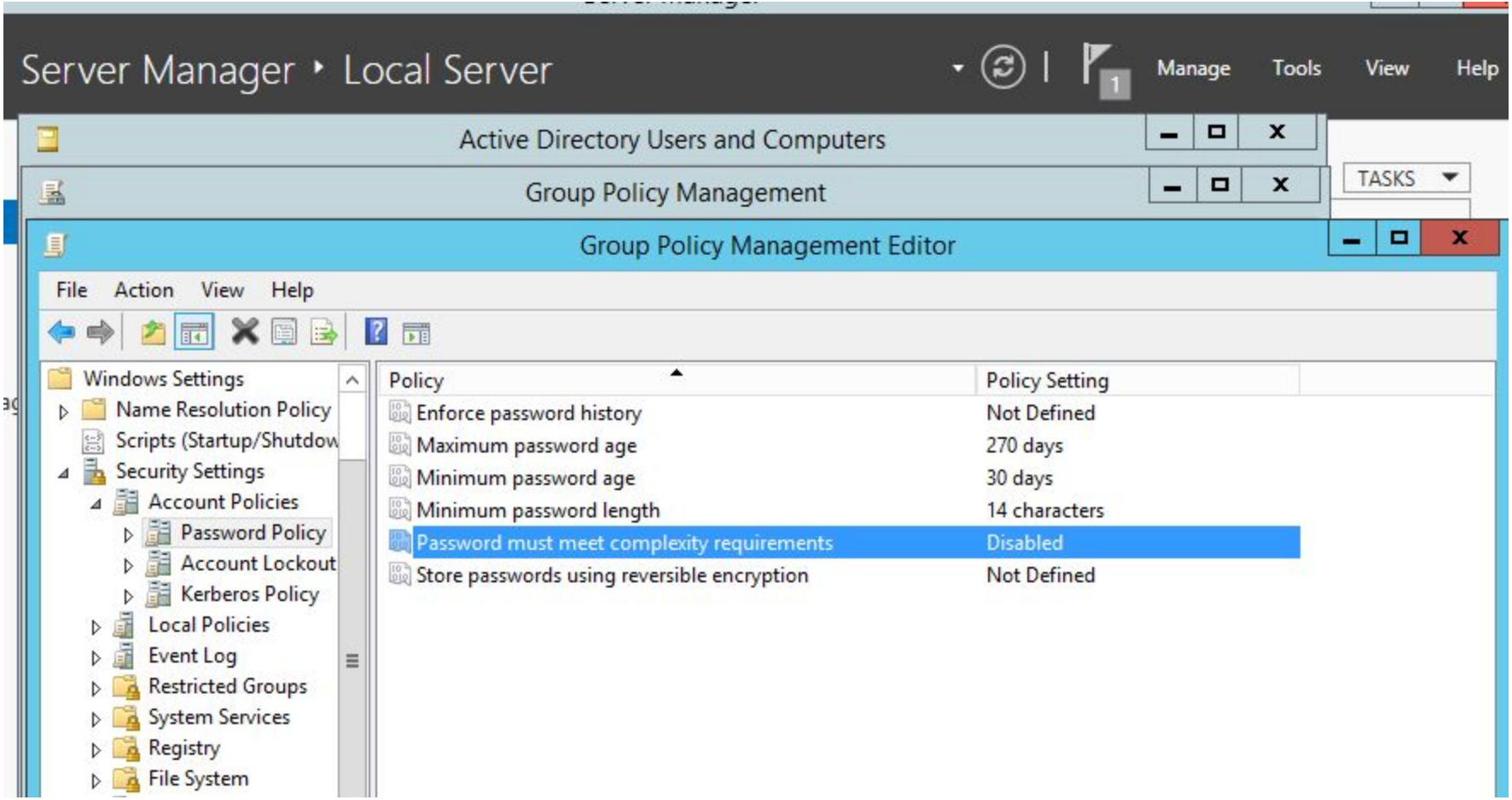
ARRANCANDO SESIÓN CON LDAP: `ssh LDAP_user@LDAP_client_IP_Address`

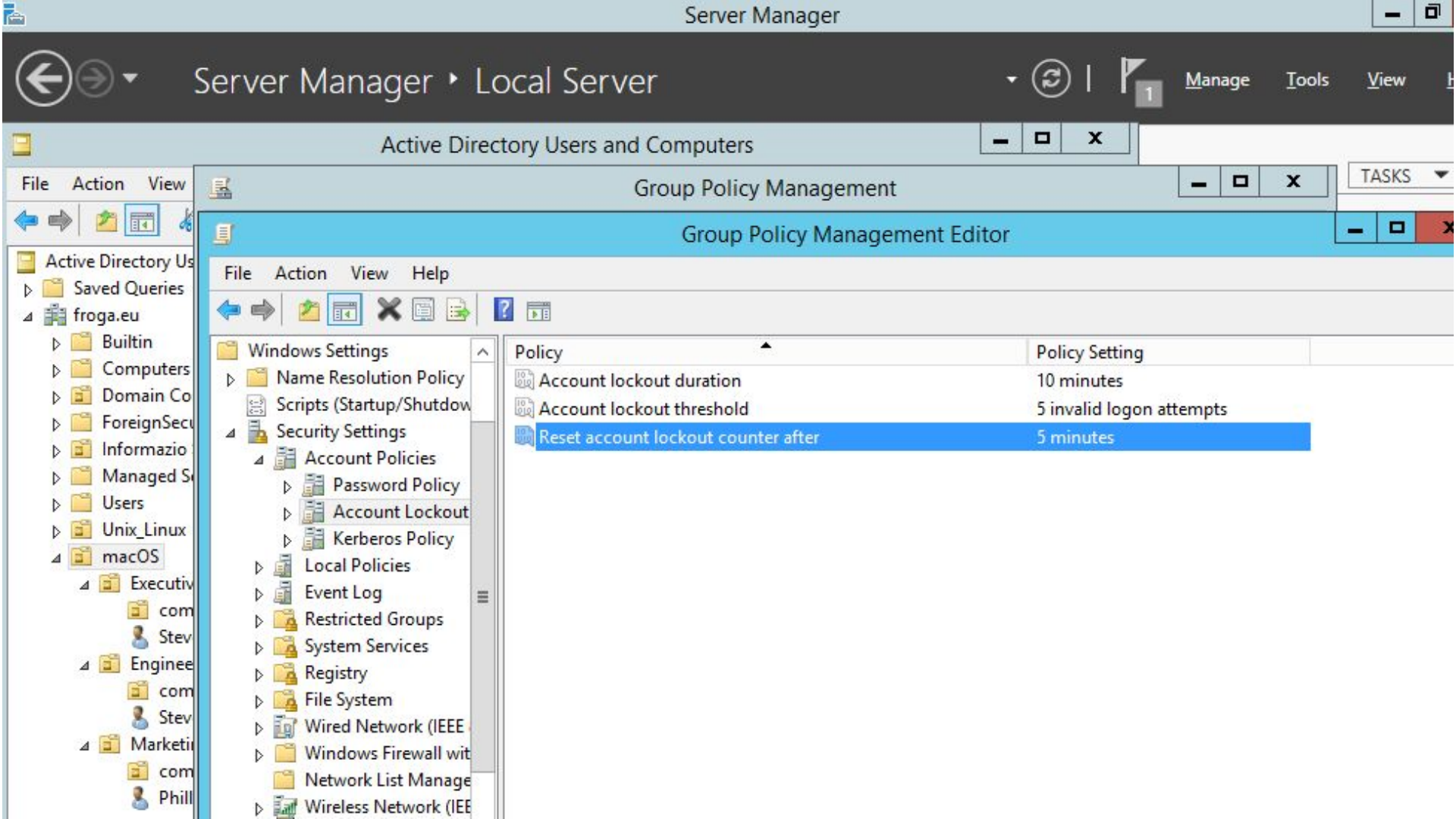
```
sudo apt-get install openssh-client openssh-server
```

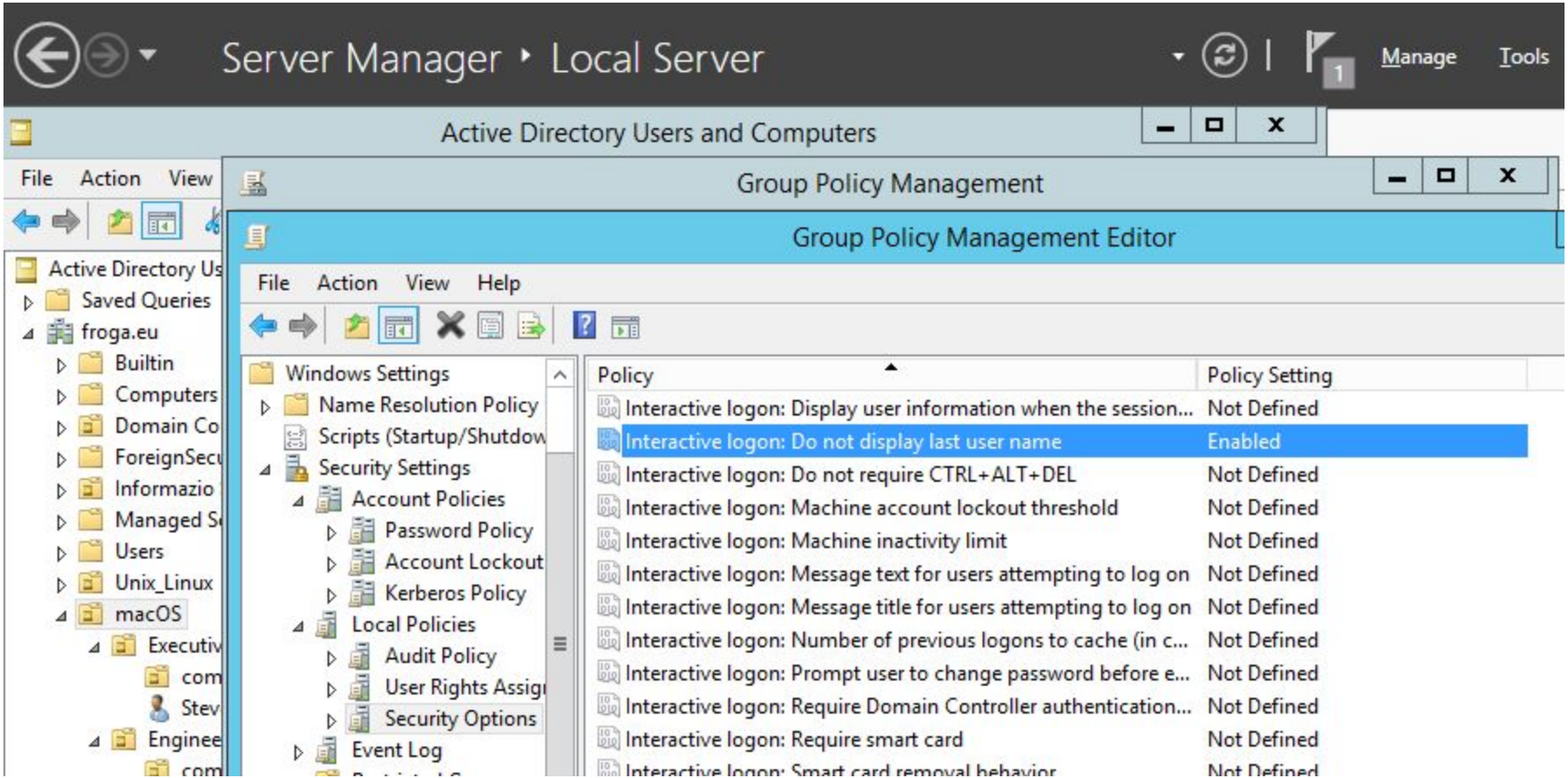

Server Manager
Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
WIN-4IQN2UN2RSE
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Application Server
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Hyper-V
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Description
Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.
< Previous
Next >
Install
Cancel
Tools
View
Help
Hide
Performance
BPA results
1
Services
Performance
BPA results
14:07
02/12/2017
CTRL DERECHA

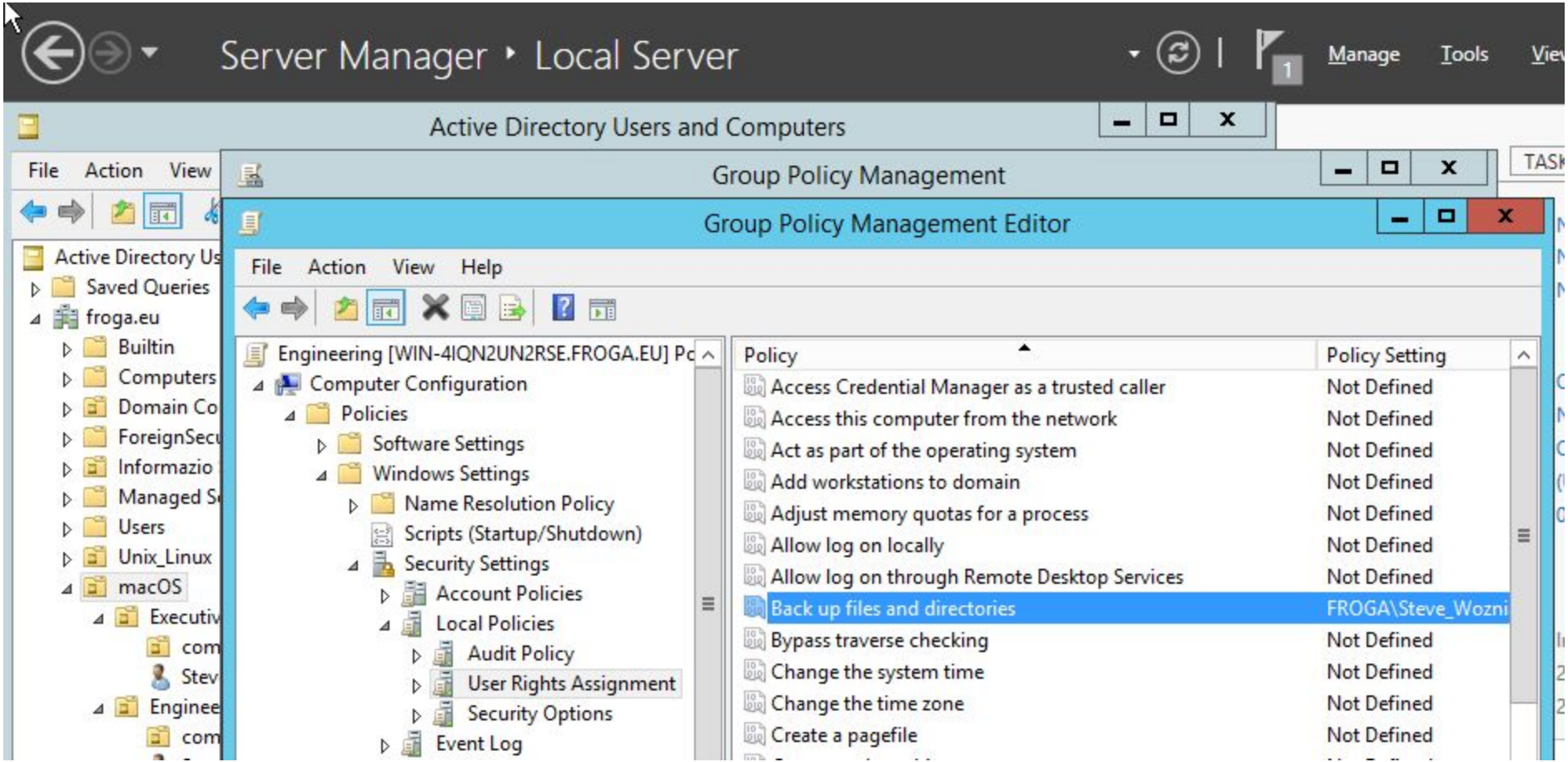

Server Manager • Local Server
Manage
Tools
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storag
NAP
Group Policy Management
Group Policy Management Editor
Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
froga.eu
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Informazio Sistemak
Managed Service Accour
Users
Unix_Linux
macOS
Executives
computers
Steve Jobs
Engineering
computers
Steve Wozniak
Marketing
computers
Phillip Schiller
Name
Type
Description
Engineering
Organizational Unit
Executives
Organizational Unit
Marketing
Organizational Unit

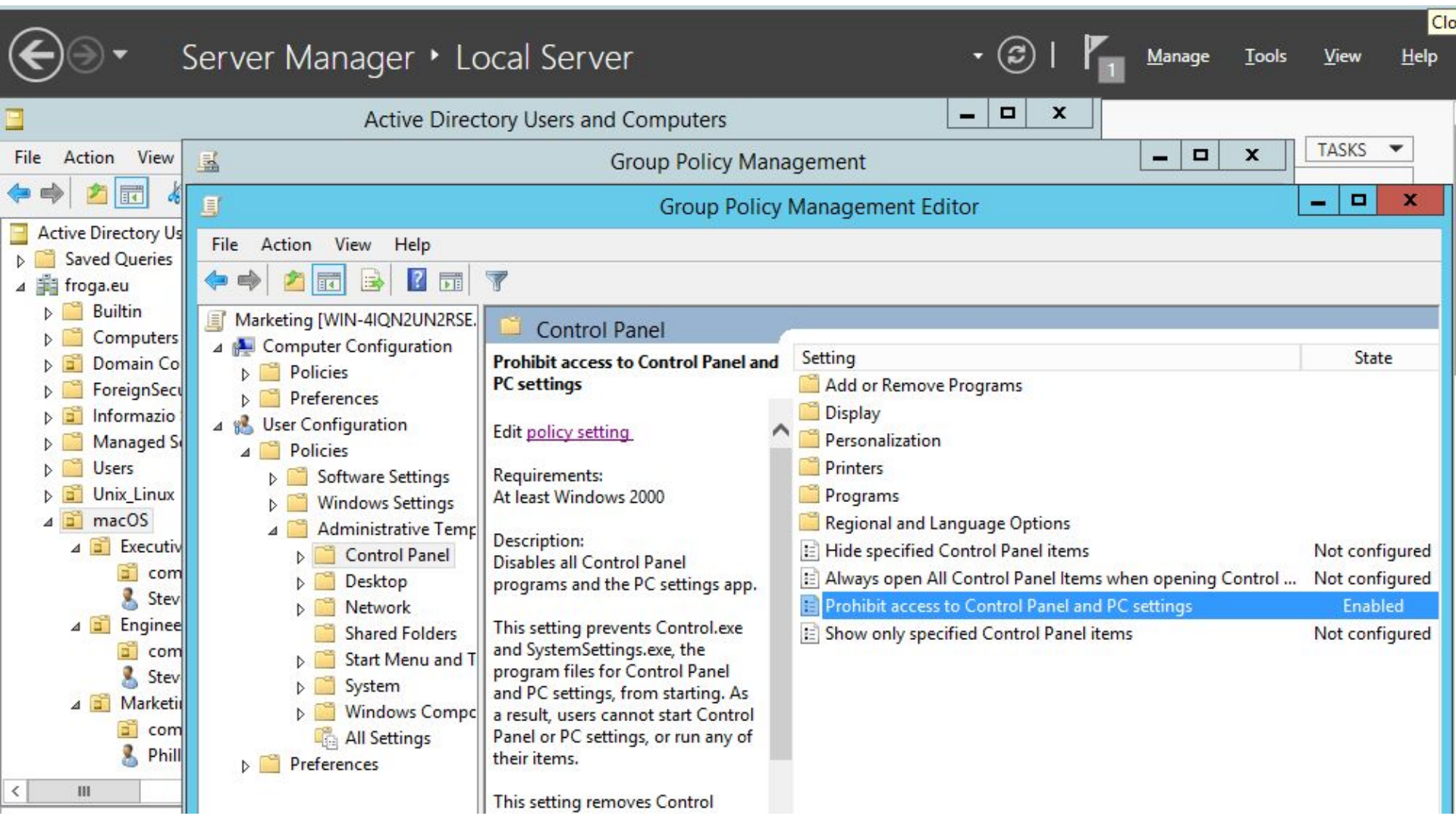

Server Manager ‣ Local Server
Manage
Tools
View
Help
Group Policy Management
File
Action
View
Window
Help
Group Policy Management
Forest: froga.eu
Domains
froga.eu
Default Domain Policy
Domain Controllers
Informazio Sistemak
macOS
iOS_macOS
Engineering
computers
Executives
computers
Marketing
computers
Unix_Linux
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
macOS
Linked Group Policy Objects
Group Policy Inheritance
Delegation
Link Order
GPO
Enforced
Link Enabled
1
iOS_macOS
No
Yes

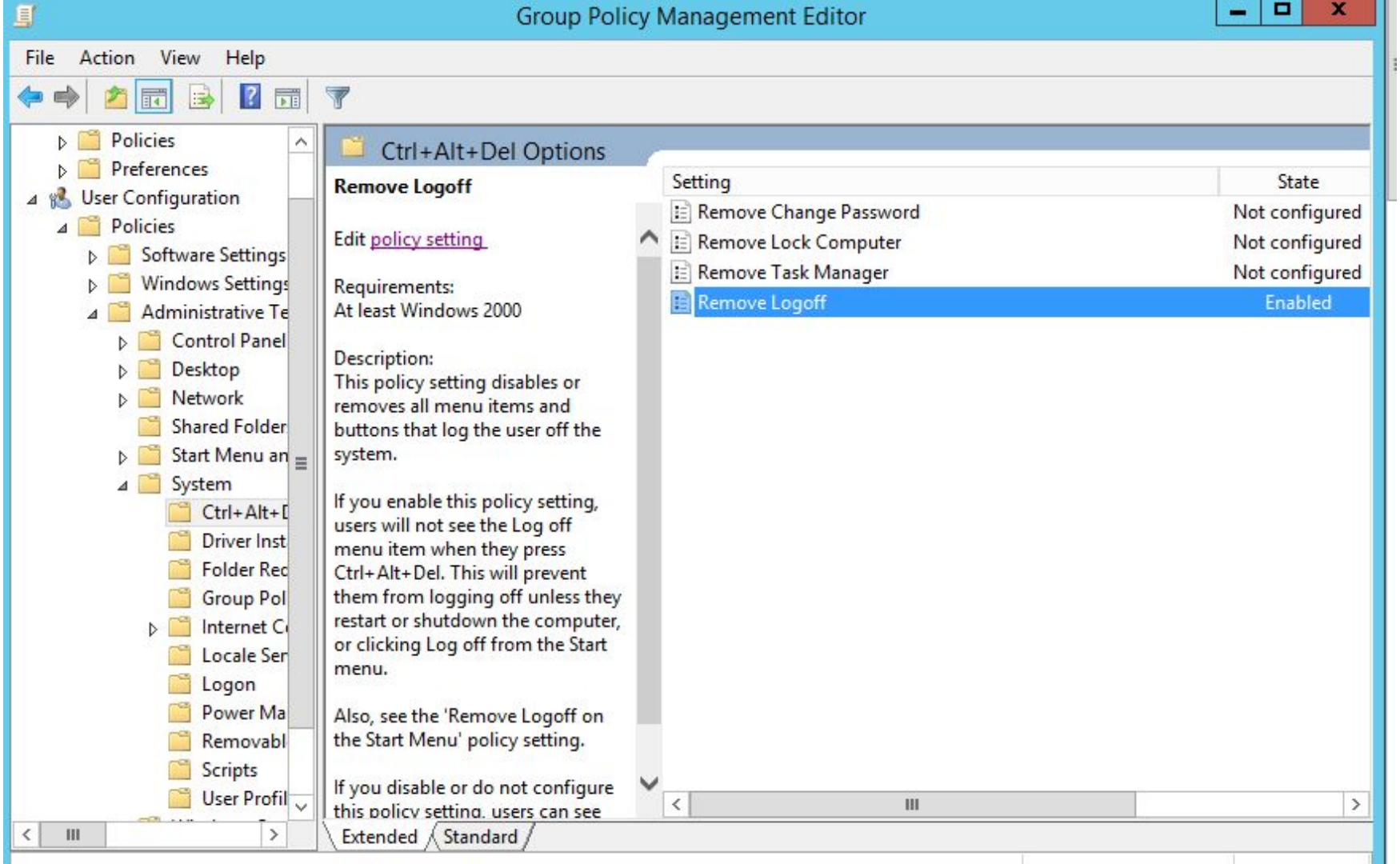

Server Manager ‣ Local Server
Manage
Tools
View
Help
Active Directory Users and Computers
Group Policy Management
TASKS
Group Policy Management Editor
File
Action
View
Help
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdow
Security Settings
Account Policies
Password Policy
Account Lockout
Kerberos Policy
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Policy
Policy Setting
Enforce password history
Not Defined
Maximum password age
270 days
Minimum password age
30 days
Minimum password length
14 characters
Password must meet complexity requirements
Disabled
Store passwords using reversible encryption
Not Defined

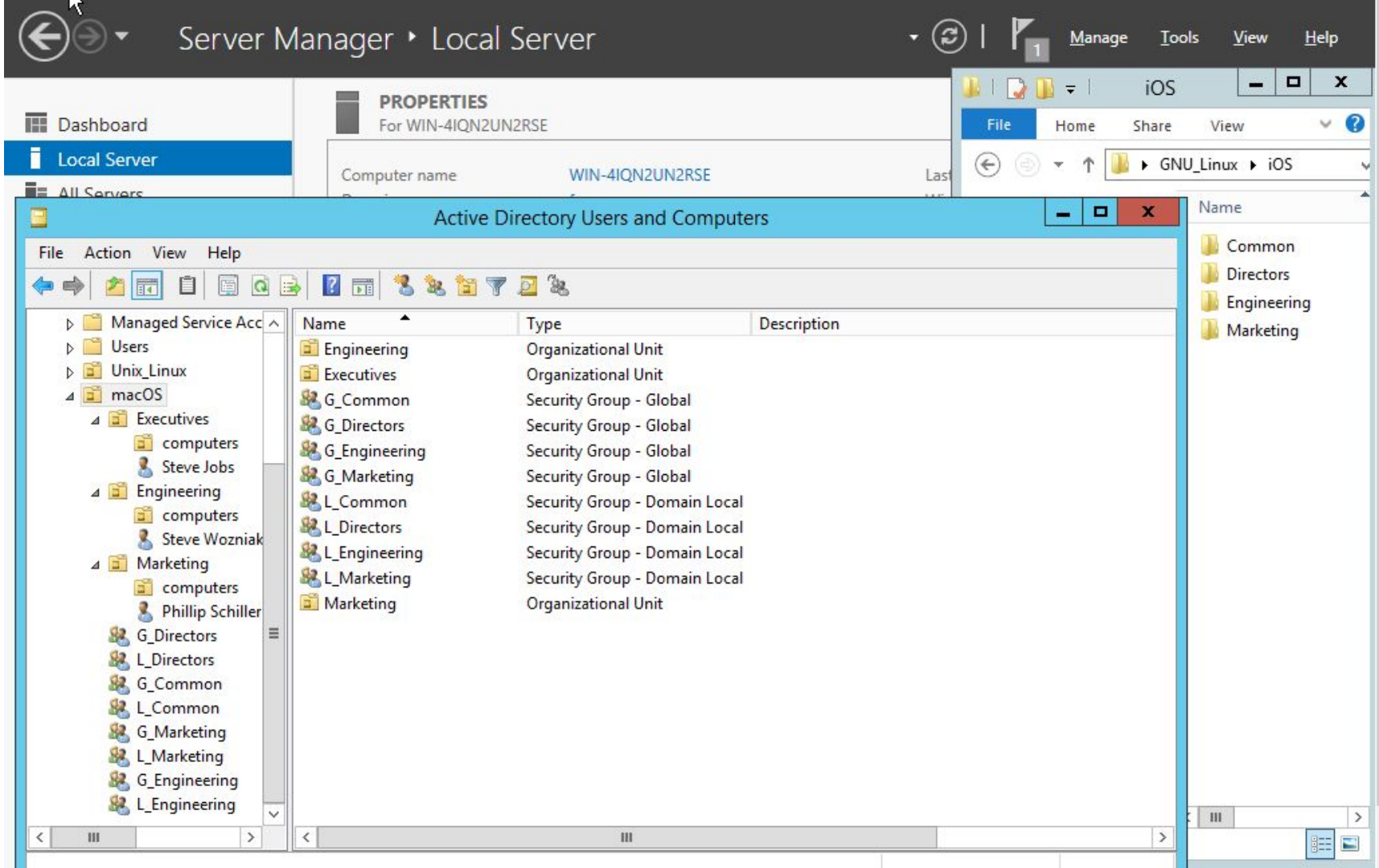

Server Manager
Server Manager ‣ Local Server
Manage
Tools
View
Active Directory Users and Computers
File
Action
View
Active Directory Us
Saved Queries
froga.eu
Builtin
Computers
Domain Co
ForeignSecu
Informazio
Managed S
Users
Unix_Linux
macOS
Executiv
com
Stev
Enginee
com
Stev
Marketi
com
Phill
Group Policy Management
TASKS
Group Policy Management Editor
File
Action
View
Help
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdow
Security Settings
Account Policies
Password Policy
Account Lockout
Kerberos Policy
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE
Windows Firewall wit
Network List Manage
Wireless Network (IEE
Policy
Policy Setting
Account lockout duration
10 minutes
Account lockout threshold
5 invalid logon attempts
Reset account lockout counter after
5 minutes


Server Manager ‣ Local Server
Manage
Tools
Active Directory Users and Computers
File
Action
View
Active Directory Us
Saved Queries
froga.eu
Builtin
Computers
Domain Co
ForeignSecu
Informazio
Managed S
Users
Unix_Linux
macOS
Executiv
com
Stev
Enginee
com
Group Policy Management
Group Policy Management Editor
File
Action
View
Help
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdow
Security Settings
Account Policies
Password Policy
Account Lockout
Kerberos Policy
Local Policies
Audit Policy
User Rights Assig
Security Options
Event Log
Policy
Policy Setting
Interactive logon: Display user information when the session...
Not Defined
Interactive logon: Do not display last user name
Enabled
Interactive logon: Do not require CTRL+ALT+DEL
Not Defined
Interactive logon: Machine account lockout threshold
Not Defined
Interactive logon: Machine inactivity limit
Not Defined
Interactive logon: Message text for users attempting to log on
Not Defined
Interactive logon: Message title for users attempting to log on
Not Defined
Interactive logon: Number of previous logons to cache (in c...
Not Defined
Interactive logon: Prompt user to change password before e...
Not Defined
Interactive logon: Require Domain Controller authentication...
Not Defined
Interactive logon: Require smart card
Not Defined


Server Manager ‣ Local Server
Manage
Tools
Active Directory Users and Computers
File Action View
Group Policy Management
Group Policy Management Editor
File Action View Help
Active Directory Us
Saved Queries
froga.eu
Builtin
Computers
Domain Co
ForeignSecu
Informazio
Managed S
Users
Unix_Linux
macOS
Executiv
com
Stev
Enginee
com
Engineering [WIN-4IQN2UN2RSE.FROGA.EU] Pc
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Policy
Policy Setting
Access Credential Manager as a trusted caller
Not Defined
Access this computer from the network
Not Defined
Act as part of the operating system
Not Defined
Add workstations to domain
Not Defined
Adjust memory quotas for a process
Not Defined
Allow log on locally
Not Defined
Allow log on through Remote Desktop Services
Not Defined
Back up files and directories
FROGA\Steve_Wozni
Bypass traverse checking
Not Defined
Change the system time
Not Defined
Change the time zone
Not Defined
Create a pagefile
Not Defined


Server Manager ‣ Local Server
Manage
Tools
View
Help
Active Directory Users and Computers
File
Action
View
Group Policy Management
TASKS
Group Policy Management Editor
File
Action
View
Help
Active Directory Us
Saved Queries
froga.eu
Builtin
Computers
Domain Co
ForeignSecu
Informazio
Managed S
Users
Unix_Linux
macOS
Executiv
com
Stev
Enginee
com
Stev
Marketi
com
Phill
Marketing [WIN-4IQN2UN2RSE.
Computer Configuration
Policies
Preferences
User Configuration
Policies
Software Settings
Windows Settings
Administrative Temp
Control Panel
Desktop
Network
Shared Folders
Start Menu and T
System
Windows Compc
All Settings
Preferences
Control Panel
Prohibit access to Control Panel and PC settings
Edit policy setting
Requirements:
At least Windows 2000
Description:
Disables all Control Panel programs and the PC settings app.
This setting prevents Control.exe and SystemSettings.exe, the program files for Control Panel and PC settings, from starting. As a result, users cannot start Control Panel or PC settings, or run any of their items.
This setting removes Control
Setting
State
Add or Remove Programs
Display
Personalization
Printers
Programs
Regional and Language Options
Hide specified Control Panel items
Not configured
Always open All Control Panel Items when opening Control ...
Not configured
Prohibit access to Control Panel and PC settings
Enabled
Show only specified Control Panel items
Not configured


Group Policy Management Editor
File
Action
View
Help
Policies
Preferences
User Configuration
Policies
Software Settings
Windows Settings
Administrative Te
Control Panel
Desktop
Network
Shared Folder
Start Menu an
System
Ctrl+Alt+D
Driver Inst
Folder Rec
Group Pol
Internet C
Locale Ser
Logon
Power Ma
Removabl
Scripts
User Profil
Ctrl+Alt+Del Options
Remove Logoff
Edit policy setting
Requirements:
At least Windows 2000
Description:
This policy setting disables or removes all menu items and buttons that log the user off the system.
If you enable this policy setting, users will not see the Log off menu item when they press Ctrl+Alt+Del. This will prevent them from logging off unless they restart or shutdown the computer, or clicking Log off from the Start menu.
Also, see the 'Remove Logoff on the Start Menu' policy setting.
If you disable or do not configure
Setting
State
Remove Change Password
Not configured
Remove Lock Computer
Not configured
Remove Task Manager
Not configured
Remove Logoff
Enabled
Extended
Standard


Server Manager ▸ Local Server
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
PROPERTIES
For WIN-4IQN2UN2RSE
Computer name
WIN-4IQN2UN2RSE
iOS
File
Home
Share
View
GNU_Linux ▸ iOS
Name
Common
Directors
Engineering
Marketing
Active Directory Users and Computers
File
Action
View
Help
Managed Service Acc
Users
Unix_Linux
macOS
Executives
computers
Steve Jobs
Engineering
computers
Steve Wozniak
Marketing
computers
Phillip Schiller
G_Directors
L_Directors
G_Common
L_Common
G_Marketing
L_Marketing
G_Engineering
L_Engineering
Name
Type
Description
Engineering
Organizational Unit
Executives
Organizational Unit
G_Common
Security Group - Global
G_Directors
Security Group - Global
G_Engineering
Security Group - Global
G_Marketing
Security Group - Global
L_Common
Security Group - Domain Local
L_Directors
Security Group - Domain Local
L_Engineering
Security Group - Domain Local
L_Marketing
Security Group - Domain Local
Marketing
Organizational Unit

FORMACIÓN

CURSO DE ZENTYAL SERVER

El Curso on-line "Zentyal para Administradores de Redes" es un curso intermedio dirigido a profesionales informáticos con experiencia en gestión de redes en pequeñas y medianas empresas (pymes). Al terminar este curso de 40 horas, los alumnos serán capaces de desplegar Zentyal como servidor de dominio & directorio, servidor de correo, gateway y servidor de infraestructura en un entorno pyme. Este curso encaja perfectamente para administradores de Windows interesados en aprender gestión de redes y usuarios basada en Linux.

COMPRAR CURSO 495€

VER MÁS

MANUAL DE ZENTYAL SERVER

El libro "Zentyal para Administradores de Redes" es una guía ideal para los que están interesados en usar Servidor Zentyal, o servidores Linux en general, en entornos pyme. El libro cubre todos los aspectos más relevantes de configuración y administración de servidores Zentyal en un entorno pyme, desde la arquitectura de Zentyal hasta todos los servicios de red requeridos por este tipo de entornos así como buenas prácticas para el mantenimiento efectivo y seguro de una red informática.

COMPRAR LIBRO 51,35

COMPRAR E-BOOK 31,41€

¿TIENES ALGUNA DUDA? SIMPLEMENTE CONTACTA CON NOSOTROS

ZENTYAL, EL SERVIDOR LINUX PARA PYMES

EL SERVIDOR LOCAL DE CORREO Y DIRECTORIO

PRUEBA EL SERVIDOR ZENTYAL DURANTE 45 DÍAS

DIRECTORY & DOMAIN SERVER

Ofrece compatibilidad nativa con Microsoft Active Directory® , permitiendo unir al dominio y gestionar clientes Microsoft® de forma sencilla.

MAIL SERVER

Ofrece un servidor de correo, junto con webmail y sincronización con dispositivos móviles via ActiveSync.

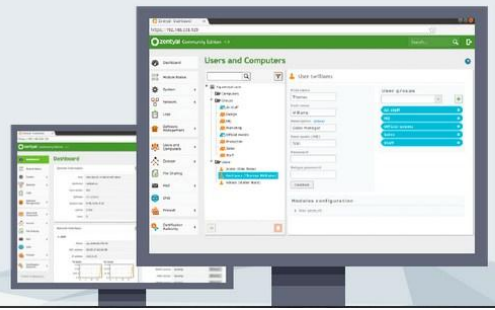
GATEWAY

Ofrece acceso fiable y seguro a Internet a la vez que ayuda a gestionar el tráfico y acelerar la navegación.

INFRASTRUCTURE SERVER

Permite gestionar de forma fácil y unificada toda la infraestructura básica de red.

SOLICITA UNA OFERTA



CARACTERÍSTICAS TÉCNICAS

Domain & Directory

- Gestión central del dominio y directorio
- Usuarios, Grupos de seguridad, Listas de Distribución, Contactos
- Múltiples Unidades Organizativas (OUs), Objetos de Directiva de Grupo (GPOs)
- Scripts NETLOGON, Perfiles móviles
- Autenticación Single Sign-On (SSO)
- SO soportados: Windows® XP/Vista/7/8/10
- Compartición de ficheros en entornos Windows® (CIFS)
- Permisos de acceso y modificación de Usuarios & Grupos (ACLs)
- Gestión de fotos de perfil
- **Software integrado:** Samba

Mail

- Protocolos soportados: SMTP, POP3, IMAP, CalDAV, CardDAV, SIEVE
- Clientes soportados: Mozilla Thunderbird®
- Webmail
- Sincronización con dispositivos móviles via ActiveSync
- Múltiples dominios virtuales de correo
- Autenticación Single Sign-On (SSO)
- Administración a través de Zentyal o Microsoft ® Active Directory
- Antivirus & Mail filter
- **Software integrado:** Postfix, Dovecot, Fetchmail, Sieve, SOGo, SOGo ActiveSync, Amavis, ClamAV, SpamAssasin

Gateway

- Configuración de red
- Encaminamiento
- Gateway
- Cortafuegos
- Proxy HTTP
- IDS/IPS
- Servicio de autenticación de red (RADIUS)
- Bloqueo de páginas web HTTPS basado en dominio
- Autenticación de usuarios en HTTP Proxy
- **Software integrado:** Iproute2, Netfilter, Squid, Suricata, FreeRADIUS

Infrastructure

- Servidor DHCP, DNS
- Servidor NTP
- Autoridad de Certificación (CA)
- Redes Privadas Virtuales (VPNs)
- Servicio de Mensajería Instantánea (IM)
- Servidor FTP
- IPSec/L2TP
- Virtualization Manager
- Antivirus con análisis de ficheros en acceso
- Backup
- **Software integrado:** BIND, ISC DHCP Software, ntpd, OpenSSL, OpenVPN, ejabbered, vsftpd, Libreswan, Libvirt/KVM, Duplicity

Soporte Técnico

- Actualizaciones de software y de seguridad
- Actualizaciones entre versiones
- Acceso a la base de conocimiento
- Soporte técnico

Software integrado: Samba, Postfix, Dovecot, Fetchmail, Sieve, SOGo, SOGo ActiveSync, Amavis, ClamAV, SpamAssasin, Iproute2, Netfilter, Squid, Suricata, FreeRADIUS, BIND, ISC DHCP Software, ntpd, OpenSSL, OpenVPN, ejabbered, vsftpd, Libreswan, Libvirt/KVM, Duplicity

ZENTYAL

SERVIDOR LINUX PARA PYMES

SOLICITA TRIAL GRATUITO

SERVIDOR DE DIRECTORIO & DOMINIO

Compatibilidad nativa con Microsoft Active Directory®.

SERVIDOR DE CORREO

Servidor de correo, webmail y sincronización con dispositivos móviles.

CORTAFUEGOS & INFRAESTRUCTURA

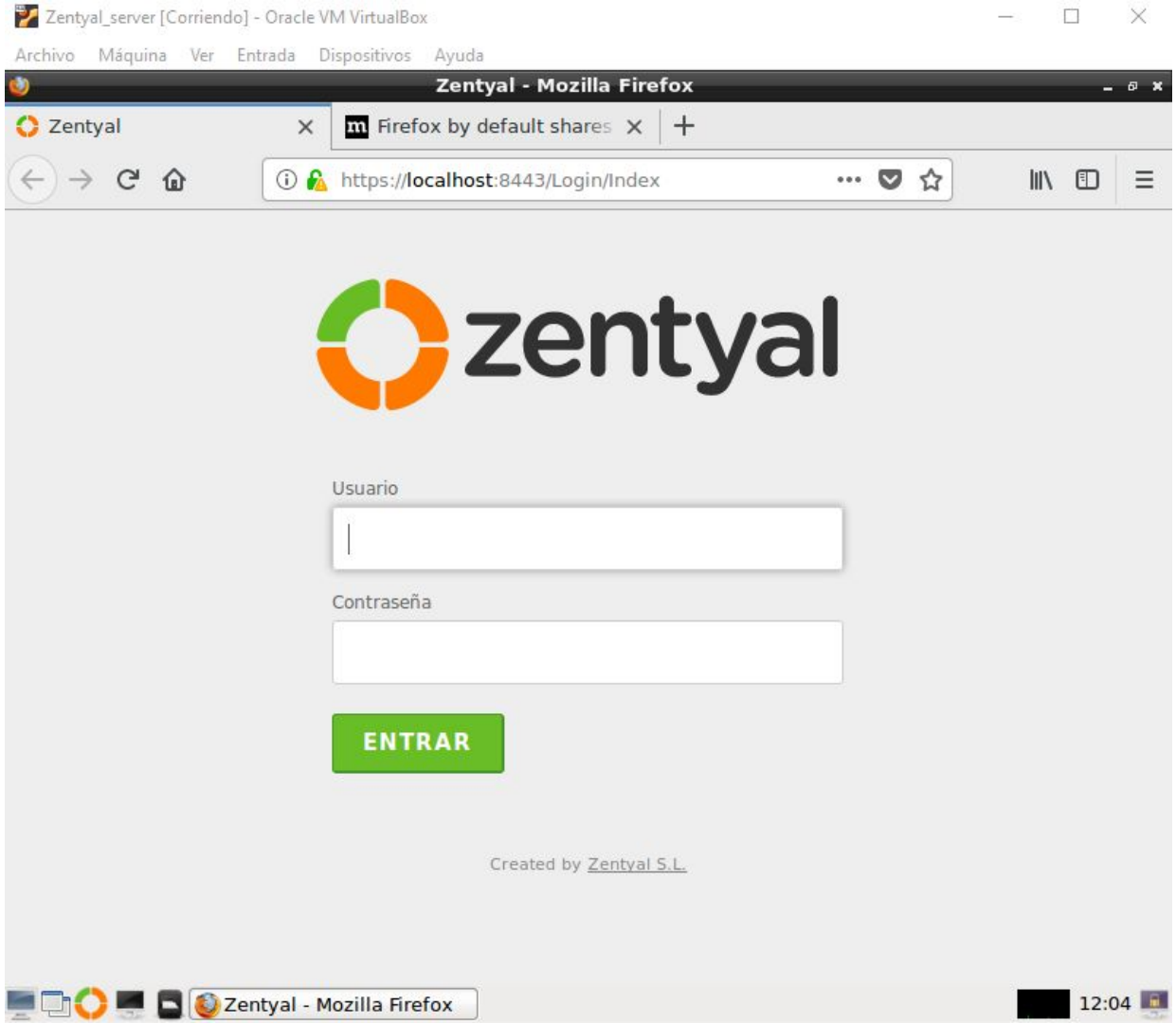
Acceso fiable y seguro a Internet y servidor de infraestructura.

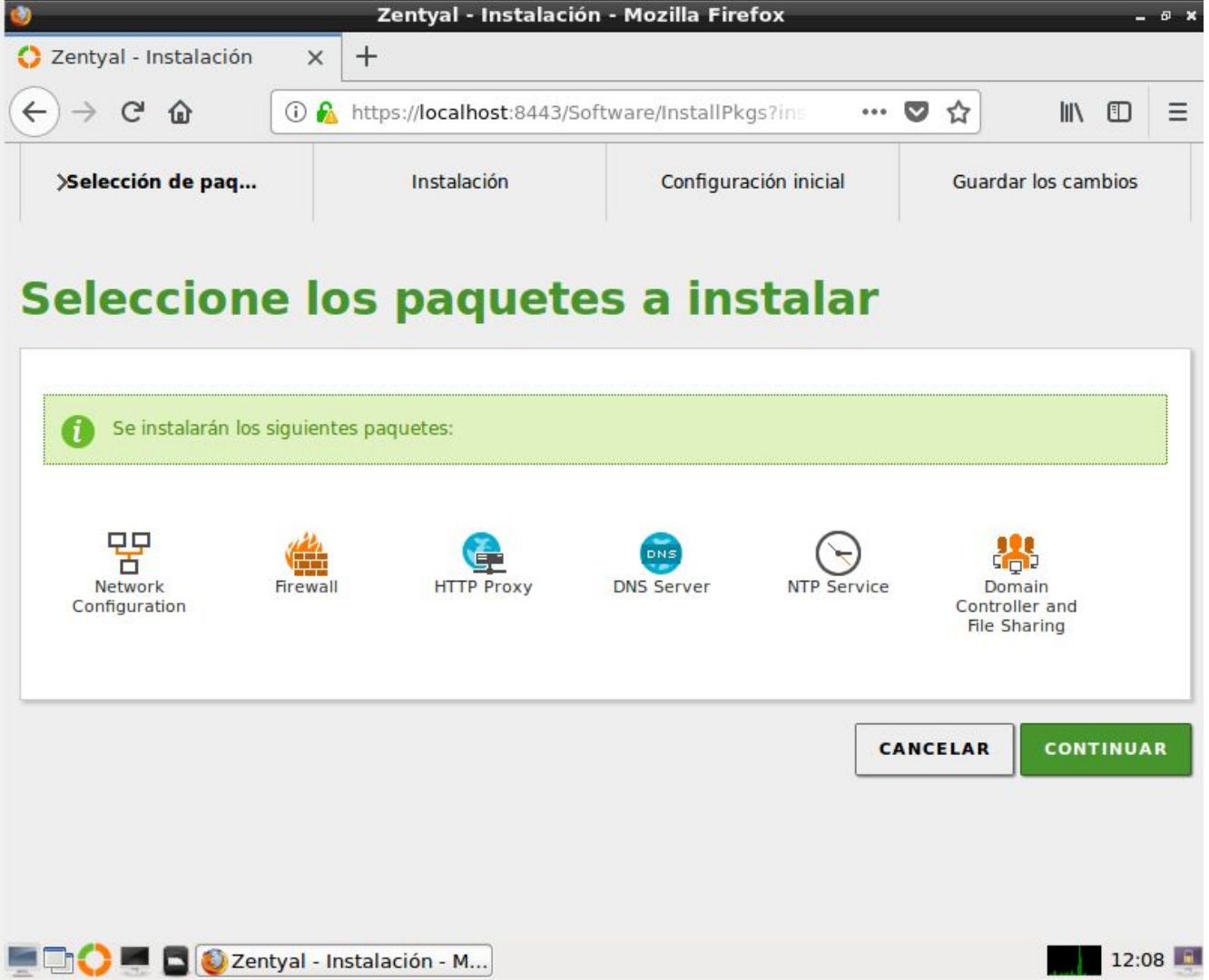
ZENTYAL 6.0 DISPONIBLE

PRUEBA EL TRIAL GRATUITO DURANTE 45 DÍAS

- Basada en Ubuntu 18.04.1 LTS
- Backup
- Autenticación de usuarios en HTTP Proxy
- Servicio de autenticación de red (RADIUS)
- Gestión de máquinas virtuales


Consola de Administrador
Consola de Usuario
Panel de control Zentyal
zentyal
[Zentyal - Mozilla Firefox]
12:05


Zentyal_server [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Zentyal - Mozilla Firefox
Zentyal
Firefox by default shares
https://localhost:8443/Login/Index
zentyal
Usuario
Contraseña
ENTRAR
Created by Zentyal S.L.
Zentyal - Mozilla Firefox
12:04


Zentyal - Instalación - Mozilla Firefox
Zentyal - Instalación
https://localhost:8443/Software/InstallPkgs?ins
Selección de paq...
Instalación
Configuración inicial
Guardar los cambios
Seleccione los paquetes a instalar
Se instalarán los siguientes paquetes:
Network Configuration
Firewall
HTTP Proxy
DNS Server
NTP Service
Domain Controller and File Sharing
CANCELAR
CONTINUAR
Zentyal - Instalación - M...
12:08

https://localhost:8443/Software/InstallPk

¡Gracias por elegir Zentyal Server!

Zentyal Server implementa los protocolos de Microsoft Active Directory® en Linux de forma nativa. ¿Buscas una versión experimental para probar el producto? ¡Zentyal Server Development Edition es para ti! Si buscas una versión para tu entorno de produción, elige la edición comercial.

Para obtener ayuda de la comunidad, echa un vistazo a la documentación oficial y al Foro Oficial de Zentyal!

http://wiki.zentyal.org/

http://forum.zentyal.org

Instalando paquetes

Operación actual: **Setting up adzapper (20090301.dfsg.1-0.2) ...**

81%

193 de 240 operaciones realizadas

Zentyal - Mozilla Firefox | [mu-sec@zentyal: ~] | 12:12

Edición Comercial de Zentyal

¡Lista para usar en un entorno de produción!

- Soporte técnico oficial
- Completamente verificado y estable
- Aseguramiento de calidad sobre las actualizaciones
- Soportada durante 4.5 años

¡Pide tu trial gratuito en www.zentyal.com/es/zentyal-server!

Instalando paquetes

Operación actual: **Setting up krb5-config (2.3) ...**

86%

206 de 240 operaciones realizadas

Zentyal - Mozilla Firefox [mu-sec@zentyal: ~] 12:12

Zentyal - Asistente de co

https://localhost:8443/Wizard

Asistente de configuración inicial

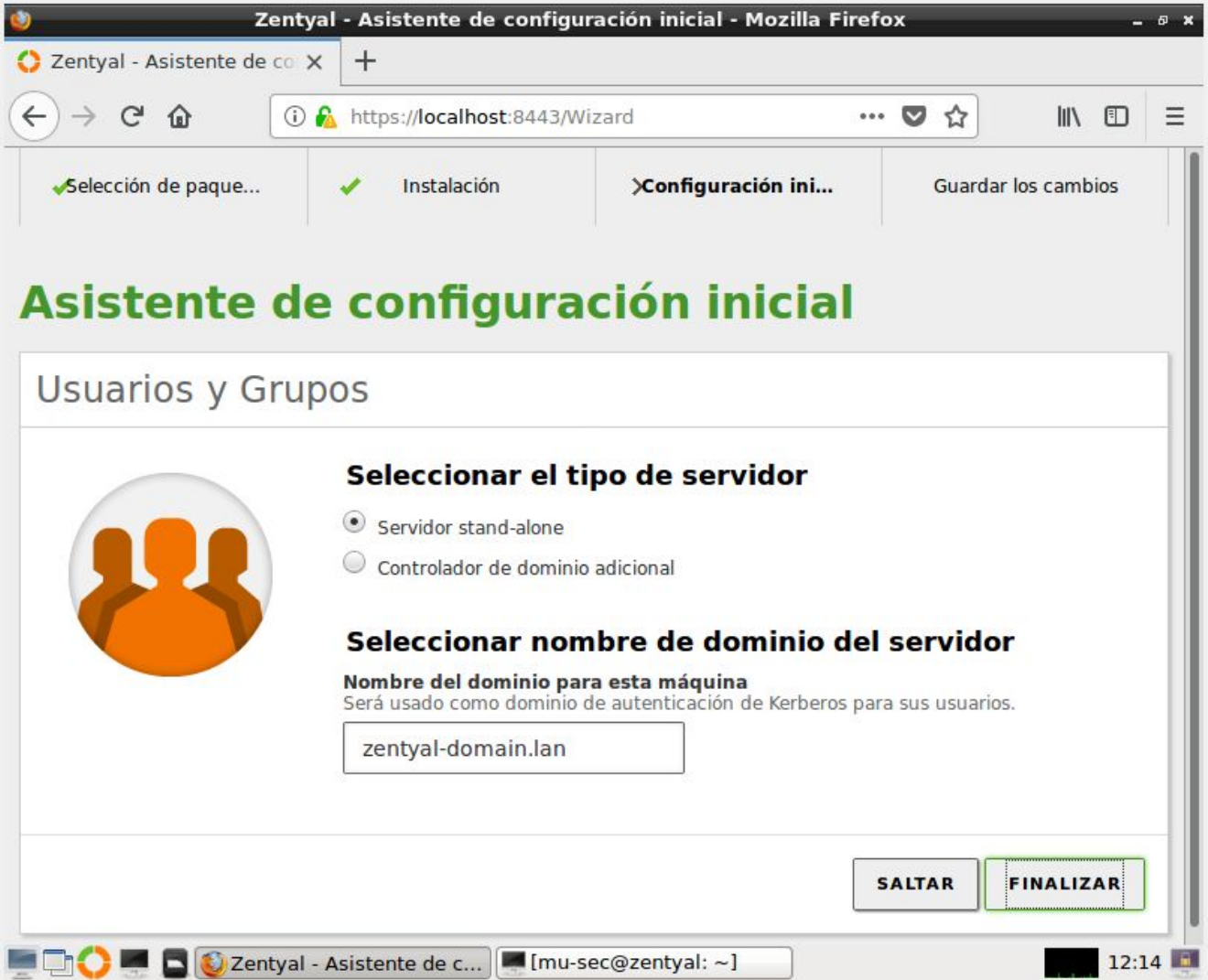
Interfaces de Red

Configurar tipos de interfaces

Las interfaces externas conectan con redes que no están bajo tu control (generalmente Internet), el tráfico proveniente de estas redes se considera no fiable por defecto, por lo que no será posible acceder a la interfaz de administración de Zentyal a través de ellas.

enp0s3	(•) Internal	( ) External
enp0s8	( ) Internal	(•) External

SALTAR SIGUIENTE


Zentyal - Asistente de configuración inicial - Mozilla Firefox
Zentyal - Asistente de co
https://localhost:8443/Wizard
Selección de paque...
Instalación
Configuración ini...
Guardar los cambios
Asistente de configuración inicial
Usuarios y Grupos
Seleccionar el tipo de servidor
Servidor stand-alone
Controlador de dominio adicional
Seleccionar nombre de dominio del servidor
Nombre del dominio para esta máquina
Será usado como dominio de autenticación de Kerberos para sus usuarios.
zentyal-domain.lan
SALTAR
FINALIZAR
Zentyal - Asistente de c...
[mu-sec@zentyal: ~]
12:14

Zentyal

https://localhost:8443/SaveChanges?noF

Compatibilidad nativa con Microsoft Active Directory®

¡Integración transparente en entornos de Windows Server®! (LDAP, DNS, Kerberos)

- Une tus clientes Windows al dominio e inicia sesión con usuarios de dominio
- Autenticación Single Sign-On (SSO) en todo el dominio
- Compartición de ficheros en entornos Windows® (CIFS)
- Gestión avanzada del dominio mediante herramientas RSAT

¡Aprende más en wiki.zentyal.org!

Guardando cambios en los módulos

Operación actual: **Habilitando módulo samba**

24%

5 de 21 operaciones efectuadas

Zentyal - Mozilla Firefox | [mu-sec@zentyal: ~] | 12:15

Zentyal - Dashboard

https://192.168.1.38:8443

Buscar

zentyal Development Edition 5.0

Buscar...

- Dashboard
- Estado de los Módulos
- Sistema
- Red
- Registros
- Gestión de software
- Usuarios y Equipos
- Dominio
- Compartición de Ficheros
- DNS
- Cortafuegos
- HTTP Proxy

Created by Zentyal S.L.

Dashboard

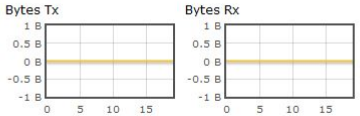
Información general

Hora	lun mar 26 12:28:39 CEST 2018
Nombre de máquina	zentyal
Versión de la platforma	5.0.10
Software	**87 actualizaciones del sistema (48 de seguridad)**
Carga del sistema	0.08, 0.33, 0.38
Tiempo de funcionamiento sin interrupciones	32 min
Usuarios	0

Interfaces de Red

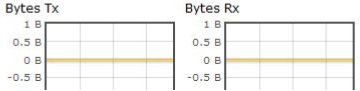
enp0s3

Estado	desactivado, interno
Dirección MAC	08:00:27:79:6d:47



enp0s8

Estado	activado, interno
Dirección MAC	08:00:27:da:5b:31
Dirección IP	192.168.1.38

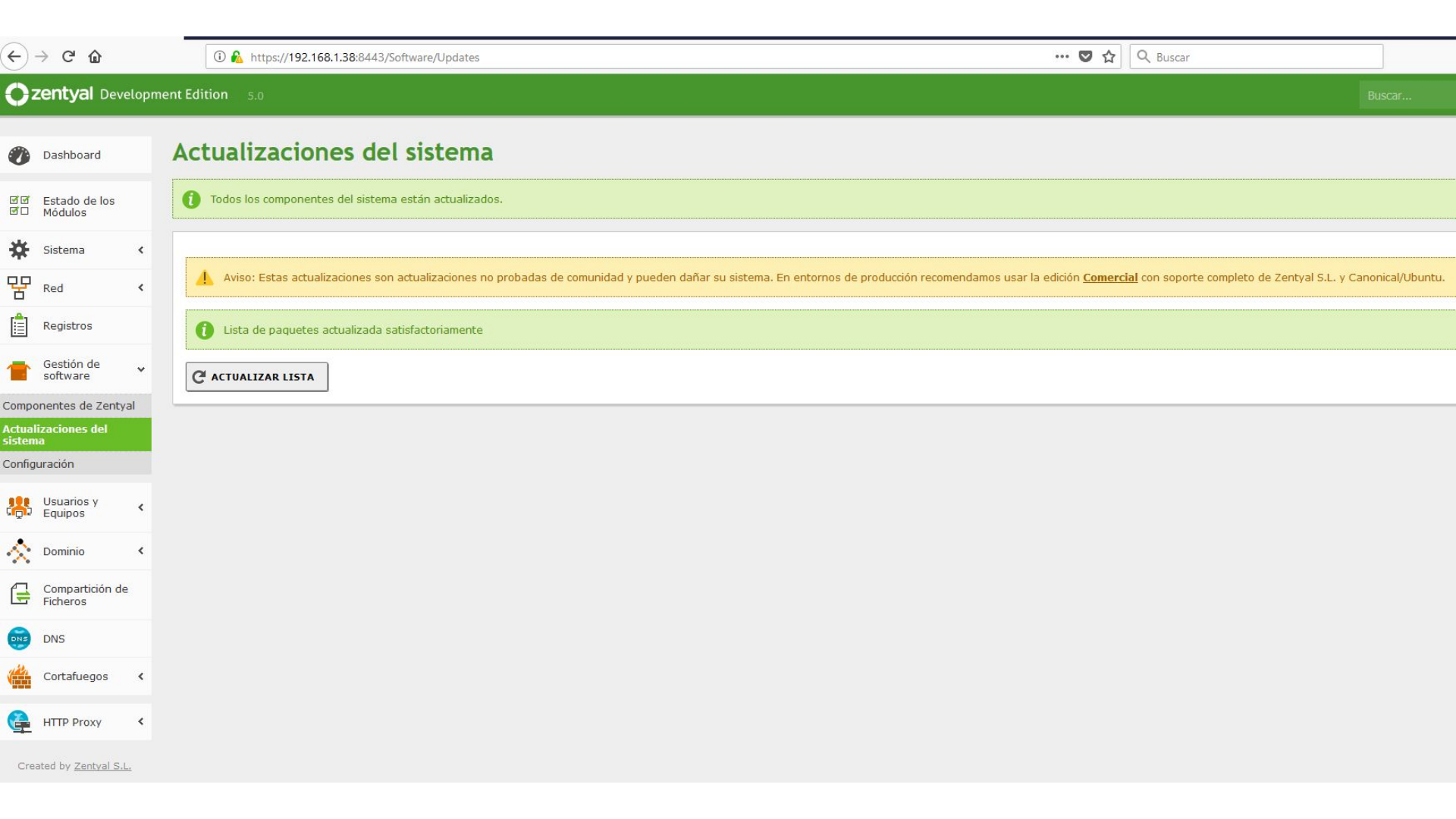


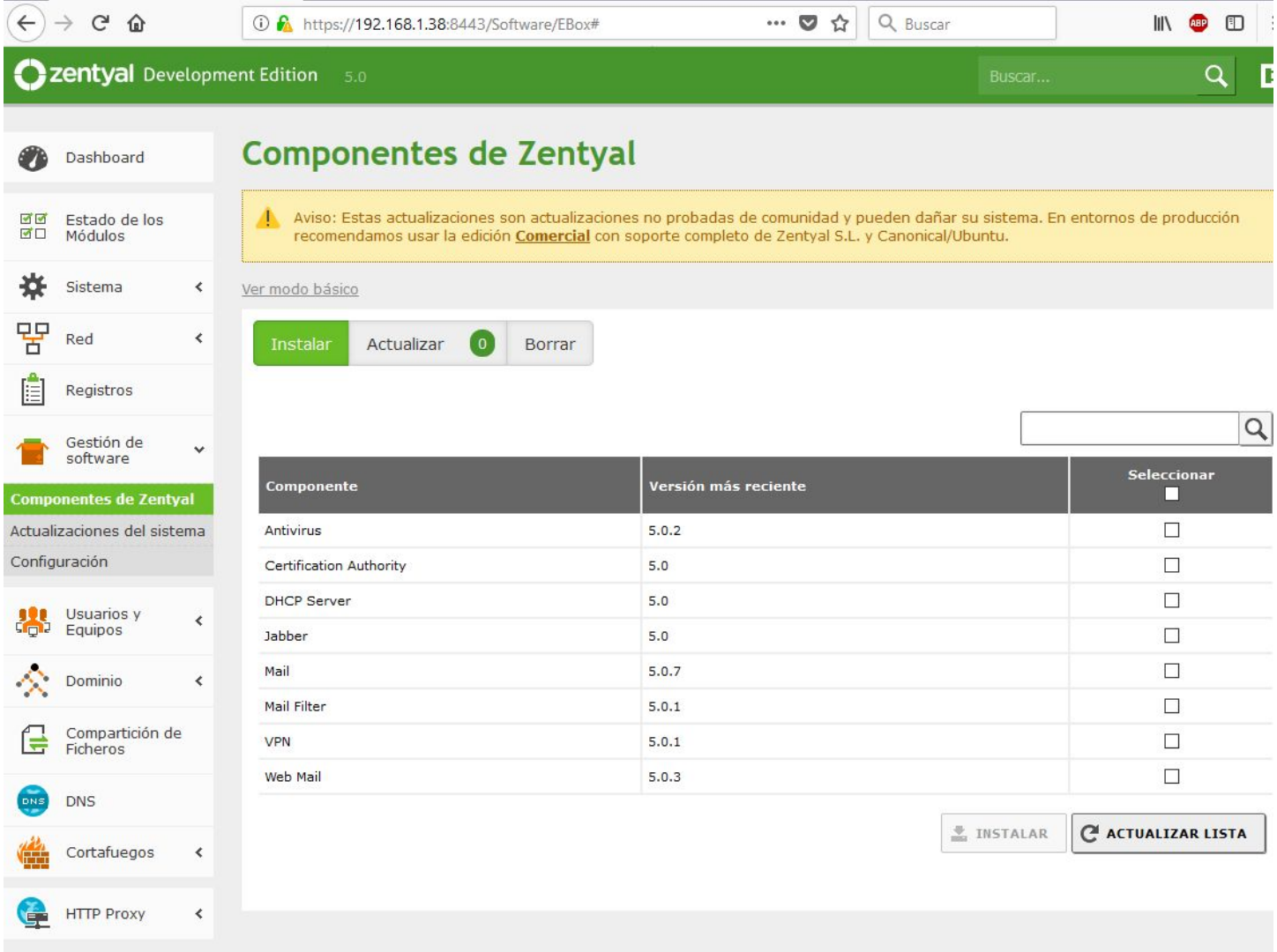
Recursos

- Documentación
- Ediciones Comerciales
- Foro
- Formación Certificada
- Reportar un bug
- Manual Oficial

Estado de los Módulos

Red	Ejecutándose	
Cortafuegos	Ejecutándose	
DNS	Ejecutándose	Reiniciar
Registros	Ejecutándose	Reiniciar
NTP	Ejecutándose	Reiniciar
Controlador de Dominio y Compartición de Ficheros	Ejecutándose	
HTTP Proxy	Deshabilitado	


https://192.168.1.38:8443/Software/Updates
Buscar
zentyal Development Edition 5.0
Buscar...
Dashboard
Estado de los Módulos
Sistema
Red
Registros
Gestión de software
Componentes de Zentyal
Actualizaciones del sistema
Configuración
Usuarios y Equipos
Dominio
Compartición de Ficheros
DNS
Cortafuegos
HTTP Proxy
Created by Zentyal S.L.
Actualizaciones del sistema
Todos los componentes del sistema están actualizados.
Aviso: Estas actualizaciones son actualizaciones no probadas de comunidad y pueden dañar su sistema. En entornos de producción recomendamos usar la edición Comercial con soporte completo de Zentyal S.L. y Canonical/Ubuntu.
Lista de paquetes actualizada satisfactoriamente
ACTUALIZAR LISTA


https://192.168.1.38:8443/Software/EBox#
Buscar
zentyal Development Edition 5.0
Buscar...
Dashboard
Estado de los Módulos
Sistema
Red
Registros
Gestión de software
Componentes de Zentyal
Actualizaciones del sistema
Configuración
Usuarios y Equipos
Dominio
Compartición de Ficheros
DNS
Cortafuegos
HTTP Proxy
Componentes de Zentyal
Aviso: Estas actualizaciones son actualizaciones no probadas de comunidad y pueden dañar su sistema. En entornos de producción recomendamos usar la edición Comercial con soporte completo de Zentyal S.L. y Canonical/Ubuntu.
Ver modo básico
Instalar
Actualizar 0
Borrar
Componente
Versión más reciente
Seleccionar
Antivirus 5.0.2
Certification Authority 5.0
DHCP Server 5.0
Jabber 5.0
Mail 5.0.7
Mail Filter 5.0.1
VPN 5.0.1
Web Mail 5.0.3
INSTALAR
ACTUALIZAR LISTA

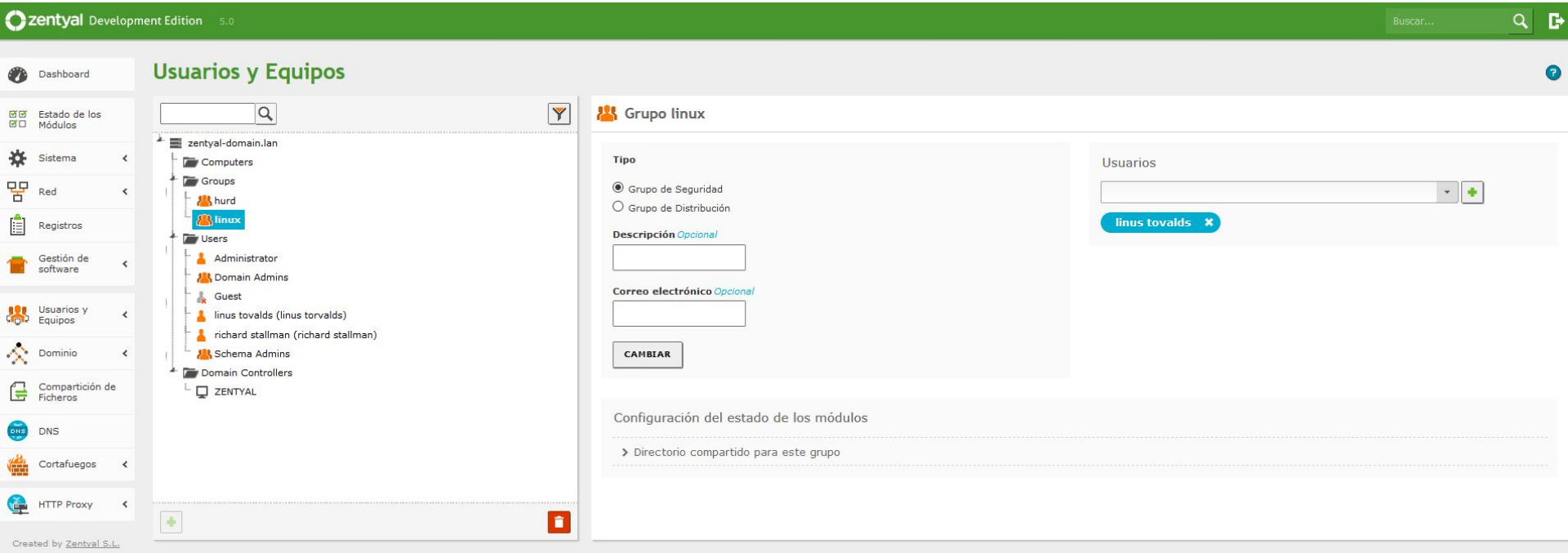
zentyal Development Edition 5.0

Buscar...

- Dashboard
- Estado de los Módulos
- Sistema
- Red
- Registros
- Gestión de software
- Usuarios y Equipos
- Dominio
- Compartición de Ficheros
- DNS
- Cortafuegos
- HTTP Proxy

Configuración del estado de los módulos

Módulo	Depende	Estado
Red		☑
Cortafuegos	Red	☑
DNS	Red	☑
Registros		☑
NTP		☑
Controlador de Dominio y Compartición de Ficheros	Red, DNS, NTP	☑
HTTP Proxy	Cortafuegos	☐


zentyal Development Edition 5.0
Buscar...
Dashboard
Estado de los Módulos
Sistema
Red
Registros
Gestión de software
Usuarios y Equipos
Dominio
Compartición de Ficheros
DNS
Cortafuegos
HTTP Proxy
Created by Zentyal S.L.
Usuarios y Equipos
zentyal-domain.lan
Computers
Groups
hurd
linux
Users
Administrator
Domain Admins
Guest
linus tovalds (linus torvalds)
richard stallman (richard stallman)
Schema Admins
Domain Controllers
ZENTYAL
Grupo linux
Tipo
Grupo de Seguridad
Grupo de Distribución
Descripción Opcional
Correo electrónico Opcional
CAMBIAR
Usuarios
linus tovalds
Configuración del estado de los módulos
Directorio compartido para este grupo

Dashboard
Estado de los Módulos
Sistema
Red
Registros
Gestión de software
Usuarios y Equipos
Gestionar
Plantilla de Usuario
Opciones de configuración de LDAP.
Dominio
Compartición de Ficheros
DNS
Cortafuegos
HTTP Proxy

Opciones de configuración de LDAP.

Información de LDAP

DN Base
DC=zentyal-domain,DC=lan

DN de Usuarios por defecto
CN=Users,DC=zentyal-domain,DC=lan

DN de Grupos por defecto
CN=Users,DC=zentyal-domain,DC=lan

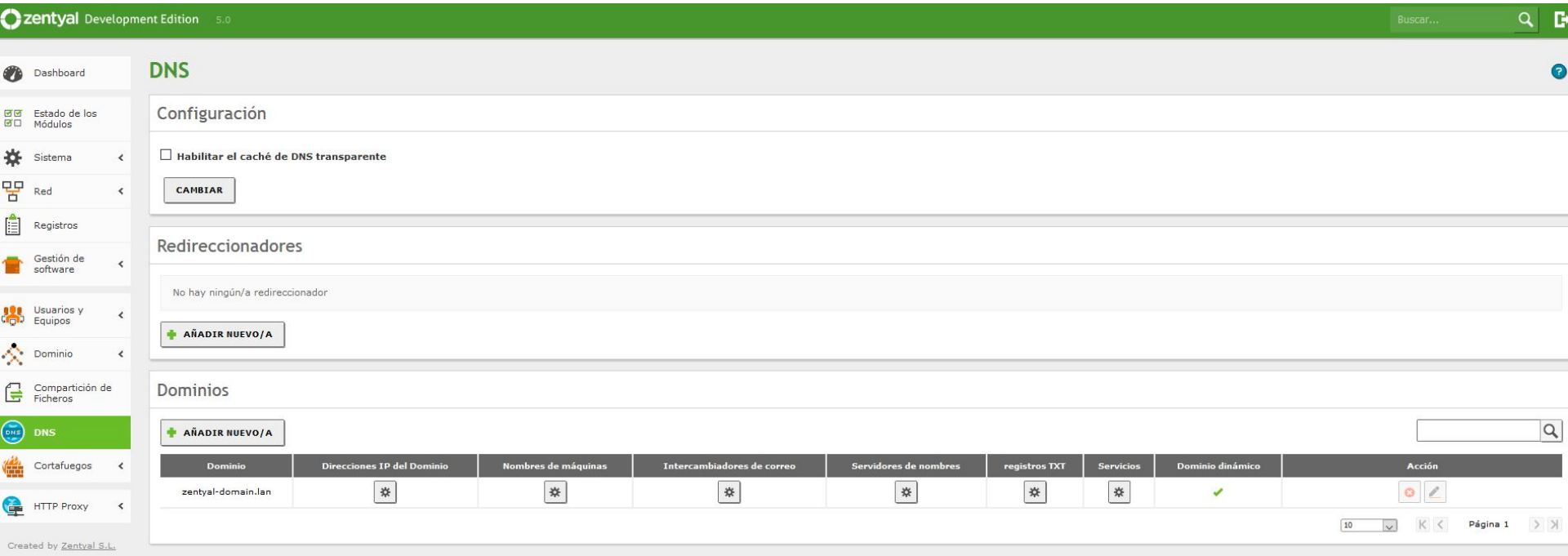
Opciones de configuración PAM

☐ **Habilitar PAM**
Hacer que los usuarios LDAP tengan cuenta en el sistema.

Shell por defecto
Este cambio se aplicará únicamente a los usuarios creados a partir de ahora.

bash

CAMBIAR


zentyal Development Edition 5.0
Buscar...
Dashboard
Estado de los Módulos
Sistema
Red
Registros
Gestión de software
Usuarios y Equipos
Dominio
Compartición de Ficheros
DNS
Cortafuegos
HTTP Proxy
Created by Zentyal S.L.
DNS
Configuración
Habilitar el caché de DNS transparente
CAMBIAR
Redireccionadores
No hay ningún/a redireccionador
AÑADIR NUEVO/A
Dominios
AÑADIR NUEVO/A
Dominio
Direcciones IP del Dominio
Nombres de máquinas
Intercambiadores de correo
Servidores de nombres
registros TXT
Servicios
Dominio dinámico
Acción
zentyal-domain.lan
10
Página 1

Dashboard

Estado de los Módulos

Sistema

Red

Registros

Gestión de software

Usuarios y Equipos

Dominio

Compartición de Ficheros

DNS

Cortafuegos

HTTP Proxy

General Settings

Access Rules

Filter Profiles

Categorized Lists

Bandwidth Throttling

HTTP Proxy

El módulo HTTP Proxy está desactivado. No olvide activarlo en la sección **Estado de los módulos** para que sus cambios se efectúen.

General Settings

☐ **Transparent Proxy**

☐ **Ad Blocking**
Remove advertisements from all HTTP traffic

Puerto

3128

Cache files size (MB)

100

CAMBIAR

Cache Exemptions

No hay ningún/a domain name address

AÑADIR NUEVO/A

Transparent Proxy Exemptions

No hay ningún/a domain name address

AÑADIR NUEVO/A

Dashboard

Estado de los Módulos

Sistema

Red

Registros

Gestión de software

Usuarios y Equipos

Dominio

Compartición de Ficheros

DNS

Cortafuegos

HTTP Proxy

General Settings

Access Rules

Filter Profiles

Categorized Lists

Bandwidth Throttling

HTTP Proxy

El módulo HTTP Proxy está desactivado. No olvide activarlo en la sección **Estado de los módulos** para que sus cambios se efectúen.

regla actualizada

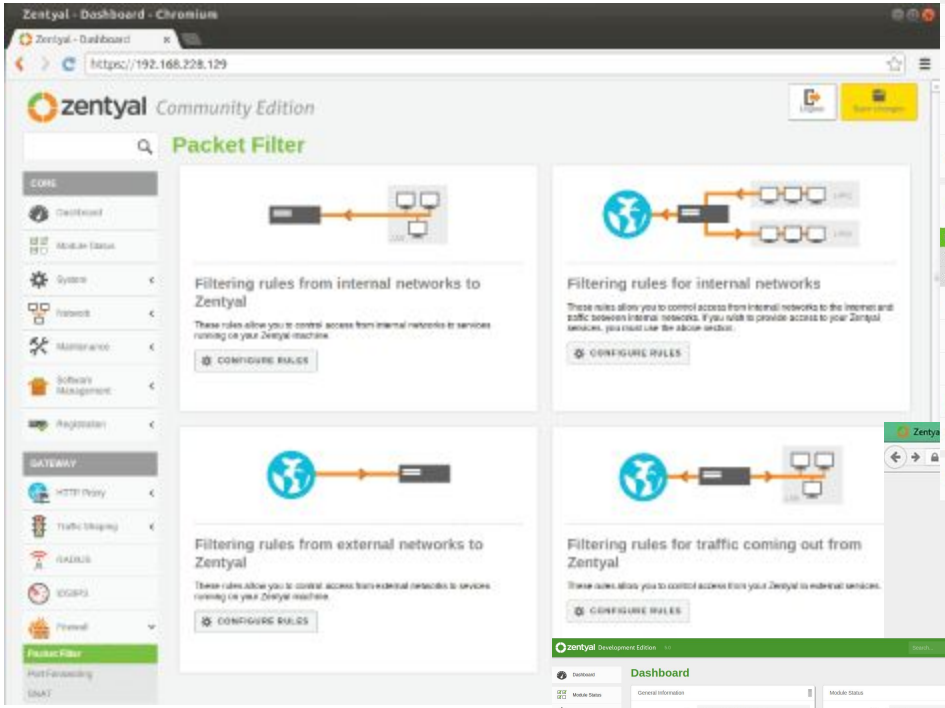
Access Rules

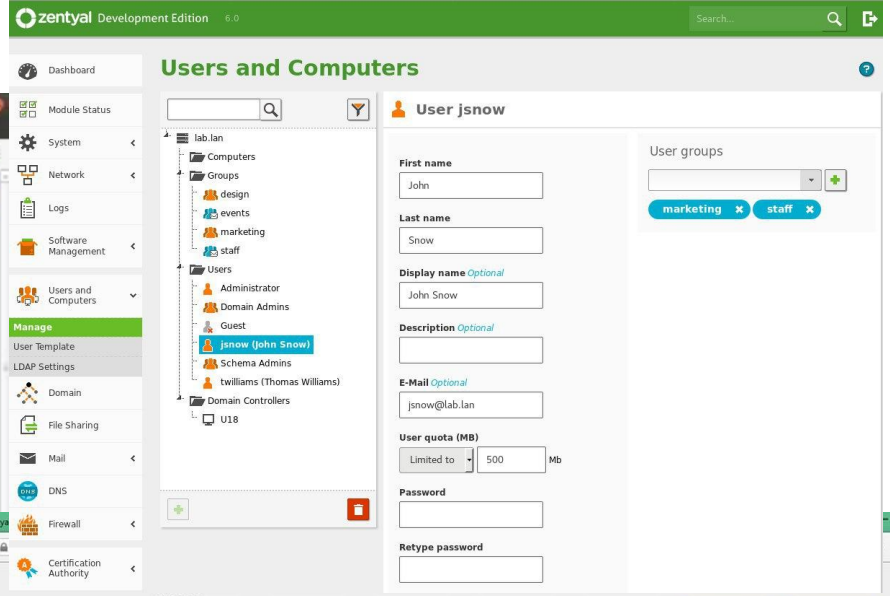
AÑADIR NUEVO/A

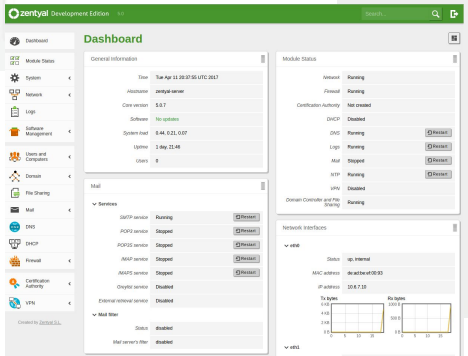
Time period	Origen	Decisión	Acción
08:00-15:00 Work days	Object: hurd	Allow All	
All time	Object: linux	Allow All	

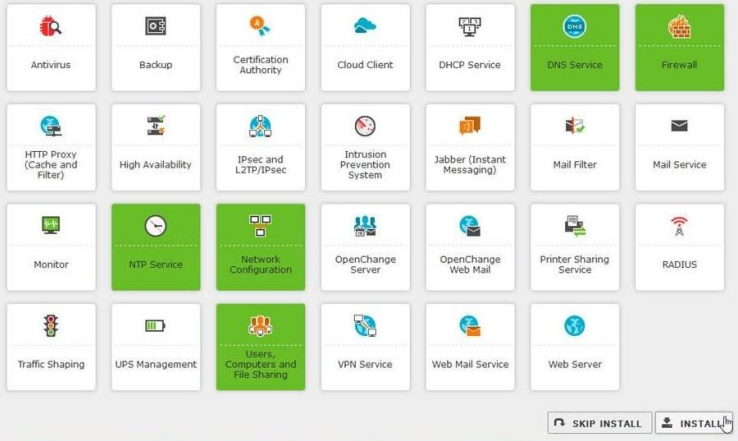
10

Página 1

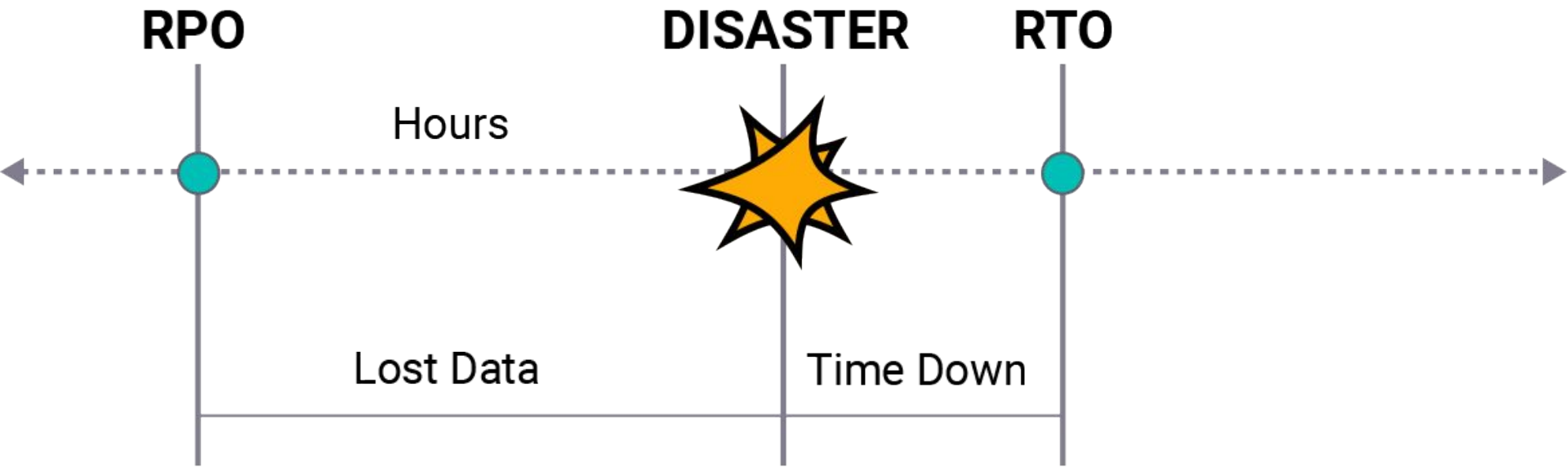

Zentyal - Dashboard - Chromium
https://192.168.228.129
zentyal Community Edition
Packet Filter
Filtering rules from internal networks to Zentyal
CONFIGURE RULES
Filtering rules for internal networks
CONFIGURE RULES
Filtering rules from external networks to Zentyal
CONFIGURE RULES
Filtering rules for traffic coming out from Zentyal
CONFIGURE RULES

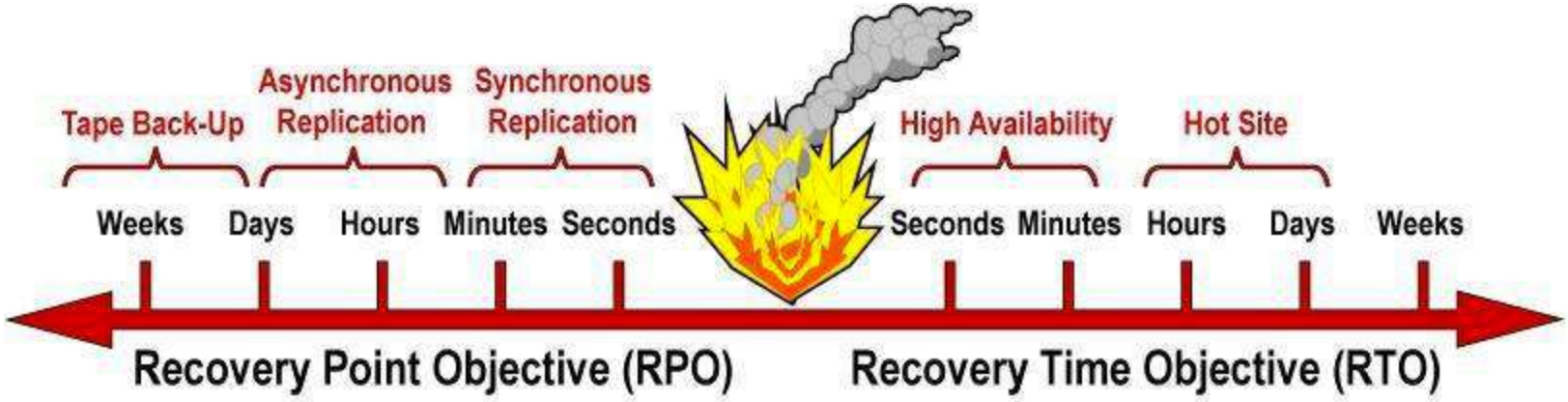

zentyal Development Edition 6.0
Users and Computers
Dashboard
Module Status
System
Network
Logs
Software Management
Users and Computers
Manage
User Template
LDAP Settings
Domain
File Sharing
Mail
DNS
Firewall
Certification Authority
lab.lan
Computers
Groups
design
events
marketing
staff
Users
Administrator
Domain Admins
Guest
jsnow (john Snow)
Schema Admins
twilliams (Thomas Williams)
Domain Controllers
U18
User jsnow
First name
John
Last name
Snow
Display name Optional
John Snow
Description Optional
E-Mail Optional
jsnow@lab.lan
User quota (MB)
Limited to
500
Mb
Password
Retype password
User groups
marketing
staff

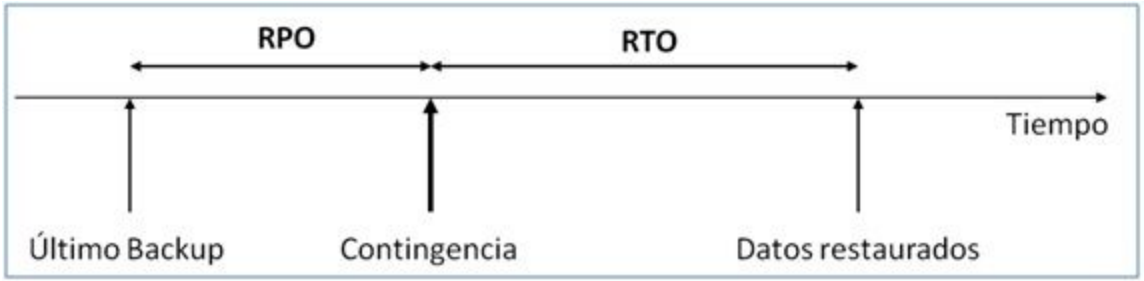

zentyal Development Edition
Dashboard


Antivirus
Backup
Certification Authority
Cloud Client
DHCP Service
DNS Service
Firewall
HTTP Proxy (Cache and Filter)
High Availability
IPsec and L2TP/IPsec
Intrusion Prevention System
Jabber (Instant Messaging)
Mail Filter
Mail Service
Monitor
NTP Service
Network Configuration
OpenChange Server
OpenChange Web Mail
Printer Sharing Service
RADIUS
Traffic Shaping
UPS Management
Users, Computers and File Sharing
VPN Service
Web Mail Service
Web Server
SKIP INSTALL
INSTALL


Backup


RPO
DISASTER
RTO
Hours
Lost Data
Time Down


Tape Back-Up
Asynchronous Replication
Synchronous Replication
High Availability
Hot Site
Weeks
Days
Hours
Minutes
Seconds
Seconds
Minutes
Hours
Days
Weeks
Recovery Point Objective (RPO)
Recovery Time Objective (RTO)


RPO
RTO
Tiempo
Último Backup
Contingencia
Datos restaurados

CobianSoft

Navigation

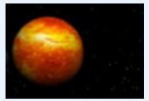
- **Home**
- **News**
- **About**
  - Personal
  - Pictures
- **Software**
  - Cobian Backup
  - ShimmerCat
  - Cobian Poirot
  - Other software
  - Obsolete
- **Forum**
- **Donations**
- **Guest book**

Hello and welcome to Cobian's site!

Welcome to Cobian's site, the home of Cobian Backup. This is both a personal site and site about software development.

Update: The new owner is James Sweeney. I'll update this site soon with more information.

Cobian Backup 11 (Gravity)



Cobian Backup, version 11 (code name Gravity) is now Out!

You can download it here.

Please feel free to walk around my site and download any of my programs. Because of the popularity of Cobian Backup, which now is in its 11th version, I am actively supporting only that product. If you have some questions about Cobian Backup, please read the Help file and the FAQ first, and if you don't find the answer to your question there, post it to the support forum and I or other users will gladly try to help you.

Here you can download some other programs developed by me as well. Some useful utilities like Cobian Herald (a mailing list server), CobView (a multipurpose Windows Shell extension) and CobDDNS (a client updater for EditZone dynamic DNS) can be downloaded from Other software.

A couple of old unsupported utilities can also be found by selecting Obsolete from the Navigation menu.

While you are here, feel free to leave some lines in my guest book too.

CobianSoft

Navigation

- Home
- News
- About
  - Personal
  - Pictures
- Software
  - Cobian Backup
  - ShimmerCat
  - Cobian Macro
  - Other software
  - Obsolete
- Forum
- Donations
- Guest book

Related

- FAQ
- Screenshot
- History
- Evolution
- Related files

Cobian Backup

Update: **The new owner is James Sweeney.** I'll update this site soon with more information.

"...If you are looking for a stable and reliable application to safeguarding your data, Cobian Backup will not disappoint you. Give it a try..." From the Softoxi review.

Click HERE to see more awards that Cobian Backup has won over the years

Cobian Backup 11 (Gravity)
Version 11, Gravity
For Windows XP, 2003, Vista, 2008, Windows 7
Windows 8, Windows 10 (See the FAQ)
Works in both 32 and 64 bits Windows
Latest version: 11.2.0.582
See what's new

Download Cobian Backup 10
Version 10 Boletus
For Windows XP, 2003, Vista, 2008, Windows 7
(works in both 32 and 64 bits Windows)
Latest version: 10.1.1.816
See what's new

Download Cobian Backup 9
Version 9 Amanita
For Windows NT, 2000, XP, 2003, Vista
Latest version: 9.5.1.212
See what's new

Download Cobian Backup 8
Version 8 Black Moon
For Windows NT, 2000, XP, 2003, Vista
Latest version: 8.4.0.202

Ads

Backup… Bacula

Bacula es un sistema *open-source* para **copias de seguridad** en red.

Bacula soporta clientes Linux, UNIX, Windows, and macOS, incluyendo un amplio abanico de unidades de cinta para *professional backup*.

Administradores y operadores pueden configurar Bacula por consola de línea de comandos, o bien a través de GUI o interfaz web, para acceder al catálogo de información almacenado en bases de datos MySQL, PostgreSQL, o SQLite.

- https://www.baculasystems.com/
- https://www.bacula.org/git/cgit.cgi/bacula/

Bacula Community Source -- `git clone http://git.bacula.org/bacula.git`

- https://www.bacula-web.org/

Powerful & Multi-Purpose Network Backup Solution

Due to its modular design, Bacula is scalable from single computer to enterprise systems consisting of hundreds of computers located over a large network.

Download Now | Learn More

Open Source

Bacula is a set of Open Source, computer programs that permit you (or the system administrator) to manage backup, recovery, and verification of computer data across a network of computers of different kinds.

Enterprise Ready

Bacula is relatively easy to use and very efficient, while offering many advanced storage management features that make it easy to find and recover lost or damaged files.

Chosen by Millions

According to Source Forge statistics (rank and downloads), Bacula is by far the most popular Open Source backup program. It has 2,5 million downloads and thousands of contributors worldwide.

New Release 9.4.1

This is a minor release to 9.4.0 (listed below) that corrects the configure process to properly detect libs3, which is needed if you want to use the new S3 driver.

The 9.4.0 release comprised of more than 13,000 lines of differences since version 9.2.2. It has updates to Baculum and small number of bug fixes and back ports from Bacula Systems Enterprise since version 9.2.2.

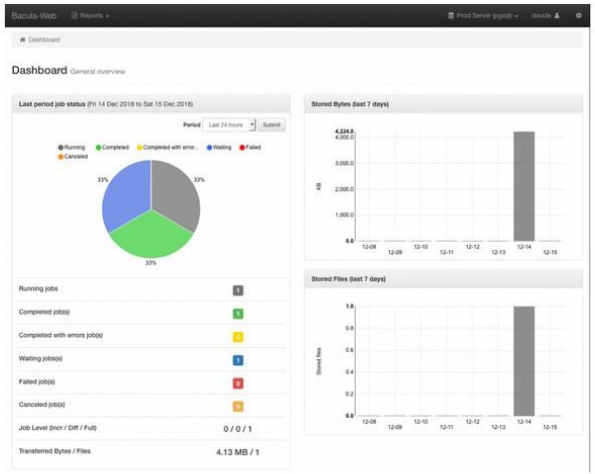
The main new feature is the addition support for using Amazon S3 (and other *identical* S3 providers), and WORM tape cassettes. Note: Azur, Oracle S3,and Goggle S3 are not compatible with Amazon S3.

Download Now

Welcome to Bacula-Web project

About

Bacula-Web is a web based reporting and monitoring tool which provides you useful information about your **Bacula** infrastructure like jobs, pools, volumes, jobs logs, clients and backup jobs reports and even more ...
Bacula-Web is free (like a bird) and released under the term of the **GPL v 2.0 license**.



Bacula-Web main dashboard

Features

- **Responsive Web UI**
- **Users authentication**
- **Mutliple Bacula catalog**
- **Dashboard**
- **Reporting & Monitoring**

For more details about Bacula-Web features, check the features chapter in the **documentation**.

Manuals

Manuals for Version 9.4.x

- New Features in Version 9.4.x HTML

- Bacula Main Reference Guide PDF /HTML
- Console and Operators Guide PDF /HTML
- Problem Resolution Guide PDF /HTML
- Utility Programs PDF /HTML
- Miscellaneous Guide PDF /HTML
- Developers' Guide PDF /HTML

- Bacula-Web GUI (project web site: www.bacula-web.org)

Recent Posts

Bacula Release 9.4.0
Bacula Status Report — 7 November 2018
Bacula Release 9.2.2
Bacula Release 9.2.1

Screenshots

Baculum

Baculum 01 – Volumes list and configuration

Baculum 02 – Clients list and status

Baculum 03 – Jobs to run

Baculum 04 – Jobs list and configuration

Baculum 05 – Graphs

Baculum 06 – Graphs zoom

Baculum 07 – Graphs

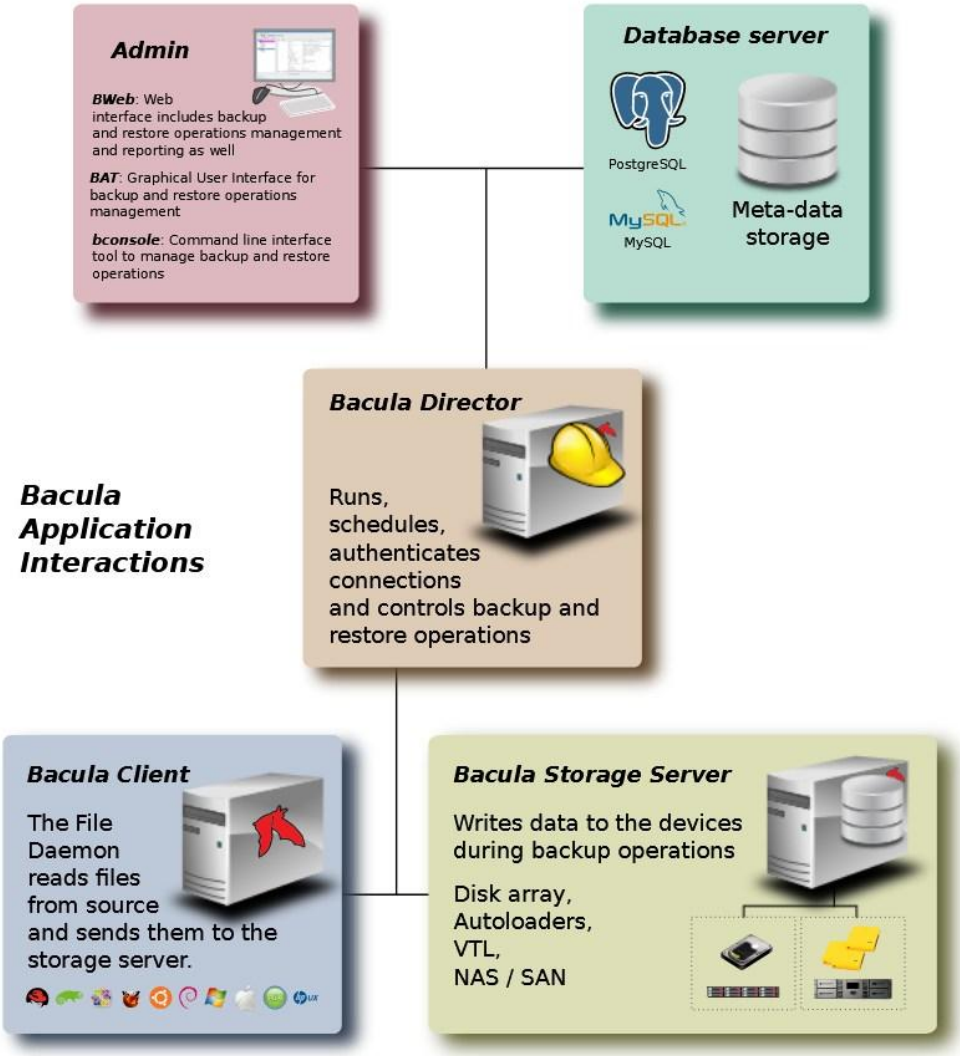
Baculum 08 – Restore wizard

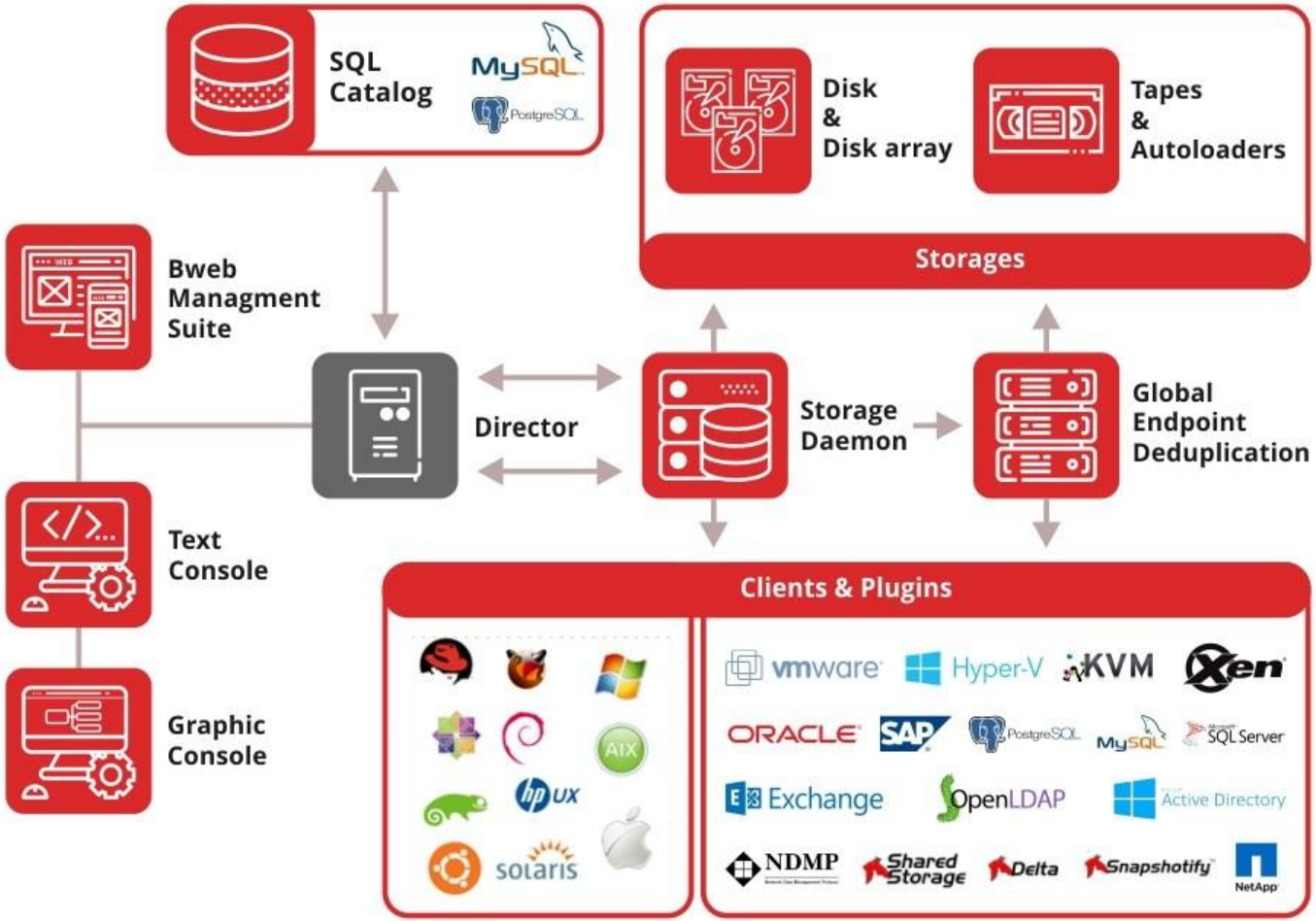
Baculum 09 – Restore wizard summary

White Papers

The following white papers have been adapted to the community version and provided for your personal use by Bacula Systems SA in the hopes that you will find them useful in producing a production backup environment with Bacula.

- Bacula API PDF
- Bacula Cloud Backup PDF
- Bacula Concept Guide PDF
- Bacula Regression Testing PDF
- Best Practices for Disk Backup PDF
- Deduplication Optimized Volumes PDF
- Disk Backup Design PDF
- Disk Migration PDF
- manual_prune.pl Perl
- Object Storage (Cloud) with Bacula PDF
- Progressive Virtual Full Backups PDF


Admin
BWeb: Web interface includes backup and restore operations management and reporting as well
BAT: Graphical User Interface for backup and restore operations management
bconsole: Command line interface tool to manage backup and restore operations
Database server
PostgreSQL
MySQL
Meta-data storage
Bacula Director
Runs, schedules, authenticates connections and controls backup and restore operations
Bacula Application Interactions
Bacula Client
The File Daemon reads files from source and sends them to the storage server.
Bacula Storage Server
Writes data to the devices during backup operations
Disk array, Autoloaders, VTL, NAS / SAN


SQL
Catalog
MySQL
PostgreSQL
Disk
&
Disk array
Tapes
&
Autoloaders
Storages
Bweb
Managment
Suite
Director
Storage
Daemon
Global
Endpoint
Deduplication
Text
Console
Graphic
Console
Clients & Plugins
AIX
hp UX
solaris
vmware
Hyper-V
KVM
Xen
ORACLE
SAP
PostgreSQL
MySQL
SQL Server
Exchange
OpenLDAP
Active Directory
NDMP
Shared Storage
Delta
Snapshotify
NetApp

Dispositivos de backup… Tipos de cintas

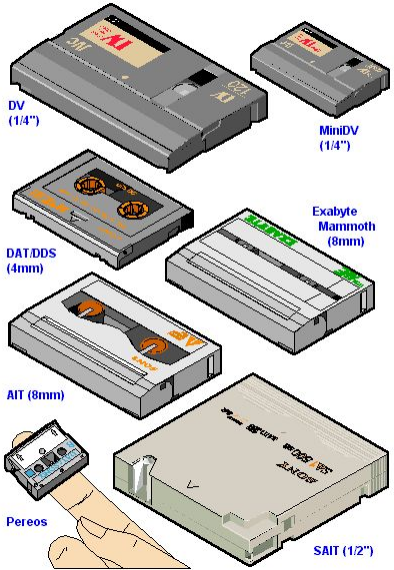
Desde las DAT, AIT, DLT y LTO, su elección dependerá tanto de la velocidad de escritura como del volumen de almacenamiento en ellas.

- Cintas DAT. Fueron desarrolladas por Sony y Philips, su velocidad de transferencia es de 3 MB/s dentro de unas dimensiones reducidas.
- Cintas DLT. Han sido desarrolladas por Digital Equipment Corp. Tiene una capacidad de hasta 80 GB con una velocidad de transferencia de hasta 32 MB/s (SuperDLT)
- Cintas AIT. Desarrolladas por Sony, tienen una velocidad de transferencia de 24 MB/s con capacidades de hasta 500 GB
- LTO / ULTRIUM. Desarrolladas por HP, IBM y Seagate, incorporan corrección de errores y compresión por hardware. Su velocidad de transferencia es de 80 MB/s y permiten capacidades superiores al 1 TB, (1600 GB en la LTO-4).


SONY
DAT
SONY
90
DAT


COMPAQ
SCSI
STANDALONE Only
Rev B01
hp
Write Protected
Tape in Use
Use Cleaning Tape
Operate Handle
Unload


Quantum.
Super DLTtape I
DLT



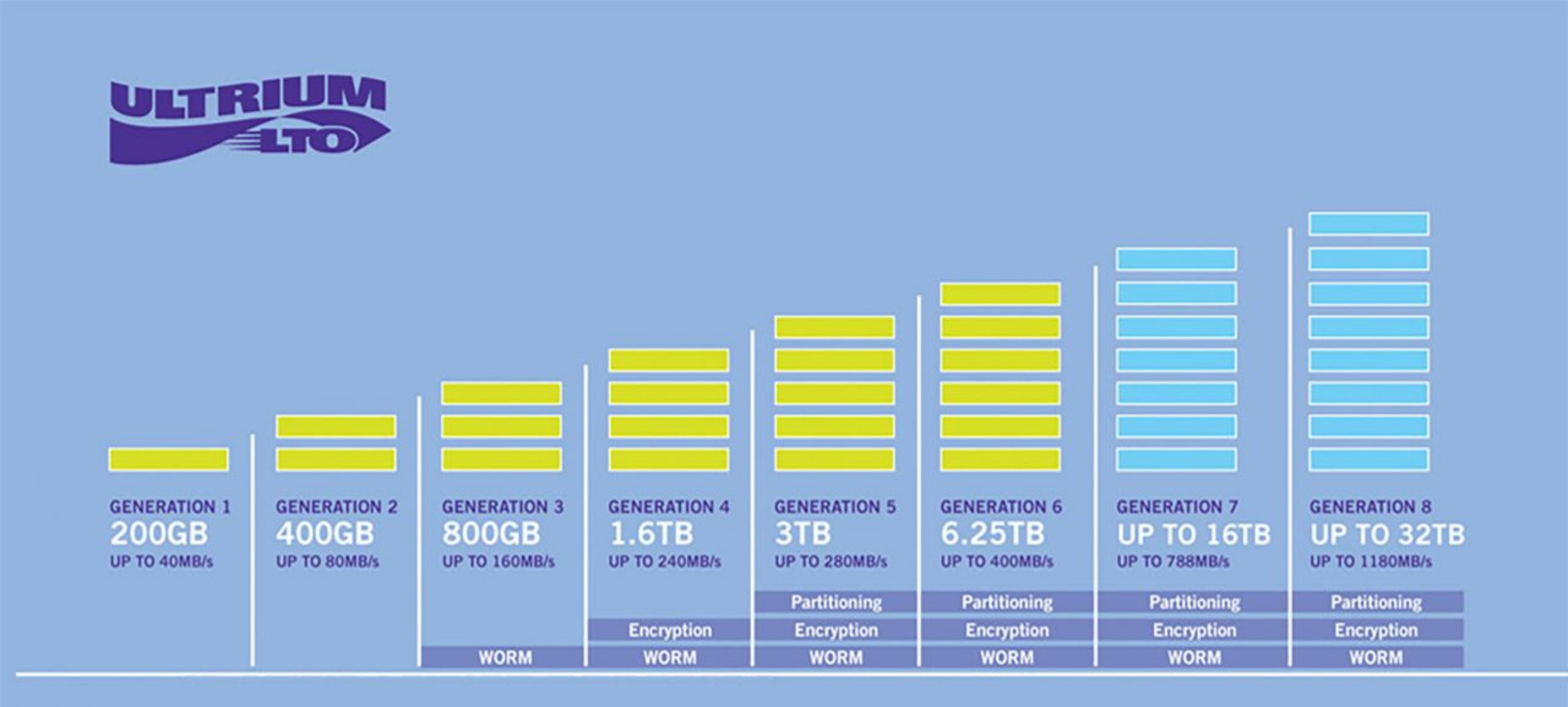

TLS-58132 / 264


TLS-5433 / 66

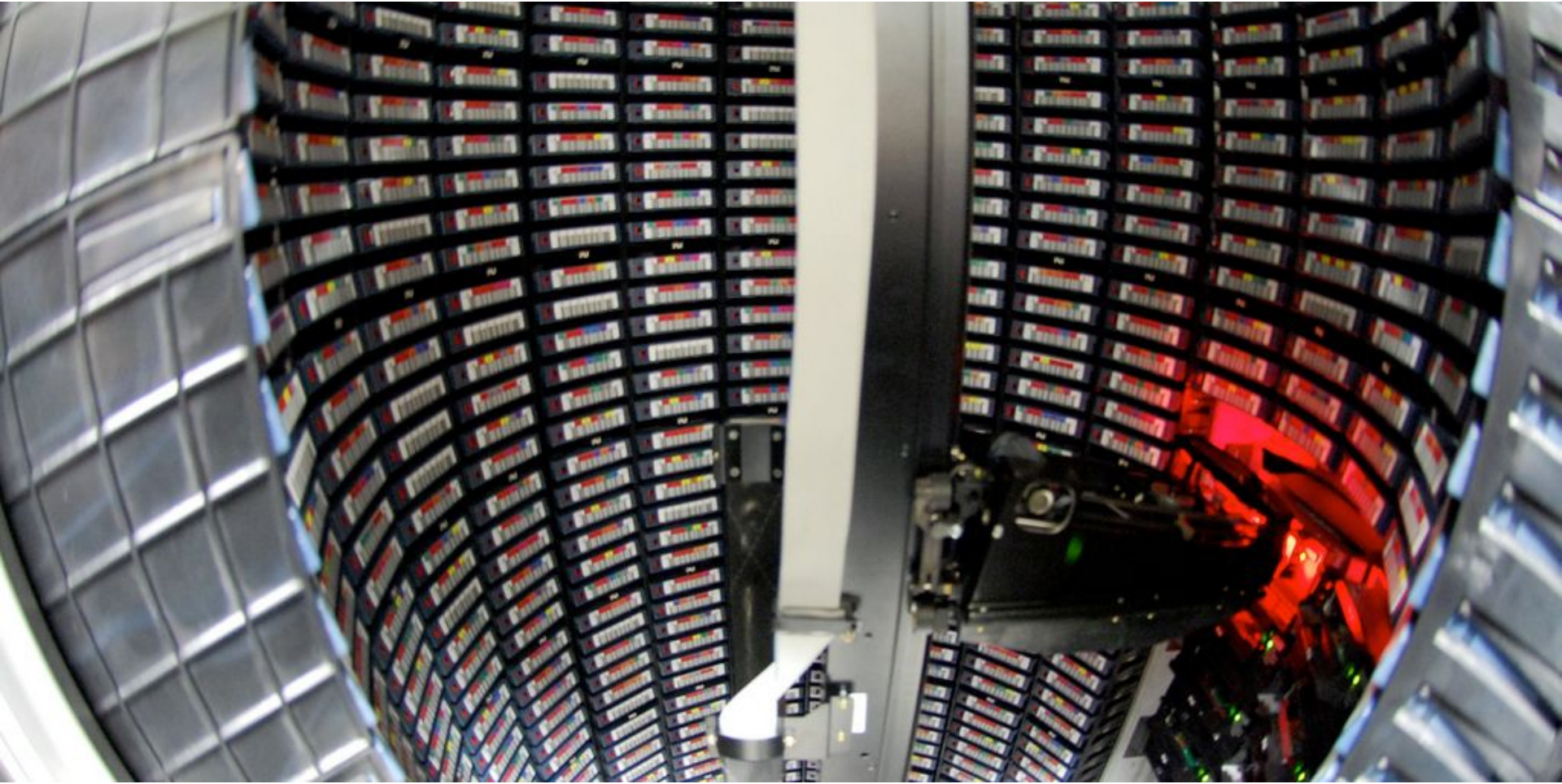

Quantum
Ultrium 4
Data Cartridge
For use in LTO Ultrium 4 drives.
800 / 1600 GB
0.5 Inch Data Cartridge
ULTRIUM LTO 4


LTO-6 Ultrium WORM
BaFe DATA CARTRIDGE
C7976BW
6.25TB*
BaFe


ULTRIUM LTO 6
Ready
Drive Error
Tape Error
Clean
Encryption
HP LTO-6 Ultrium 6650



LTO ULTRIUM ROADMAP



FreeNAS Storage Operatin

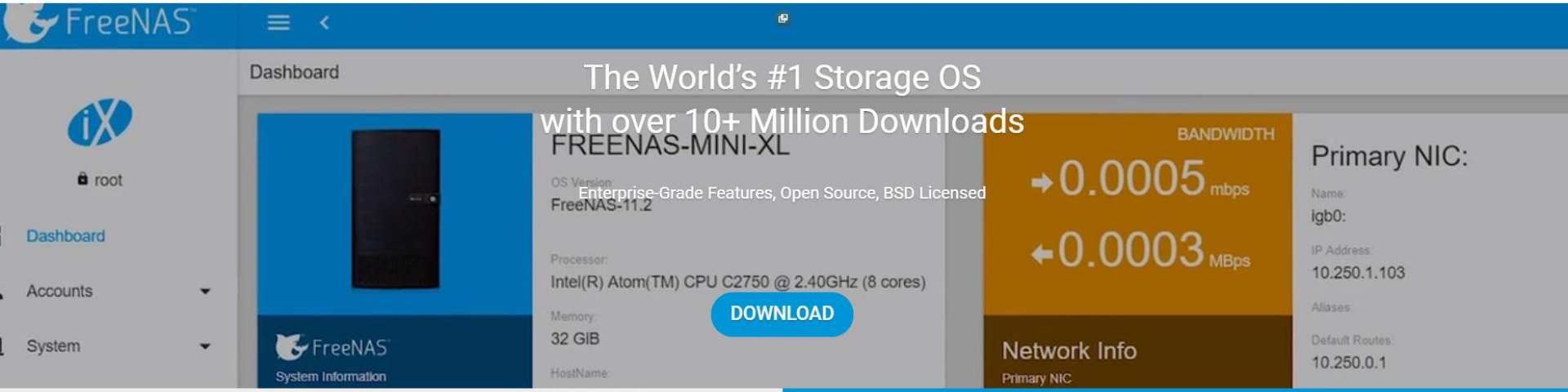
freenas.org

FreeNAS

About Products For Home For Business Blog Our Community Get Help

The World's #1 Storage OS with over 10+ Million Downloads

Enterprise-Grade Features, Open Source, BSD Licensed



What is FreeNAS?

FreeNAS is an operating system that can be installed on virtually any hardware platform to share data over a network. FreeNAS is the simplest way to create a centralized and easily accessible place for your data. Use FreeNAS with ZFS to protect, store, backup, all of your data. FreeNAS is used everywhere, for the home, small business, and the enterprise.

What is ZFS?

ZFS is an enterprise-ready open source file system, RAID controller, and volume manager with unprecedented flexibility and an uncompromising commitment to data integrity. It eliminates most, if not all of the shortcomings found in legacy file systems and hardware RAID devices. Once you go ZFS, you will never want to go back.

Web Interface

File Sharing

Snapshots

Replication

Features

File Sharing

File sharing is what FreeNAS does best. Every major operating system is supported with SMB/CIFS (Windows file shares), NFS (Unix file shares) and AFP (Apple File Shares) as well as FTP, iSCSI (block sharing), WebDAV and other methods of sharing data over the network are available. iSCSI also supports VMware VAAI, Microsoft ODX and Microsoft Windows Server 2008 and 2012 R2 Clustering.

Most operating systems, including Windows, Mac OS X, many Linux distributions, and PC-BSD® can connect using SMB shares with little or no additional configuration needed on the client side. Most Unix-like operating systems support connecting with NFS out of the box, and free clients are widely available. AFP is primarily used by Mac OSX and is well suited for a network environment that only connects with Macintosh clients. FreeNAS® also supports Time Machine backups.

Web Interface

If FreeNAS has one goal, it's simplifying complex administrative tasks for as wide a user base as possible. Every aspect of a FreeNAS system can be managed from a Web User Interface. A setup Wizard further simplifies configuration at installation time or later in the setup process. Volume creation, or the setting of permissions on individual shares or performing software updates, can be done without missing a critical step or encountering a silent failure.

Of course, the FreeNAS Team knows we can't think of everything. Many services have advanced configuration options available from the Web User Interface that is available in advanced menus. The full power of the FreeBSD shell environment is also available just a click away or through SSH. Ultimately, FreeNAS makes NAS deployment easier than ever but doesn't get between you and the solution you need.

Data Protection

ZFS is designed for data integrity from top to bottom. RAID-Z, the software RAID that is part of ZFS, offers single parity protection like RAID 5, but without the "write hole" vulnerability thanks to the copy-on-write architecture of ZFS. The additional levels RAID-Z2 and RAID-Z3 offer double and triple parity protection, respectively. A software mirror option is also available. The FreeNAS Volumes screen lists each possible parity arrangement based on the number of disks you select when creating a new volume.

Every ZFS filesystem is also verified with checksums from top to bottom to ensure data integrity. If inconsistencies are found, parity blocks can be used to repair corrupt data. A regular scrub is turned on by default and can be rescheduled or configured from the web interface.

Snapshots

Thanks to ZFS, snapshots of the entire filesystem can be made and saved at any time. As long as a snapshot exists, administrators can access files as they were when the snapshot was made.

Snapshots can be made on a one-off basis or scheduled as a cron job from the web interface. At any time, the entire filesystem can be rolled back to the most recent snapshot. Older snapshots can be cloned and accessed to recover data from that version of the filesystem. From the web interface, users can see how much space a particular snapshot is occupying on the volume and delete, clone, or roll back to individual snapshots as needed.

Replication

ZFS Snapshots are more than just local backups – they can be used to create remote backups as well. Replicating snapshots of the filesystem to a remote ZFS filesystem creates a complete duplicate there. Furthermore, additional snapshots of the same filesystem can be sent incrementally, reducing the size of each backup to the changes that were made between snapshots. In case of catastrophic damage to a local ZFS filesystem (such as disk failure in excess of parity protection or irrecoverable log device failure), any backed-up snapshot can be sent to a new ZFS filesystem, recovering all data up to that backup.

Encryption

FreeNAS is the first and only open source project to offer encryption on ZFS volumes! A full-volume encryption option is available during volume creation, providing industry standard AES-XTS encryption which can be hardware-accelerated (when the processor has AES-NI capability).

Encrypted volumes can only be read by FreeNAS systems in possession of the master key for that volume. The user can optionally create a passphrase to add extra protection for their system against loss or theft.

Encryption allows for confidence when retiring and recycling hard drives because the drives no longer need to be wiped provided the master keys are obliterated.

Backup Services

- Windows Backup
- Apple Time Machine
- rsync
- TrueOS Life Preserver

Plugins

FreeNAS® supports the core features of a NAS appliance out of the box. However, many users like to enhance their NAS appliance with third party software for media streaming, alternative protocols, or web applications.

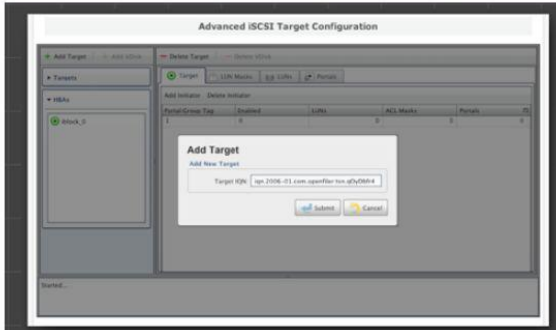
To make sure your NAS can do everything you want, FreeNAS offers a third-party plugin system based on the FreeBSD jails system and the PBI system from PC-BSD. The plugin system isolates third-party software from the core operating system but allows plugins access to user-specified directories and configuration from the main Web User Interface.

- **bacula** Network backup solution (server)
- **BitTorrent (Sync)** Fast, private file sharing for teams and individuals. Data moves directly from device to device, skipping the cloud.

openfiler

Screenshots | Download

Home | Products | Support | Buy | About



Unified Storage

NAS Features - CIFS, NFS, HTTP

SAN Features - iSCSI, FC

High Availability / Failover

Block Replication (LAN & WAN)

Web-based Management

Cost-free Storage Capacity Expansion

Download Openfiler
Free

MOTOROLA

Pratt & Whitney
A United Technologies Company

BillMeLater
a PayPal service

METROPOLITAN POLICE
Working together for a safer London

Contact Us | Purchase Support | Download Openfiler

License | Terms & Conditions | Privacy Policy --- [e] info@openfiler.com --- [t] +44 (0)845 056 8743 --- [t] +1 678 383 4234 --- [f] +1 404 592 0330

Panorámica de la Ciberseguridad… Estado del arte

- La mejor prevención radica en la **formación y concienciación** para la capacitación de las personas, con objeto de **evitar ataques de ingeniería social y la mala praxis por negligencia** en los procesos internos: Abrir adjuntos y enlaces de origen desconocidos, phishing, usb infectado, etc.
- El **Firewall y Antivirus** corporativo son tan solo los primeros requisitos en seguridad perimetral, resultando necesario el mantenimiento periódico de todos sistemas, la monitorización y actualización constante (bastionado) de sistemas críticos y **fortificación** (de la configuración por defecto) que garantice la ausencia de vulnerabilidades explotables.
- Sistemas **antimalware** y **Detección de intrusiones** son buenas prácticas propuestas como contramedidas a implementar.
- Diseño de arquitectura de redes seguras. La importancia de la correcta **segmentación de redes y subredes** es vital en entornos de producción industriales e infraestructuras organizativas.

VirusTotal es un servicio gratuito que **analiza archivos y URLs sospechosas** facilitando la rápida detección de virus, gusanos, troyanos y todo tipo de malware.

Archivo | URL | Buscar

No hay archivo seleccionado **Seleccionar**

Tamaño máximo: 128MB

Al hacer click en 'Analizar', acepta nuestros Términos del servicio y permite que VirusTotal comparta este fichero con la comunidad de seguridad. Vea nuestra Política de privacidad para más detalles.

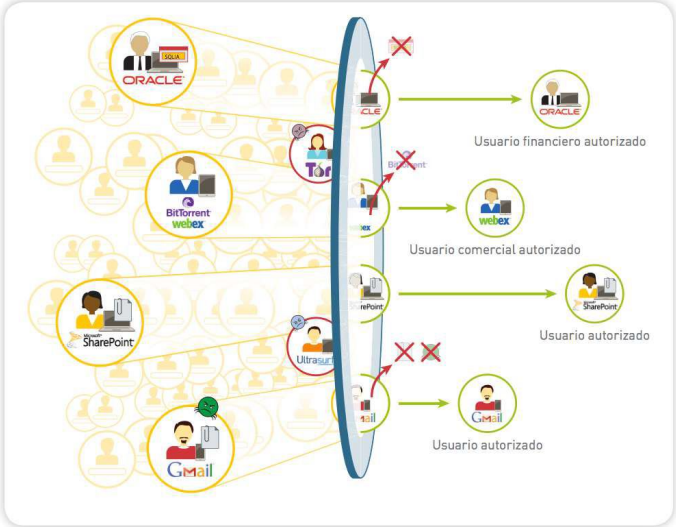
Analizar


Protección perimetral

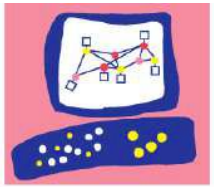
Panorámica de la Ciberseguridad… Firewall:

Tipos de Cortafuegos:

- Cortafuegos de nivel de red.
- Cortafuegos de nivel de aplicación.
- Cortafuegos con inspección de tráfico y detección de intrusiones.
- Cortafuegos de nueva generación.

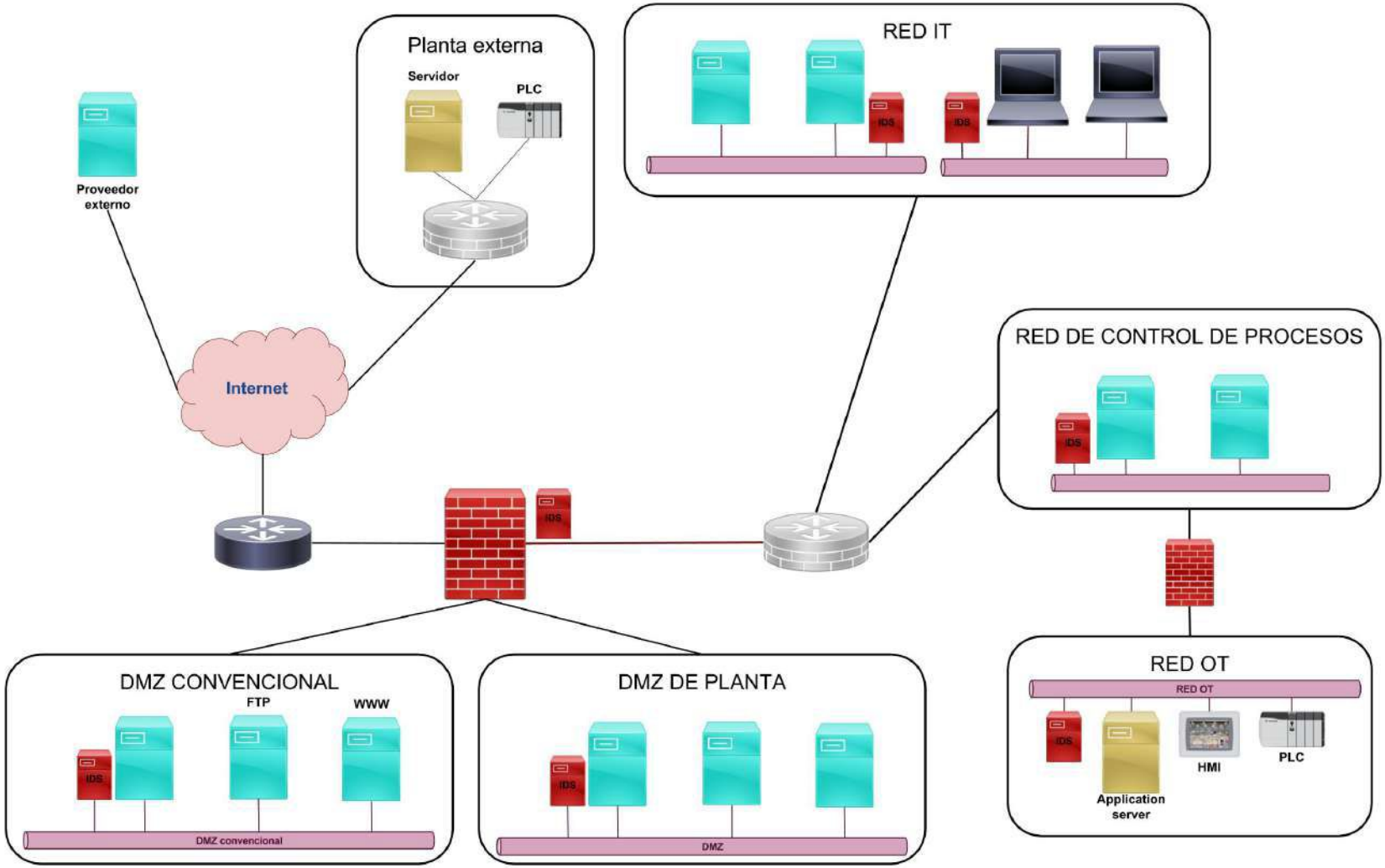


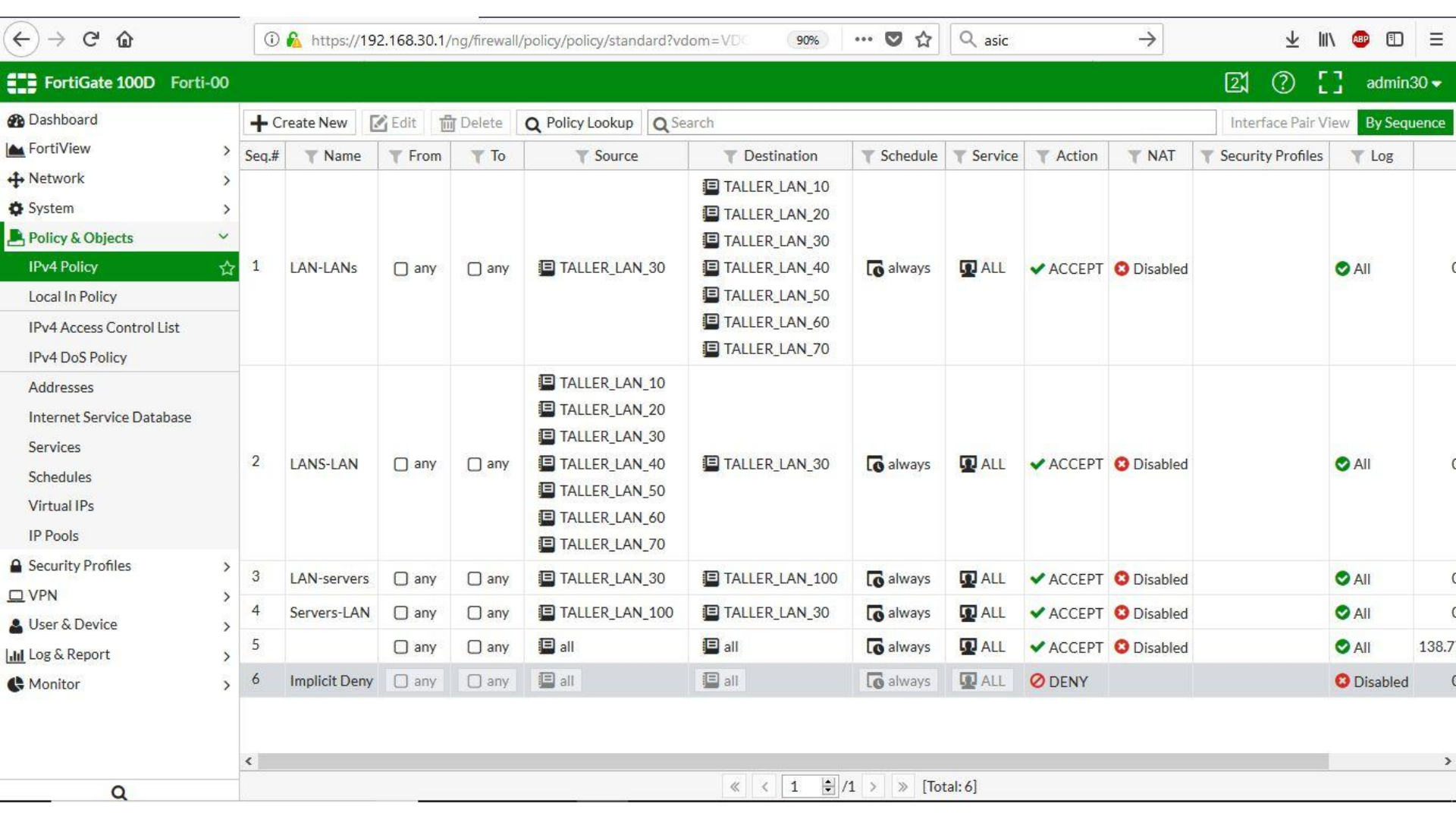
Panorámica de la Ciberseguridad… Firewall

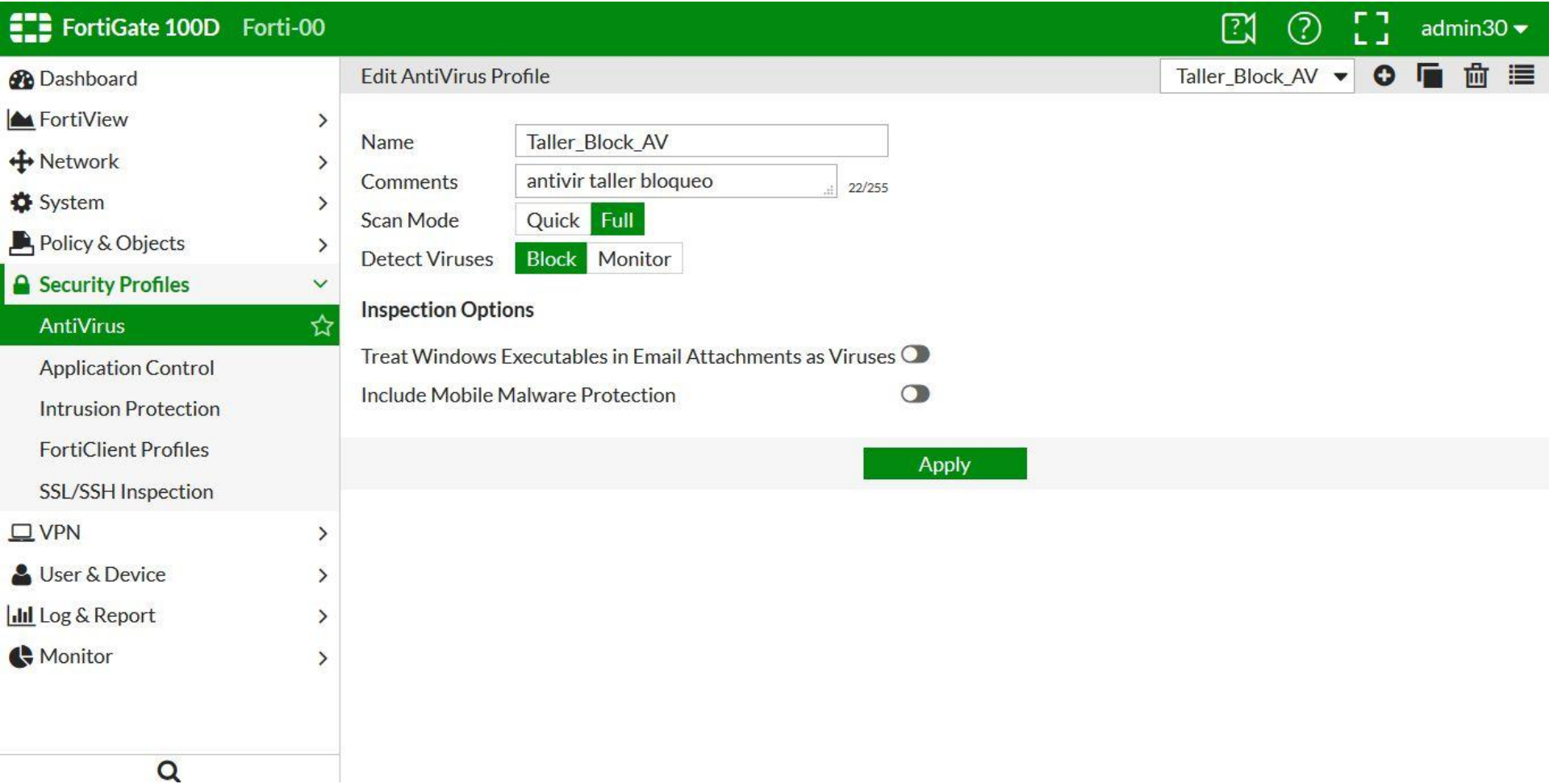


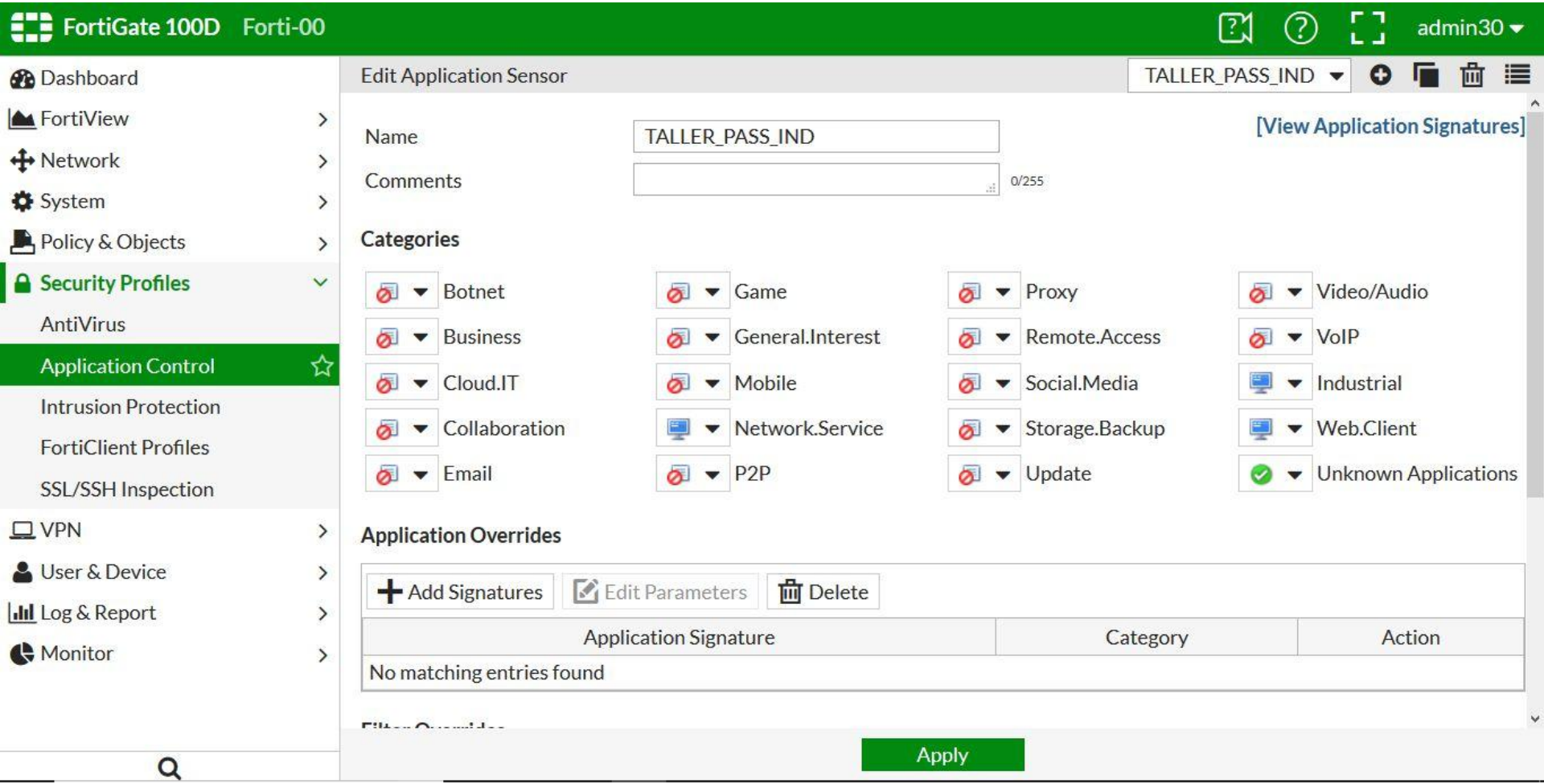
Funcionalidades a valorar:

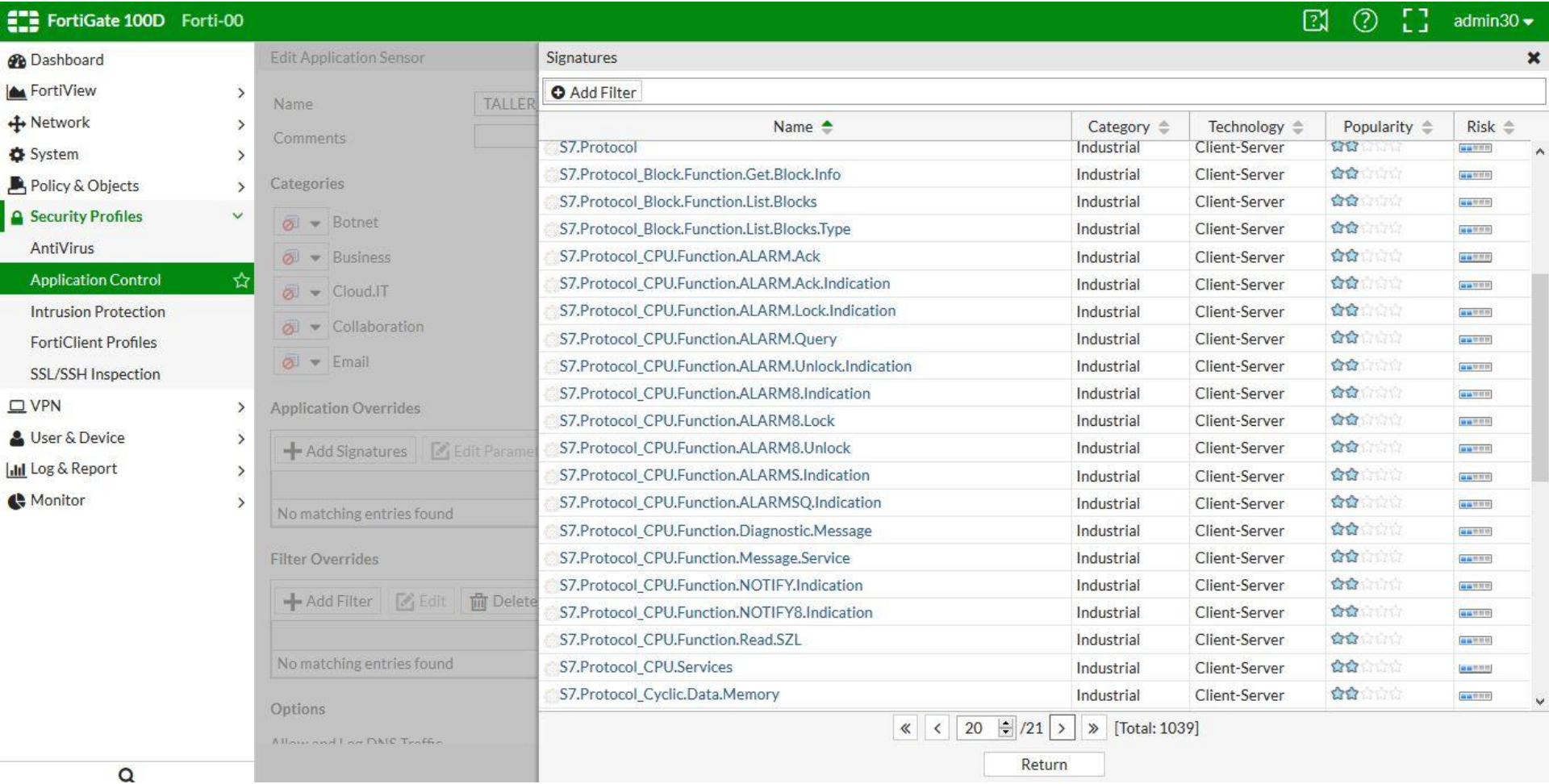
- Filtrado a nivel de aplicació
- Inspección de contenidos.
- Antivirus.
- Detección de ataques no conocidos.
- Rendimiento con todas las funcionalidades activadas.
- Control de usuarios.
- Limitación de ancho de banda por aplicación o usuario.

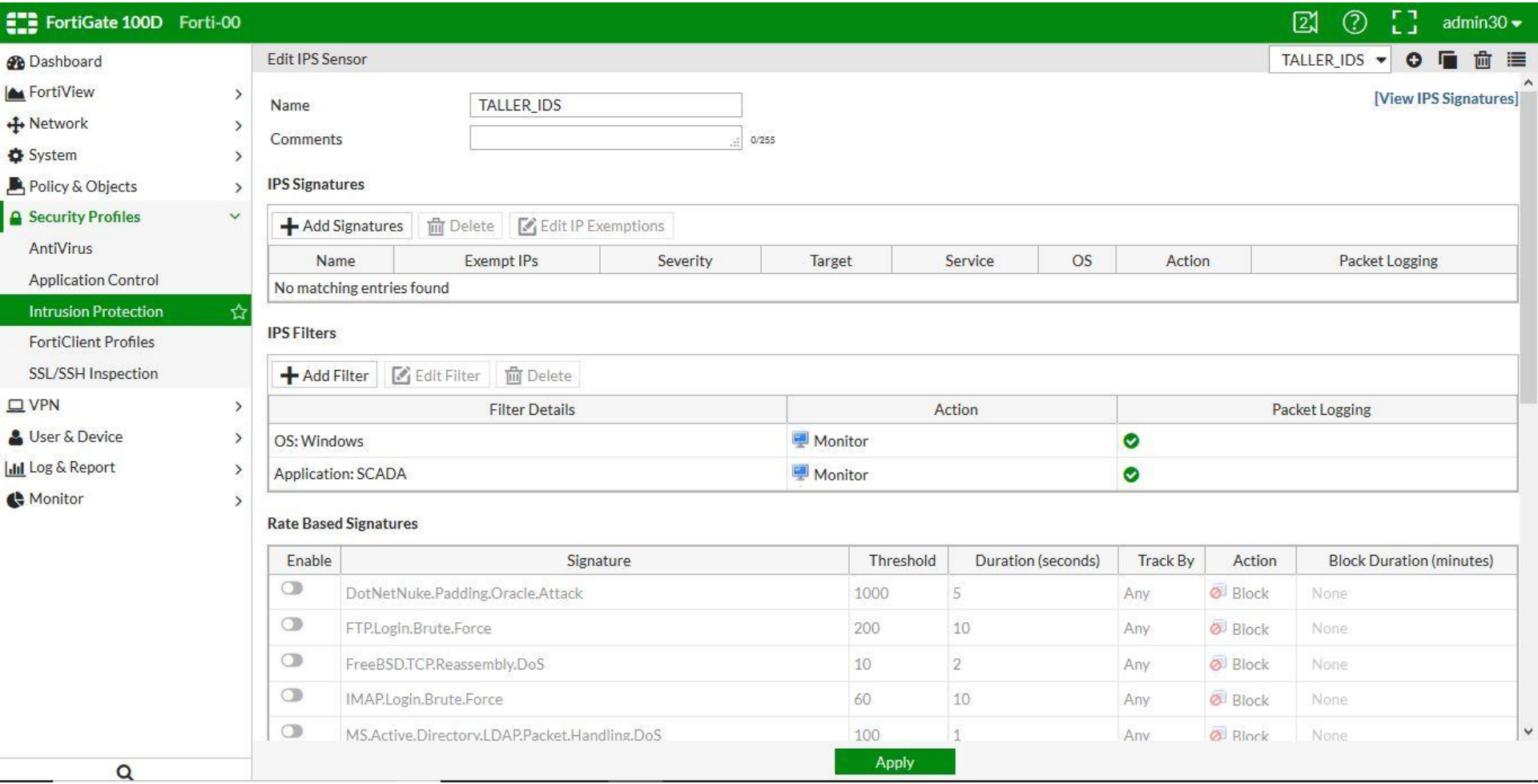

Planta externa
Servidor
PLC
RED IT
IDS
IDS
Proveedor externo
Internet
RED DE CONTROL DE PROCESOS
IDS
IDS
DMZ CONVENCIONAL
FTP
WWW
IDS
DMZ convencional
DMZ DE PLANTA
IDS
DMZ
RED OT
RED OT
IDS
HMI
PLC
Application server

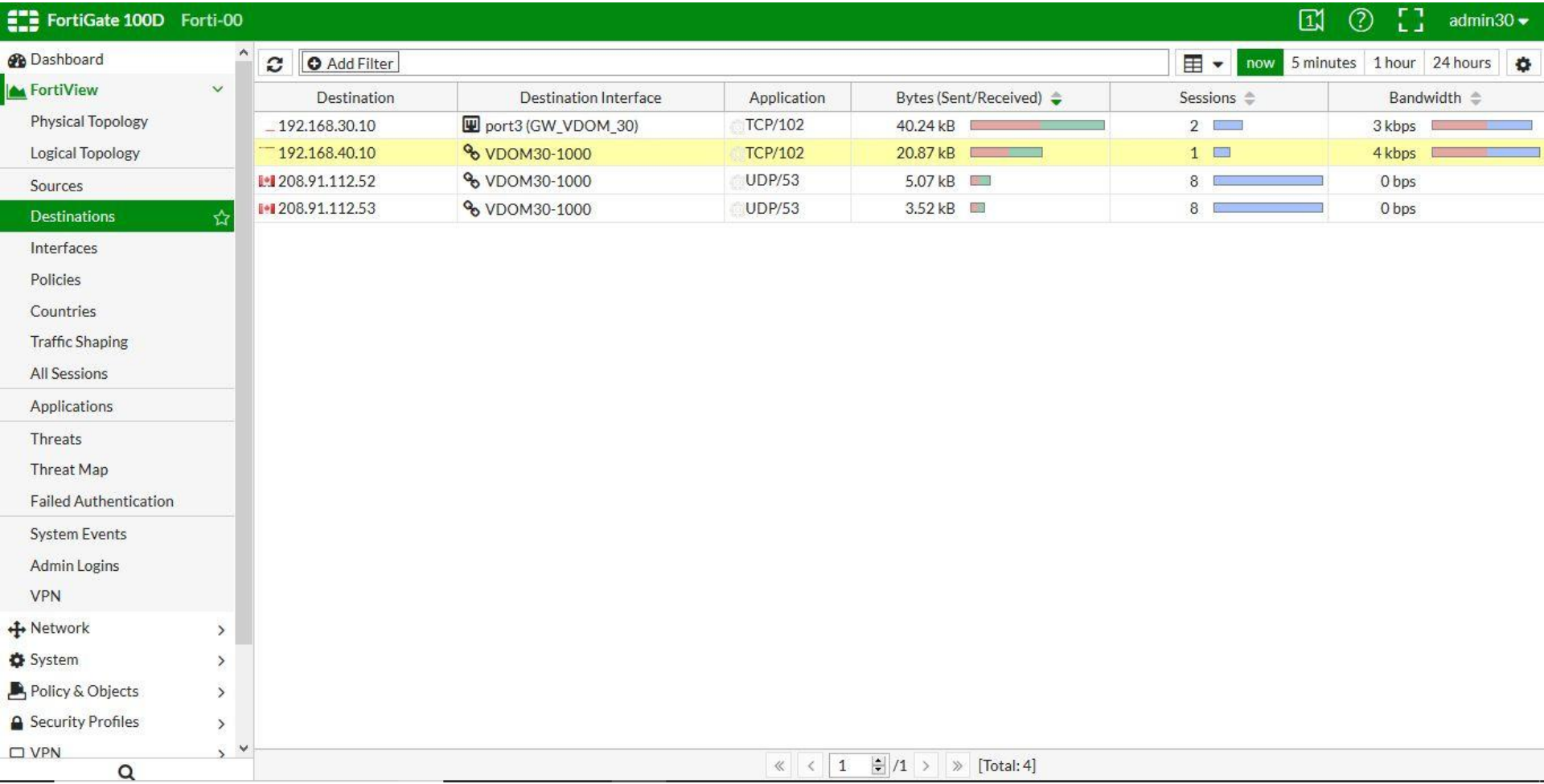

https://192.168.30.1/ng/firewall/policy/policy/standard?vdom=VD
90%
asic
FortiGate 100D Forti-00
admin30
Dashboard
FortiView
Network
System
Policy & Objects
IPv4 Policy
Local In Policy
IPv4 Access Control List
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Security Profiles
VPN
User & Device
Log & Report
Monitor
Create New
Edit
Delete
Policy Lookup
Search
Interface Pair View
By Sequence
Seq.# Name From To Source Destination Schedule Service Action NAT Security Profiles Log
1 LAN-LANs any any TALLER_LAN_30 TALLER_LAN_10 TALLER_LAN_20 TALLER_LAN_30 TALLER_LAN_40 TALLER_LAN_50 TALLER_LAN_60 TALLER_LAN_70 always ALL ACCEPT Disabled All
2 LANS-LAN any any TALLER_LAN_10 TALLER_LAN_20 TALLER_LAN_30 TALLER_LAN_40 TALLER_LAN_50 TALLER_LAN_60 TALLER_LAN_70 TALLER_LAN_30 always ALL ACCEPT Disabled All
3 LAN-servers any any TALLER_LAN_30 TALLER_LAN_100 always ALL ACCEPT Disabled All
4 Servers-LAN any any TALLER_LAN_100 TALLER_LAN_30 always ALL ACCEPT Disabled All
5 any any all all always ALL ACCEPT Disabled All
6 Implicit Deny any any all all always ALL DENY Disabled
1 /1 [Total: 6]

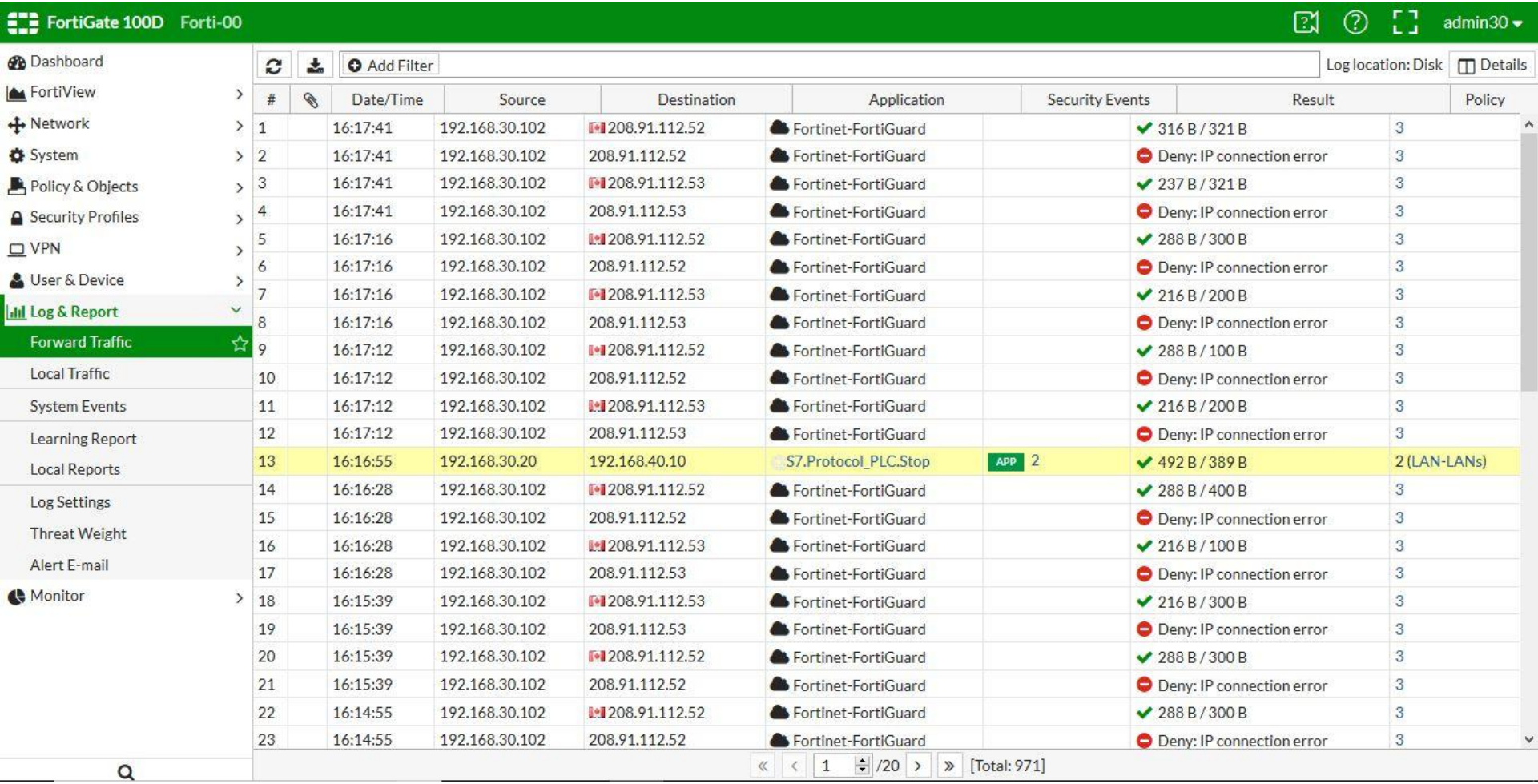

FortiGate 100D
Forti-00
admin30
Dashboard
FortiView
Network
System
Policy & Objects
Security Profiles
AntiVirus
Application Control
Intrusion Protection
FortiClient Profiles
SSL/SSH Inspection
VPN
User & Device
Log & Report
Monitor
Edit AntiVirus Profile
Taller_Block_AV
Name
Taller_Block_AV
Comments
antivir taller bloqueo
22/255
Scan Mode
Quick
Full
Detect Viruses
Block
Monitor
Inspection Options
Treat Windows Executables in Email Attachments as Viruses
Include Mobile Malware Protection
Apply


FortiGate 100D
Forti-00
admin30
Dashboard
FortiView
Network
System
Policy & Objects
Security Profiles
AntiVirus
Application Control
Intrusion Protection
FortiClient Profiles
SSL/SSH Inspection
VPN
User & Device
Log & Report
Monitor
Edit Application Sensor
TALLER_PASS_IND
[View Application Signatures]
Name
TALLER_PASS_IND
Comments
0/255
Categories
Botnet
Game
Proxy
Video/Audio
Business
General.Interest
Remote.Access
VoIP
Cloud.IT
Mobile
Social.Media
Industrial
Collaboration
Network.Service
Storage.Backup
Web.Client
Email
P2P
Update
Unknown Applications
Application Overrides
Add Signatures
Edit Parameters
Delete
Application Signature
Category
Action
No matching entries found
Apply


FortiGate 100D Forti-00
admin30
Dashboard
FortiView
Network
System
Policy & Objects
Security Profiles
AntiVirus
Application Control
Intrusion Protection
FortiClient Profiles
SSL/SSH Inspection
VPN
User & Device
Log & Report
Monitor
Edit Application Sensor
Name
Comments
Categories
Botnet
Business
Cloud.IT
Collaboration
Email
Application Overrides
Add Signatures
No matching entries found
Filter Overrides
Add Filter
Edit
Delete
No matching entries found
Options
Signatures
Add Filter
Name
Category
Technology
Popularity
Risk
S7.Protocol
Industrial
Client-Server
S7.Protocol_Block.Function.Get.Block.Info
S7.Protocol_Block.Function.List.Blocks
S7.Protocol_Block.Function.List.Blocks.Type
S7.Protocol_CPU.Function.ALARM.Ack
S7.Protocol_CPU.Function.ALARM.Ack.Indication
S7.Protocol_CPU.Function.ALARM.Lock.Indication
S7.Protocol_CPU.Function.ALARM.Query
S7.Protocol_CPU.Function.ALARM.Unlock.Indication
S7.Protocol_CPU.Function.ALARM8.Indication
S7.Protocol_CPU.Function.ALARM8.Lock
S7.Protocol_CPU.Function.ALARM8.Unlock
S7.Protocol_CPU.Function.ALARMS.Indication
S7.Protocol_CPU.Function.ALARMSQ.Indication
S7.Protocol_CPU.Function.Diagnostic.Message
S7.Protocol_CPU.Function.Message.Service
S7.Protocol_CPU.Function.NOTIFY.Indication
S7.Protocol_CPU.Function.NOTIFY8.Indication
S7.Protocol_CPU.Function.Read.SZL
S7.Protocol_CPU.Services
S7.Protocol_Cyclic.Data.Memory
20
/21
[Total: 1039]
Return


FortiGate 100D Forti-00
admin30
Dashboard
FortiView
Network
System
Policy & Objects
Security Profiles
AntiVirus
Application Control
Intrusion Protection
FortiClient Profiles
SSL/SSH Inspection
VPN
User & Device
Log & Report
Monitor
Edit IPS Sensor
TALLER_IDS
[View IPS Signatures]
Name
TALLER_IDS
Comments
0/255
IPS Signatures
Add Signatures
Delete
Edit IP Exemptions
Name
Exempt IPs
Severity
Target
Service
OS
Action
Packet Logging
No matching entries found
IPS Filters
Add Filter
Edit Filter
Delete
Filter Details
Action
Packet Logging
OS: Windows
Monitor
Application: SCADA
Monitor
Rate Based Signatures
Enable
Signature
Threshold
Duration (seconds)
Track By
Action
Block Duration (minutes)
DotNetNuke.Padding.Oracle.Attack
1000
5
Any
Block
None
FTP.Login.Brute.Force
200
10
Any
Block
None
FreeBSD.TCP.Reassembly.DoS
10
2
Any
Block
None
IMAP.Login.Brute.Force
60
10
Any
Block
None
MS.Active.Directory.LDAP.Packet.Handling.DoS
100
1
Any
Block
None
Apply


FortiGate 100D
Forti-00
admin30
Dashboard
FortiView
Physical Topology
Logical Topology
Sources
Destinations
Interfaces
Policies
Countries
Traffic Shaping
All Sessions
Applications
Threats
Threat Map
Failed Authentication
System Events
Admin Logins
VPN
Network
System
Policy & Objects
Security Profiles
VPN
Add Filter
now
5 minutes
1 hour
24 hours
Destination
Destination Interface
Application
Bytes (Sent/Received)
Sessions
Bandwidth
192.168.30.10
port3 (GW_VDOM_30)
TCP/102
40.24 kB
2
3 kbps
192.168.40.10
VDOM30-1000
TCP/102
20.87 kB
1
4 kbps
208.91.112.52
VDOM30-1000
UDP/53
5.07 kB
8
0 bps
208.91.112.53
VDOM30-1000
UDP/53
3.52 kB
8
0 bps
1
/1
[Total: 4]


FortiGate 100D Forti-00
admin30
Dashboard
FortiView
Network
System
Policy & Objects
Security Profiles
VPN
User & Device
Log & Report
Forward Traffic
Local Traffic
System Events
Learning Report
Local Reports
Log Settings
Threat Weight
Alert E-mail
Monitor
Add Filter
Log location: Disk
Details
| Date/Time | Source | Destination | Application | Security Events | Result | Policy
1 16:17:41 192.168.30.102 208.91.112.52 Fortinet-FortiGuard 316 B / 321 B 3
2 16:17:41 192.168.30.102 208.91.112.52 Fortinet-FortiGuard Deny: IP connection error 3
3 16:17:41 192.168.30.102 208.91.112.53 Fortinet-FortiGuard 237 B / 321 B 3
4 16:17:41 192.168.30.102 208.91.112.53 Fortinet-FortiGuard Deny: IP connection error 3
5 16:17:16 192.168.30.102 208.91.112.52 Fortinet-FortiGuard 288 B / 300 B 3
6 16:17:16 192.168.30.102 208.91.112.52 Fortinet-FortiGuard Deny: IP connection error 3
7 16:17:16 192.168.30.102 208.91.112.53 Fortinet-FortiGuard 216 B / 200 B 3
8 16:17:16 192.168.30.102 208.91.112.53 Fortinet-FortiGuard Deny: IP connection error 3
9 16:17:12 192.168.30.102 208.91.112.52 Fortinet-FortiGuard 288 B / 100 B 3
10 16:17:12 192.168.30.102 208.91.112.52 Fortinet-FortiGuard Deny: IP connection error 3
11 16:17:12 192.168.30.102 208.91.112.53 Fortinet-FortiGuard 216 B / 200 B 3
12 16:17:12 192.168.30.102 208.91.112.53 Fortinet-FortiGuard Deny: IP connection error 3
13 16:16:55 192.168.30.20 192.168.40.10 S7.Protocol_PLC.Stop APP 2 492 B / 389 B 2 (LAN-LANs)
14 16:16:28 192.168.30.102 208.91.112.52 Fortinet-FortiGuard 288 B / 400 B 3
15 16:16:28 192.168.30.102 208.91.112.52 Fortinet-FortiGuard Deny: IP connection error 3
16 16:16:28 192.168.30.102 208.91.112.53 Fortinet-FortiGuard 216 B / 100 B 3
17 16:16:28 192.168.30.102 208.91.112.53 Fortinet-FortiGuard Deny: IP connection error 3
18 16:15:39 192.168.30.102 208.91.112.53 Fortinet-FortiGuard 216 B / 300 B 3
19 16:15:39 192.168.30.102 208.91.112.53 Fortinet-FortiGuard Deny: IP connection error 3
20 16:15:39 192.168.30.102 208.91.112.52 Fortinet-FortiGuard 288 B / 300 B 3
21 16:15:39 192.168.30.102 208.91.112.52 Fortinet-FortiGuard Deny: IP connection error 3
22 16:14:55 192.168.30.102 208.91.112.52 Fortinet-FortiGuard 288 B / 300 B 3
23 16:14:55 192.168.30.102 208.91.112.52 Fortinet-FortiGuard Deny: IP connection error 3
1 /20
[Total: 971]

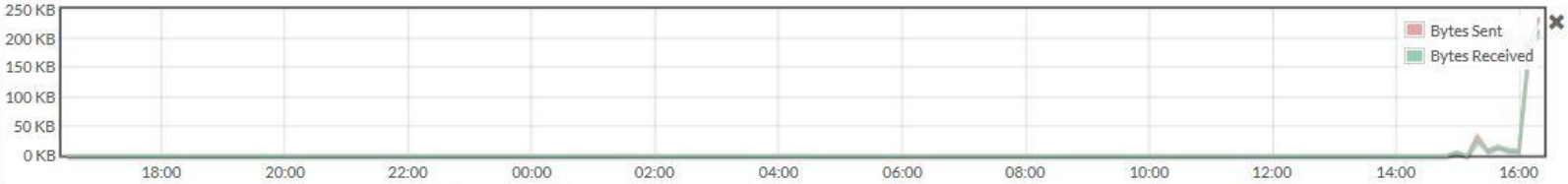
FortiGate 100D Forti-00

admin30

- Dashboard
- FortiView
  - Physical Topology
  - Logical Topology
  - Sources
  - Destinations
  - Interfaces
  - Policies
  - Countries
  - Traffic Shaping
  - All Sessions
  - Applications
  - Threats
  - Threat Map
  - Failed Authentication
  - System Events
  - Admin Logins
  - VPN
- Network
- System
- Policy & Objects
- Security Profiles
- VPN

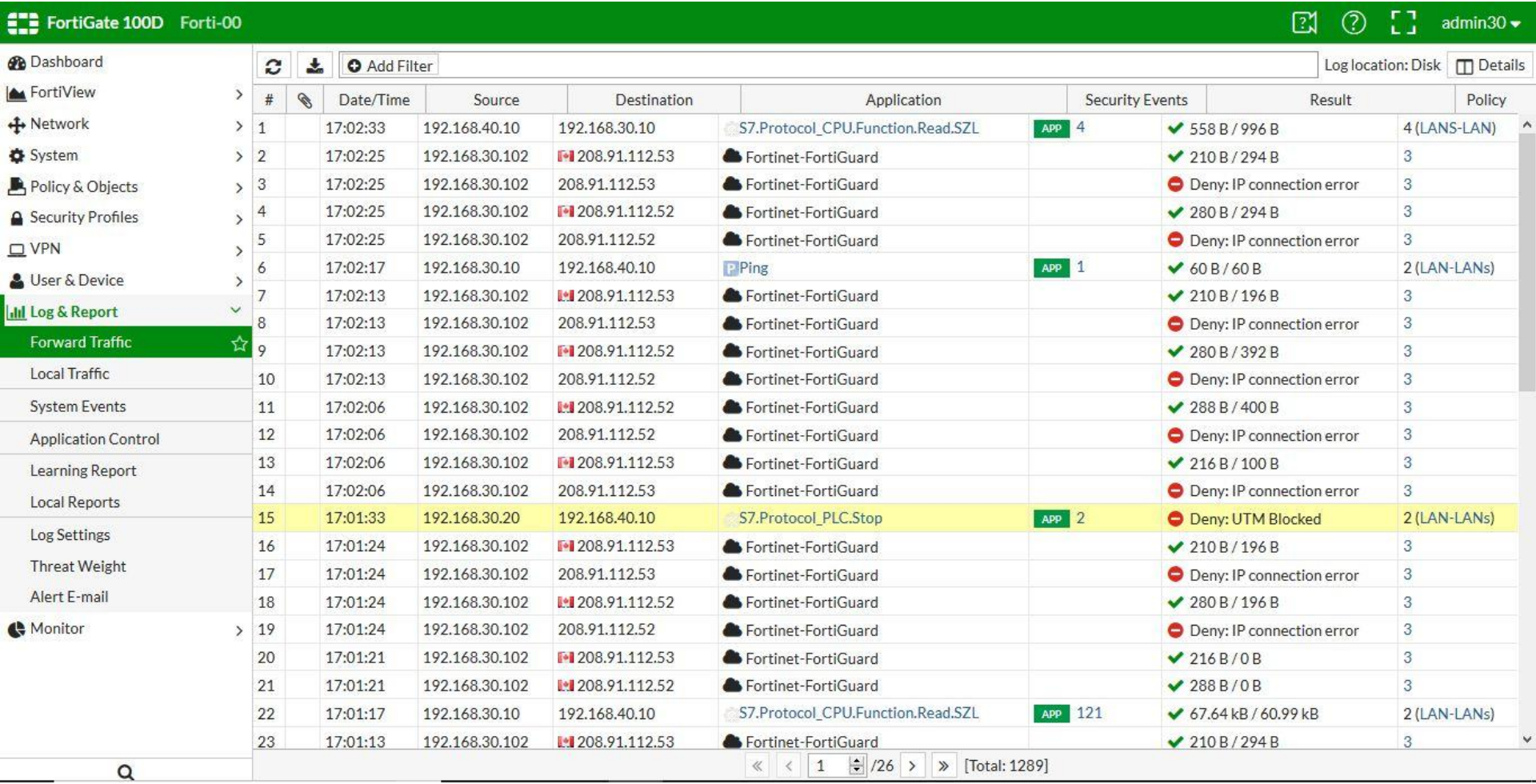
Add Filter | now | 5 minutes | 1 hour | 24 hours

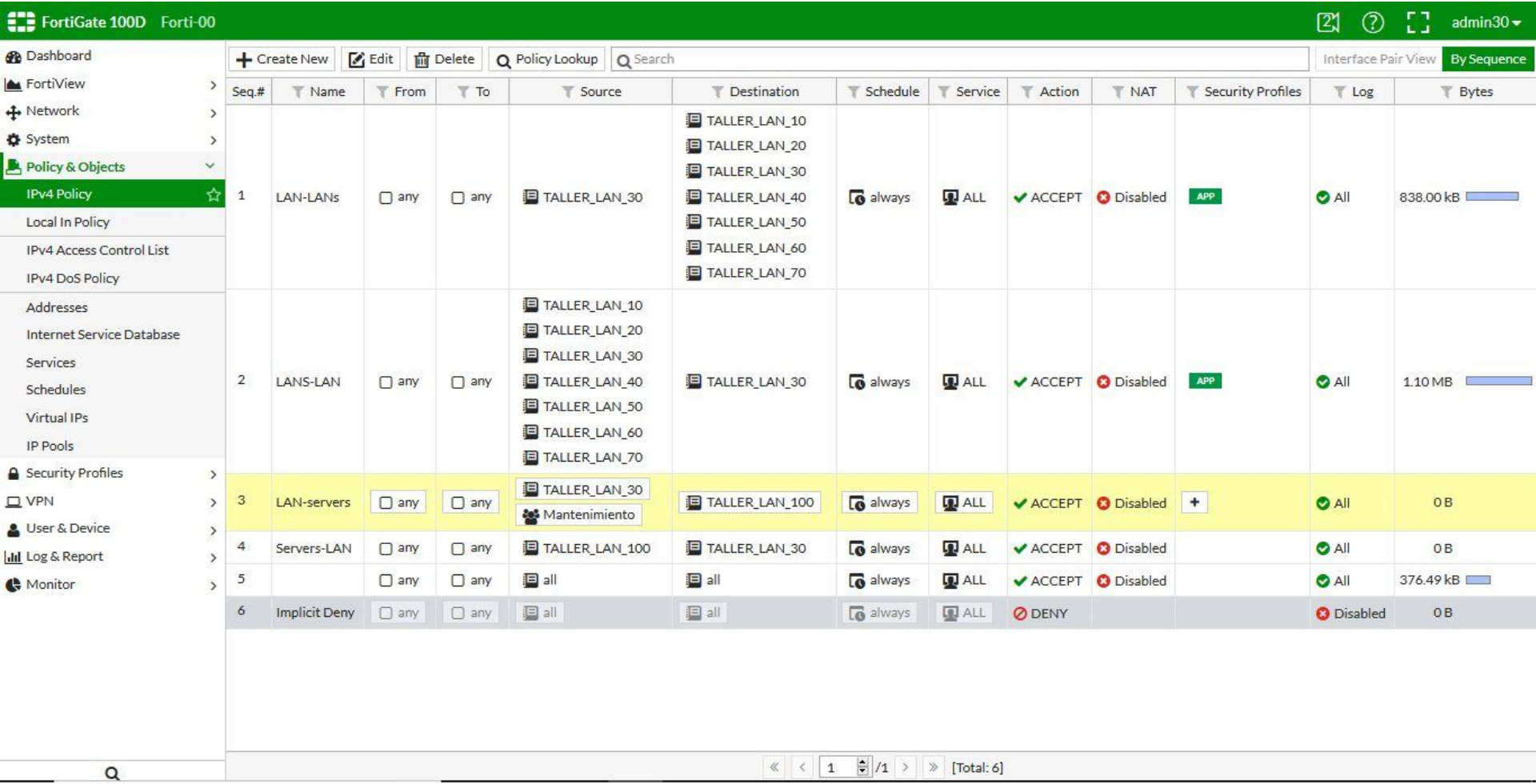
Some configuration dependencies have not been met for applications

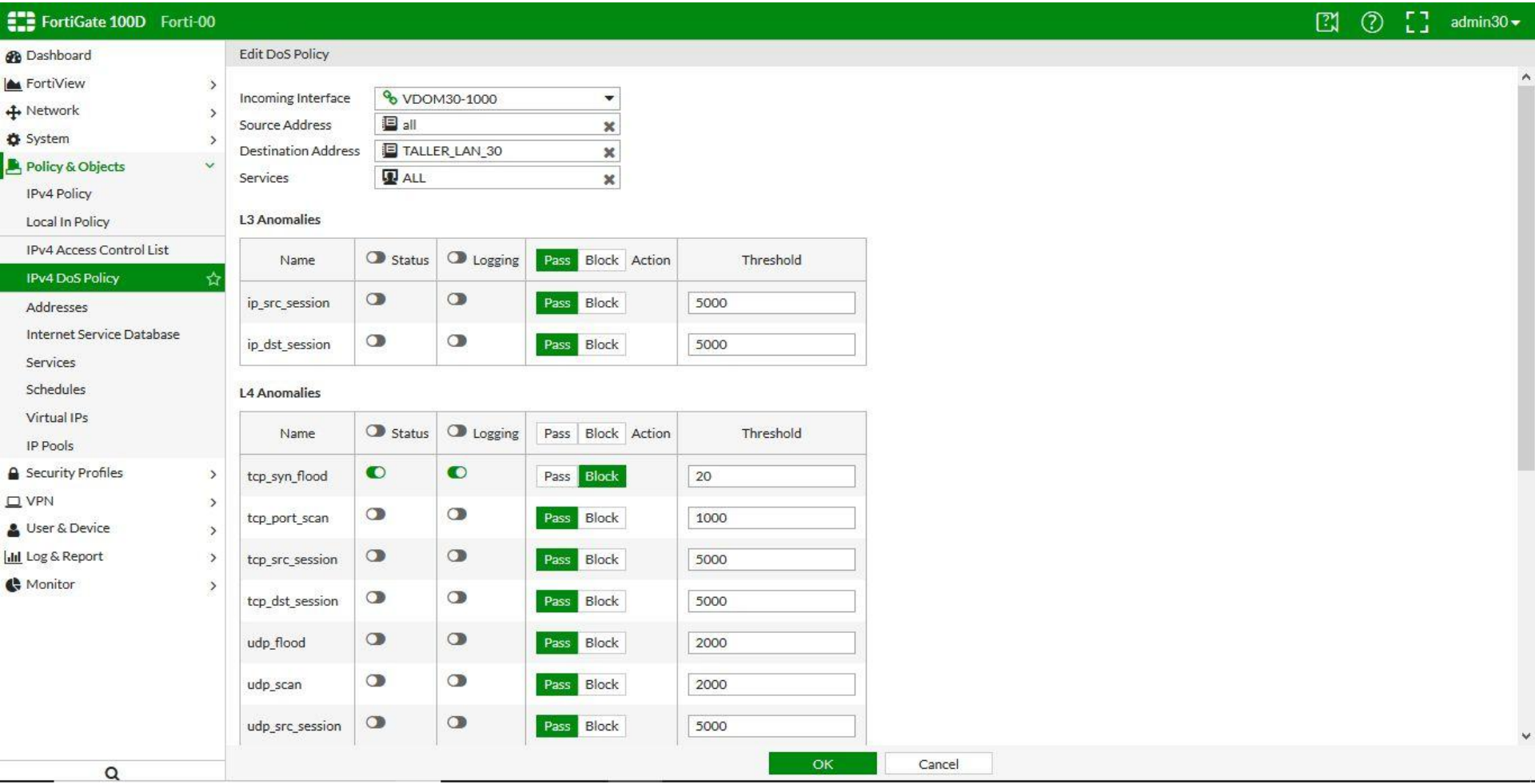


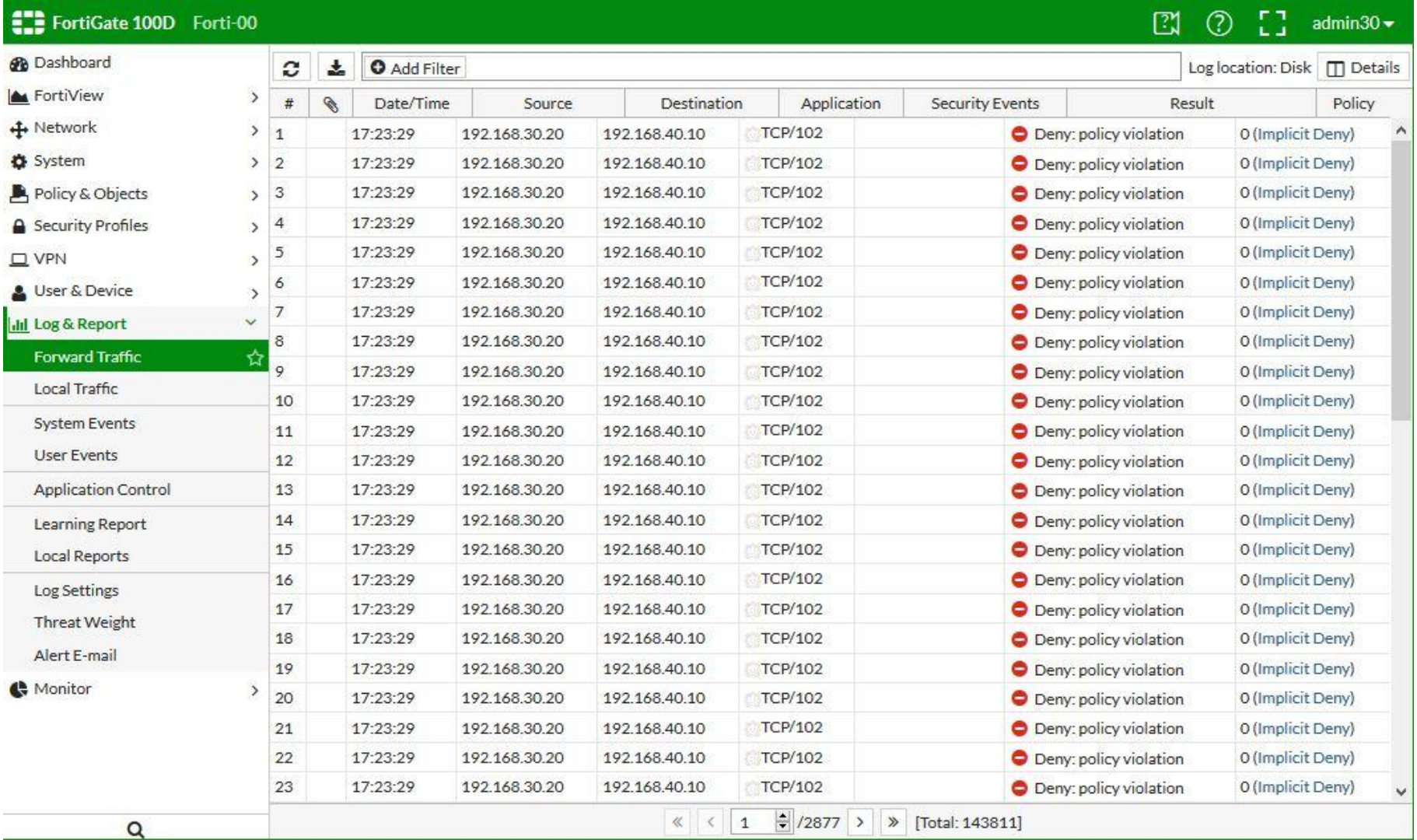
Application	Category	Risk	Bytes (Sent/Received)	Sessions (Blocked/Allowed)
S7.Protocol	Industrial		881 B	1

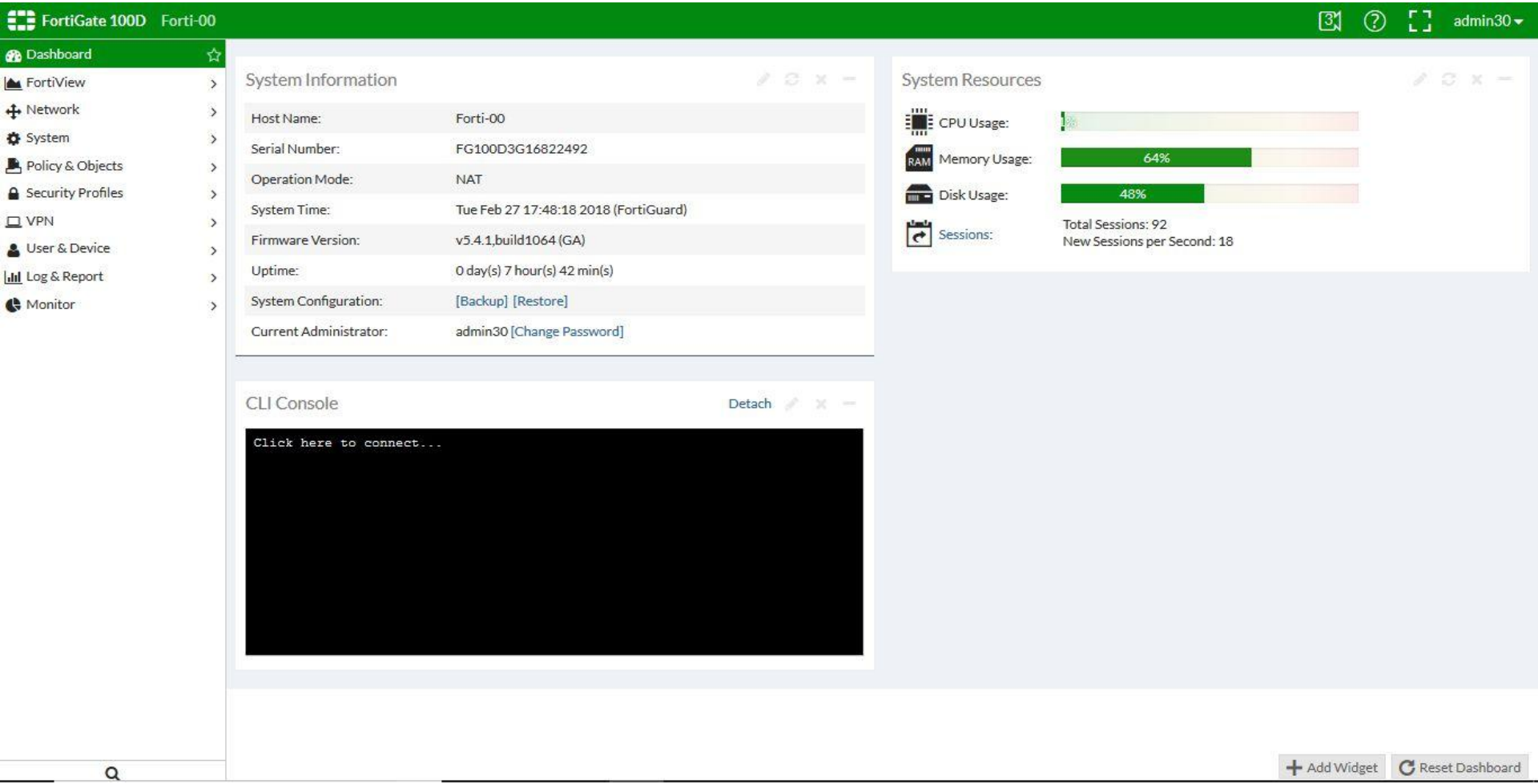
1 /1 [Total: 1]


FortiGate 100D Forti-00
admin30
Dashboard
FortiView
Network
System
Policy & Objects
Security Profiles
VPN
User & Device
Log & Report
Forward Traffic
Local Traffic
System Events
Application Control
Learning Report
Local Reports
Log Settings
Threat Weight
Alert E-mail
Monitor
Add Filter
Log location: Disk
Details
Date/Time Source Destination Application Security Events Result Policy
1 17:02:33 192.168.40.10 192.168.30.10 S7.Protocol_CPU.Function.Read.SZL APP 4 558 B / 996 B 4 (LANS-LAN)
2 17:02:25 192.168.30.102 208.91.112.53 Fortinet-FortiGuard 210 B / 294 B 3
3 17:02:25 192.168.30.102 208.91.112.53 Fortinet-FortiGuard Deny: IP connection error 3
4 17:02:25 192.168.30.102 208.91.112.52 Fortinet-FortiGuard 280 B / 294 B 3
5 17:02:25 192.168.30.102 208.91.112.52 Fortinet-FortiGuard Deny: IP connection error 3
6 17:02:17 192.168.30.10 192.168.40.10 Ping APP 1 60 B / 60 B 2 (LAN-LANs)
7 17:02:13 192.168.30.102 208.91.112.53 Fortinet-FortiGuard 210 B / 196 B 3
8 17:02:13 192.168.30.102 208.91.112.53 Fortinet-FortiGuard Deny: IP connection error 3
9 17:02:13 192.168.30.102 208.91.112.52 Fortinet-FortiGuard 280 B / 392 B 3
10 17:02:13 192.168.30.102 208.91.112.52 Fortinet-FortiGuard Deny: IP connection error 3
11 17:02:06 192.168.30.102 208.91.112.52 Fortinet-FortiGuard 288 B / 400 B 3
12 17:02:06 192.168.30.102 208.91.112.52 Fortinet-FortiGuard Deny: IP connection error 3
13 17:02:06 192.168.30.102 208.91.112.53 Fortinet-FortiGuard 216 B / 100 B 3
14 17:02:06 192.168.30.102 208.91.112.53 Fortinet-FortiGuard Deny: IP connection error 3
15 17:01:33 192.168.30.20 192.168.40.10 S7.Protocol_PLC.Stop APP 2 Deny: UTM Blocked 2 (LAN-LANs)
16 17:01:24 192.168.30.102 208.91.112.53 Fortinet-FortiGuard 210 B / 196 B 3
17 17:01:24 192.168.30.102 208.91.112.53 Fortinet-FortiGuard Deny: IP connection error 3
18 17:01:24 192.168.30.102 208.91.112.52 Fortinet-FortiGuard 280 B / 196 B 3
19 17:01:24 192.168.30.102 208.91.112.52 Fortinet-FortiGuard Deny: IP connection error 3
20 17:01:21 192.168.30.102 208.91.112.53 Fortinet-FortiGuard 216 B / 0 B 3
21 17:01:21 192.168.30.102 208.91.112.52 Fortinet-FortiGuard 288 B / 0 B 3
22 17:01:17 192.168.30.10 192.168.40.10 S7.Protocol_CPU.Function.Read.SZL APP 121 67.64 kB / 60.99 kB 2 (LAN-LANs)
23 17:01:13 192.168.30.102 208.91.112.53 Fortinet-FortiGuard 210 B / 294 B 3
1 /26
[Total: 1289]


FortiGate 100D Forti-00
admin30
Dashboard
FortiView
Network
System
Policy & Objects
IPv4 Policy
Local In Policy
IPv4 Access Control List
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Security Profiles
VPN
User & Device
Log & Report
Monitor
Create New
Edit
Delete
Policy Lookup
Search
Interface Pair View
By Sequence
Seq.# Name From To Source Destination Schedule Service Action NAT Security Profiles Log Bytes
1 LAN-LANs any any TALLER_LAN_30 TALLER_LAN_10 TALLER_LAN_20 TALLER_LAN_30 TALLER_LAN_40 TALLER_LAN_50 TALLER_LAN_60 TALLER_LAN_70 always ALL ACCEPT Disabled APP All 838.00 kB
2 LANS-LAN any any TALLER_LAN_10 TALLER_LAN_20 TALLER_LAN_30 TALLER_LAN_40 TALLER_LAN_50 TALLER_LAN_60 TALLER_LAN_70 TALLER_LAN_30 always ALL ACCEPT Disabled APP All 1.10 MB
3 LAN-servers any any TALLER_LAN_30 Mantenimiento TALLER_LAN_100 always ALL ACCEPT Disabled + All 0 B
4 Servers-LAN any any TALLER_LAN_100 TALLER_LAN_30 always ALL ACCEPT Disabled All 0 B
5 any any all all always ALL ACCEPT Disabled All 376.49 kB
6 Implicit Deny any any all all always ALL DENY Disabled 0 B
1 /1 [Total: 6]


FortiGate 100D Forti-00
admin30
Dashboard
FortiView
Network
System
Policy & Objects
IPv4 Policy
Local In Policy
IPv4 Access Control List
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Security Profiles
VPN
User & Device
Log & Report
Monitor
Edit DoS Policy
Incoming Interface VDOM30-1000
Source Address all
Destination Address TALLER_LAN_30
Services ALL
L3 Anomalies
Name Status Logging Pass Block Action Threshold
ip_src_session Pass Block 5000
ip_dst_session Pass Block 5000
L4 Anomalies
Name Status Logging Pass Block Action Threshold
tcp_syn_flood Pass Block 20
tcp_port_scan Pass Block 1000
tcp_src_session Pass Block 5000
tcp_dst_session Pass Block 5000
udp_flood Pass Block 2000
udp_scan Pass Block 2000
udp_src_session Pass Block 5000
OK
Cancel


FortiGate 100D
Forti-00
admin30
Dashboard
FortiView
Network
System
Policy & Objects
Security Profiles
VPN
User & Device
Log & Report
Forward Traffic
Local Traffic
System Events
User Events
Application Control
Learning Report
Local Reports
Log Settings
Threat Weight
Alert E-mail
Monitor
Add Filter
Log location: Disk
Details
| Date/Time | Source | Destination | Application | Security Events | Result | Policy
1 17:23:29 192.168.30.20 192.168.40.10 TCP/102 Deny: policy violation 0 (Implicit Deny)
2 17:23:29 192.168.30.20 192.168.40.10 TCP/102 Deny: policy violation 0 (Implicit Deny)
3 17:23:29 192.168.30.20 192.168.40.10 TCP/102 Deny: policy violation 0 (Implicit Deny)
4 17:23:29 192.168.30.20 192.168.40.10 TCP/102 Deny: policy violation 0 (Implicit Deny)
5 17:23:29 192.168.30.20 192.168.40.10 TCP/102 Deny: policy violation 0 (Implicit Deny)
6 17:23:29 192.168.30.20 192.168.40.10 TCP/102 Deny: policy violation 0 (Implicit Deny)
7 17:23:29 192.168.30.20 192.168.40.10 TCP/102 Deny: policy violation 0 (Implicit Deny)
8 17:23:29 192.168.30.20 192.168.40.10 TCP/102 Deny: policy violation 0 (Implicit Deny)
9 17:23:29 192.168.30.20 192.168.40.10 TCP/102 Deny: policy violation 0 (Implicit Deny)
10 17:23:29 192.168.30.20 192.168.40.10 TCP/102 Deny: policy violation 0 (Implicit Deny)
11 17:23:29 192.168.30.20 192.168.40.10 TCP/102 Deny: policy violation 0 (Implicit Deny)
12 17:23:29 192.168.30.20 192.168.40.10 TCP/102 Deny: policy violation 0 (Implicit Deny)
13 17:23:29 192.168.30.20 192.168.40.10 TCP/102 Deny: policy violation 0 (Implicit Deny)
14 17:23:29 192.168.30.20 192.168.40.10 TCP/102 Deny: policy violation 0 (Implicit Deny)
15 17:23:29 192.168.30.20 192.168.40.10 TCP/102 Deny: policy violation 0 (Implicit Deny)
16 17:23:29 192.168.30.20 192.168.40.10 TCP/102 Deny: policy violation 0 (Implicit Deny)
17 17:23:29 192.168.30.20 192.168.40.10 TCP/102 Deny: policy violation 0 (Implicit Deny)
18 17:23:29 192.168.30.20 192.168.40.10 TCP/102 Deny: policy violation 0 (Implicit Deny)
19 17:23:29 192.168.30.20 192.168.40.10 TCP/102 Deny: policy violation 0 (Implicit Deny)
20 17:23:29 192.168.30.20 192.168.40.10 TCP/102 Deny: policy violation 0 (Implicit Deny)
21 17:23:29 192.168.30.20 192.168.40.10 TCP/102 Deny: policy violation 0 (Implicit Deny)
22 17:23:29 192.168.30.20 192.168.40.10 TCP/102 Deny: policy violation 0 (Implicit Deny)
23 17:23:29 192.168.30.20 192.168.40.10 TCP/102 Deny: policy violation 0 (Implicit Deny)
1 /2877
[Total: 143811]


FortiGate 100D Forti-00
admin30
Dashboard
FortiView
Network
System
Policy & Objects
Security Profiles
VPN
User & Device
Log & Report
Monitor
System Information
Host Name: Forti-00
Serial Number: FG100D3G16822492
Operation Mode: NAT
System Time: Tue Feb 27 17:48:18 2018 (FortiGuard)
Firmware Version: v5.4.1,build1064 (GA)
Uptime: 0 day(s) 7 hour(s) 42 min(s)
System Configuration: [Backup] [Restore]
Current Administrator: admin30 [Change Password]
CLI Console
Detach
Click here to connect...
System Resources
CPU Usage:
Memory Usage: 64%
Disk Usage: 48%
Sessions:
Total Sessions: 92
New Sessions per Second: 18
Add Widget
Reset Dashboard

FortiGate 100D Forti-00

admin30

- Dashboard
- FortiView
  - Physical Topology
  - Logical Topology
  - Sources
  - Destinations
  - Interfaces
  - Policies
  - Countries
  - Traffic Shaping
  - All Sessions
- Applications
- Threats
- Threat Map
- Failed Authentication
- System Events
- Admin Logins
- VPN
- Network
- System
- Policy & Objects
- Security Profiles
- VPN
- User & Device
- Log & Report
- Monitor

Add Filter

now | 5 minutes | 1 hour | 24 hours

Source	Device	Threat Score (Blocked/Allowed)	Bytes (Sent/Received)	Sessions (Blocked/Allowed)
192.168.20.10		10	947.36 kB	21
user11 (192.168.30.10)		5	912.99 kB	12
192.168.30.102		4270	387.13 kB	1672
192.168.40.10		0	141.13 kB	40
192.168.20.20		0	3.60 kB	5
192.168.20.102		15	2.60 kB	6
192.168.50.20		0	2.50 kB	4
192.168.30.20		4268160	2.29 kB	142275
192.168.40.20		0	993 B	1
192.168.50.100		5	444 B	2
192.168.10.10		5	148 B	2
192.168.70.20		0	100 B	1
192.168.30.101		190	0 B	38

1 /1 [Total: 13]

Dashboard
FortiView
Physical Topology
Logical Topology
Sources
Destinations
Interfaces
Policies
Countries
Traffic Shaping
All Sessions
Applications
Threats
Threat Map
Failed Authentication
System Events
Admin Logins
VPN
Network
System
Policy & Objects
Security Profiles
VPN
User & Device
Log & Report
Monitor

Add Filter | now | 5 minutes | 1 hour | 24 hours

Destination	Destination Interface	Application	Bytes (Sent/Received)	Sessions (Blocked/Allowed)
192.168.30.10	port3 (GW_VDOM_30)	PING, icmp/0/05, 4 More...	1.10 MB	82
192.168.40.10	unknown-0	S7.Protocol_PLC.Stop, S7.Protocol_CPU.Function.Read.SZL, 3 More...	909.90 kB	142284
208.91.112.52	unknown-0	UDP/53, DNS	216.29 kB	838
208.91.112.53	unknown-0	UDP/53, DNS	162.26 kB	823
193.146.78.26	VDOM30-1000	TCP/443, HTTPS	7.09 kB	41
192.168.100.254	VDOM30-1000	HTTP	5.02 kB	2
192.168.10.10	VDOM30-1000	PING, icmp/0/05	952 B	3
192.168.100.1	VDOM30-1000	PING	360 B	1
192.168.1.1	VDOM30-1000	PING, icmp/0/05	296 B	2
192.168.10.1	VDOM30-1000	PING	240 B	1
17.173.254.222	unknown-0	UDP/16385	0 B	1
17.173.254.223	unknown-0	UDP/16386	0 B	1

1 /1 [Total: 12]

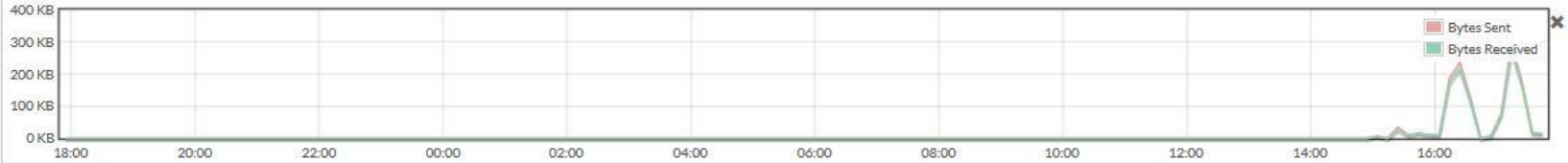
FortiGate 100D Forti-00

admin30

- Dashboard
- FortiView
  - Physical Topology
  - Logical Topology
  - Sources
  - Destinations
  - Interfaces
  - Policies
  - Countries
  - Traffic Shaping
  - All Sessions
  - Applications
  - Threats
  - Threat Map
  - Failed Authentication
  - System Events
  - Admin Logins
  - VPN
- Network
- System
- Policy & Objects
- Security Profiles
- VPN
- User & Device
- Log & Report
- Monitor

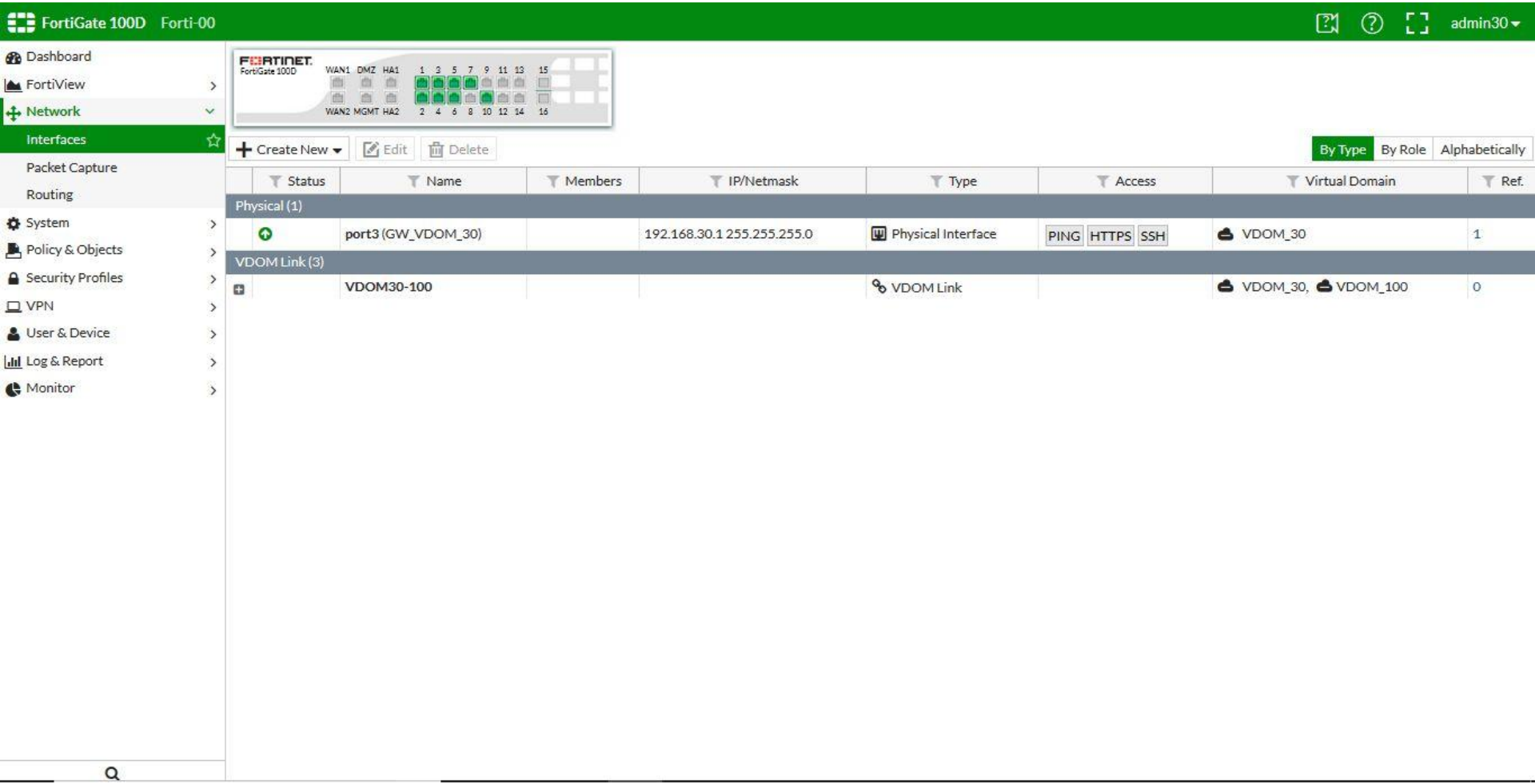
Add Filter

now | 5 minutes | 1 hour | 24 hours



Policy	Source Interface	Destination Interface	Bytes (Sent/Received)	Sessions (Blocked/Allowed)
4 (LANS-LAN)	VDOM30-1000	port3 (GW_VDOM_30)	1.10 MB	78
2 (LAN-LANs)	port3 (GW_VDOM_30)	VDOM30-1000	910.26 kB	13
3	port3 (GW_VDOM_30)	port3 (GW_VDOM_30)	389.35 kB	1714
5 (LAN-servers)	port3 (GW_VDOM_30)	VDOM30-1000	4.38 kB	1
0 (Implicit Deny)	port3 (GW_VDOM_30)	VDOM30-1000	642 B	142273

1 /1 [Total: 5]


FortiGate 100D
Forti-00
admin30
Dashboard
FortiView
Network
Interfaces
Packet Capture
Routing
System
Policy & Objects
Security Profiles
VPN
User & Device
Log & Report
Monitor
WAN1 DMZ HA1
WAN2 MGMT HA2
Create New
Edit
Delete
By Type
By Role
Alphabetically
Status
Name
Members
IP/Netmask
Type
Access
Virtual Domain
Ref.
Physical (1)
port3 (GW_VDOM_30)
192.168.30.1 255.255.255.0
Physical Interface
PING HTTPS SSH
VDOM_30
1
VDOM Link (3)
VDOM30-100
VDOM Link
VDOM_30, VDOM_100
0

FortiGate 100D Forti-00

admin30

- Dashboard
- FortiView
- Network
- System
- Policy & Objects
- Security Profiles
- VPN
  - IPsec Tunnels
  - IPsec Concentrator
  - IPsec Wizard
  - IPsec Tunnel Templates
  - SSL-VPN Portals
  - SSL-VPN Settings
  - SSL-VPN Personal Bookmarks
  - SSL-VPN Realms
- User & Device
- Log & Report
- Monitor

VPN Creation Wizard

1 VPN Setup > 2 Authentication > 3 Policy & Routing

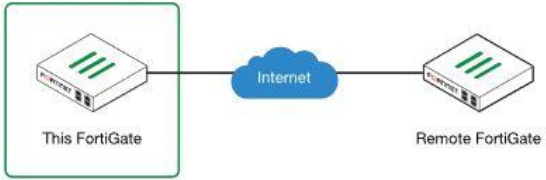
Name

Template Type: Site to Site | Remote Access | Custom

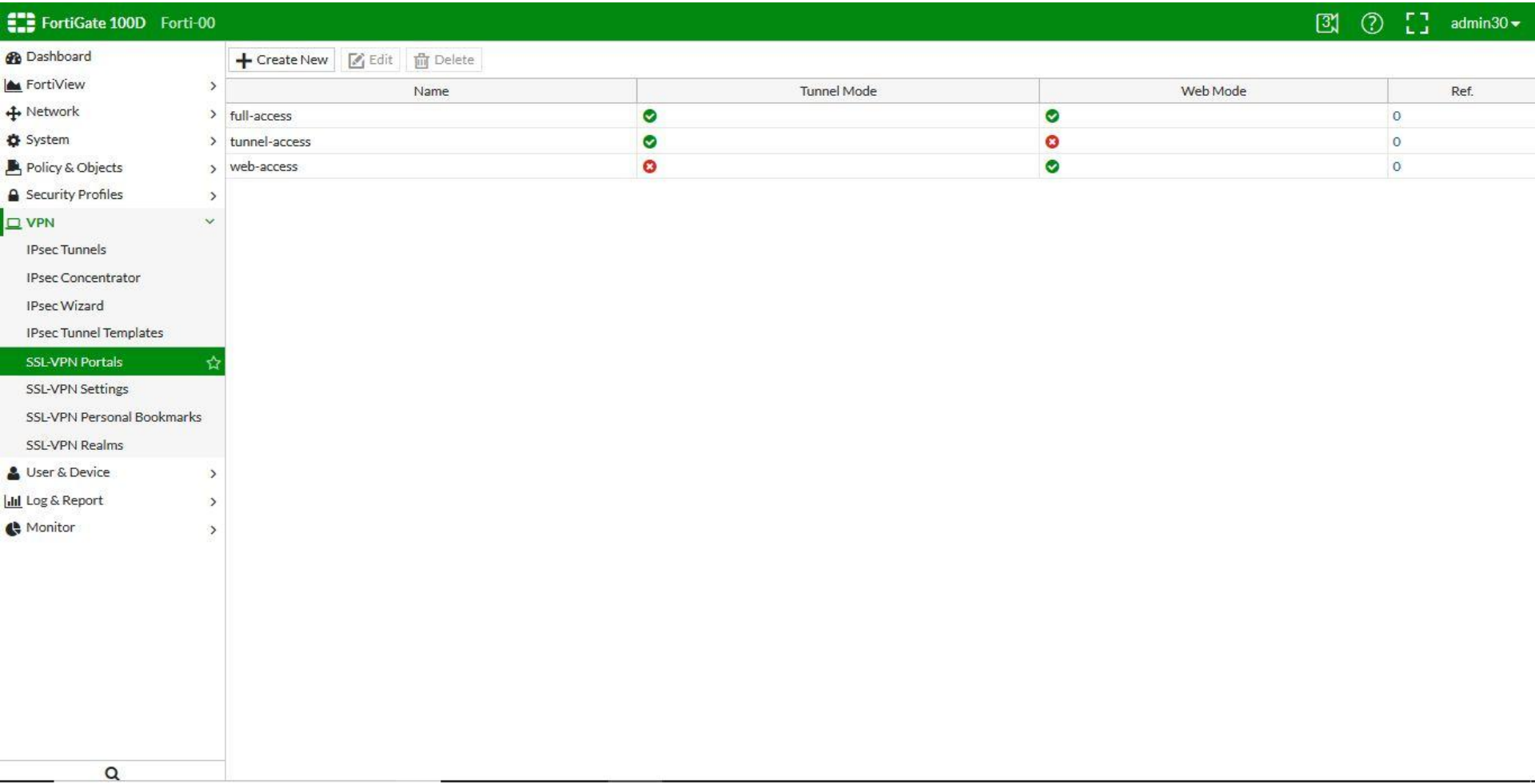
Remote Device Type: FortiGate | Cisco

NAT Configuration: No NAT between sites | This site is behind NAT | The remote site is behind NAT

Site to Site - FortiGate



< Back | Next > | Cancel


FortiGate 100D
Forti-00
admin30
Dashboard
FortiView
Network
System
Policy & Objects
Security Profiles
VPN
IPsec Tunnels
IPsec Concentrator
IPsec Wizard
IPsec Tunnel Templates
SSL-VPN Portals
SSL-VPN Settings
SSL-VPN Personal Bookmarks
SSL-VPN Realms
User & Device
Log & Report
Monitor
Create New
Edit
Delete
Name
Tunnel Mode
Web Mode
Ref.
full-access
0
tunnel-access
0
web-access
0

TOFINO SECURITY
A BELDEN BRAND

Search

Why Tofino? Products Resources Support Sales Blog About Us 中文 Log In

HEADLINES | Belden Delivers Groundbreaking Cyber Security Solution for Energy Sector →

Tofino Xenon and Configurator 3.2

Belden Inc., a global leader in signal transmission solutions for mission-critical applications, has released the next generation of its Tofino Security solutions for industrial control systems. The new Tofino Xenon and Tofino Configurator (TC 3.2) ...

Learn more...

Loadable Security Modules

Rather than hard-coding a fixed set of security features, the Tofino Industrial Security Solution packages each individual security function in a firmware module called a Loadable Security Module (LSM)...

Learn more...

Securing EtherNet/IP Control Systems

This paper discusses the creation of a DPI firewall for EtherNet/IP and Common Industrial Protocol (CIP™)...

Learn more...

Contacts: Office: 1-510-438-9071 **Office (Toll Free):** 1-855-400-9071

Contact

Magic Quadrant

Figure 1. Magic Quadrant for Enterprise Network Firewalls

Source: Gartner (May 2016)

Figure 1. Magic Quadrant for Enterprise Network Firewalls

Source: Gartner (October 2018)

Magic Quadrant

Figure 1. Magic Quadrant for Unified Threat Management (SMB Multifunction Firewalls)

Source: Gartner (June 2017)

Figure 1. Magic Quadrant for Unified Threat Management (SMB Multifunction Firewalls)

Source: Gartner (September 2018)

Gartner

Panorámica de la Ciberseguridad… Estado del arte

Los riesgos de ciberseguridad se materializan en incidentes que comprenden desde la denegación de servicios (DoS) web y BBDD, toma de control de los sistemas, formar parte de (botnets) redes zombies, el robo de credenciales, ... hasta la destrucción de nuestros sistemas.

Las consecuencias para la organización incluyen desde la manipulación de contenido con usuario privilegiado, el defacement, el espionaje, el mantenimiento de puertas traseras, extracción y robo de información, ... hasta la utilización de nuestros sistemas como pasarela para llevar a cabo terceros ataques.

According to Microsoft,

the potential cost of cyber crime to the global community is a mind-bobbgling

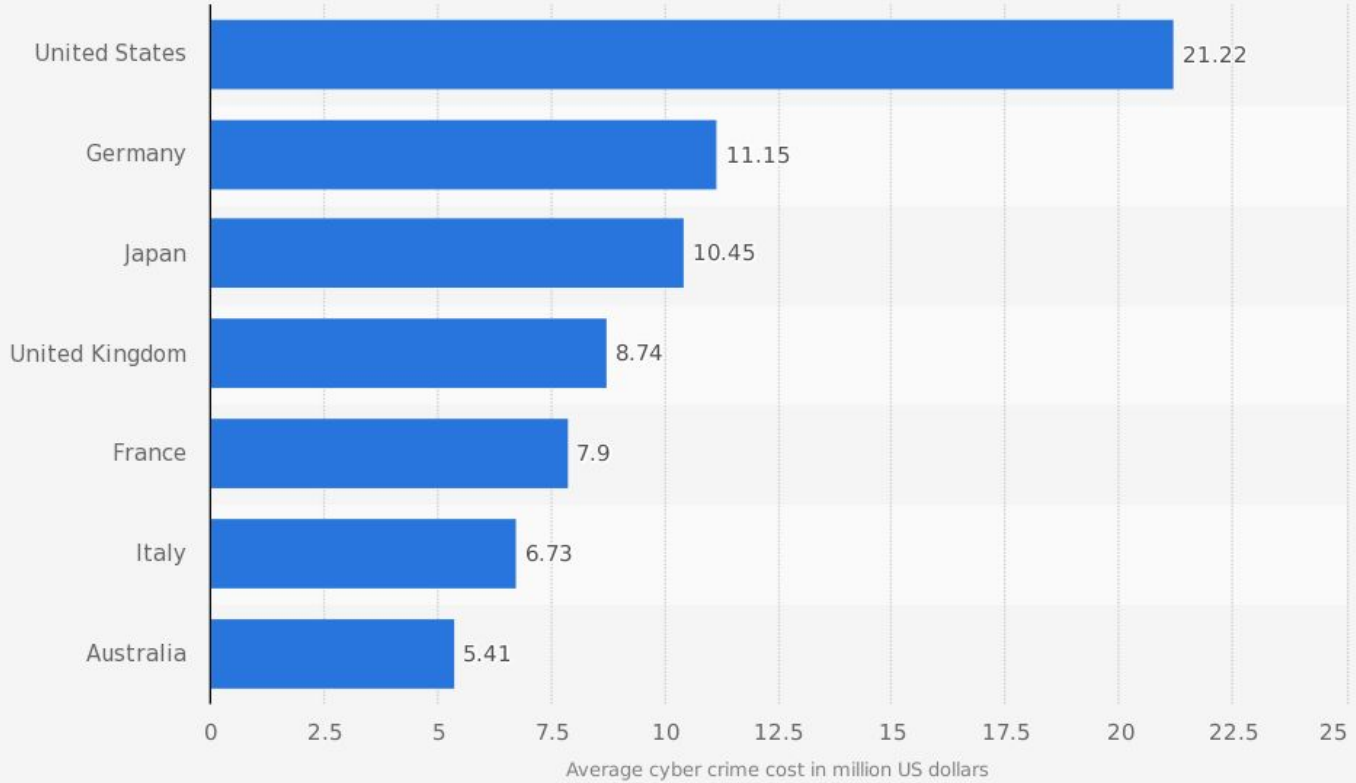
$500 billion,

and a data breach will cost the average company about

$3.8 million

63 percent of all **network intrusions** and **data breaches** are due to **compromised user credentials**

Average annualized cost of cyber attacks on companies in selected countries as of August 2017 (in million U.S. dollars)



Sources
Ponemon Institute; Accenture

Additional Information:
Worldwide; Ponemon Institute; August 2017; 254 organizations

2017 COST OF CYBER CRIME STUDY FROM ACCENTURE AND PONEMON INSTITUTE

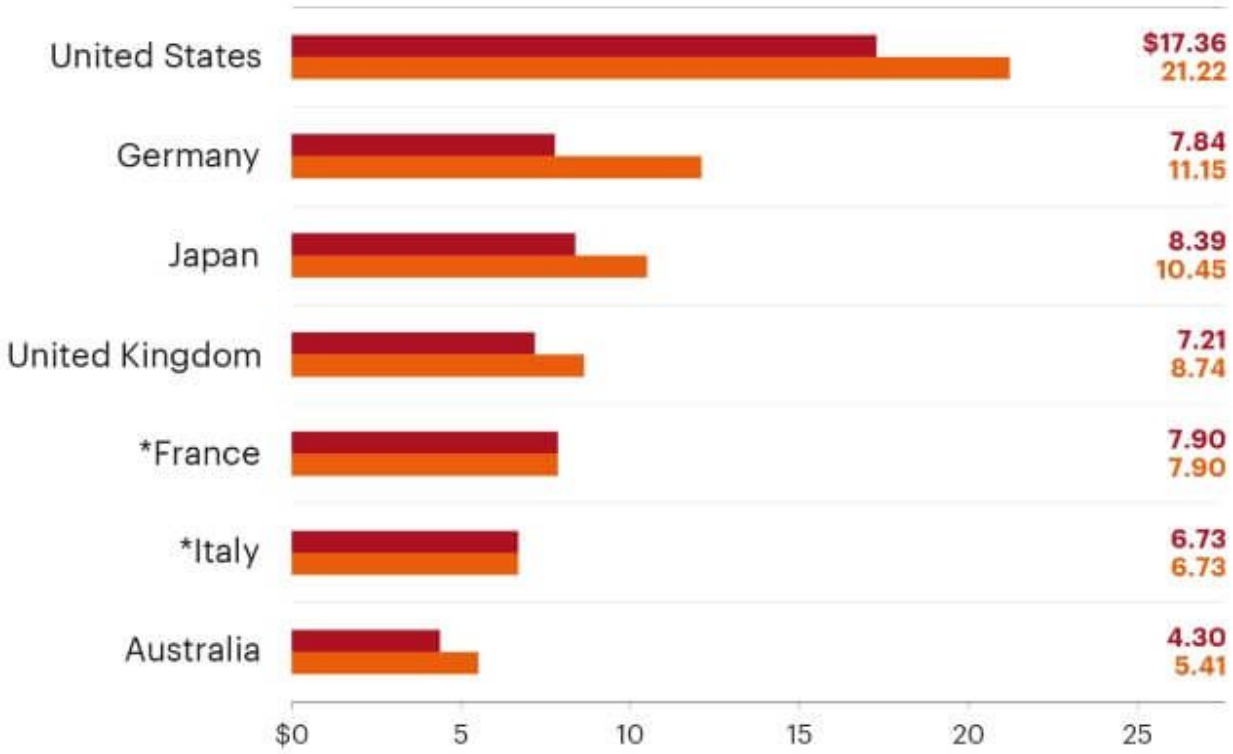


FIGURE 2

Total cost of cyber crime in seven countries

*Historical data does not exist for newly added country samples

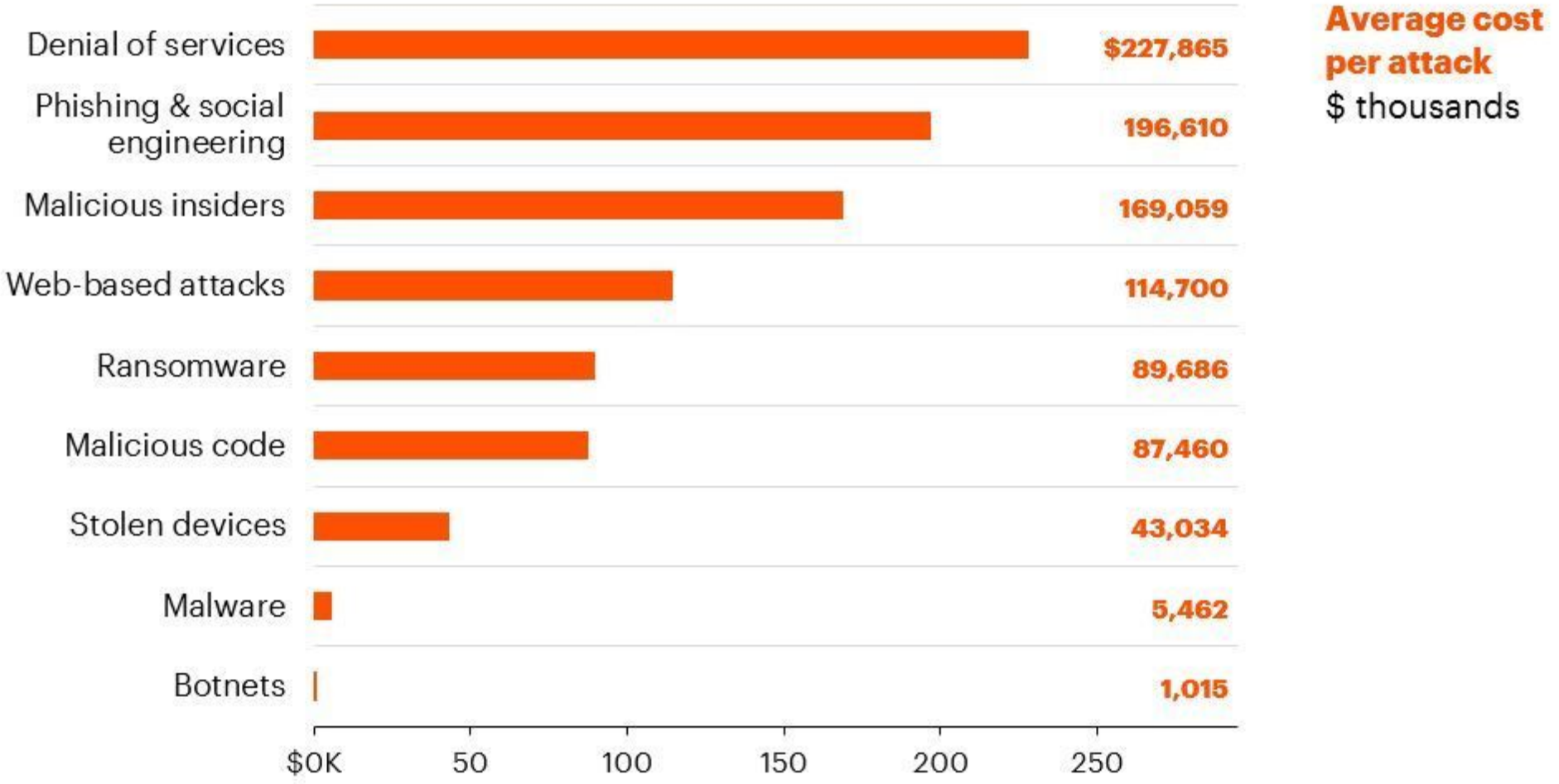
Legend

US$ millions

n = 254

- FY2016 (US$ millions)
- FY 2017 (US$ millions)


Virus y software malicioso que provocan pérdidas de productividad
38%
Uso inapropiado que los empleados hacen de los recursos de IT
36%
Pérdida física de dispositivos o medios que contienen datos
31%
Pérdida física de dispositivos móviles que exponen a la organización a riesgos
29%
Intercambio inapropiado de datos mediante dispositivos móviles
27%
Pérdida de acceso a servicios internos
25%
Pérdida de acceso a servicios orientados al diente
25%
Virus y software malicioso que provocan pérdidas de productividad
21%
Pérdida física de dispositivos móviles que exponen a la organización a riesgos
20%
Pérdida física de dispositivos o medios que contienen datos
20%
Uso inapropiado que los empleados hacen de los recursos de IT
20%
Intercambio inapropiado de datos mediante dispositivos móviles
19%
Pérdida de acceso a servicios internos
18%
Pérdida de acceso a servicios orientados al diente
2%
0%
10%
20%
30%
40%


Average cost per attack
$ thousands
Denial of services
$227,865
Phishing & social engineering
196,610
Malicious insiders
169,059
Web-based attacks
114,700
Ransomware
89,686
Malicious code
87,460
Stolen devices
43,034
Malware
5,462
Botnets
1,015
$0K
50
100
150
200
250

Panorámica de la Ciberseguridad…

Ciberespacio como “**territorio sin ley**”: **sin fronteras ni poderes**.

Vivimos en una sociedad hiperconectada y no somos conscientes de los riesgos que asumimos por el uso de la tecnología, a título personal, además de profesional.

La legislación siempre va muy por detrás de la tecnología y sus riesgos.

CYBERWAR

CYBERWAR T1

LA SERIE

EPISODIOS

VÍDEOS

Ben Makuch se adentra en la geopolítica de la piratería informática y los sistemas de vigilancia, en un viaje por todo el mundo para reunirse con hackers, funcionarios gubernamentales y disidentes e investigar el ecosistema de la guerra cibernética.

Compártelo en:

CYBERWAR T1

LA SERIE
EPISODIOS
VÍDEOS

TEMPORADA 1 TEMPORADA 2

TEMPORADA 2

CYBERWAR T2: EP.1. HACKING THE ELECTION

Episodio 1

Sabemos que Rusia hackeó el Comité Nacional del Partido Demócrata para influir en las elecciones de 2016. Ben trata de localizar a los hackers.

VER MÁS

CYBERWAR T2: EP.2. PUTIN TRUMPS AMERICA

Episodio 2

Las tropas de la OTAN se reúnen a lo largo de la frontera rusa, mientras las autoridades estadounidenses lidian con la intromisión electoral de Putin.

VER MÁS

CYBERWAR T2: EP.3. MEMETIC WARFARE

Episodio 3

Los memes son el arma más fuerte de la derecha alternativa en la lucha cultural en línea de Estados Unidos, y alteran el paisaje político e ideológico

VER MÁS

CYBERWAR T2: EP.4. CYBER KILL LISTS

Episodio 4

Estados Unidos construye una máquina de matar global utilizando información para identificar y eliminar a sospechosos de terrorismo.

VER MÁS

CYBERWAR T2: EP.5. ACTIVIST LIVES MONITORED

Episodio 5

Las agencias de inteligencia se asocian con empresas para espiar a ciudadanos estadounidenses. Algunos activistas luchan contra esta cibervigilancia.

VER MÁS

Malware y firmware falso para marcapasos, el gran peligro de estos dispositivos

Distances for Hacking Car Features

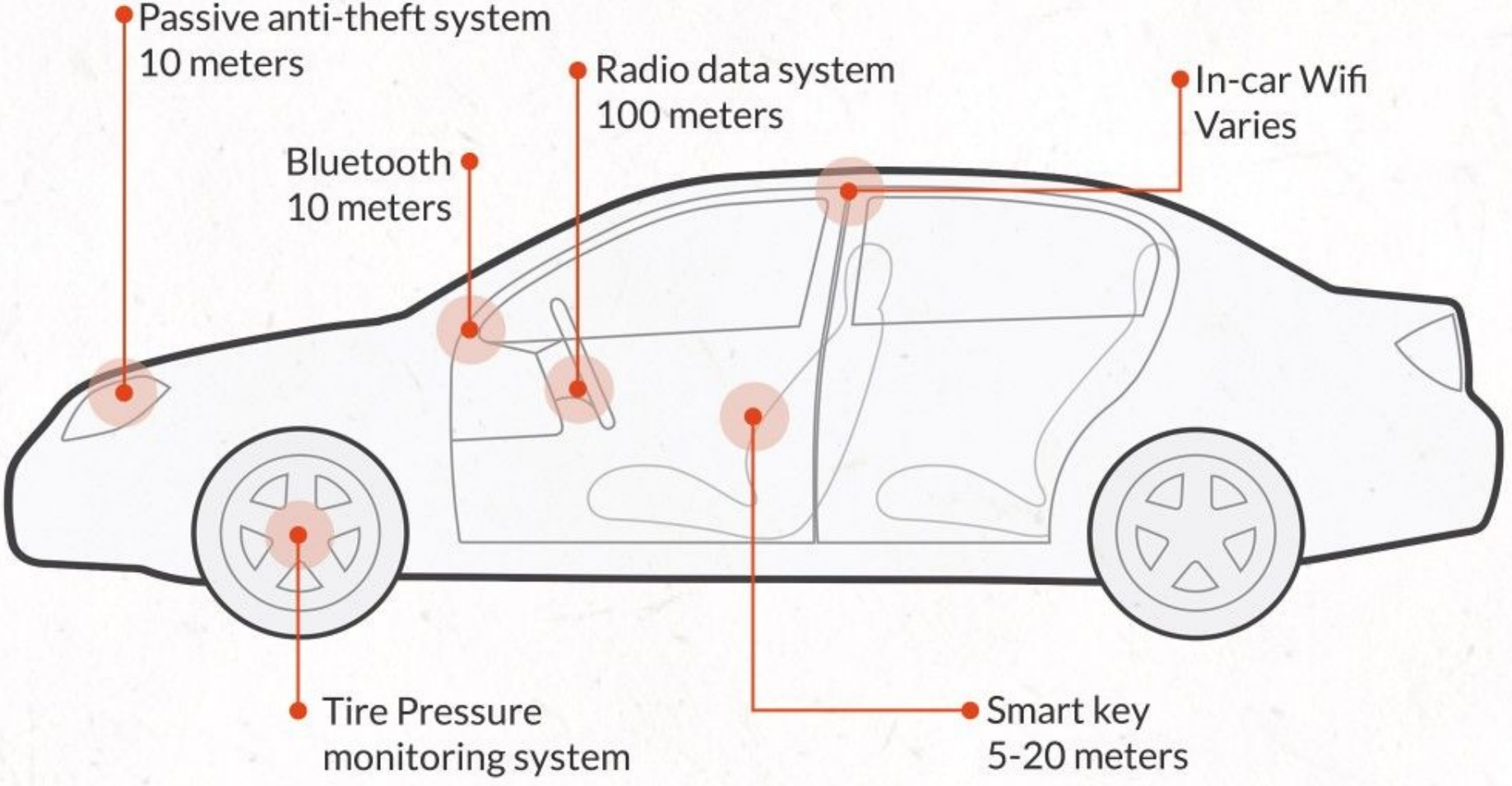
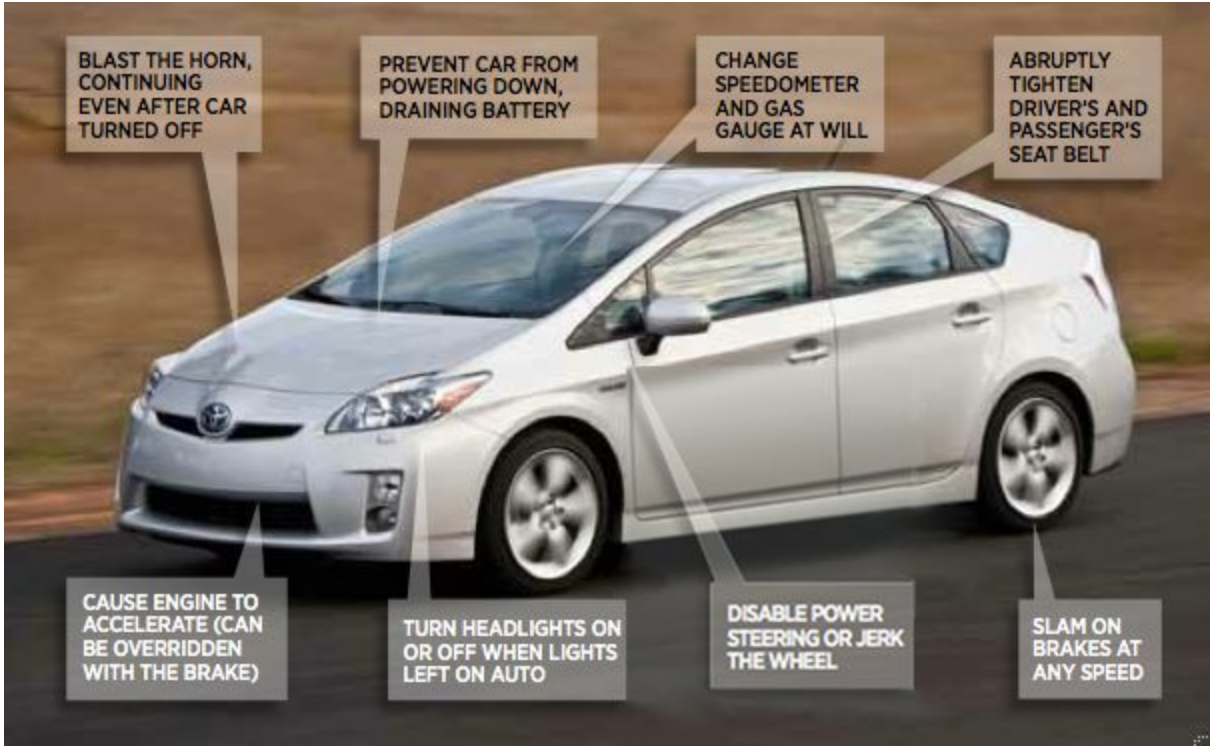
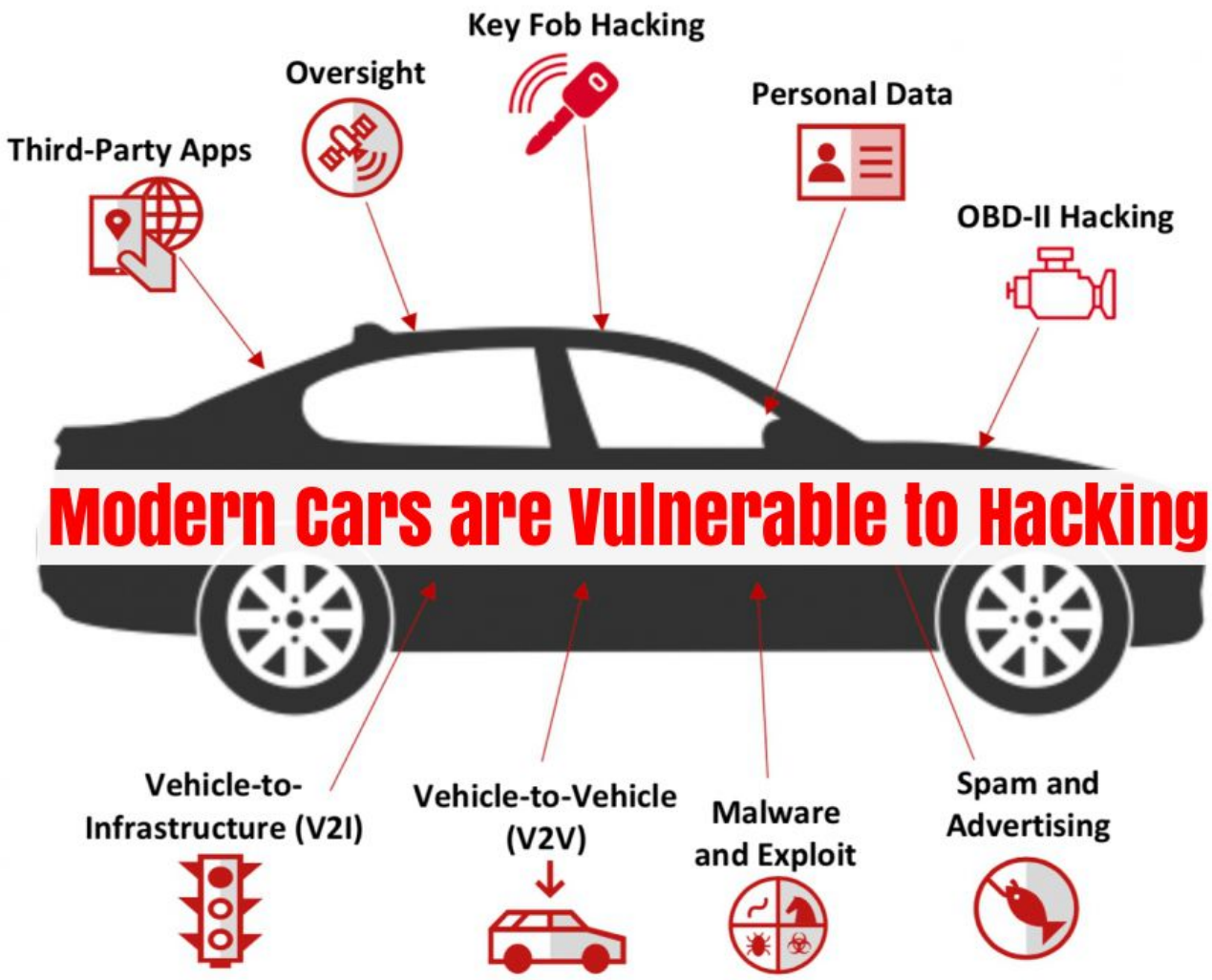


ILLUSTRATION: CNNMONEY


BLAST THE HORN, CONTINUING EVEN AFTER CAR TURNED OFF
PREVENT CAR FROM POWERING DOWN, DRAINING BATTERY
CHANGE SPEEDOMETER AND GAS GAUGE AT WILL
ABRUPTLY TIGHTEN DRIVER'S AND PASSENGER'S SEAT BELT
CAUSE ENGINE TO ACCELERATE (CAN BE OVERRIDDEN WITH THE BRAKE)
TURN HEADLIGHTS ON OR OFF WHEN LIGHTS LEFT ON AUTO
DISABLE POWER STEERING OR JERK THE WHEEL
SLAM ON BRAKES AT ANY SPEED


Key Fob Hacking
Oversight
Personal Data
Third-Party Apps
OBD-II Hacking
Modern Cars are Vulnerable to Hacking
Vehicle-to-Infrastructure (V2I)
Vehicle-to-Vehicle (V2V)
Malware and Exploit
Spam and Advertising

Two ways thieves hack into keyless cars

Hackers buy radio-frequency hacking device via online or from the local electronics store.

This gadget is used to "eavesdrop" and steal the rolling code.

The device is used to "attack" the locking system, tricking it into responding with a rolling code. The device captures the rolling code and cracks it.

Once the car is unlocked, there is no key needed to start the engine.

61 **the cybergibbons**
@cybergibbons

Seguir

FFS. @shodanhq, port 10001, telnet, ctrl-A I20100. Hundreds of these open. What was Veeder thinking?

```
Trying 72.95.116.176...
Connected to static-72-95-116-176.port.east.myfairpoint.net.
Escape character is '^]'.
^AI20100

I20100
JAN 22, 2015 19:23

277190 HOLDEN LEADBE
729 MAIN RD
HOLDEN ME,04429
207-843-6411

IN-TANK INVENTORY

TANK PRODUCT             VOLUME TC VOLUME   ULLAGE   HEIGHT    WATER     TEMP
  1  REGULAR                 6581         0     5420    51.65     0.00    35.27
  2  SUPER                    918         0     3155    26.55     0.00    41.09
  3  DIESEL SLAVE            2251         0     1822    51.97     0.00    38.03
  4  DIESEL MASTER           2192         0     1881    50.87     0.00    38.34
```

1:06 - 23 ene. 2015

54 Retweets **34** Me gusta

La Asociación Mediterránea de Peritos de las Tecnologías de la Información y Comunicación (Aspertic), ha advertido que 189 gasolineras españolas, especialmente las autónomas (sin empleados) se encuentran en grave riesgo en caso de ciberataque debido a las casi nulas medidas de seguridad para impedir que un tercero pueda penetrar en sus sistemas y controlar de forma remota las válvulas de los tanqu (684/041283)

Situación: Pendiente de contestación

Data límite de contestación: 20/04/2018

▶ Iniciativa

02/03/2018

Hasta 189 gasolineras españolas se pu hackear fácilmente, denuncian peritos informáticos

La Voz de Galicia

«Hackers» éticos de Vigo alertan a la UE de fallos de seguridad en gasolineras

Entre cinco y siete estaciones de servicio en riesgo están ubicadas en Galicia

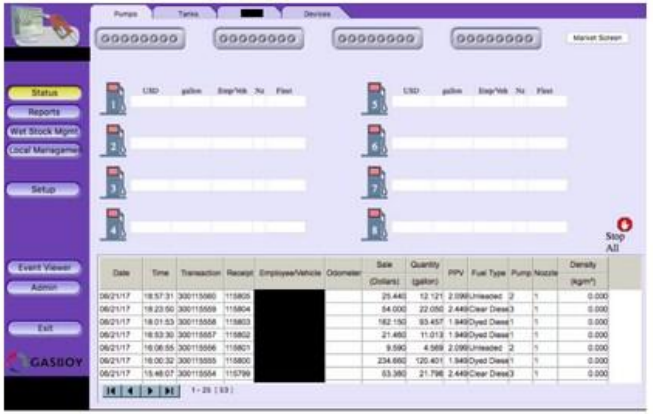
IoT

Several Gas Station Design Flaws Allows Attackers to Change the Price and Take Full Control on the Gas Station Remotely

By Priya James - February 28, 2018 0

KASPERSKY lab

Reserved CVEs	Description
CVE-2017-14728	Hardcoded Administrator Credentials
CVE-2017-14850	Persistent XSS
CVE-2017-14851	SQL Injection
CVE-2017-14852	Insecure Communication
CVE-2017-14853	Code injection
CVE-2017-14854	Buffer Overflow allows RCE



La Policía investiga si una gasolinera de 'low cost' pudo ser manipulada para que se pudiera repostar gratis

Ocurrió durante todo el fin de semana. Hasta que dicho surtidor fue precintado, numerosas personas acudieron a llenar el depósito de su coche al correrse la voz

Los propietarios de la gasolinera han presentado una denuncia en la Comisaría de la Policía Nacional de Dos Hermanas y han puesto a disposición de la misma las imágenes de las cámaras de seguridad, para tratar de **averiguar si esta 'singular' circunstancia se pudo deber a una avería o a la manipulación intencionada** del servicio informático que posibilita el repostaje a cambio del pago con dinero en efectivo o con tarjeta; algo que, según han informado fuentes policiales a este Diario Digital, ya están investigando.

Desde primeras horas de la mañana de este lunes, personal de la gasolinera **'Petroprix', que se encuentra cerrada al público**, realiza distintos trabajos para tratar de solucionar la avería y volver a ofrecer el servicio con normalidad.


PETROPRIX
Terminal de pago en efectivo
638 423 799
Atención al cliente
ESPAÑOL
ENGLISH
Identificar Usuario
Bienvenido a PETROPRIX
SE ENCUENTRA EN EL TERMINAL DE PAGO EN EFECTIVO
Empezar
ATENCIÓN ! NO DEVUELVE CAMBIO
PETROPRIX
DIESEL
0.000 €/L
0.000 €/L
GASOLINA 95
24 HORAS
DESATENDIDA
Upgrade your VNC Server license in order to benefit from premium security features and performance enhancements. Visit the RealVNC web site for more information.
5:44
28/03/2018

Panorámica de la Ciberseguridad… Estado del arte

No existe La **seguridad total**

(sino una seguridad gestionada…)

- Debemos valorar el impacto económico del riesgo que estamos corriendo,
- Frente al coste de las salvaguardas.

Panorámica de la Ciberseguridad… Estado del arte

- Cada vez somos más vulnerables al crimen en Internet.
- La frecuencia de los incidentes es mayor, así como su sofistificación.
- No existe una base legal bien definida.
- El carácter distribuido de los incidentes genera problemas de jurisdicción.
- No existen estructuras funcionales de cooperación.
- Hoy en día, no está clara la responsabilidad de los incidentes.
- La concienciación de los usuarios es mínima.
- El crimen organizado cuenta con multitud de recursos.
- El anonimato y la facilidad de “operar” en Internet.
- Necesitamos nuevas herramientas, servicios y CAPACITACIÓN para hacer frente.

Panorámica de la Ciberseguridad… **Objetivos** principales

- **Disponibilidad** y accesibilidad de los sistemas y datos, sólo para uso autorizado.
- **Autenticación**; Trazabilidad y registros de auditoría.
- **Integridad** de los datos y del sistema.
- **Confidencialidad**.
- No-repudio; Confiabilidad.

Panorámica de la Ciberseguridad… **Objetivos** principales

Disponibilidad

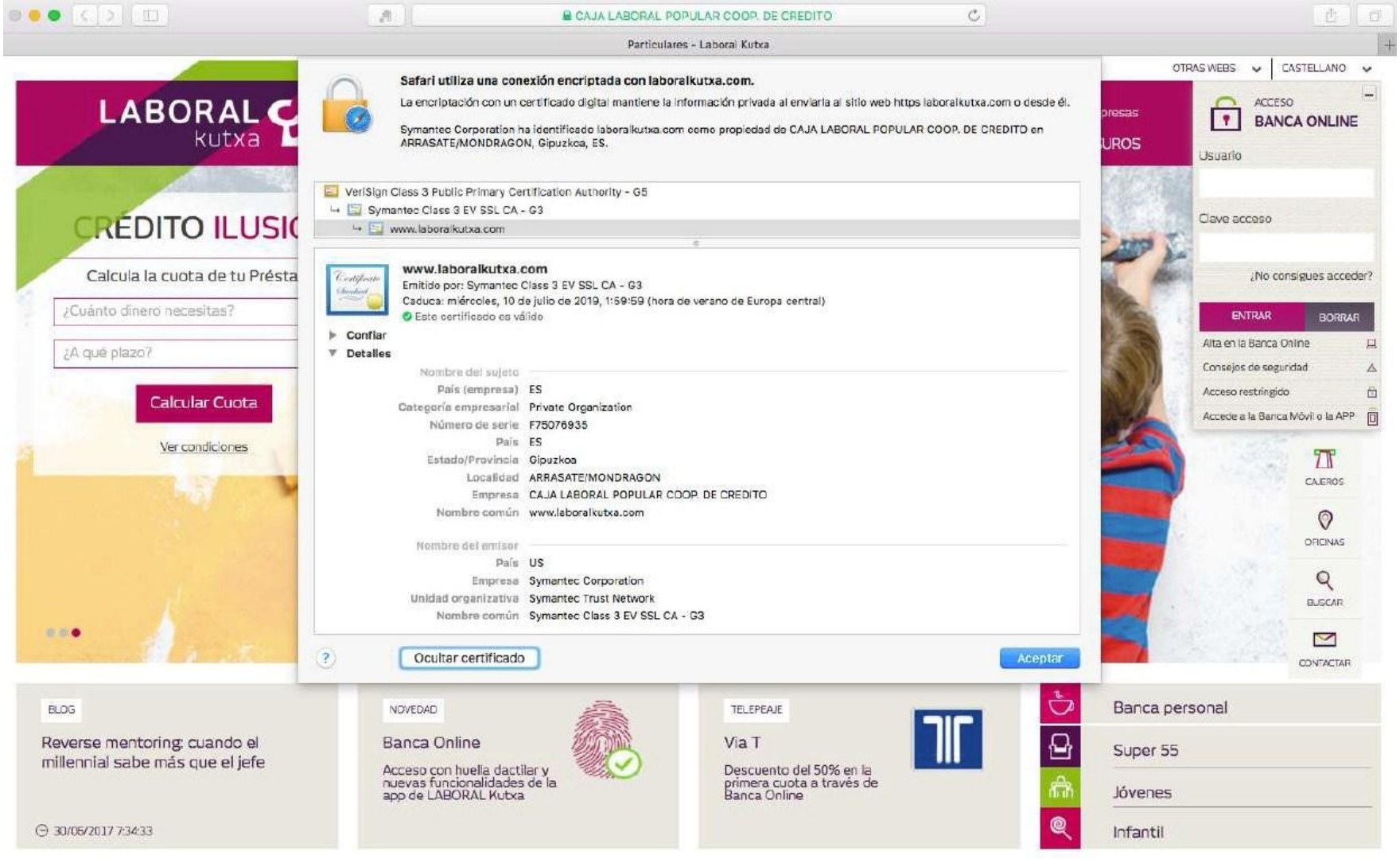
Indice de disponibilidad	Tiempo de inactividad anual
97,00%	11 días
98,00%	7 días
99,00%	3 días y 15 horas
99,90%	8 horas y 48 minutos
99,99%	53 minutos
99,999%	5 minutos
99,9999%	32 segundos

Panorámica de la Ciberseguridad… **Objetivos** principales

Disponibilidad

Si asociamos los determinados niveles de porcentaje de disponibilidad a "categorías" de equipamientos, podemos tener las siguientes relaciones:

- Un sistema con una disponibilidad del 90% se considera que se trata de un sistema no gestionado.
- Un sistema con una disponibilidad del 99% se considera un sistema gestionado.
- Un sistema que alcanza un 99,9% de disponibilidad se puede considerar un sistema bien gestionado.
- Un sistema con un 99,99% de disponibilidad se considera como un sistema tolerante a fallos.
- Un 99,999% de disponibilidad se puede definir como un sistema de alta disponibilidad.
- Con 99,9999% se corresponde con lo que se denomina como un sistema de muy alta disponibilidad.
- Y por último con 99,99999% de disponibilidad podríamos decir que estamos frente a un sistema de ultra alta disponibilidad.


CAJA LABORAL POPULAR COOP. DE CREDITO
Particulares - Laboral Kutxa
OTRAS WEBS
CASTELLANO
LABORAL kutxa
CRÉDITO ILUSIO
Calcula la cuota de tu Présta
¿Cuánto dinero necesitas?
¿A qué plazo?
Calcular Cuota
Ver condiciones
Safari utiliza una conexión encriptada con laboralkutxa.com.
La encriptación con un certificado digital mantiene la información privada al enviarla al sitio web https laboralkutxa.com o desde él.
Symantec Corporation ha identificado laboralkutxa.com como propiedad de CAJA LABORAL POPULAR COOP. DE CREDITO en ARRASATE/MONDRAGON, Gipuzkoa, ES.
VeriSign Class 3 Public Primary Certification Authority - G5
Symantec Class 3 EV SSL CA - G3
www.laboralkutxa.com
www.laboralkutxa.com
Emitido por: Symantec Class 3 EV SSL CA - G3
Caduca: miércoles, 10 de julio de 2019, 1:59:59 (hora de verano de Europa central)
Este certificado es válido
Confiar
Detalles
Nombre del sujeto
País (empresa) ES
Categoría empresarial Private Organization
Número de serie F75076935
País ES
Estado/Provincia Gipuzkoa
Localidad ARRASATE/MONDRAGON
Empresa CAJA LABORAL POPULAR COOP. DE CREDITO
Nombre común www.laboralkutxa.com
Nombre del emisor
País US
Empresa Symantec Corporation
Unidad organizativa Symantec Trust Network
Nombre común Symantec Class 3 EV SSL CA - G3
Ocultar certificado
Aceptar
ACCESO
BANCA ONLINE
Usuario
Clave acceso
¿No consigues acceder?
ENTRAR
BORRAR
Alta en la Banca Online
Consejos de seguridad
Acceso restringido
Accede a la Banca Móvil o la APP
CAJEROS
OFICINAS
BUSCAR
CONTACTAR
BLOG
Reverse mentoring: cuando el millennial sabe más que el jefe
30/06/2017 7:34:33
NOVEDAD
Banca Online
Acceso con huella dactilar y nuevas funcionalidades de la app de LABORAL Kutxa
TELEPEAJE
Vía T
Descuento del 50% en la primera cuota a través de Banca Online
Banca personal
Super 55
Jóvenes
Infantil

Panorámica de la Ciberseguridad… Entidades y organismos implicadas

- Desarrolladores de software.
- Fabricantes de productos.
- Integradores de datos en el sistema.
- Organizaciones o usuarios finales (clientes y proveedores).
- Organizaciones de evaluación y certificadores
- Administradores de sistemas y de seguridad.

Conceptos de Ciberseguridad:

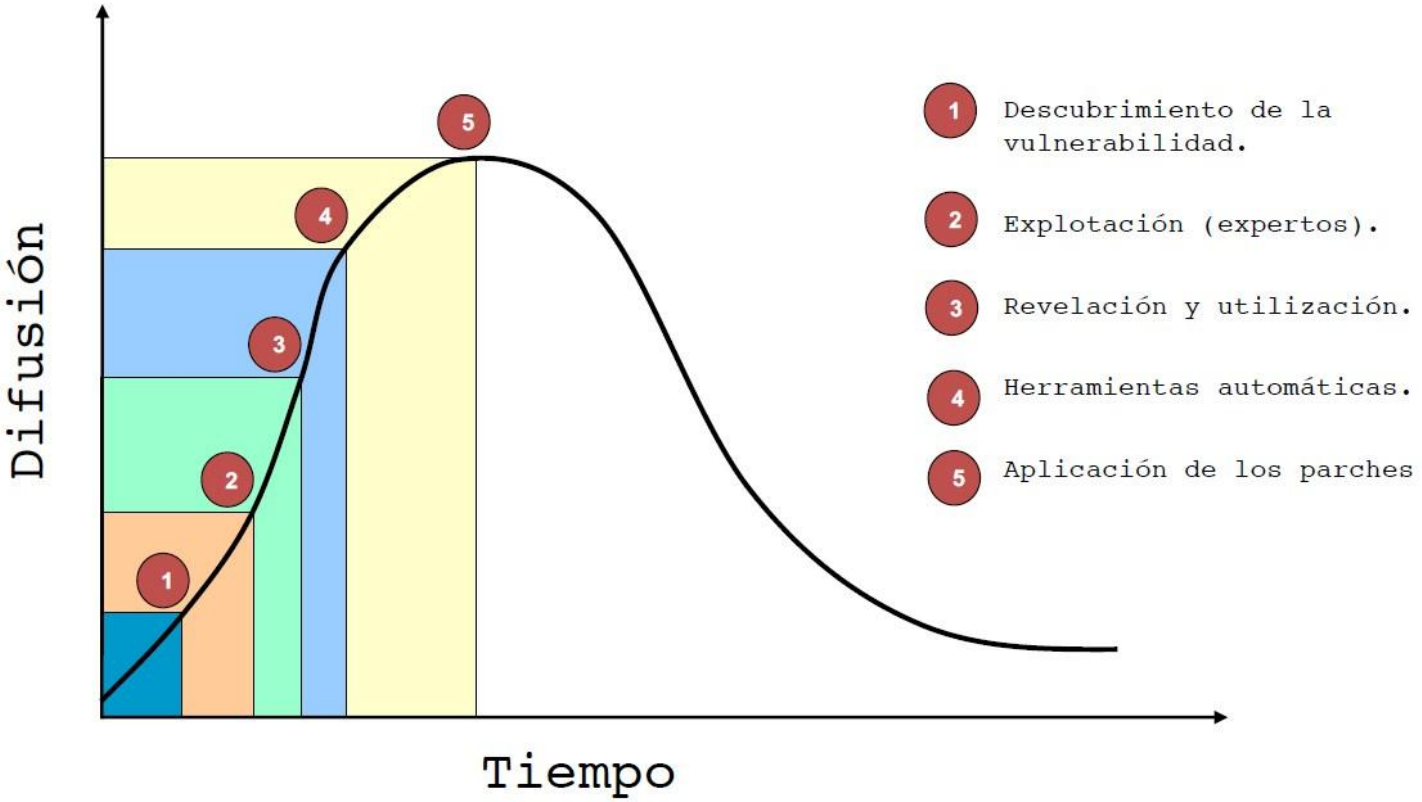
- Vulnerabilidad
- Política de seguridad
- Amenaza
- Ataque
- Componentes de ciberseguridad

Conceptos de Ciberseguridad:

Vulnerabilidad de seguridad:

- Debilidad o deficiencia que presentan los activos y permite a la amenaza materializarse.
- Vulnerabilidades son errores de programación (bugs) y/o fallos de diseño, la implementación, la operación, o la gestión de un sistema; que, con independencia de las intenciones, pueden ser aprovechados (explotados) por un atacante para violar la política seguridad.
- Por sí sola, no causa daño alguno, pero posibilita que se materialice una amenaza sobre el activo afectado.

Conceptos de Ciberseguridad... **Ciclo de vida** de una Vulnerabilidad:



Conceptos de Ciberseguridad... Vulnerabilidades en sistemas:

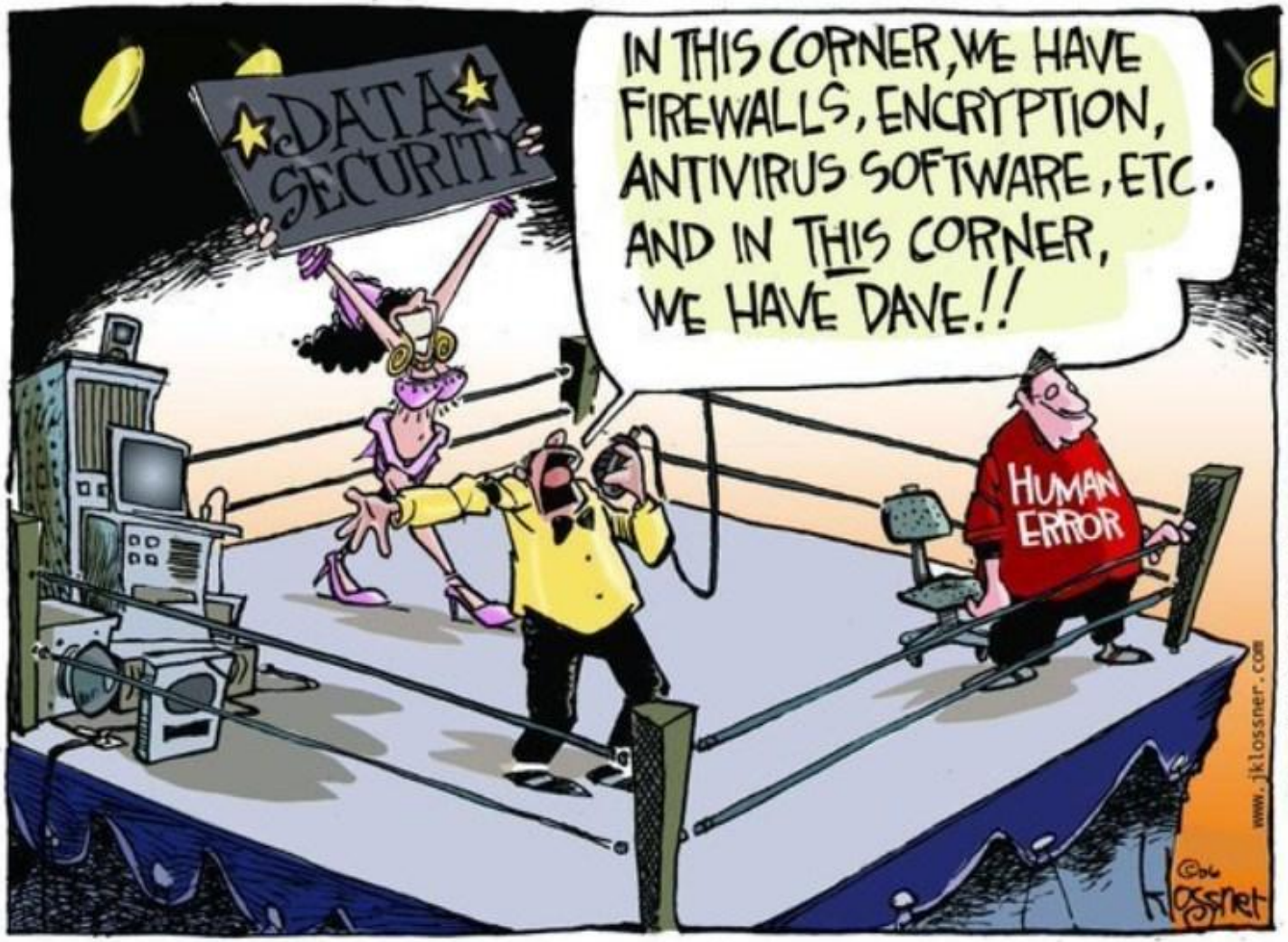
- Sistemas Operativos y aplicaciones débiles.
- Protocolos de comunicaciones inseguros.
- Usuarios confiados.

Conceptos de Ciberseguridad... Sistemas Operativos y aplicaciones débiles:

- Los sistemas son cada vez más complejos e interconectados
- Número de vulnerabilidades en aumento.
- Aplicaciones modulares e interconectadas
- Sistemas operativos de estaciones de trabajo con niveles de seguridad bajos.
- Las tecnologías de seguridad son cada vez mejores, pero también lo son las de los atacantes.

Conceptos de Ciberseguridad... Protocolos de comunicaciones inseguros:

- Protocolo TCP/IP deliberadamente simple, sencillo. Pero inseguro.
- Niveles de aplicación y transporte carecen de mecanismos de seguridad.
- Información que transita: comercial, económica y privada.
- Servicios (mail, ftp, telnet, www) de la red pobres en mecanismos de seguridad.
- Redes WiFi.



Conceptos de Ciberseguridad... Usuarios confiados:

- Dejadez, desconocimiento, falta de tiempo y presupuesto.
- Poca o nula formación de usuarios finales.
- Cuentas de usuarios no controladas y desprotegidas.
- Política de elección de contraseñas débil; Utilización de la misma contraseña en sitios seguros y no seguros.
- Ordenadores personales fácilmente accesibles.

Conceptos de Ciberseguridad:

Política de seguridad

- Conjunto de reglas y prácticas que definen y regulan los servicios de seguridad de una organización o sistema.
- Protege los recursos críticos de amenazas latentes en el entorno.
- Garantiza la continuidad de los sistemas de la información.
- Disminuye el riesgo de pérdida, manipulación o indisponibilidad de la información.
- Asegura el cumplimiento de los objetivos de la organización.

Conceptos de Ciberseguridad:

Políticas de seguridad:

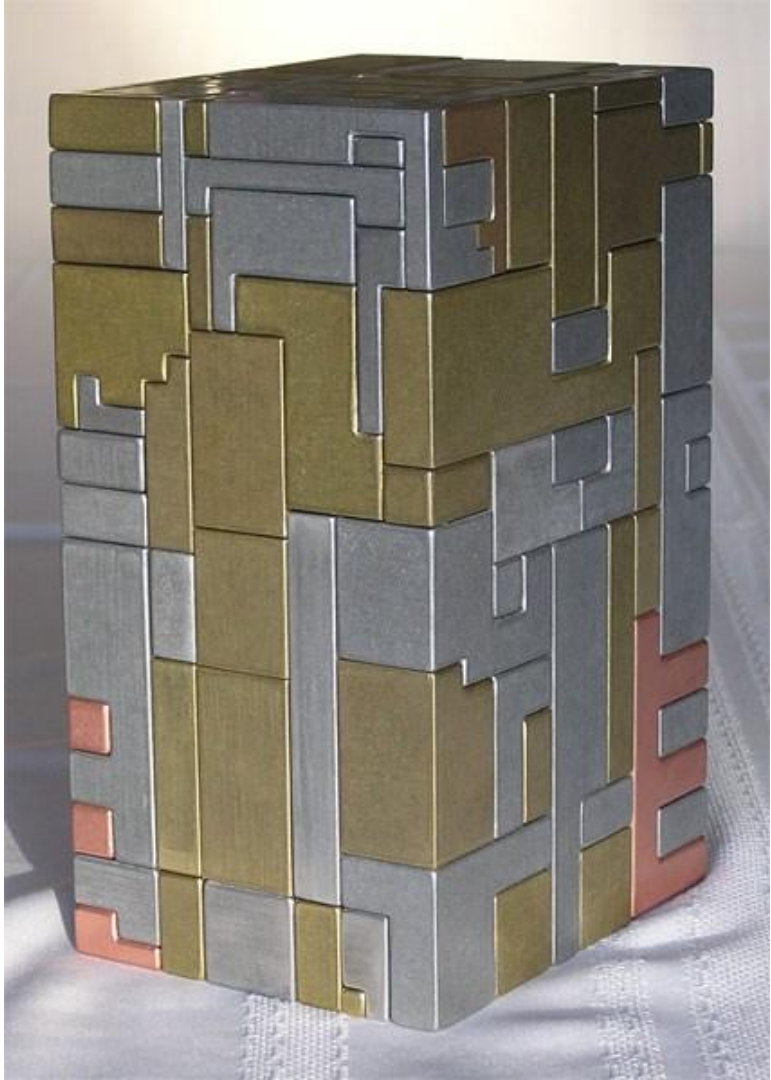
- https://www.incibe.es/protege-tu-empresa/herramientas/politicas
- https://www.incibe.es/protege-tu-empresa/kit-concienciacion
- https://www.incibe.es/protege-tu-empresa/guias
- https://www.incibe.es/protege-tu-empresa/formacion
- https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-director-seguridad


It's yellow, it's ugly, it doesn't match anything,
but it can save lives.
Safety vest and reflective triangle will be obligatory in every vehicle. Get equipped now.
ROAD SAFETY
WE ARE ALL RESPONSIBLE

Conceptos de Ciberseguridad:

Amenazas desconocidas:

- *¿Puede este objeto suponer una **amenaza**?*



Conceptos de Ciberseguridad:

Amenazas desconocidas:

- ***Vamos a analizarlo**:*

Conceptos de Ciberseguridad:

Amenazas desconocidas:

- *Montando las piezas adecuadas del modo adecuado...*

Conceptos de Ciberseguridad… Amenazas desconocidas:

Conclusiones:

- **No hay seguridad sin contexto.**
  - Si no sabemos qué estamos buscando, es difícil localizarlo.
  - Necesitamos conocer qué debemos buscar, con objeto de localizar amenazas desconocidas, anomalías y usos indebidos.

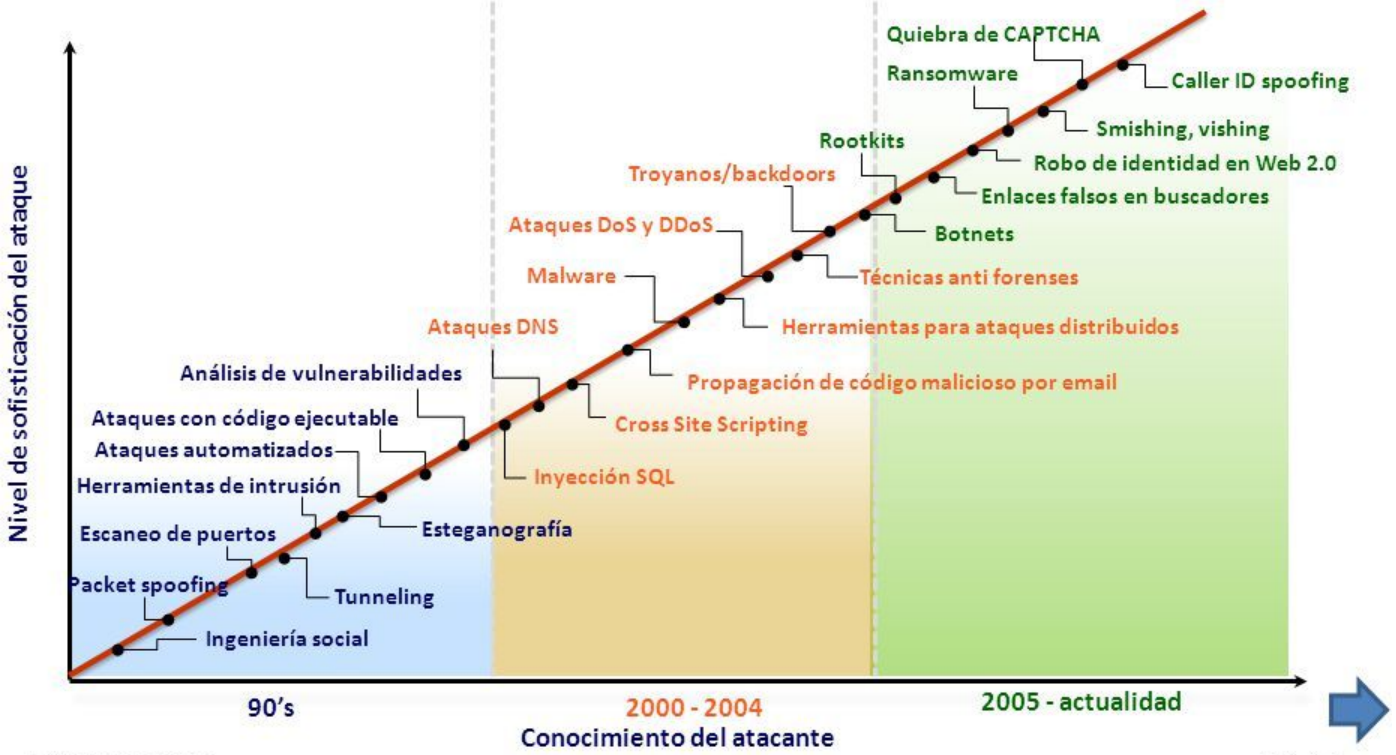
Conceptos de Ciberseguridad:

Amenaza de seguridad:

- Violación de la seguridad en potencia.
- Evento desfavorable que puede materializarse explotando una vulnerabilidad para causar una infracción de la seguridad, atentando con consecuencias negativas contra los activos y la seguridad de la información.
- Dicha violación puede ser provocada de manera intencionada por un atacante o de manera no intencionada, como por ejemplo un desastre natural.

Nuevos escenarios y retos comerciales

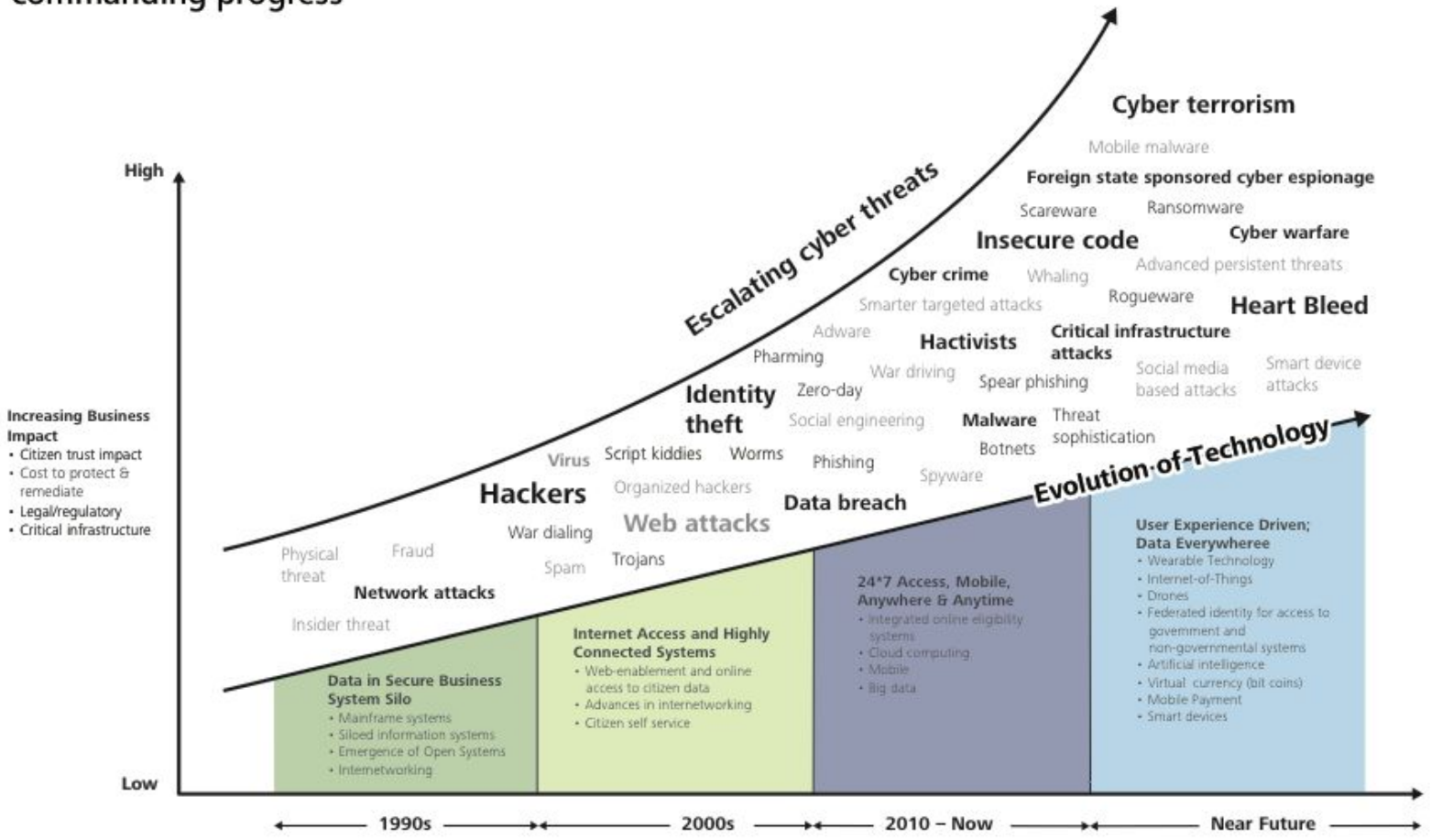
Evolución de los riesgos en seguridad – Amenazas informáticas



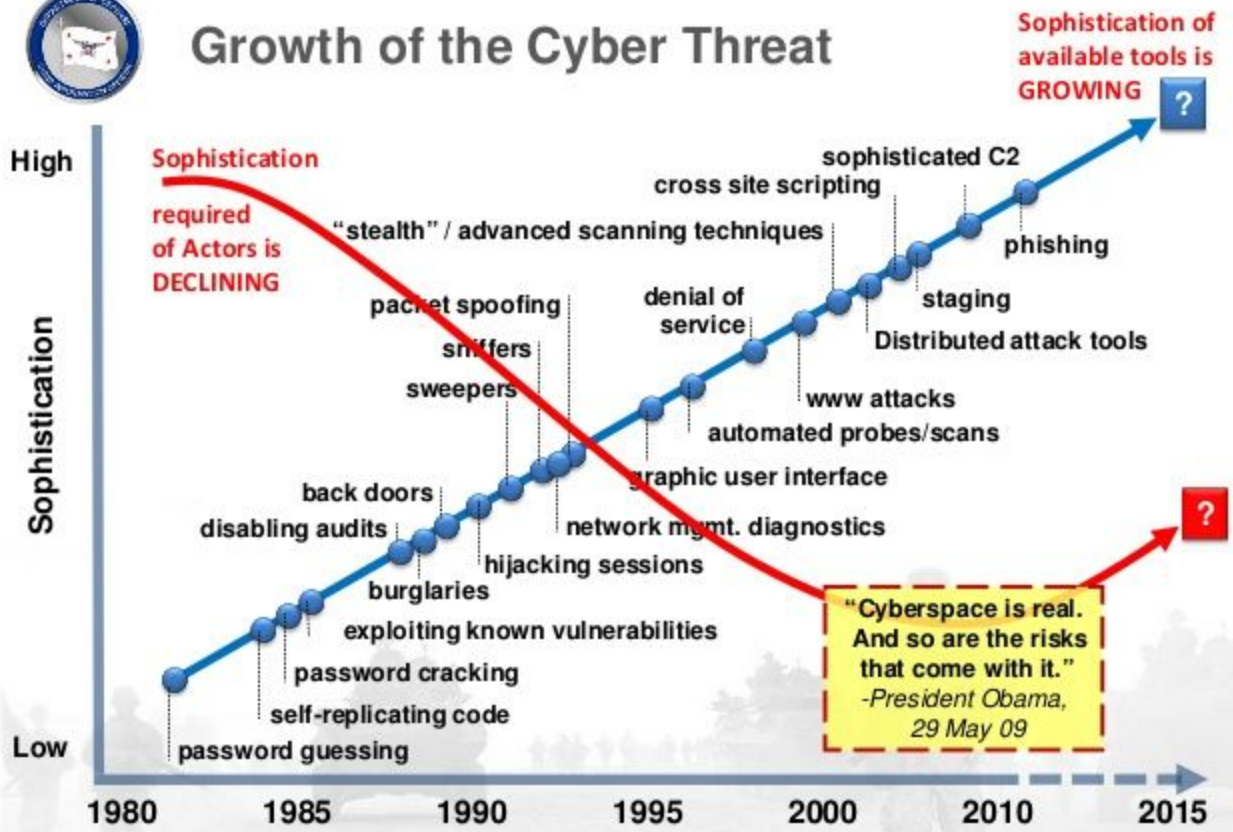
José Maranguni ch Racchumi
Presidente del COPREDE – ASBANC
Gerente del ASPF – Banco de Crédito del Perú

Adaptado de:
- Information Security as an institutional priority - Allen, J. Carnegie Mellon University - CERT/SEI ,USA - 2005
- Cano, J. – Convergencia de la Inseguridad de la Información. Universidad de los Andes, Colombia - 2008

Figure 29: Evolving technology and rapidly escalating cyber threats call for a deliberate approach to make commanding progress



Growth of the Cyber Threat



Conceptos de Ciberseguridad:

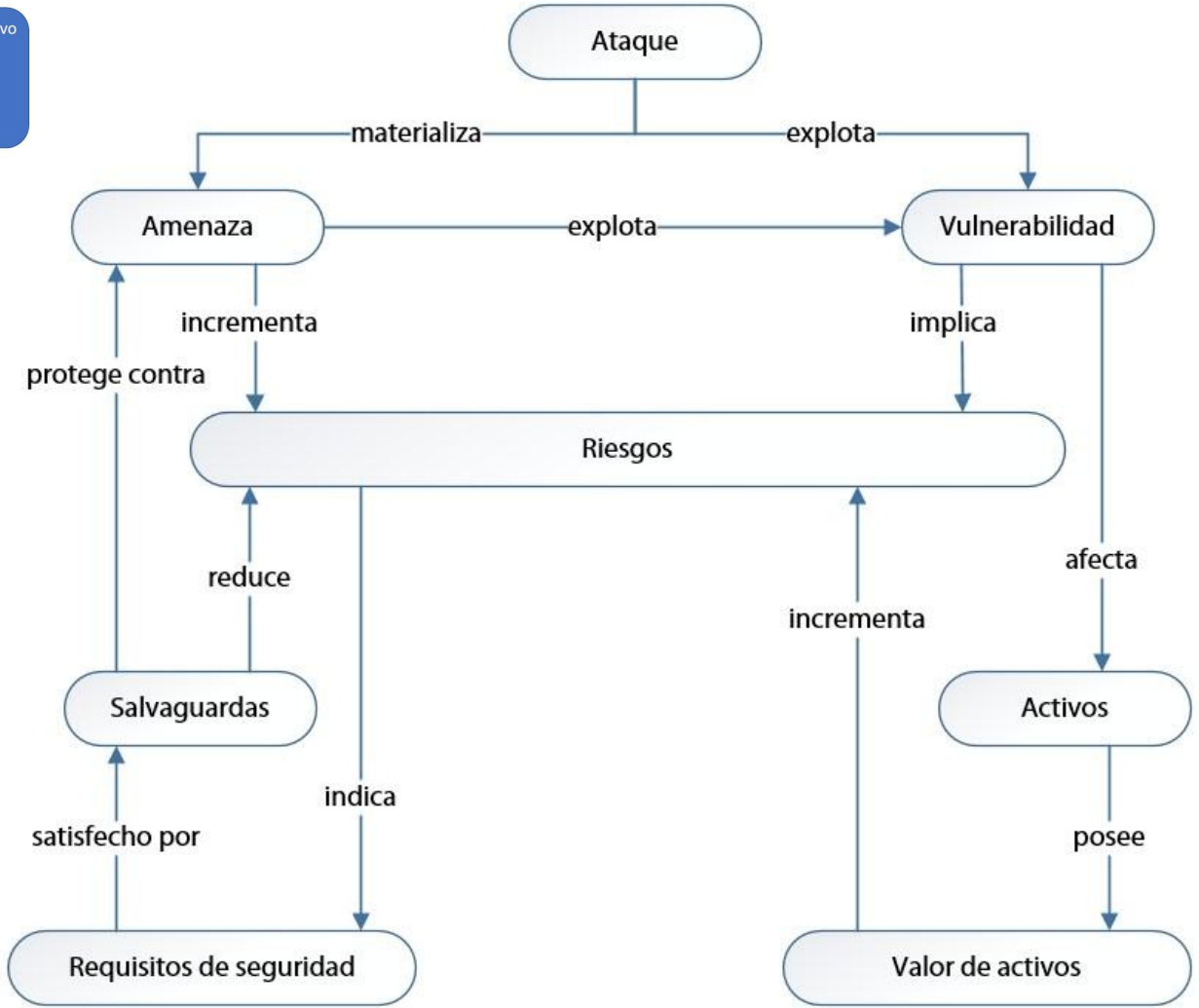
- **Evento** de seguridad: Ocurrencia detectada en el estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de los controles o una situación desconocida hasta el momento y que puede ser relevante para la seguridad.
- **Incidente** de seguridad: evento (considerado amenaza para la seguridad del sistema) que puede provocar interrupción o degradación del servicio reduciendo su calidad, o bien puede afectar a la confidencialidad, disponibilidad o integridad de la información, durante el procesado, su almacenamiento o transmisión.

Conceptos de Ciberseguridad:

- **Impacto**: Consecuencia de materializarse una amenaza sobre un activo aprovechando una vulnerabilidad.
- **Riesgo**: Estimación del grado de exposición (la probabilidad) de un activo a que una amenaza se materialice. Posibilidad que se produzca un impacto sobre un activo, de modo que una amenaza explote una vulnerabilidad y se produzca, dando lugar al ataque y generando impacto.


AMENAZA
SISTEMA DE INFORMACIÓN
RIESGO
VULNERABILIDAD

Conceptos de Ciberseguridad:

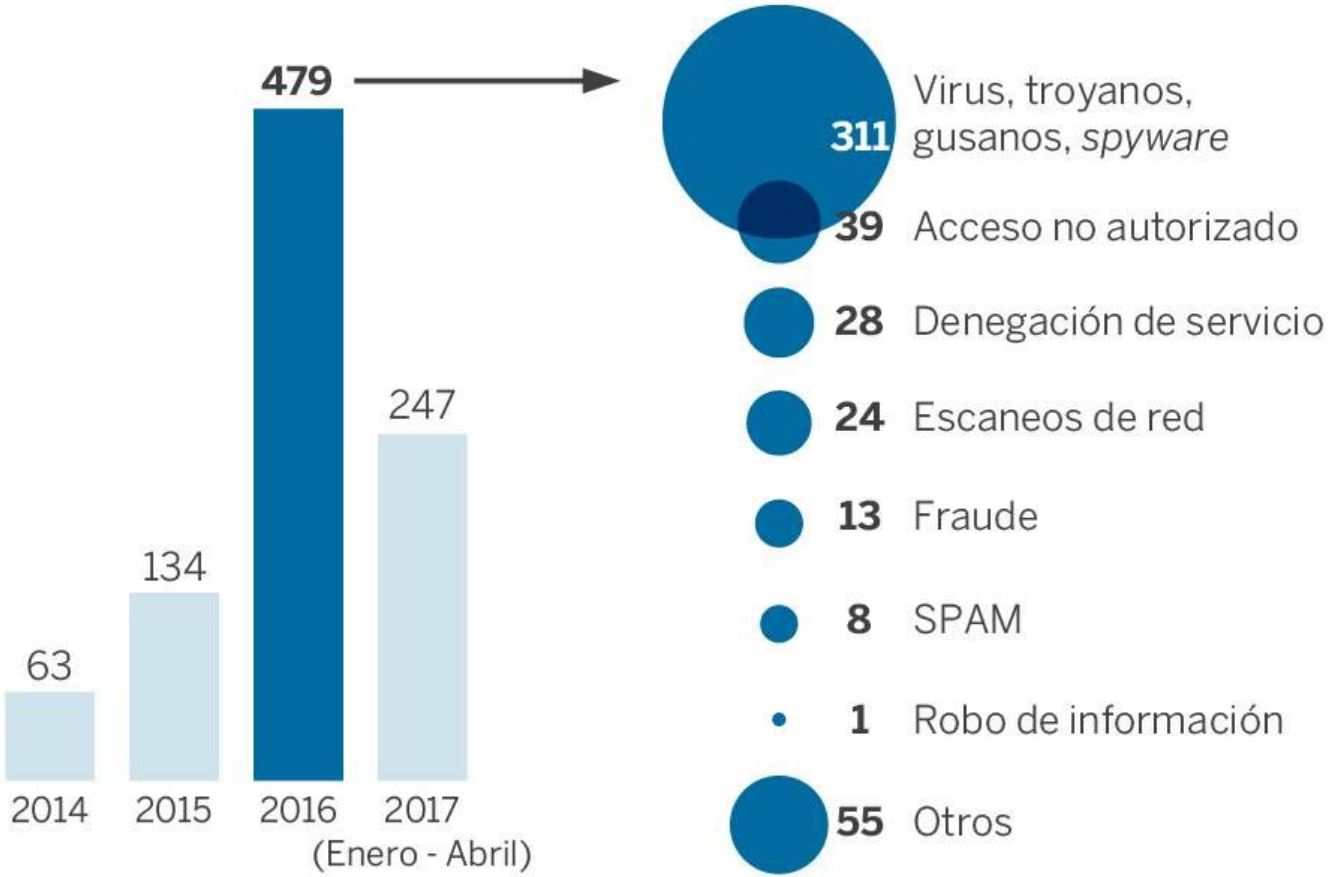


Conceptos de Ciberseguridad:

Ataque:

- Agresión a la seguridad de un sistema fruto de un acto (intencionado y deliberado) que viola la política de seguridad de un sistema.
- Un ataque puede ser **Activo** (altera el sistema, sus recursos y operaciones) o **Pasivo** (trata de aprender o emplear información del sistema, pero no afecta al propio sistema, ni tampoco a su funcionamiento).

CIBERATAQUES A INFRAESTRUCTURAS CRÍTICAS



Fuente: INCIBE (Instituto Nacional de Ciberseguridad). EL PAÍS

EVOLUCIÓN DE CIBERATAQUES

Conceptos de Ciberseguridad... **Botnet** (red de zombies)

- Blog
- Avisos de seguridad
- RGPD para pymes
- ¿Qué te interesa?
- Kit de concienciación
- Hackend
- Políticas de seguridad
- Juego de Rol
- ¿Conoces tus riesgos?
- Formación
- Guías
- Sellos de confianza
- Formulario de contacto

Servicio Antibotnet

Una botnet es un conjunto de ordenadores controlados remotamente por un atacante que pueden ser utilizados en conjunto para realizar actividades maliciosas como envío de spam, ataques de DDOS, propagar virus, y cometer otros tipos de delitos y fraudes en la Red. En nuestra empresa muchas veces conocemos esta situación cuando el ordenador funciona muy lento o algunas aplicaciones han dejado de funcionar.

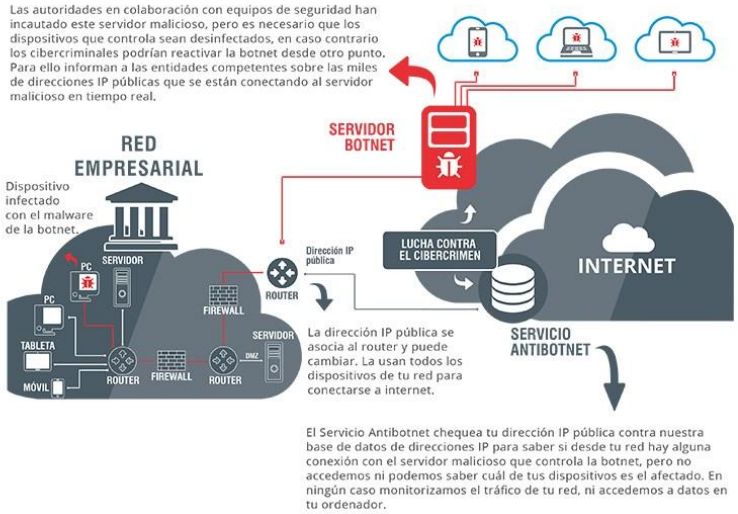
Para que puedas comprobarlo, ponemos a disposición de tu empresa un **servicio gratuito** que permite saber de manera fácil y sencilla si algún equipo de tu empresa está infectado por una botnet.

¿Cómo funciona el servicio antibotnet para empresas?

INCIBE recopila información que permite conocer la existencia de ordenadores que forman parten de una botnet.

Las empresas que dispongan de una red de ordenadores, que analizan el tráfico de red a través de un sistema de monitorización, pueden integrar el componente facilitado por INCIBE que permite mostrar una alerta de manera automática, en el caso de que alguna de las IPs de la empresa forme parte de una botnet.

De forma más gráfica, el esquema de funcionamiento del servicio antibotnet imágenes el siguiente:



Conceptos de Ciberseguridad:

Ataque DoS:

- Ataque a sistema o red que se apropia de sus recursos.
- Provoca que dicho recurso sea inaccesible a l@s usuari@s legítim@s.
- DDoS es la variante distribuida donde una serie de sistemas comprometidos atacan un único sistema para causar el cese de la prestación de servicio.

https://mad-rabbit.com/example-of-a-ddos-attack/

Conceptos de Ciberseguridad:

Ataque MiTM

- Ataque en el se adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que la víctima conozca que el enlace entre ellas se ha visto comprometido.
- El atacante adquiere la capacidad de observar e interceptar mensajes entre las víctimas.