



Tus mejores armas:



Conoce tus equipos de seguridad
y crea una política de seguridad
confiable.





SITUACION ACTUAL DE LAS REDES



Planteamiento 1

- Migración a una nueva tecnología de seguridad.

Aplicaciones críticas.



Tiempo sin servicio

Usuarios afectados

Costo de ventana



Planteamiento 1

- Conocimiento de tu politica de seguridad.

Puertos Expuestos

Reglas en Uso

Objetos sobrantes



Cambios en los equipos



Planteamiento 3

- Cumplimiento a estándares de seguridad.

PCI

Socks



ISO 27001



Planteamiento 4

- Tu soporte es reactivo o activo.



Planteamiento 5

Confianza en los Mobiles.



Confianza en el Endpoint.

Confianza en la Nube.



Confianza en el perímetro

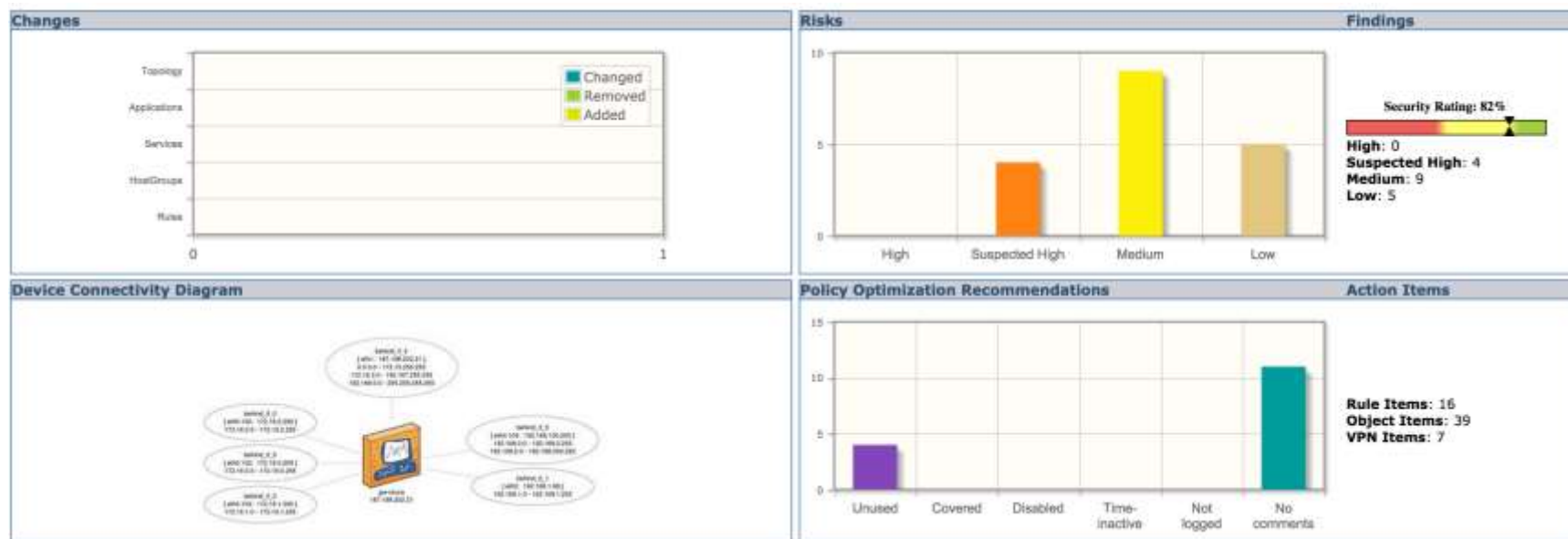




ALGOSEC EN LA MEJORA DE LAS POLITICAS



Analisis de la politica de seguridad



- Analisis y cumplimiento en 1-Click

algosec Firewall Analyzer - Provider Edition

General

ISO/IEC 27001 Compliance Report

62% Compliant

The AlgoSec Firewall Analyzer ISO/IEC 27001 Compliance report is based on the ISO/IEC 27001:2013 International Standard "Information technology - Security techniques - Information security management systems - Requirements" and on the companion ISO/IEC 27002:2013 "Code of practice for information security management" International Standard. This compliance report is concerned with the control objectives that apply to the organizations' firewalls, which are a central part of any organization's Information Security Management System (ISMS).



- Analisis detallado de las malas configuraciones de la politica

| | Code | Risk Description | Status |
|----|------|---|--------|
| 1. | I01 | "Any" service can enter your network | ✓ |
| 2. | I02 | TCP on all ports can enter your network | ✓ |
| 3. | I03 | UDP on all ports can enter your network | ✓ |
| 4. | I07 | Risky Microsoft services can enter your network | ✗ |
| 5. | D01 | "Any" service between internal networks | ✗ |
| 6. | F01 | Insecure external access to firewall | ✓ |
| 7. | F02 | Insecure internal access to firewall | ✗ |
| 8. | I04 | Telnet can enter your network | ✗ |



Analisis del rule base

| RULE | RISKS | NAME | SOURCE | DESTINATION | SERVICES | ACTION | COMMENT | TRAFFIC COUNT |
|----------|-------|-----------------|-------------------------|-------------------------|---|--------|---------|---------------|
| Trust 1 | 1 | Mobile Access | * Any | ext-fw | TCP https TCP Remote_Desktop_Protocol TCP CPMI TCP http TCP ssh ?? icmp-proto TCP IMAP-SSL TCP SMTPS TCP smtp TCP ftp TCP HTTP_and_HTTPS_proxy TCP bbb_1935 TCP bbb_9123 TCP bbb_587 | accept | | 15,840 |
| Trust 2 | 1 2 1 | | * Any | broad-255 | * Any | accept | | 226 |
| Trust 4 | 1 1 | | grp_soad@Any | * Any | * Any | accept | | 1,893 |
| Trust 5 | 1 | | manu-gw gw-shura | manu-gw gw-shura | * Any | accept | | 0 |
| Trust 6 | 1 | VPN Traffic | vpn-soad redes-shura | vpn-soad redes-shura | * Any | accept | | 0 |
| Trust 7 | 1 | | tunnel-broker ext-fw | ext-fw tunnel-broker | * Any | accept | | 0 |
| Trust 8 | 1 1 | Management Rule | redes-shura | gw-shura mgmt-shura | * Any | accept | | 10,614 |
| Trust 10 | 2 | | redes-shura | * Any | * Any | accept | | 1,640,055 |





Check Point[®]
SOFTWARE TECHNOLOGIES LTD.

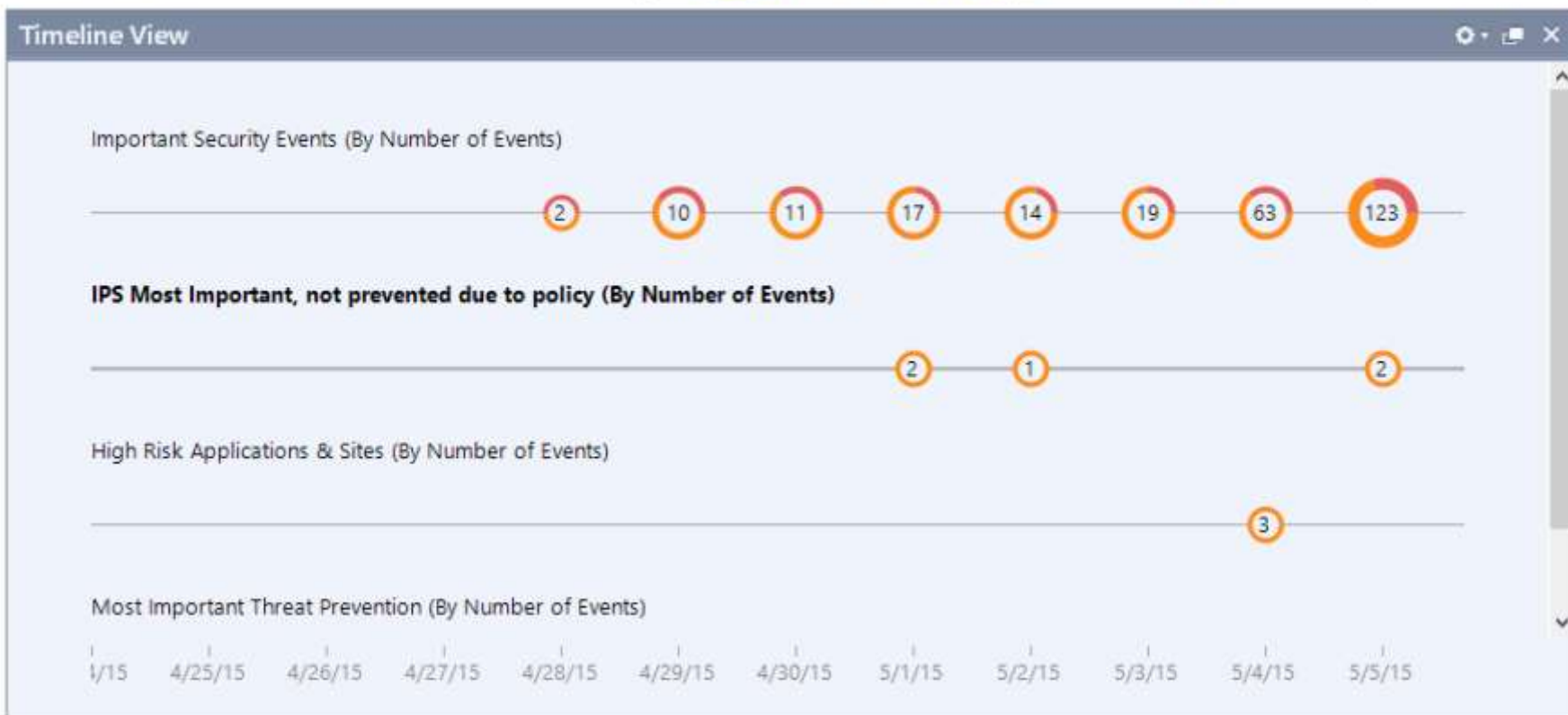
CHECK POINT COMO SOLUCION DE SEGURIDAD



Analisis de toda la infraestructura

Overview

View: [Icons] Last 7 Days Customize View



Resumen de Endpoints

The screenshot displays the Check Point Endpoint Security console. At the top, there are navigation tabs for Overview, Policy, Users and Computers, Reporting, and Deployment. The main content area is titled 'Overview' and includes a summary of 180 endpoints discovered in the organization. It also shows active alerts, such as 10 endpoints in a warned state and 11 infected with malware. A 'Security Status' section on the left provides progress bars for various security features. The main table below shows deployment progress for two users, Amy Lee and Bob Smith, both on USA Laptops, with software deployment status 'Completed'.

Security Summary for the Organization

- 180 Endpoints discovered in the Entire organization
- 112 are aligned with the organizational security policy (62.22%)
- 36 have security warnings (20%)
- 32 have security violations (17.78%)

Active Alerts

- 10 Endpoints are in warned state according to their Compliance policy
- 7 Endpoints have deployment errors
- 11 Endpoints are currently infected with malware

Note: Alerts are updated every 10 minutes

Security Status

Deployment Progress: 13 / 150

Blades Health-check: 115

Disk Encryption Status: 100

Anti-Malware Update: 100

Malware Infections: 100

Deployment Progress Table

| User Name | Computer Name | Software Deployment Status | Package Name | Package Version | Deploy Time | Installed Blades | Error Code | Error Description | Endpoint Client Ver |
|-----------|---------------|----------------------------|--------------|-----------------|-------------|--------------------------------------|------------|-------------------|---------------------|
| Amy Lee | USA Laptop | Completed | Off | 1 | Never | Device... Device... Full DL... | N/A | N/A | N/A |
| Bob Smith | USA Laptop | Completed | Off | 1 | Never | Device... Device... Full DL... | N/A | N/A | N/A |

Control de todo el trafico

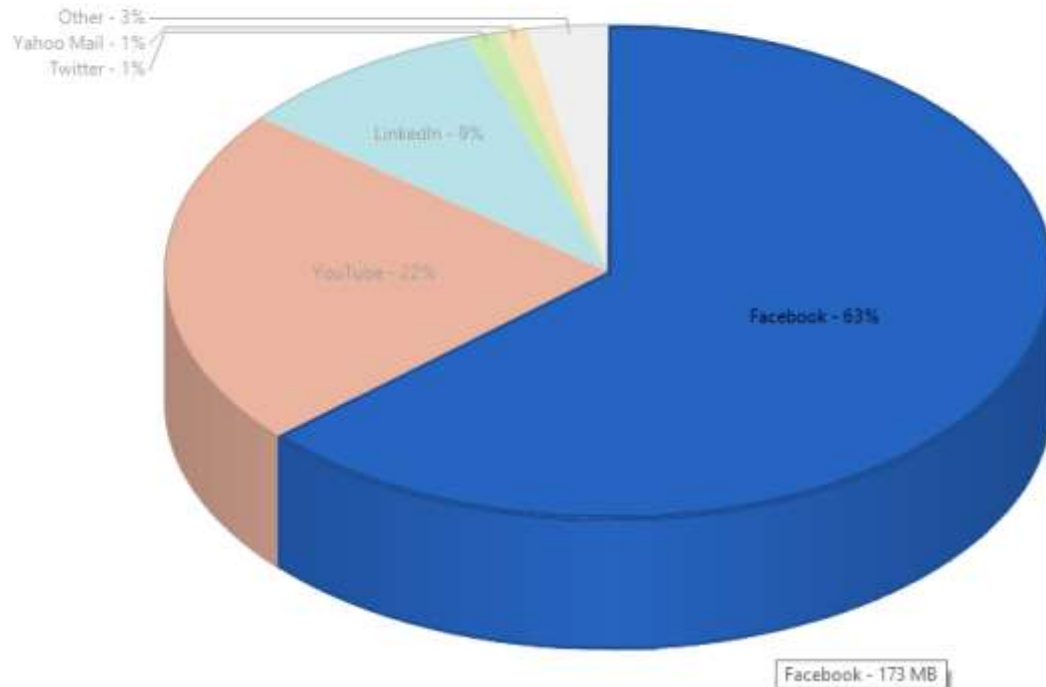
The screenshot displays a network security management interface with the following components:

- Navigation Bar:** Overview, Events, Timelines, Charts, Maps, Reports, Policy.
- Left Sidebar:** Custom and Predefined event categories including Important Security Events, DLP, IPS, Threat Prevention, DDoS Protector, Endpoint, Anti Malware, Full Disk Encryption, Compliance, Media Encryption, Identity Awareness, Mobile Access, Ticketing, and 3D Security Analysis tools.
- Main Panel - All Events:**
 - Filters: Last 12 Hours, 5000 events.
 - Top Events:**
 - 16% - Application Acti
 - 6% - DLP Incident
 - 5% - Invalid TCP Flags
 - 5% - HTTP on Non Sta
 - 68% - Other
 - Top Sources:**
 - 10% - N/A
 - 1% - GuyCash-laptop
 - 1% - JudyJosh-desktop
 - 1% - RachelBrash-desk
 - 87% - Other
 - Top Destinations:** No filter applied.
 - Top Users:** No filter applied.
 - Top Source Countries:** No filter applied.
- Event List Table:**

| Count | Product Name | Event Name | Start T... | Source | Destination | Service |
|-------|---------------------------------|--------------------------------|----------------|--------------------|-----------------|----------------|
| 10 | Check Point Threat Emulation | Threat Emulation Incident | 8... | 10 Sources | 10 Destinations | |
| 6 | Check Point Anti-Bot | Bot Incident | 3... | 6 Sources | 6 Destinations | http [tcp/80] |
| 3 | Check Point DLP | DLP Incident | 3... | 3 Sources | 3 Destinations | |
| 2 | Check Point Anti-Virus | Virus Incident | 2... | 2 Sources | 2 Destinations | tcp/8080 |
| 45 | Check Point IPS Software BL... | 10 Event Names | 1... | 43 Sources | 43 Destinations | 10 A |
| 21 | Check Point DLP | DLP Incident | 3... | 14 Sources | 15 Destinations | |
| 9 | Check Point DDoS Protector | HTTP Page Flood Attack | 3... | 9 Destinations | tcp/0 | Http |
| 8 | Check Point Anti-Bot | Bot Incident | 3... | 8 Sources | 8 Destinations | |
| 7 | Endpoint Anti-Malware | Malware Infection | | | | |
| 5 | Check Point Security Gateway | Port scan from external net... | 4... | 5 Sources | 5 Destinations | <Multi Value> |
| 1 | Media Encryption and Port Pr... | Media Encryption File Oper... | 14:17:33 05... | 192.116.2.151 | | |
| 1 | Check Point Anti-Virus | Virus Incident | 08:51:49 05... | DarrenDash-lapt... | 192.91.2.51 | domain [udp... |
| 40 | Check Point DDoS Protector | 2 Event Names | 1... | 44 Sources | 42 Destinations | Anc |
| 22 | Media Encryption and Port P... | 2 Event Names | 2... | 22 Sources | | |
- Threat Emulation Detail View:**
 - Severity:** Critical
 - General Event Information:**
 - Event Name: Threat Emulation Incident
 - Product: Check Point Threat Emulation
 - Category: ---
 - ID: ---
 - Ticketing:**
 - Event Owner: ---
 - Event Comment: ---
 - Traffic:**
 - Source: Multi value...
 - Destination: Multi value...
 - Service: ---
 - Event Detection:**
 - Start Time: 04:35:23 05 May 2015 - 14:55:12 05 May 2015
 - Active: Completed
 - Origin: ---
 - Detected By: ---

Reportes aplicativos & usuarios

| Count | Application / Site | Matched Category | User | Traffic | Dropped | Browse Time | Start Time |
|-------|--------------------|-------------------|--------------------|-----------|---------|-------------|-------------------|
| 7 | Facebook | Social Networking | 7 Users | 172.83 MB | | 00:14:22 | |
| | Facebook | Social Networking | Gloria Cash | 24.69 MB | | 00:00:16 | 13:37:01 05 Ma... |
| | Facebook | Social Networking | Ginger Cash | 24.69 MB | | 00:00:40 | 12:38:49 05 Ma... |
| | Facebook | Social Networking | Gabriel Cash | 24.69 MB | | 00:02:30 | 10:57:40 05 Ma... |
| | Facebook | Social Networking | Isabella Whitewash | 24.69 MB | | 00:05:00 | 10:22:13 05 Ma... |
| | Facebook | Social Networking | Florence Flash | 24.69 MB | | 00:00:40 | 08:10:42 05 Ma... |
| | Facebook | Social Networking | Michael Mash | 24.69 MB | | 00:05:00 | 07:19:15 05 Ma... |
| | Facebook | Social Networking | Floyd Flash | 24.69 MB | | 00:00:16 | 05:37:23 05 Ma... |



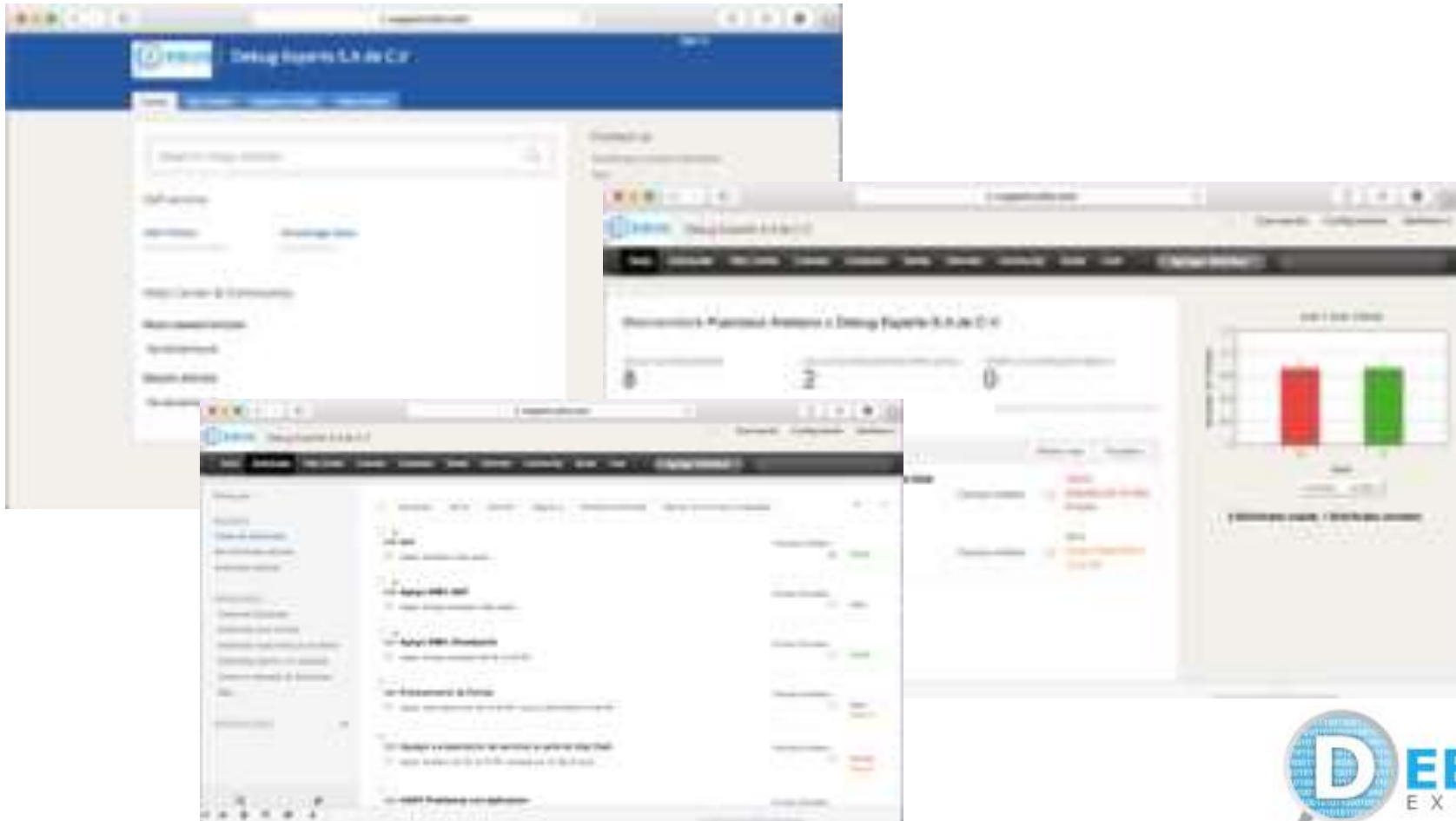
Check Point
como solucion
de seguridad



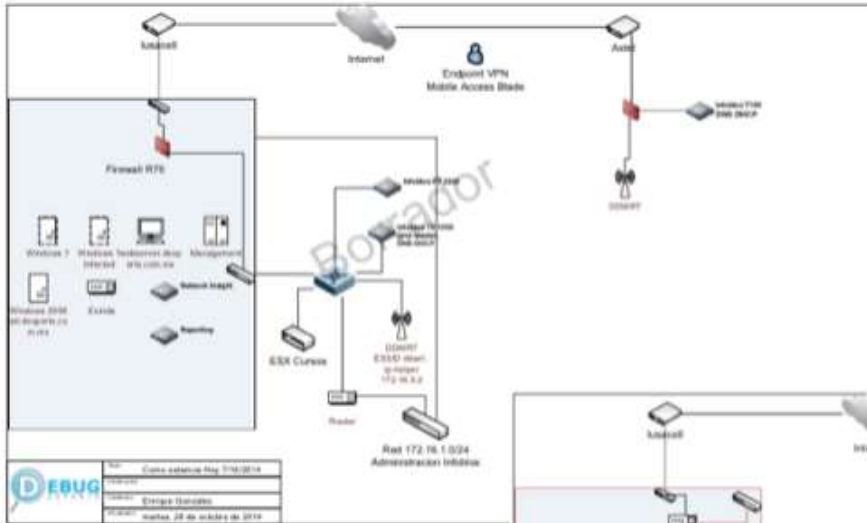
DEBUG EXPERTS MONITOREO Y SOPORTE



Sistema de Tickets

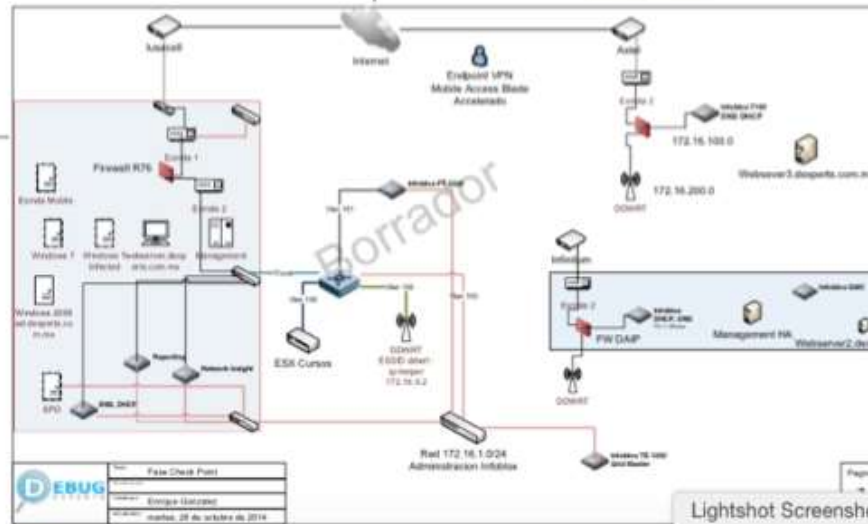


Documentacion al dia



MEMORIA TECNICA

Pueblo Bonito



Lightshot Screenshot



Soporte por ingenieros calificados



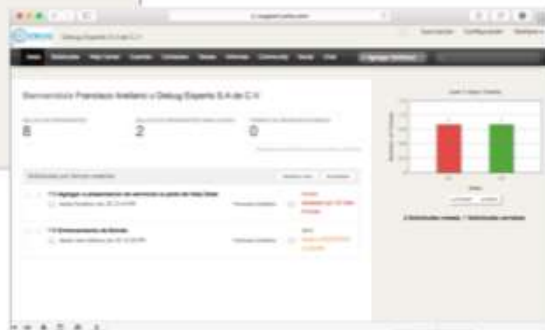
Correo destino:
Soporte-cliente@dexperts.com.mx



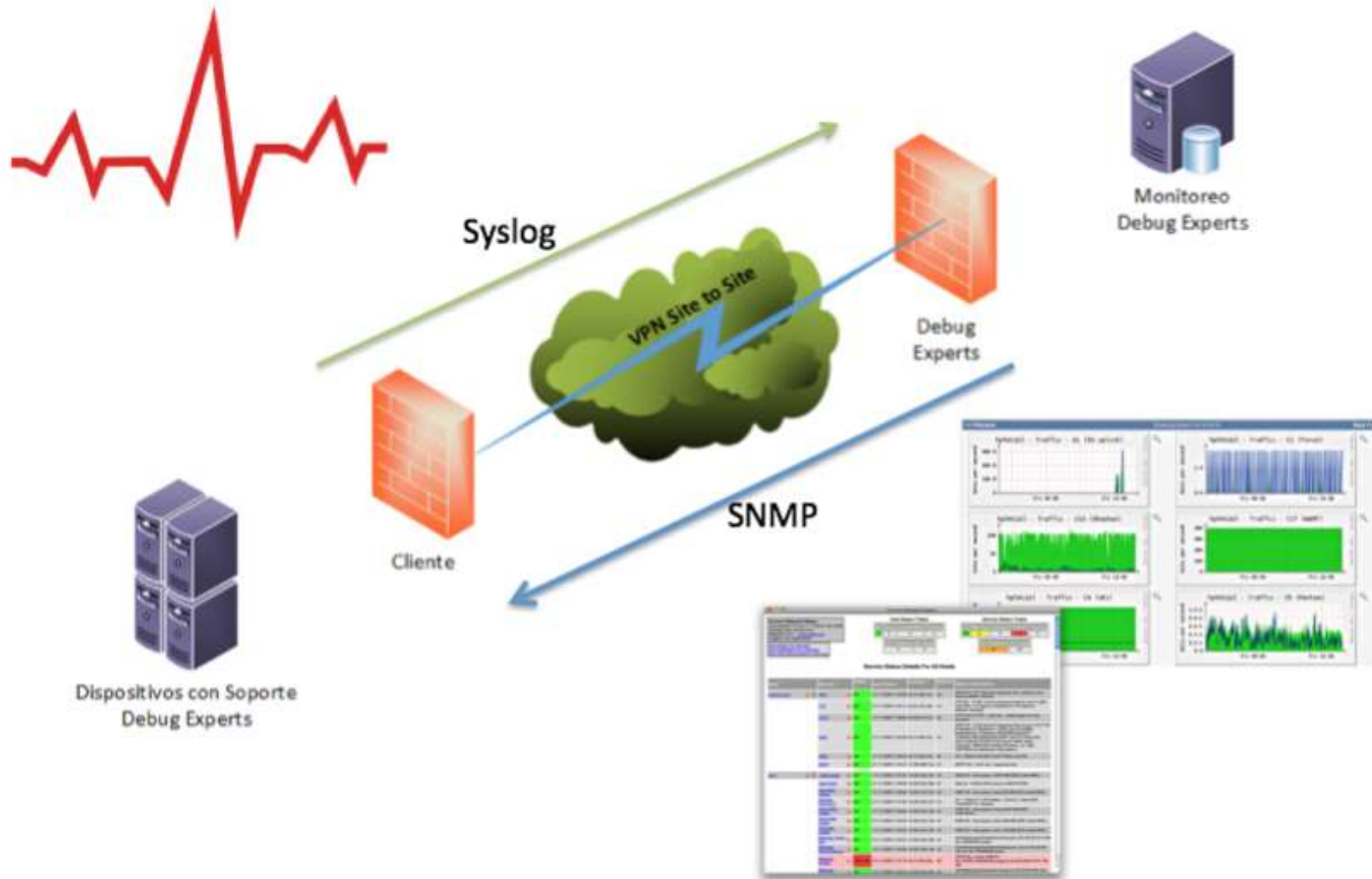
Ingeniero
asignado



Ingeniero de
respaldo



Sistema de monitoreo



Alertas

Notification Type: PROBLEM

Service: Memory Usage

Host: 172.16.0.2

Address: 172.16.0.2

State: WARNING

Info:

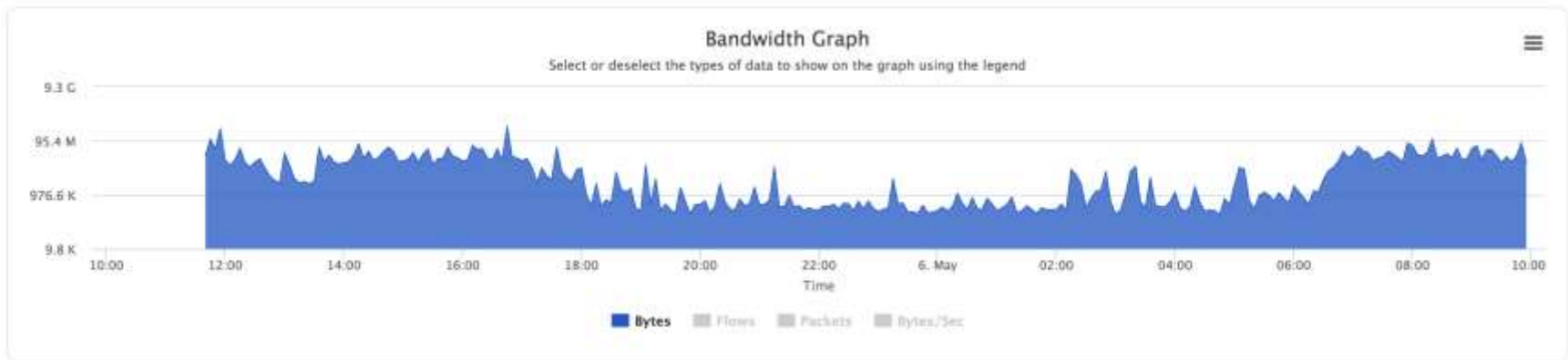
Physical memory: 89%used(7058MB/7940MB) (80%) : WARNING

Date/Time: 2015-04-29 14:23:14

Respond: monitor.dexperts.com.mx/rr.php?uid=18-483-91d06befb11ae03635eece3ee81eab07



Analisis de equipos

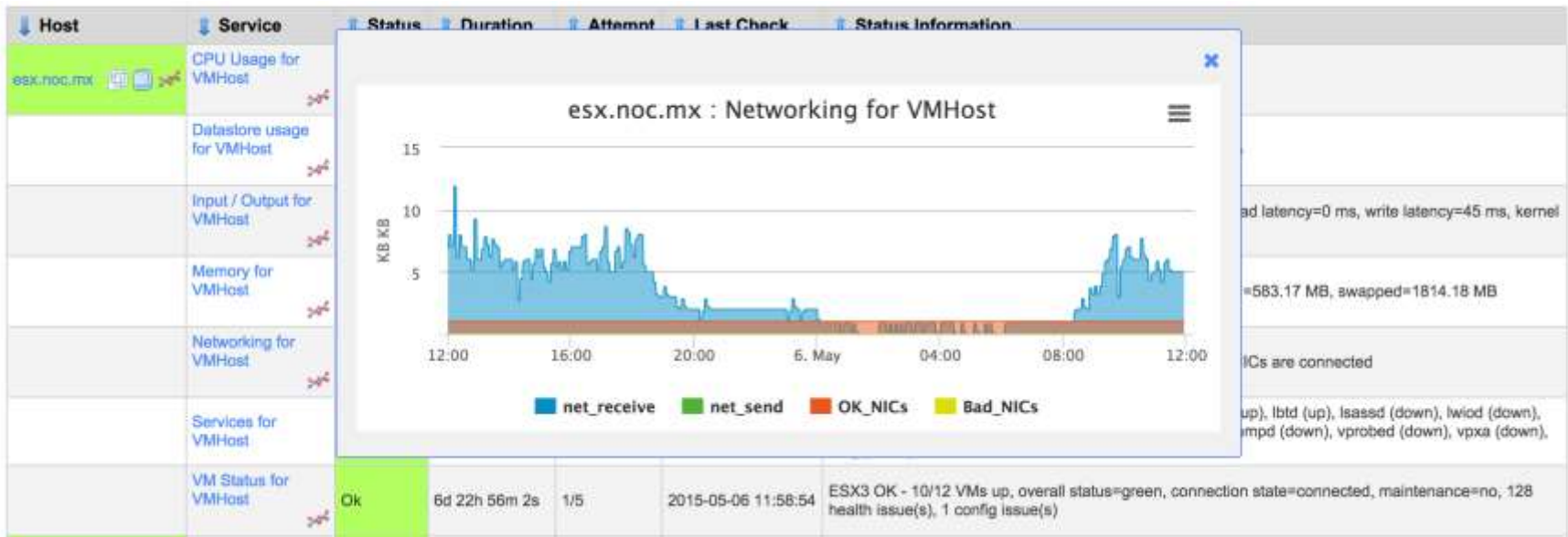


Top 5 Talkers

| Destination IP | % Bytes | Source IP | % Bytes | Dest. Port | % Bytes | Src. Port | % Bytes |
|--------------------------------|---------|--------------------------------|---------|-----------------------|---------|-----------------------|---------|
| 207.248.239.42 | 63.5 | 81.171.112.87 | 6.2 | 13572 | 8.2 | 80 | 35.9 |
| 192.168.1.141 | 3.5 | 5.196.91.222 | 7.9 | 38766 | 7.7 | 443 | 33.3 |
| 192.168.1.239 | 3.5 | 207.248.239.42 | 5.6 | 443 | 6.8 | 38140 | 1.9 |
| 192.168.92.189 | 2.1 | 192.168.92.189 | 4.0 | 17574 | 2.5 | 389 | 1.3 |
| 192.168.92.5 | 1.8 | 23.2.164.167 | 2.9 | 80 | 1.7 | 10724 | 0.9 |



Se monitorean los servicios



Infosecurity

- 1 Chromecast
- 2x 1 año completo de monitoreo para 1 equipo de seguridad o de su eleccion.

