



# Trellix

21 – 24 OCTOBER 2024

## EMEA & LTAM Partner Tech Summit

Lisbon, Portugal

Trellix Network Security  
LTAM Team



# Agenda

- Acerca de nosotros
- Trellix Intrusion Prevention System
- Planificando un despliegue de Trellix IPS
- Diseño de una política IPS
- Configuración de Sensores para Prevención de Intrusiones
- Ajuste fino de políticas

# Acerca de nosotros



Julio Quinteros

Director Trellix Professional  
Services



Alejandro Garcia

Solutions Engineer



# Trellix

## Trellix IPS

Network Security

Julio Quinteros

Director Trellix Professional Services

October, 2024

# Descripción General de Trellix Intrusion Prevention System

## Award – Winning Next-Generation Intrusion Prevention System

- Trellix Intrusion Prevention System (IPS) is a next-generation intrusion detection and prevention system (IDPS) that discovers and blocks sophisticated malware threats across the network.
- Trellix IPS combines intelligent threat prevention with intuitive security management to improve detection accuracy and streamline security operations.

Superior Detection and  
Reduced Complexity

Signatureless Defense

- Intelligent and scalable high-performance management solution
- Protection against Stealthy threats

Integrated Security

Cloud Scalability

# Descripción General de Trellix Intrusion Prevention System (cont.)

## Powerful Protection with Deep Packet Inspection

- Detects and prevents initial incursion
- Prevents C&C traffic and exfiltration
- Prevents exploits, DoS, DDoS, malware download and network misuse

## High performance visibility

- 100% SSL visibility
- L7 Visibility and Analytics
- 100 Gbps throughput for high load north-south network traffic



Reports via network sensors to centralized console



Trellix  
IPS



Searches for malicious activity with a deep network-packet inspection



Scans variety of file types as they travel across the network



Rich source of network activity for Network Detection and Response

# Motores de Trellix IPS

## DDOS Firewall

- IP, User , Application blocking
- IoC feed Ingestion.
- Geo Location




## Signature Based Detection

- - L4 to L7 Inspection
- - HTTP 1.1 and 2.0
- - Evasion Detection
- - Deep File Inspection
- - Botnet, Callback Detection



## Signature Less Detection

- - GAM
- - IP, File, URL Reputation (GTI)
- - TIE
- - IVX
- - DGA
- - L7 DDoS



## Network Threat Visibility

- Network Threat Visibility
- MITRE ATT&CK mapping and Visualization
- NDR
- - L7 Metadata, Netflow, Alerts
- XDR



Inbound and Outbound SSL  
Ipv4 and IPv6  
Large Enterprise scale with Manager of Manager  
High Availability of Sensor & Manager, Active Failover, Passive Failover.  
Physical – Up to 100 Gbps Inspection Capacity, Software Controlled Capacity Upgrade.  
Virtual 1, 5 Gbps – ESX and KVM  
Cloud – AWS GWLB, Azure, OCI\* with autoscaling.  
Dynamic Signature Update – Weekly, Emergency Releases, Custom Signature.  
Dynamic Signature Update  
Federal Certifications



Improved  
Security



Extreme  
Performance



Superior  
Architecture



Complete Threat  
Visibility via  
Extensive Platform  
Integrations



Advanced Analytics,  
Heuristics and  
Machine Learning



Layered  
Signature  
and Signatureless  
Detection



New Advanced  
Malware Engines



Enhanced MS  
Deep File Inspection



3<sup>rd</sup> party Threat  
Feeds and SNORT  
Signature Support



Additional and  
Enhanced Evasion  
Detections





Improved  
Security



Extreme  
Performance



Superior  
Architecture



100% SSL  
Traffic Visibility  
(Inbound & Outbound)



Dynamic  
Key Support



L7 Visibility  
and Analytics



Up to 100Gbps  
IPS Throughput



Active  
Failover



Built-in  
Passive Failover



High  
Availability



Improved  
Security



Extreme  
Performance



Superior  
Architecture



100Gbps  
Throughput



Higher Throughput  
in a Smaller Form  
Factor



Greater Power  
Efficiency



Stackable – Add  
Capacity as Needed



Seamlessly Secure Private, Public  
and Hybrid Cloud Environments  
(e.g., AWS, Azure, Oracle, VMware, OpenStack)



Higher Port Density,  
Flexible Port Modules

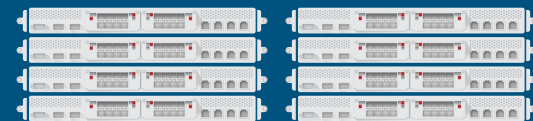
# Trellix NS9500: Rendimiento, Escalabilidad, Protección



Single NS9500



100 Gbps  
NS9500

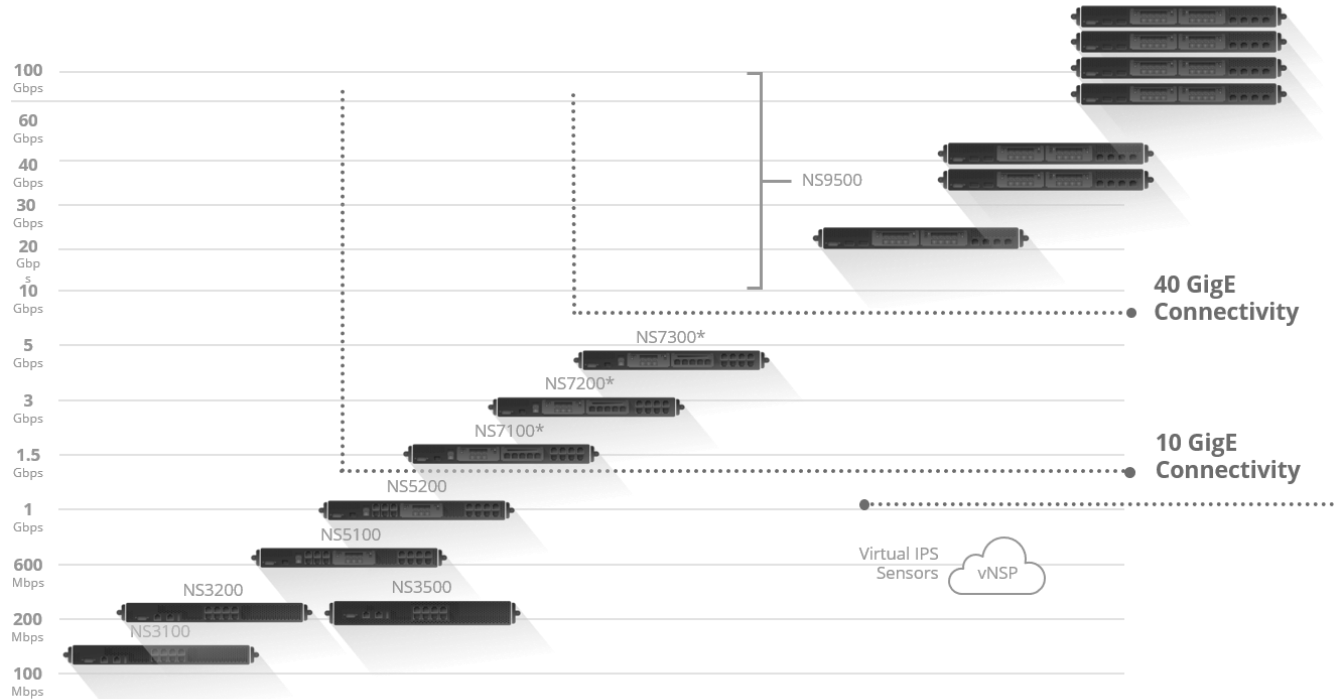


100 Gbps HA NS9500

Up to 30 Gbps Throughput in a Single sensor  
Up to 100 Gbps Throughput Using Stacking Architecture

# Dispositivos Network Security Appliances

## Sensors



# Detección de Zero Day Malware

NSP – Emulation  
Deep File Analysis



GAM  
(Browser)



Adobe PDF



JavaScript



Adobe  
Flash

IVX – Sandboxing  
Dynamic Analysis



Run Time  
DLLs



Network  
Operations

File  
Operations



Process  
Operations



Delayed  
Execution

IVX – Sandboxing  
Static Code Analysis



Unpacking

Disassembly of Code

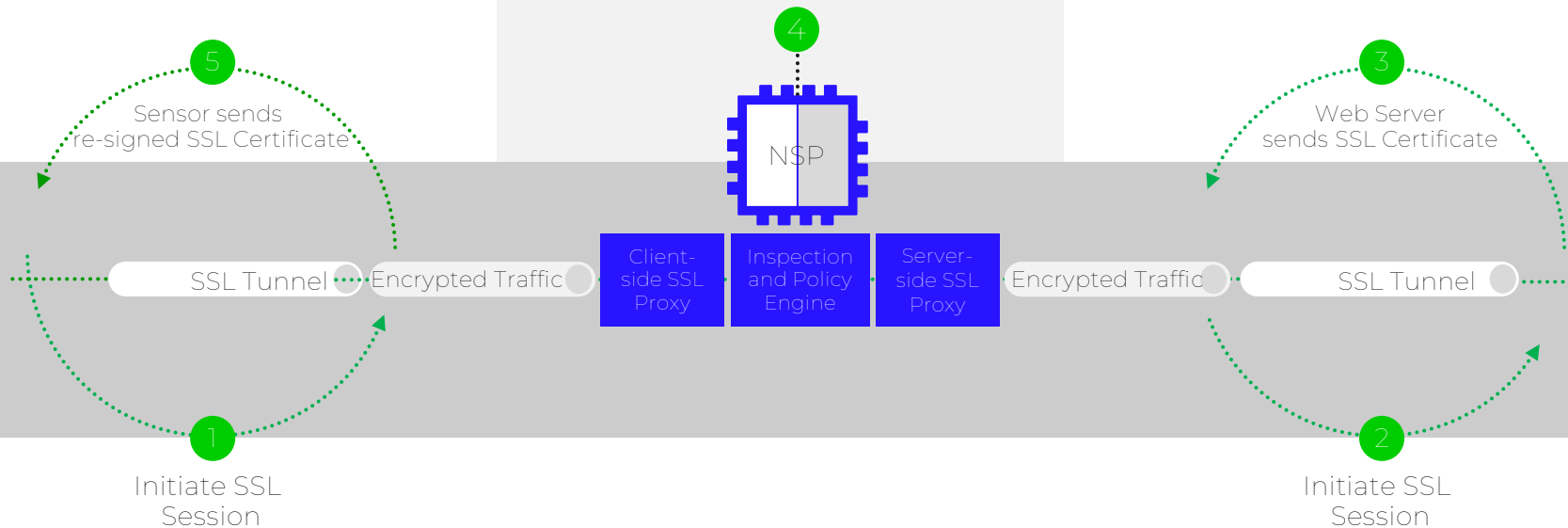
Calculate Latent  
Code

Familial  
Resemblance

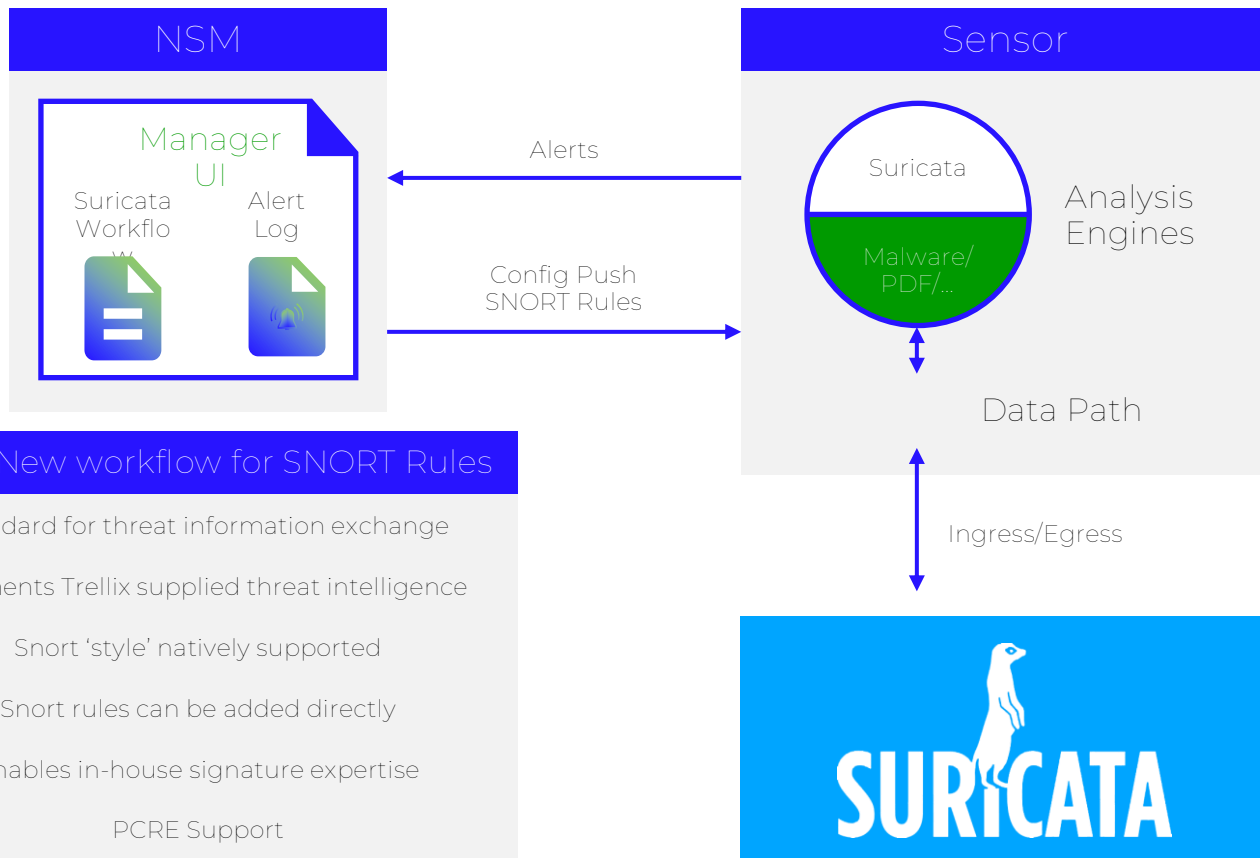
# Descifrado Outbound SSL

Solution – Proxy Mode Outbound SSL

Sensor modifies the certificate by substituting its own public key and CRL details. Sensor then re-signs the certificate using a key with a chain of trust to a CA that is trusted by the client



# Soporte Firmas de SNORT



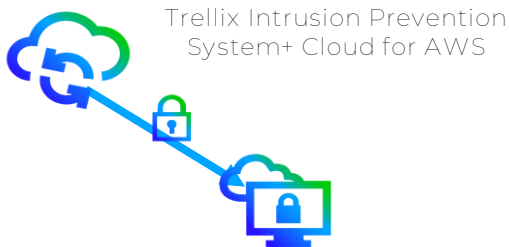
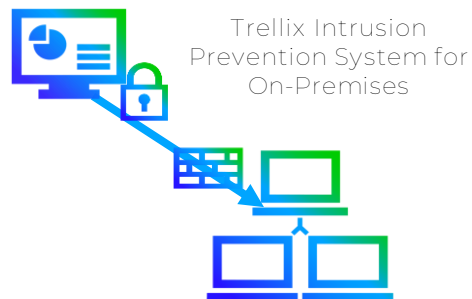
# Trellix Intrusion Prevention - Despliegue

Trellix Intrusion Prevention System can be deployed as either:

- On-Prem
- On Cloud for AWS

## Trellix Intrusion Prevention System for On-Premises:

- ❑ Discovers and Blocks threats across networks.
- ❑ Uses Advanced detection and emulation techniques to defend against stealthy attacks and offers protection with high degree of accuracy and speed.



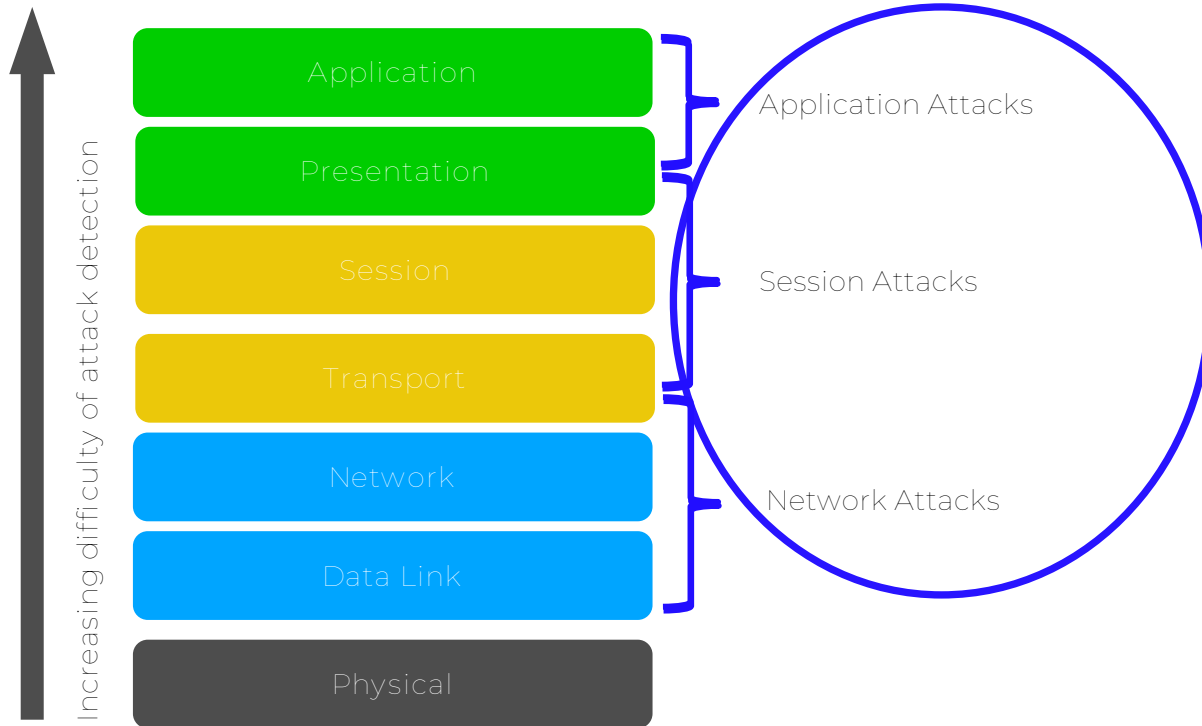
## Trellix Intrusion Prevention System + Cloud for AWS:

- ❑ Protects vulnerable assets from known and unknown exploits with signature-based and signatureless detection.
- ❑ Employs the Trellix IVX dynamic analysis engine to detect new exploits before they enter the network.
- ❑ Integrates with AWS Gateway Load Balancer to deliver high availability and automatic scaling.
- ❑ Reduced Operational Complexity.

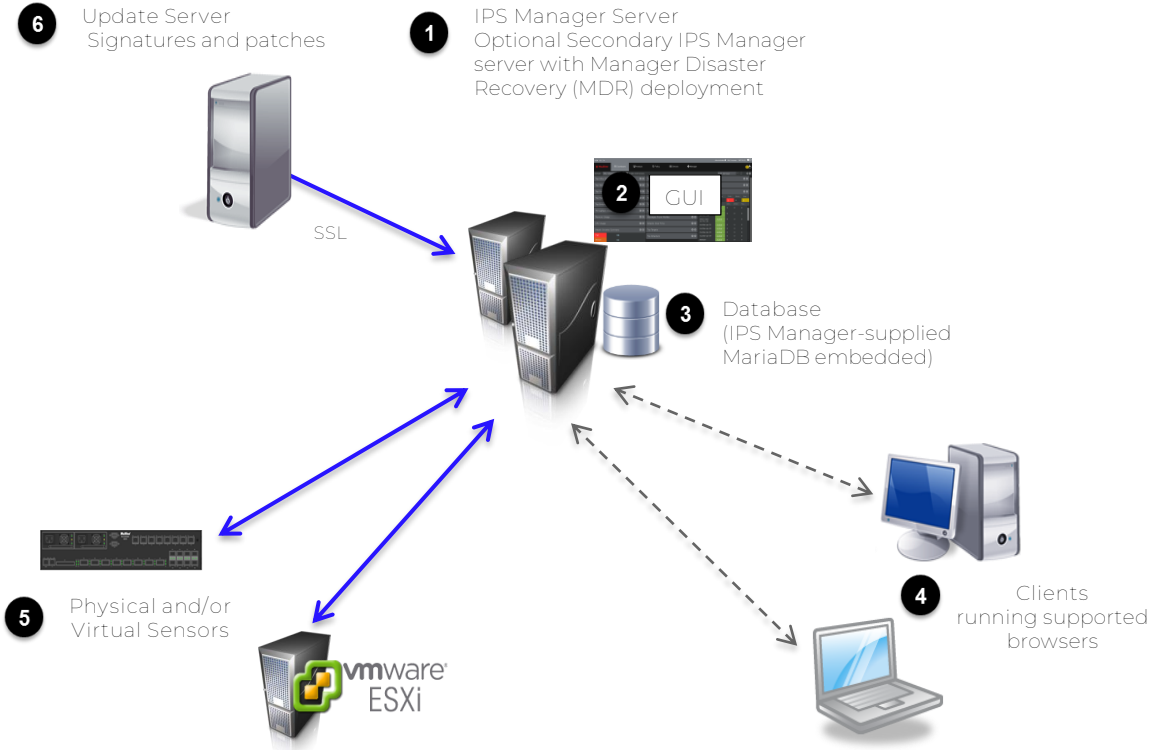


# Capas de Protección

What does IPS Manager Protect?



# Componentes Trellix IPS



The Manager Disaster Recovery (MDR) feature provides a Standby Manager in case the Primary IPS Manager fails.

# Framework de Detección de Ataques

## Traffic Flow Identification

- Sensor identifies flows by protocol (UDP/TCP) and endpoint ports and IP addresses (source and destination).
- Timer-based flow context is implemented for stateless UDP traffic.
- Traffic is divided into flows and passed to appropriate protocol parsing engine.

## Protocol Parsing

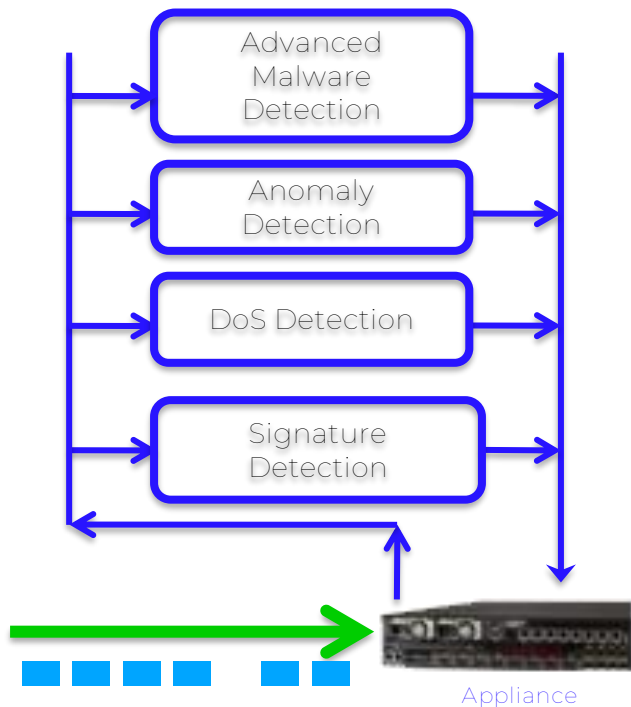
- Protocol specifications parse through networks flows to validate traffic and divide it into protocol fields.
- It is then actively tested against IPS Manager-supplied or custom attack definitions.
- Since the parsing process is fully stateful, it allows detection of anomalies in the protocol's behavior.

## Packet Searches

- IPS Manager passes traffic flows identified as belonging to any particular protocol to packet search protocol specification engine for further parsing.
- It presents each direction of flow to attack definitions.
- Packet search tests typically take form of specific ordered pattern matches to prevent false positives and performance issues.

# Análisis de Tráfico con Diferentes Motores

Parsed Data Passes through Various Detection Engines



- Advanced Malware Detection: Based on selected file types and report confidence level to determine probability of infection.
- Anomaly Detection: Examines data using baseline to detect abnormal behavior.
- DoS Detection: Combines threshold-based and self-learning profile-based detection.
- Signature Detection: Searches flow for multiple triggers (sub-signatures) in protocol fields using embedded signature files.

# Detección en Base a Firmas

Uses well known Patterns to Predict/Detect similar subsequent similar attempts



Example: Seeing “default.ida” means Code Red attack.

## Benefits:

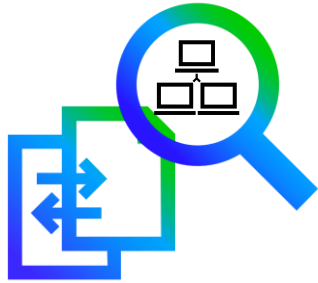
- Effective for well-known attacks.
- Updates the database as new attacks are detected.

## Challenges:

- Updates the database frequently.
- Leaves your network unprotected against new and complex attacks that do not match existing signatures.

# Detección de DoS/DDoS

Combines Threshold/Profile-Based Detection with Self-Learning



Example: Comparing normal traffic to today's traffic.

Detected through:

- Self-learning: Study patterns and adapt behavior over time.
- Exceeded Thresholds: Network behavior changes.
- Signature Matching: Matches attack pattern.

# Detección de Anomalías

Looks for Patterns that do not Match Specifications, such as RFCs



Example: Web traffic with syntax not in compliance to HTTP specification.

Statistical Anomaly:

- Too much UDP traffic, compared to TCP Traffic.
- High traffic volume high at a typically low volume time.

Application Anomaly:

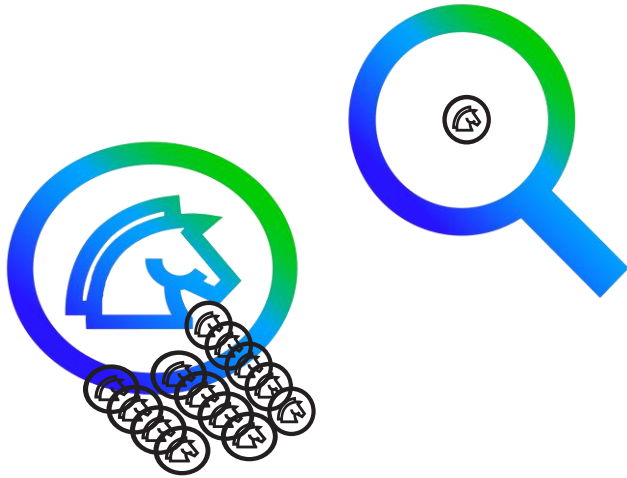
- Shell code in unexpected fields of a packet.

Protocol Anomaly:

- HTTP traffic on non-shared port.
- Corrupted Checksums.

# Detección de Malware Avanzado

## Scans File Types and Reports Confidence Level



Example: High confidence indicates high probability of infection.

### Symptoms:

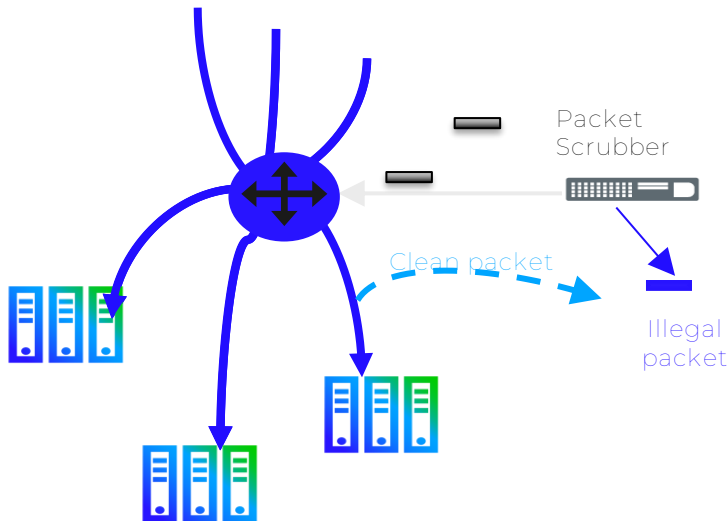
- Poor performance
- Longer startup times
- Unexpected closing/stopping of browser
- Unresponsive or redirected links
- Pop-up advertising
- Additional toolbars on browser



# Normalización de Tráfico

## In-line Sensor Deployments

- Cleans malformed packets (packet scrubbing).
- Prevents hosts from responding to malformed packets.
- Drops illegal packets (fragments).



Recall TCP handshake:

- Client performs active open by sending a synchronization (SYN) request to server.
- Server replies with a SYN-ACK (acknowledgment) response.
- Client sends ACK back to server.

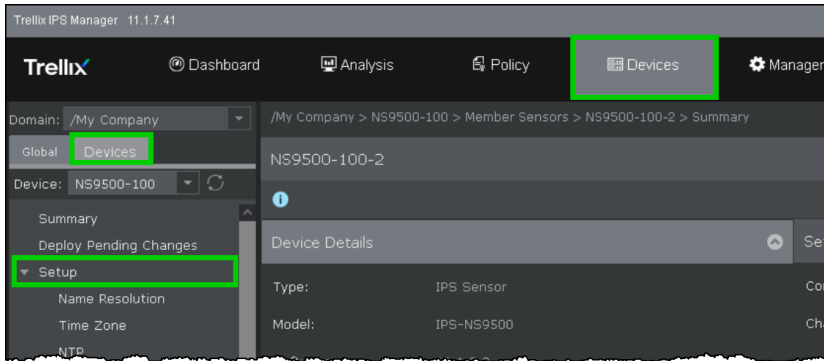
Issues corrected in normalization:

- Removes TCP Timestamp when it is not negotiated.
- Removes maximum segment size (MSS) when it appears in non-TCP packet.

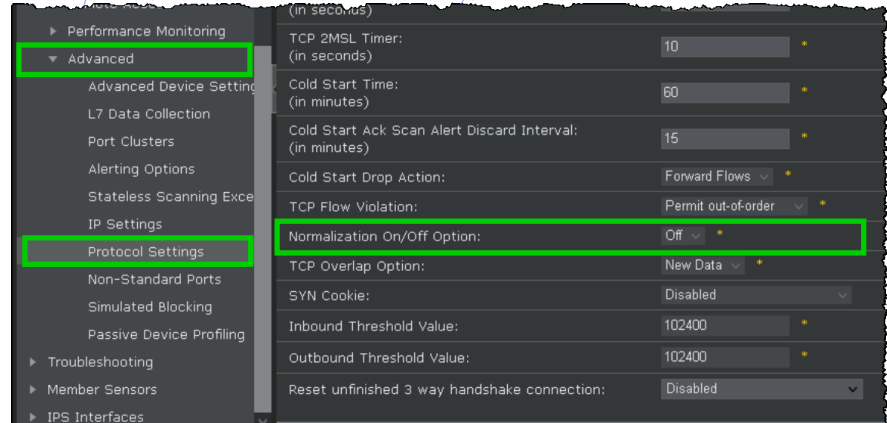
# Normalización de Tráfico (cont.)

## In-line Sensor Deployments

Devices > Setup



Setup > Advanced Protocol Settings



In Trellix IPS Packet scrubbing must be *manually* enabled. Dropping off illegal packets is a default Sensor behavior.

This can be configured under the Devices tab.

Devices tab > < Domain > > Devices > Sensor. (sensor name)

Next go to Setup → Advanced → Protocol Settings and enable Normalization On/Off Option

# 10 simples pasos para usar Trellix IPS

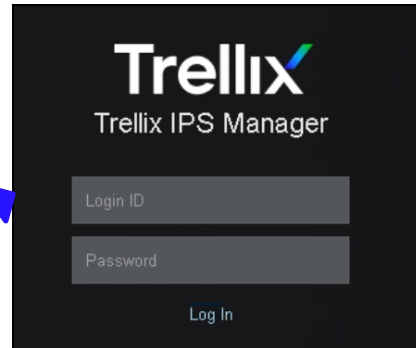
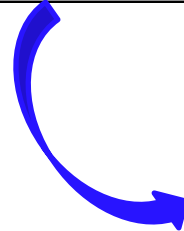
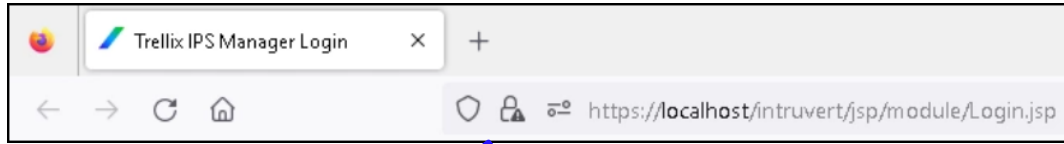


- 1) Install the Manager Software
- 2) Set up and configure the Sensor(s)
- 3) Establish trust between the Manager and the Sensor(s)
- 4) Configure policies in the Manager
- 5) Configure the Update Server and download the latest signature sets
- 6) View alerts
- 7) Tune your Trellix IPS deployment
- 8) Check the system faults status
- 9) Block malicious or unwanted traffic
- 10) Generate Reports

# Ingresar a Trellix IPS Manager

After installation, the Trellix IPS Manager can be accessed using the URL:

<https://localhost/intruvert/jsp/module/Login.jsp>



Desktop shortcut after installation

This is the logon page for the standard version of Trellix IPS Manager. The customer must use the *valid credentials* to log in to the Manager.

# Descripción General del Web UI de Trellix IPS Manager

Trellix IPS Manager 11.1.7.41

Trellix

Dashboard Analysis Policy Devices Manager 1

Domain: /My Company

/My Company > Summary

Summary

1

Manager Software Version: 11.1.7.41

Last Reboot: 2023-Sep-12 09:59:35 GMT-05:00

Central Manager Synchronization: ---

Hostname: NSPMGR ( 10.10.10.207 )

Product Registration: ✔ Registered

Manager GUID: f1fb100d-b8eb-489c-8118-b0caeb4a5448

Protections

		Active Version	Latest Version
1	Signature Set	<span style="color: red;">!</span> 11.9.0.7	11.10.9.3
2	Callback Detectors	<span style="color: red;">!</span> 2723	3627

Connected Users

	Name	IP Address	Logon Time
1	Administrator	127.0.0.1	2023-Sep-13 09:46:11 GMT-05:00

The Manager user interface is a two-tiered structure to facilitate ease of navigation.

1. Use the top Menu bar to logically navigate around the user interface basis the task you want to perform.
2. Using the left navigation pane, you can manage your tasks with more ease in your enterprise level deployments.

# Descripción General del Web UI de Trellix IPS Manager (cont.)

## Dashboard Tab

The **Dashboard** tab is the central interface from which all Manager interface components are available. The **Dashboard** tab is divided into two sections: the top menu bar and the lower monitors' section.

The screenshot shows the Trellix IPS Manager Dashboard interface. The top navigation bar includes the domain '/My Company', a checkbox for 'Include Child Domains', a time period selector set to 'Last 14 days', a refresh button, and a settings gear icon. The main area is divided into several monitors:

- Top Malware Files:** A table showing malware file paths and their counts. A callout box labeled 'Monitors' points to this section.
- Top Endpoints Using Risky URLs:** A table showing IP addresses and their counts. A callout box labeled 'Time period for which the information is displayed across all Monitors' points to the 'Last 14 days' selector.
- Abnormal System Health:** A summary section with a 'Device Summary' and 'Manager Summary' table.
- System Faults:** A table showing system status for the Manager and Device.
- Top Risky URLs:** A table showing risky URLs and their counts.

Callouts for 'Refresh' and 'Settings' point to their respective icons in the top right corner.

File Path	Count
"ArtemisTest.exe"/5db32a316f079fe7947...	18
/BP_MobileMalware.jar/012ca7db8d5bae46...	2
/file2pcap_files/ArtemisPDF_Test.pdf/...	2
/2164018_478.rar/e6568a5957670ceb7d2...	2
zgKwwhEpEbucnBgCNfx.gZ/079455de5891f7...	1
/protocolo18792731.zip/370c0827026658...	1
/Artemis-Medium.exe/603f5be29e9ea922d...	1
/Artemis-VeryLow-Troj.exe/f22f09a8c4c...	1
/file2pcap_files/suspect.apk/f70664bb...	1

IP Address	Count
10.253.216.12	238
122.166.5.140	9
2001:0DB8:85A3:08D3:1319:8A2E:0370:7348	2
203.0.113.195	2
10.10.10.1	1
123.123.123.123	1
123.123.123.156	1
5555:0000:0000:0000:0000:0000:0000:0009	1

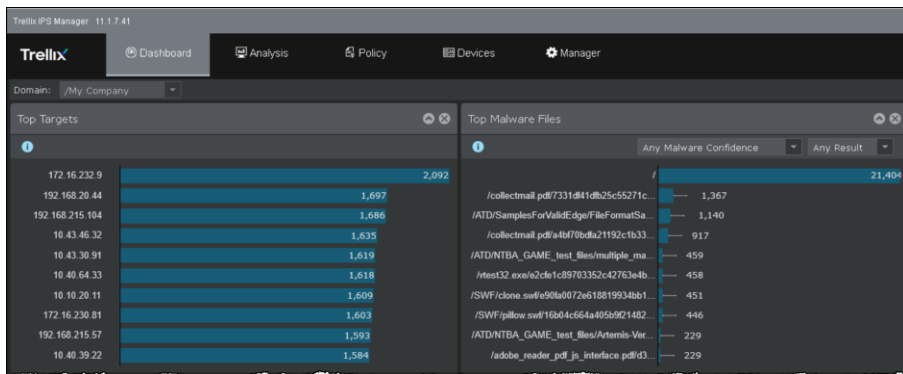
Component	Status	Critical	Error	Warn...
Manager	Up	0	0	2
Device	Active	3	0	2

URL	Count
http://red.test.com/testcapfile.png/...	174

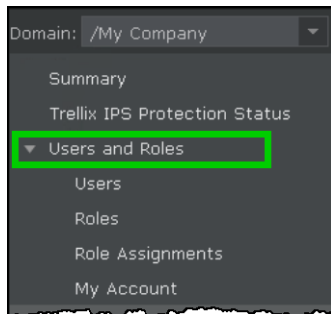
# Descripción General del Web UI de Trellix IPS Manager (cont.)

## Key Features

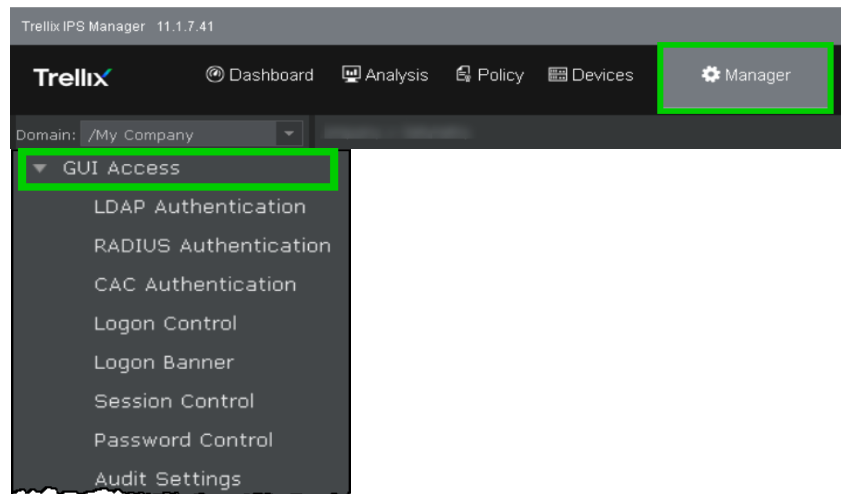
- Web-based management GUI.



- Helps configure Users, Roles, Role assignments, and Admin domains.



- Authentication to: Local, LDAP, RADIUS, and CAC servers.

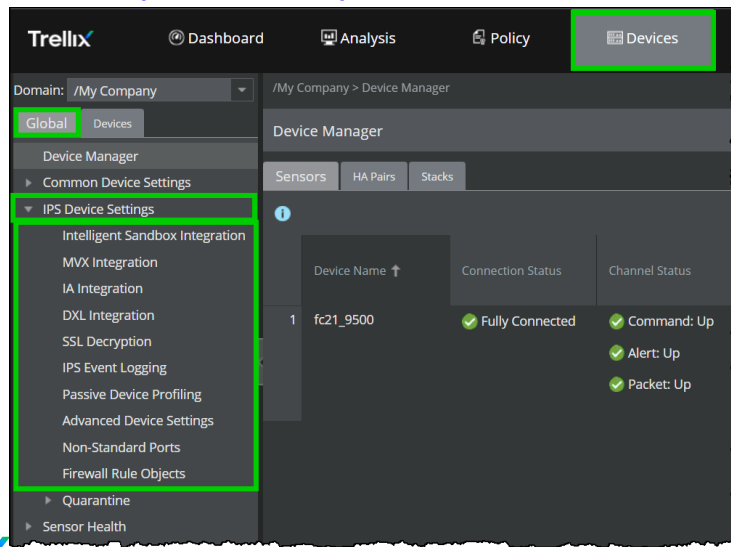


# Descripción General del Web UI de Trellix IPS Manager (cont.)

## Key Features (continued)

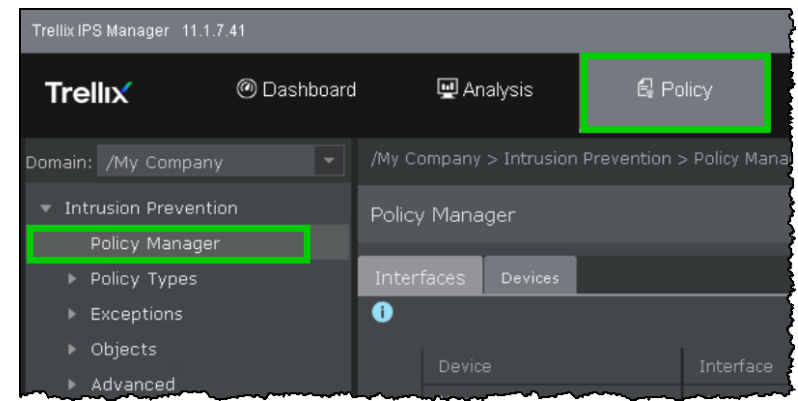
- Integration of new features like, MITRE Attack, Network Investigator (IA) integration, AWS-GWLB integration, Allow-List and Block-List, MVX and IVX integration, VM 5K support, Licenses and Sigsets.

*Devices > [Admin Domain] > Global tab > IPS Device Settings*



- Policy Management

*Policy > Intrusion Prevention > Policy Manager*



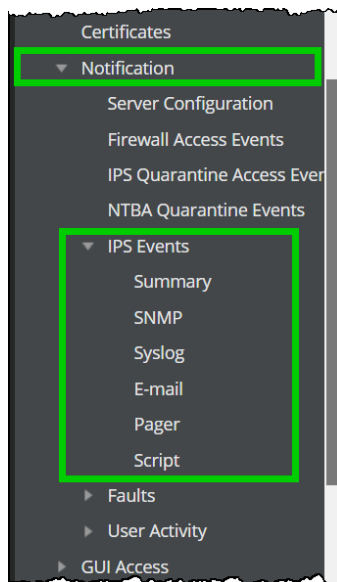
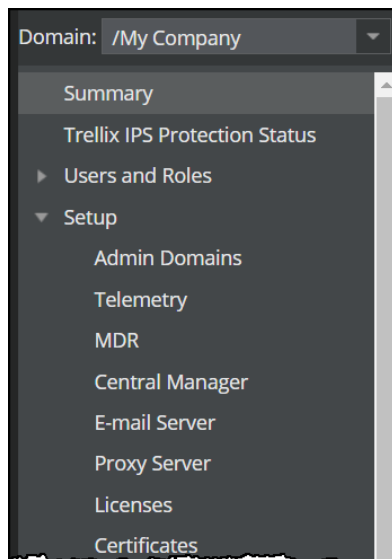


# Descripción General del Web UI de Trellix IPS Manager (cont.)

## Key Features (continued)

- Sends Notifications and Alerts

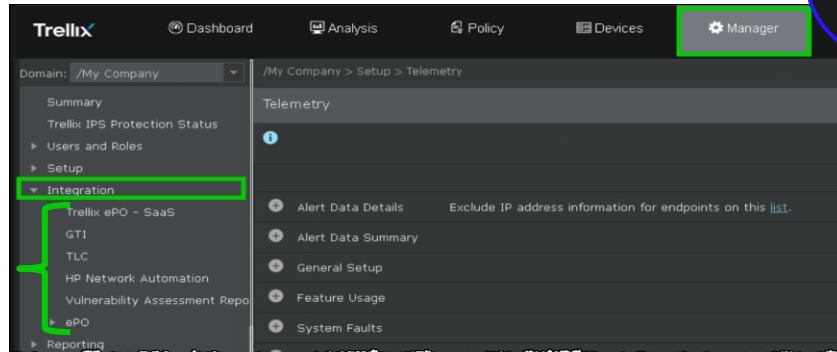
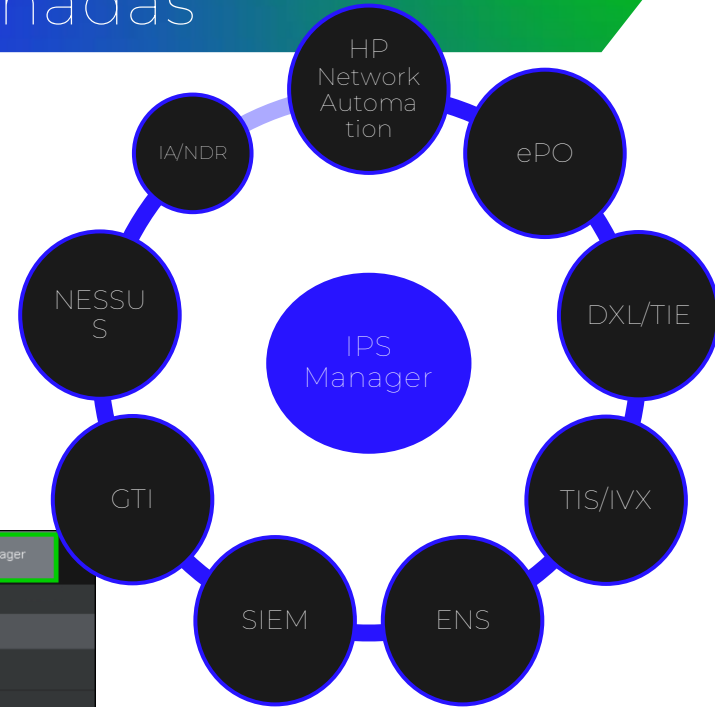
*Manager > [Admin Domain] > Setup > Notification > IPS Events*



# Soluciones de Seguridad Relacionadas

## Management, Monitoring, Reporting, and Threat Information Sharing

- HP Network Automation
- Logon Collector Security Information and Event Management (SIEM) Products
- Trellix Intelligent Sandbox (TIS) / Intelligent Virtual Execution (IVX)
- Network Investigator (IA – NDR)
- Data Exchange Layer (DXL)/Threat Intelligence Exchange (TIE)
- ePolicy Orchestrator (ePO)
- Security Information and Event Management (SIEM)
- Endpoint Security (ENS)
- Global Threat Intelligence (GTI)
- Nessus



# Mejoras de Trellix IPS

## New introduced Enhancements

New

Support for HTTP2 based traffic inspection

Starting with this release of 11.1, the Trellix IPS supports HTTP2 inspection for the following scenarios:

- HTTP2 Prior Knowledge
- Externally decrypted HTTP2 over TLS

Note: HTTP2 upgrade (h2c) scenario is not supported.

Few points to consider prior to enabling the HTTP2 traffic inspection:

- The Sensor requires a reboot when you enable or disable HTTP2 Traffic Scanning. You can check the Sensor reboot status from Device Manager or status CLI.
- HTTP2 Traffic Scanning can be enabled only when HTTP Response Traffic Scanning is enabled.
- HTTP2 Server Push Traffic Scanning can be enabled only when HTTP2 Traffic Scanning is enabled.
- HTTP2 traffic inspection requires a sigset with HTTP2 features.
- Only NS7500 and NS9500 Sensors support HTTP2 traffic inspection.
- HTTP2 performance numbers align with HTTP 1.1 for the supported Sensor models.

# Mejoras de Trellix IPS (cont.)

## New introduced Enhancements

New

The following Sensor CLI commands are included:

Command	Description
show h2 config	Displays details related to HTTP2 status, flow allocation, and decoded packet status.
show h2 connections	Displays statistics details related to HTTP2 context connections.
show h2 frames	Displays multiple frames counter details and settings-frames statistics.
show h2 header-decoder	Displays the HTTP2 header block decode status.
show h2 resource	Displays statistics details related to available and total allocations of HTTP2 resources.
show h2 streams	Displays statistics details related to HTTP2 streams.

The following Sensor CLI command is updated:

Debug Mode:

show feature status - Displays the enable/disable status for a certain features.

# Mejoras de Trellix IPS (cont.)

## New introduced Enhancements

New

Defining and enforcing user-specific blocking strategy to make self-adaptable IPS policies

- No longer need to use bulk edit
- Simple and automated IPS policy management to block attacks
- Define and store one or more customizable rules for blocking attacks during the attack set profile configuration
- Manager automatically correlated the blocking criteria set with the new and existing attack signatures
- Enables IPS policies to automatically block attacks that match the blocking strategy – makes them self-adaptable to new signature set release
- Minimizes need to manually edit IPS policies to block attacks

Steps required

- Create or edit an attack set profile that includes rules for blocking attacks as per your blocking strategy
- Once the attack set profile with your blocking criteria is configured, you can use the same attack set profile during IPS policy configuration
- Enforce the IPS policy at the interface and sub-interface level for the required Sensor(s)
- Deploy these configuration changes to the required devices

# Mejoras de Trellix IPS (cont.)

## New introduced Enhancements

New

- Users can configure the Manager to forward MITRE attack details to Syslog and SNMP servers
- The variables introduced to forward MITRE attack details are IV\_TACTIC, IV\_TECHNIQUE, IV\_SUBTECHNIQUE, and IV\_TTPID
- Choose the appropriate variables while configuring the Notification Profile

The following Sensor CLI command is updated:

show acl stats – Displays the count of packets matching the Stateless ACL rule which skipped the proxy engine

Updated platform, environment, or operating system support

- New 7600 and 3600 sensors
- MITRE attack Mapping
- IX On-Prem and Cloud integration
- Network Investigator/NDR Integration
- Manager support on KVM
- The IPS Manager uses MariaDB version 10.6.14 that includes additional security against new vulnerabilities
- The IPS Manager uses JDK version 8u372 that includes additional security against new vulnerabilities
- Double NIC support, and IPv6 support on Linux NSM

# Trellix

## Planificando un Despliegue



# Despliegue de Trellix Intrusion Prevention System

## Overview

The process of setting up and running Trellix IPS falls under the following basic levels:

1. Decide where to deploy Trellix Intrusion Prevention System Sensor.
2. Setting up the Sensor for the desired deployed mode.
3. Install the IPS Manager Software.
4. Establish Sensor to Manager communication.
5. Configure the Manager.
6. Tune your deployment.
7. Update sensor signature sets and software.
8. Viewing and working with data generated by Trellix IPS Manager.



# Prerequisitos para la instalación del Manager

## Windows Based Manager

A dedicated Server



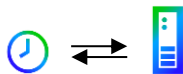
Trellix recommends you use a dedicated server, hardened for security, and placed on its own subnet.

Must have administrator / root privileges



You must have Administrator/ root privileges on your Windows server to Install the IPS Manager Software and its embedded Database.

Synchronize time with IPS Manager Server



It is essential that you synchronize the time on the IPS Manager Server with the current time. If the time is changed on the Manager server, the Manager will lose connectivity with all Trellix Intrusion Prevention System Sensors (Sensors) and the Trellix IPS Update Server, thereby resulting into loss of data.

# Despliegue de Manager Único y Central

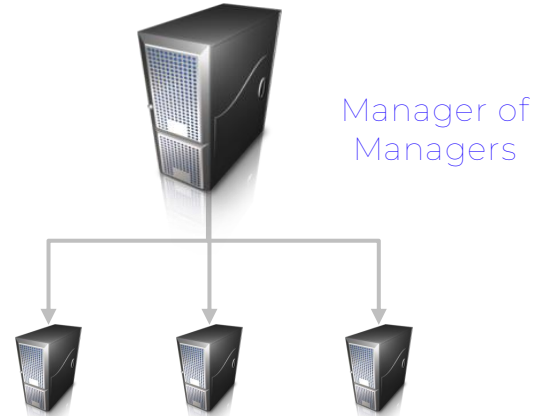
This is different from MDR (Manager Disaster Recovery)

Single IPS Manager



The **Manager Disaster Recovery (MDR)** feature provides a Standby Manager in case the Primary IPS Manager fails.

Central IPS Manager



*Central Manager* is a centralized system managing multiple Managers. It's the Main manager interconnected to various single Managers.

# Despliegue de Manager Único y Central (cont.)

The Manager installs:

- Trellix IPS Manager
- Trellix IPS Manager Database

## Standalone IPS Manager:

- This system acts as the IPS Manager Server.
- It hosts the Manager software and database. It runs on supported Windows Server OS (64-bit only).

## The Central Manager:

- Manages configurations and pushes them globally to Configured IPS Managers.
- The Central Manager allows users to create a management hierarchy that centralizes policy creation, management, and distribution across multiple Trellix IPS Manager(s).
- Regional IPS Managers can add their own region-specific rules and policies but cannot modify any configuration established by the Central Manager.
- Sensor configuration and threat analysis tasks are performed at the individual IPS Manager level.
- The Central Manager's single sign-on mechanism manages the authentication of global users across IPS Managers.

# Standalone IPS Manager and Central Manager

Unit	IPS as a Standalone	IPS as a Central Manager
	Recommended	Recommended
Operating System	Windows Server 2012, 2016, 2019, 2022 Standard Windows Server 2012, 2016, 2019, 2022 R2 Standard	Windows Server 2022 Data center Edition operating system
CPU	1.5 Ghz	2.4Ghz or faster
Memory	=> 32GB	=> 32GB
Disk Space	300GB	500GB or more
Network	1 Gbps Card	1 Gbps Card
Monitor	32-bit color (1440 x 900)	1920 x 1080
Browser	Microsoft Edge Mozilla Firefox Google Chrome	Microsoft Edge Mozilla Firefox Google Chrome

# Alta Disponibilidad y Recuperación de Desastres – Manager Disaster Recovery (MDR)

## MDR Pair Deployment

- With MDR, two Manager Servers are deployed as part of Trellix IPS.
- One host is configured as the Primary system, and the other as the Secondary. Each uses the same major release Manager software with mirrored databases.
- The Secondary Manager remains in a standby state by default and monitors the health status of the Primary Manager and retrieves Sensor configuration information from the Primary Manager.

Switchover, or failover from the Primary to the Secondary, can be manual/voluntary or involuntary.

If the Primary Manager is found *unavailable* during 'health checks' performed by the Secondary Manager, the control switches over to the Secondary Manager.

Primary Manager



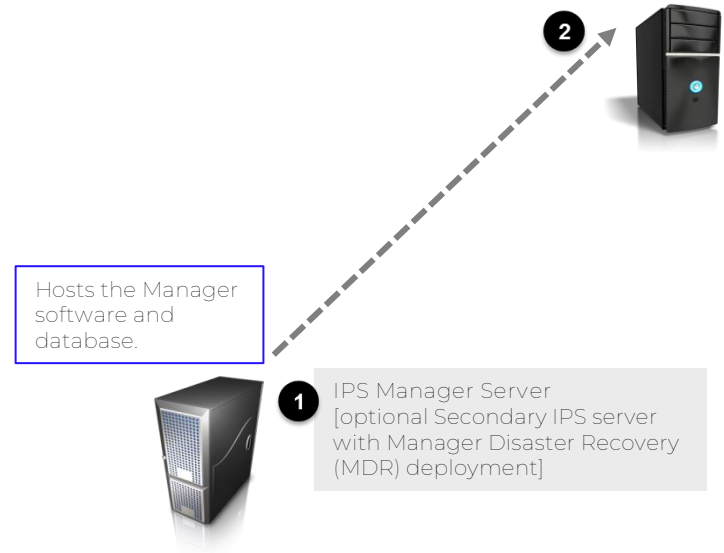
Secondary Manager

# Manager Disaster Recovery (MDR) (cont.)

## Switchover

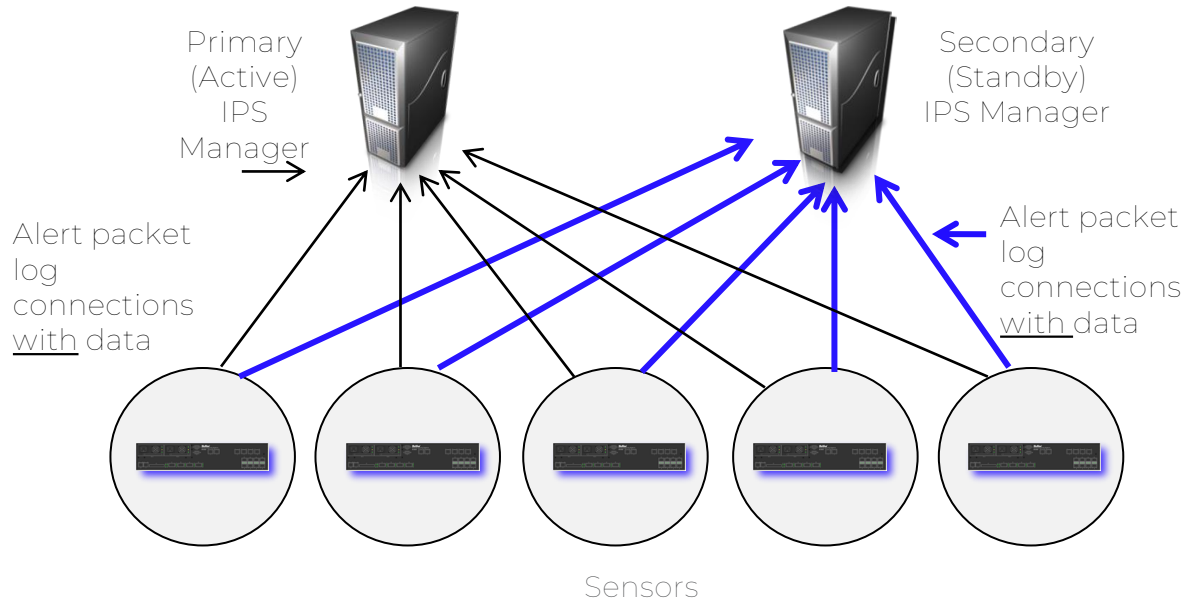
- Can be manual/voluntary or involuntary.
- The Secondary Manager performs regular “health checks” on the Primary Manager.
- Once the Secondary Manager is active, the Primary moves to standby.
- All “in-flight transactions” are lost upon failover from Primary to Secondary Manager.
- Once the Primary Manager has recovered, you can switch control back to the Primary system.
- After switch-back, alert and packet log data is copied from Secondary to Primary Manager.
- Recommended against making any configuration modifications on the Secondary Manager.
- You have a choice whether to retain the configuration on the Primary or overwrite with changes made on the Secondary.

Manager Disaster Recovery (MDR) feature provides a Standby Manager in case the Primary IPS Server fails.



# Manager Disaster Recovery (MDR) (cont.)

## MDR Pair Deployment



*Communication of an MDR pair with Sensors*

- A Sensor connected to MDR pair maintains communication with both Managers at all times.
- Real-time synchronization between the MDR pair ensures that the data present in the active mode is exactly mirrored in the standby.
- If the Sensor cannot send the alert to either of the Managers, the alert is saved in the Sensor's buffer.
- The maximum number of alerts and packet logs restored with synchronization is 10,000.

# Determinando los Requerimientos de la Base de Datos

## Considerations

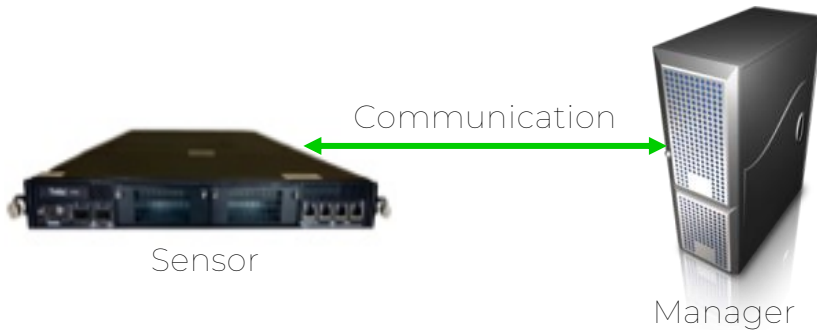
The Manager installation set includes a database for installation that is embedded on the target Manager server.

- Governed by many factors that are mostly unique to the deployment scenario.
- 2 governing principles to the manager Database management are:
  - Amount of data you wish to retain in the database
  - The time period for which (for how long) the data must be retained
- Things to consider when determining the size of the Manager Database:
  - Aggregate alert and packet log volume from all Sensors
  - Lifetime of alert and packet log data



# Estableciendo la comunicación Sensor a Manager

The size of the network and bandwidth requirements determine the number and type of Sensors required to successfully and efficiently protect the network.



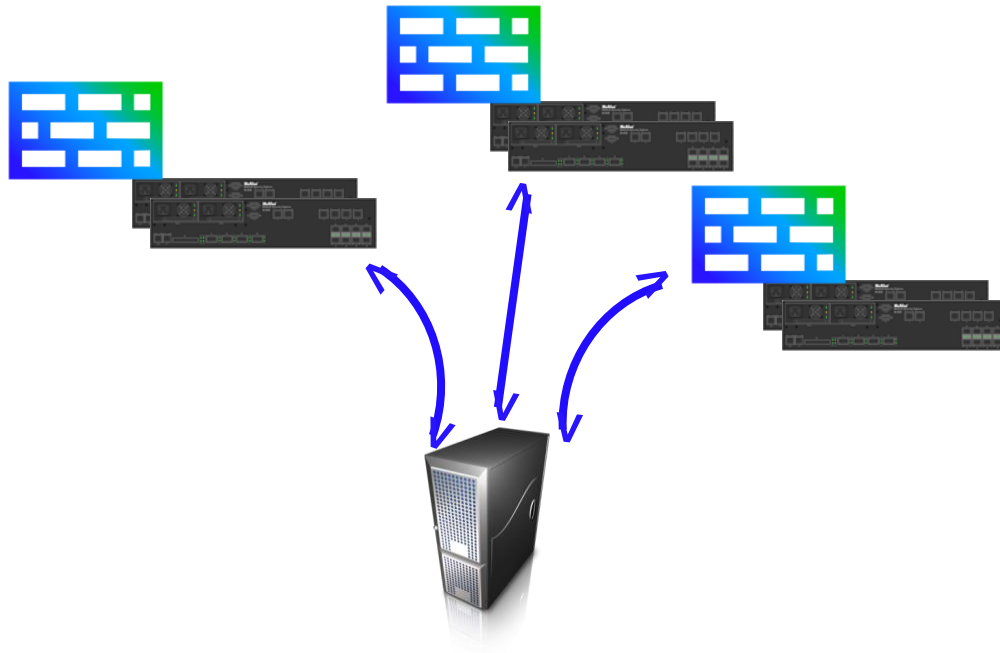
Ping the Manager from the Sensor to check if the communication has been established.

To Install the Sensor:

- ✓ The Physical Device -The Sensor
- ✓ A Console PC
- ✓ PuTTY - Telnet software.
- ✓ Network Details:
  - Sensor name & Password
  - Define the IP Type: IPV4, IPV6 or both
  - Sensor's IP address
  - Sensor's sub net mask address
  - Feed in the Manager IP address
  - Configure the Sensor Default Gateway
- ✓ Shared Secret Key – establishes "Trust relationship" between the Sensor and the Manager

# Determinando el número de Sensores para el Manager

Can 100 Sensors Actually be Supported?



How many Sensors can be deployed with one IPS Manager?

# Determinando el número de Sensores para el Manager (cont.)

## Answer

- Highly dependent upon existing network factors and deployment options.
- No specific X=N response.
- General rule is not to exceed 50 Sensors for any given IPS Manager.

### Considerations:

- ❑ Number of updates
- ❑ Alerts and packet logs
- ❑ Non-tuned policies
- ❑ Sub-interfaces

- ❑ The Sensor and Manager exchange information generally every two minutes to verify the Sensor status is Up (operating).
- ❑ When the manager detects the first poll failure, it reduces the polling interval to every 30 seconds to verify the status of the communication channel and eliminate the possibility of a failed poll due to packet loss.
- ❑ If the Sensor is still un-reachable after 10 minutes, the polling frequency reverts to its normal value of two minutes.

# Despliegue de Sensor

## Pre-installation:

- Stagger your Sensor deployment in phases.
- Know traffic capacities at the points where Sensor is located.
- Choose Sensor location and deployment modes.
- Identify capacity limitations.
- Determine location (domain) in the Manager.
- For physical Sensors, ensure there is appropriate rack space and power.

## Installation:

- Have a computer available for direct console connection to the Sensor for initial configuration.
- Configure name, network, secret key, establish trust.
- Ensure you have HyperTerminal or PuTTY.
- Ensure network connectivity between the NSM and the Sensor.
- Know what adjacent devices to connect to for network monitoring.
- Build a test plan.

# Despliegue de Sensores (cont.)

Scalable for Growth

Branch Site



Enterprise Campus



Data Center



Large network with many access points, file servers, and machines in use may require a larger level of deployment than small office with single access point and few machines.

## Despliegue de Sensores (cont.)

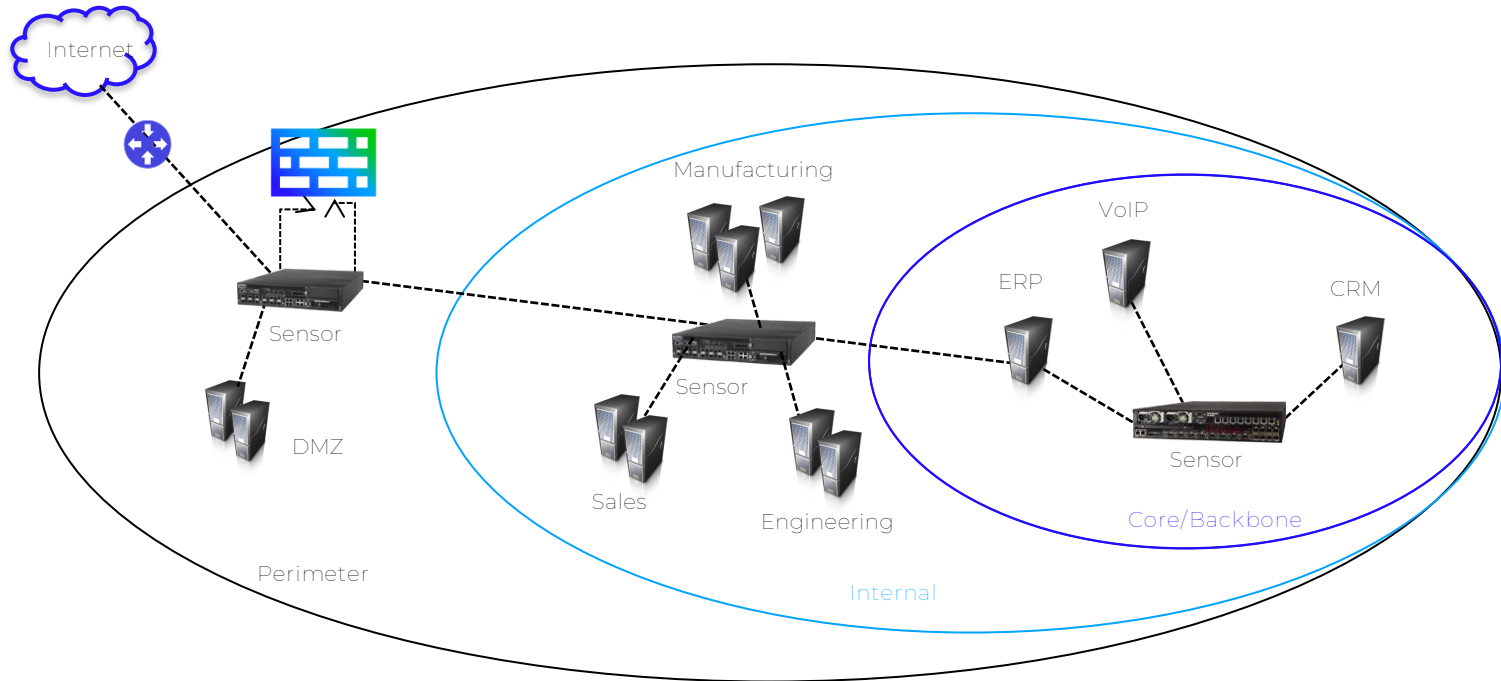
Deployment of Trellix IPS requires specific knowledge of your Network's security needs.

Things to consider are:

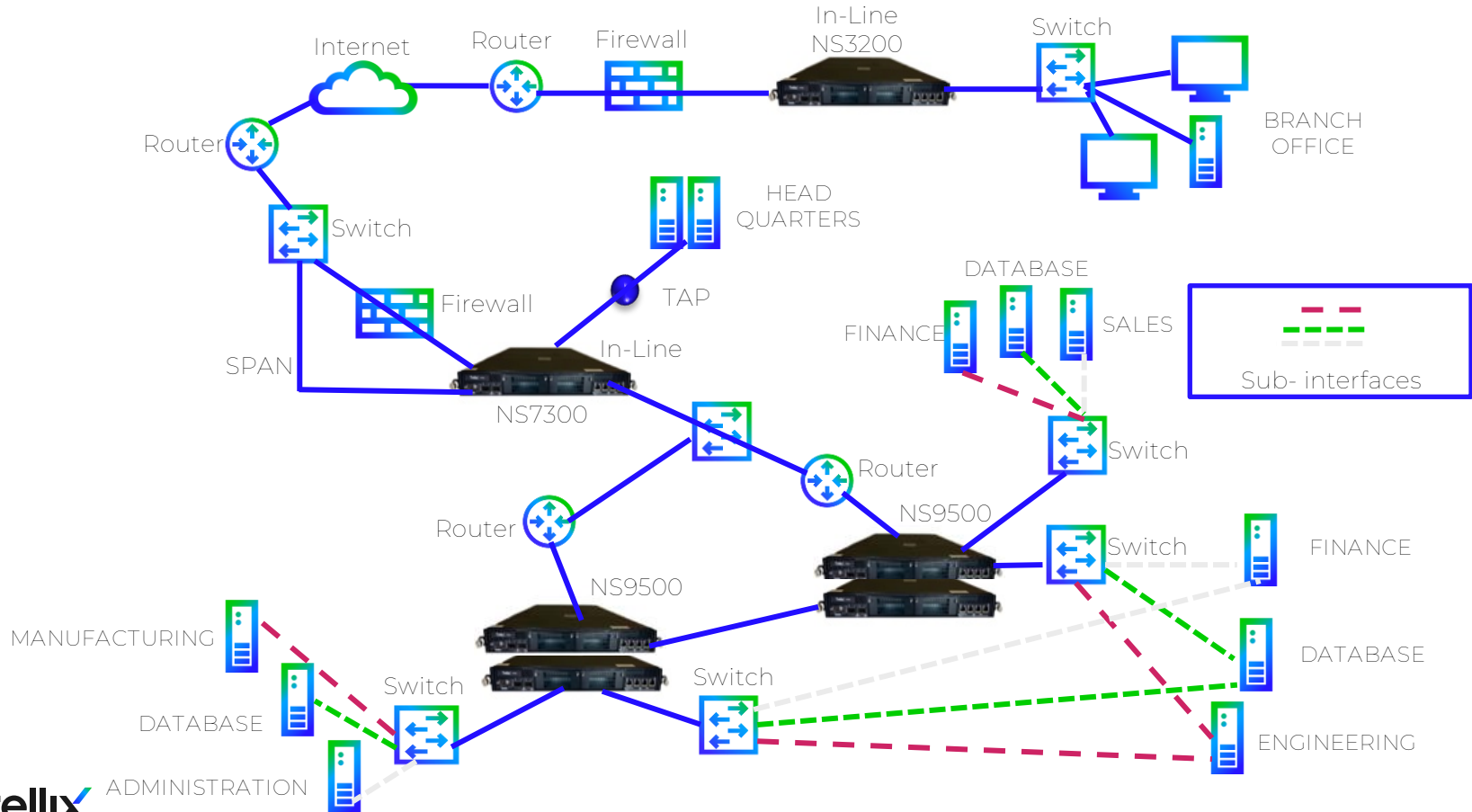
- Size of the Network
- Access points between your network and the Internet
- Critical Servers that require protection within your network (Firewalls and Anti-virus)
- Complexity of your network topology
- Traffic flow across your network
- Sensor Bandwidth

# Determinando la Ubicación de los Sensores

## Example Topography



# Redes Grandes: Perímetro, Core, e Interna

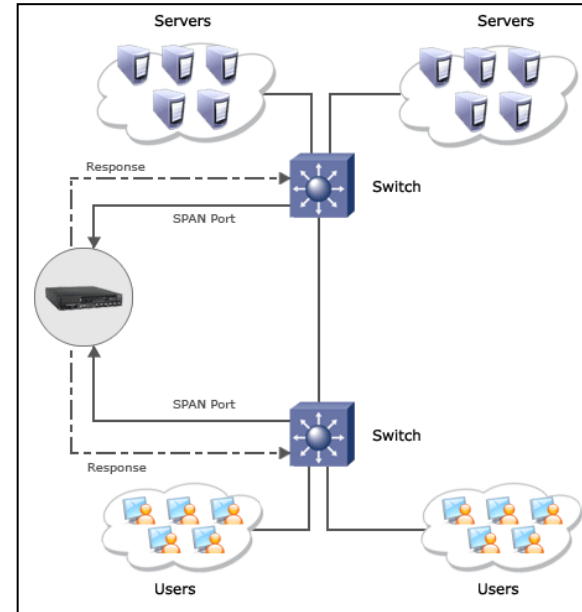




# Modos de Operación

## Switch Port Analyzer (SPAN) mode

- SPAN port forwards incoming/outgoing traffic to Sensor for monitoring.
- Traffic is half-duplex.
  - ❑ One monitoring port required.
  - ❑ Response port sends TCP resets.
- Does not prevent attacks from reaching target.
- Easy to saturate.
- 100Mbps limit.
  - ❑ Can prevent all packets from being copied.
  - ❑ Sensor can report false alarms or miss real attacks.



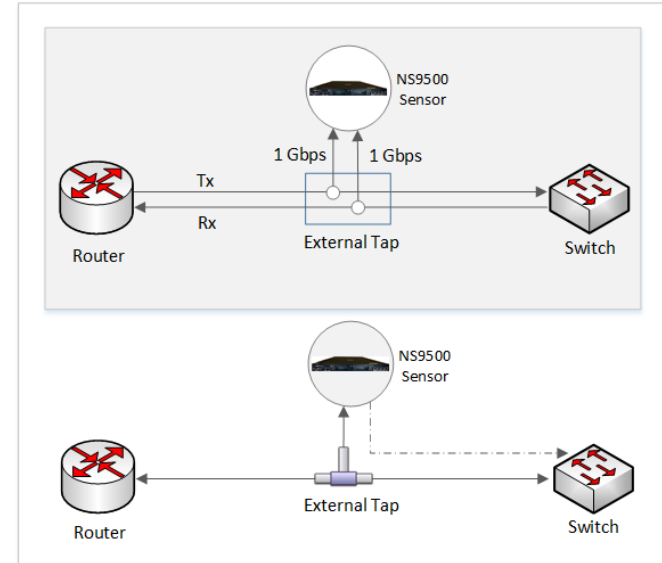
Sensor is connected to SPAN port of switch or port on hub.

# Modos de Operación (cont.)

## Test Access Point (TAP) mode

Sensors with GE monitoring ports require external taps. The external taps are full-duplex; they connect in-line with the network segment, copy the traffic, and send the copies to the Sensor for analysis.

- Traffic is full-duplex.
- Split into separate transmit and receive channels.
  - ❑ TAP makes exact copy of traffic and sends to the Sensor for analysis.
  - ❑ Sensor requires transmit and receive interfaces to monitor both channels.
- Does not prevent attacks from reaching target.
- Not supported on virtual Sensors.



NS-9500 Sensor deployed in external tap mode

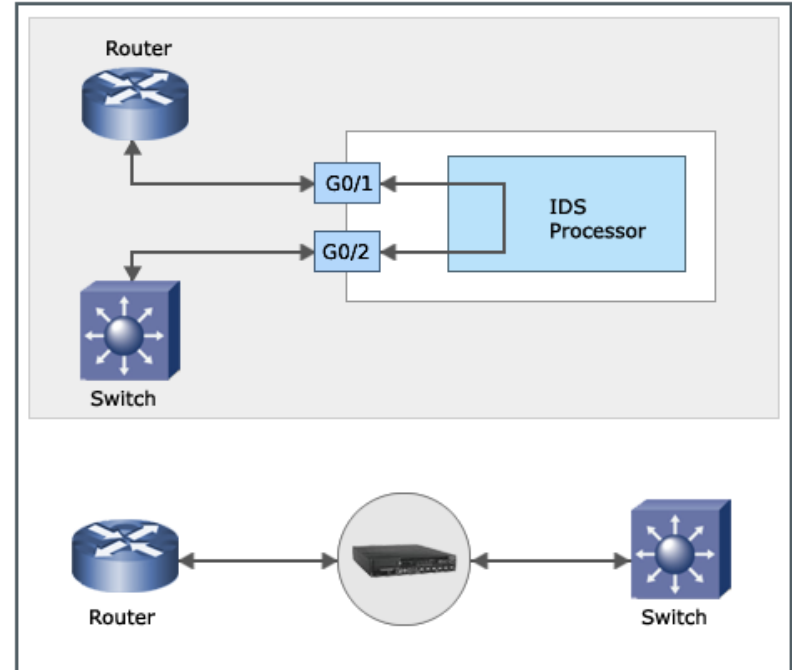
# Operating Modes (continued)

## In-line Mode (recommended)

- Directly in path of network segment.
- Sensors route all incoming traffic through designated port pair.
- Enabled by default.
- Benefits:
  - ❑ Only mode that prevents attacks from reaching target.
  - ❑ Supports packet scrubbing.
  - ❑ Processes at wire-speed.
  - ❑ Prioritizes traffic during heavy load conditions.



Note:  
When deployed in-line, you must specify whether the Sensor port is monitoring inside or outside of the network it is protecting.



# Fail-Close y Fail-Open (solo modo in-line)

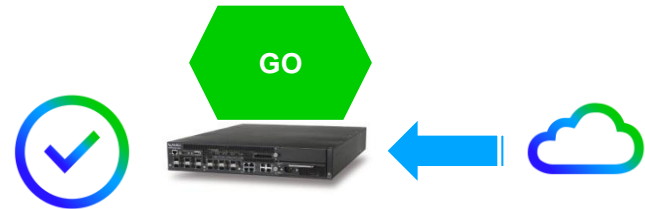
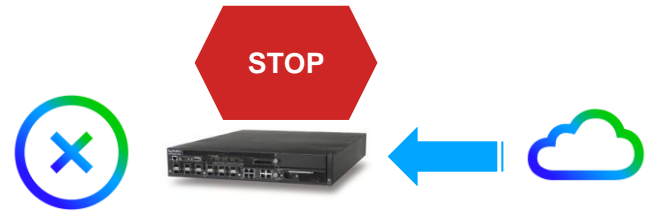
## Sensor Maintenance and Outage Situations

### Fail-close:

- Default configuration
- Traffic stops at Sensor
- No extra hardware but can cause downtime or bottleneck

### Fail-open:

- Optional bypass kit (sold and deployed separately). Does not apply to Sensors with copper ports
- Allows traffic to flow but no threat analysis/detection.
- Active fail-open goes into bypass without any interaction required with Sensor.
- Passive fail-open uses control connection to Sensor.

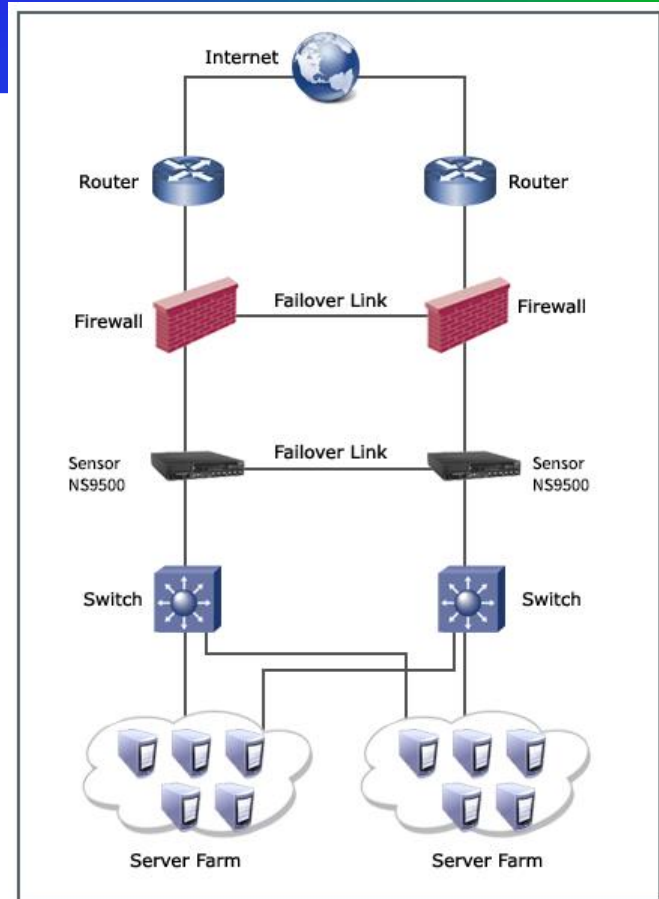


# Configuración de Fail-Over

## In-Line mode only

- In typical failover configurations, one device is the template device while the other is the peer.
- In the HA pair, the configurations applied on the template device are also applied on the peer.
- The template device is the active device and performs normal network functions while the peer is the standby, ready to take control should the active device fail.
- Both the Sensors are active at all times monitoring packets and operate normally.

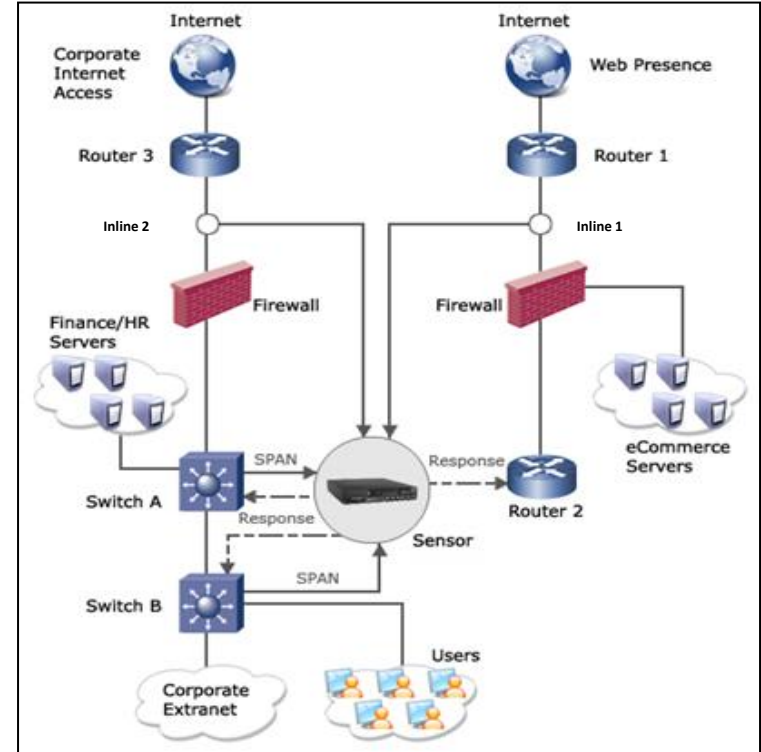
*Two NS9500 Sensors are placed in-line, connected to each other via cables, and configured to act as a HA pair.*



# Monitoreo de Múltiples Puertos

## Combination of TAP, SPAN, and In-line Modes

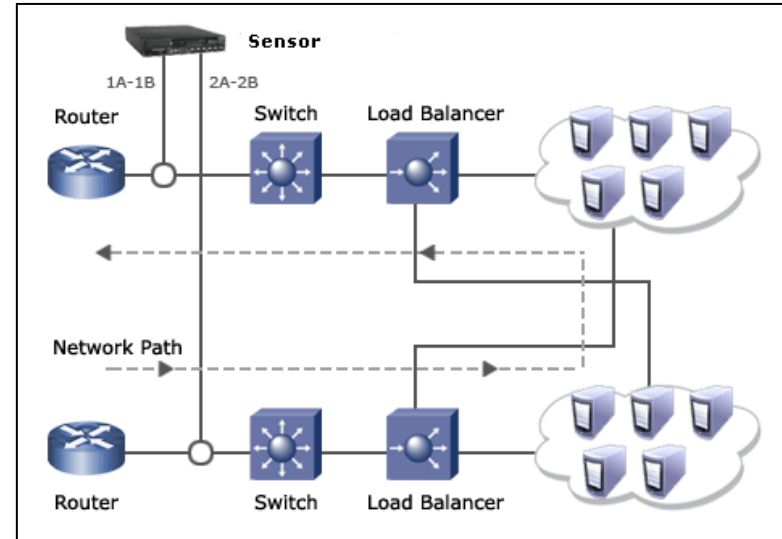
- Inline 1: Ports G1/1 and G1/2 run in Tap mode and respond to attacks via Response port R1.
- Inline 2: Ports G2/1 and G2/2 run in Tap mode and respond to attacks via Response port R2.
- SPAN from Switch A: Port G2/3 runs in SPAN mode and inject response packets back to the switch through the SPAN port.
- SPAN from Switch B: Port G2/4 runs in SPAN mode and responds to attacks via Response port R3.



# Grupos de Interfaces (Port Clustering)

## Single Logical Interface for State and Analysis

- Recommended for asymmetric routing.
  - ❑ TCP connection does not always send and receive along with same path.
  - ❑ Single-interface Sensor may only see receive and not response traffic.
- Normalize impact of traffic flows split across multiple interfaces.
  - ❑ Maintains state
  - ❑ Avoids information loss

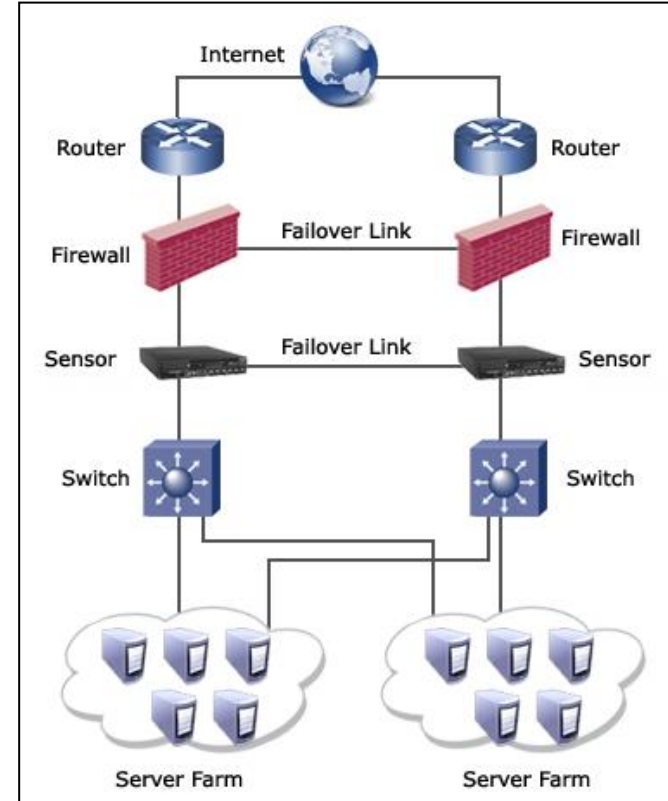


*Four ports are wired in pairs by default (two interfaces). Peer ports 1A and 1B can monitor one direction of an asymmetric transmission, while peer ports 2A and 2B can monitor the other direction.*

# Alta Disponibilidad

## Failover Pair with Identical Sensors for Redundancy

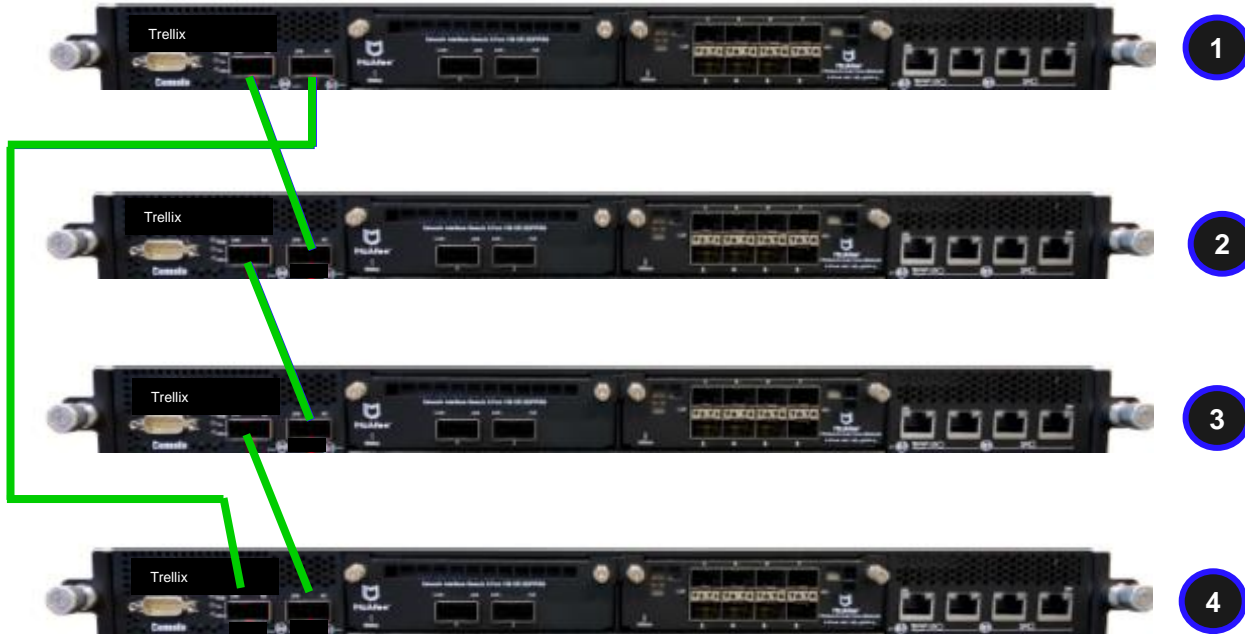
- Both failover Sensors are active and operate normally at all times.
- Detects attacks even when traffic is asymmetric.
- Traffic is copied and shared to maintain state.
- State is synchronized at all times.
- Both Sensors can see all packets, but only one raises an alert when attack is detected.





# Alta Disponibilidad (cont.)

## Example Hardware



- Failover pairs are connected an interconnection cable or cables.

# Topologías de Red

Two paths -  
Active/Passive

- Two ways in and out of the network.
- Only one way available at any given time.
- Active Path is passing traffic.
- Passive path is standing by in the event of a failure.

Two paths -  
Active/Active

- Two active paths maintained to and from internet.
- Provides double the available bandwidth.
- Not designed to share traffic unless there is failure.
- Flow is established on one path and all packets traverse that path.
- May be asymmetrically routed where inbound traffic comes in on path A and outbound traffic goes out on path B.

A single path

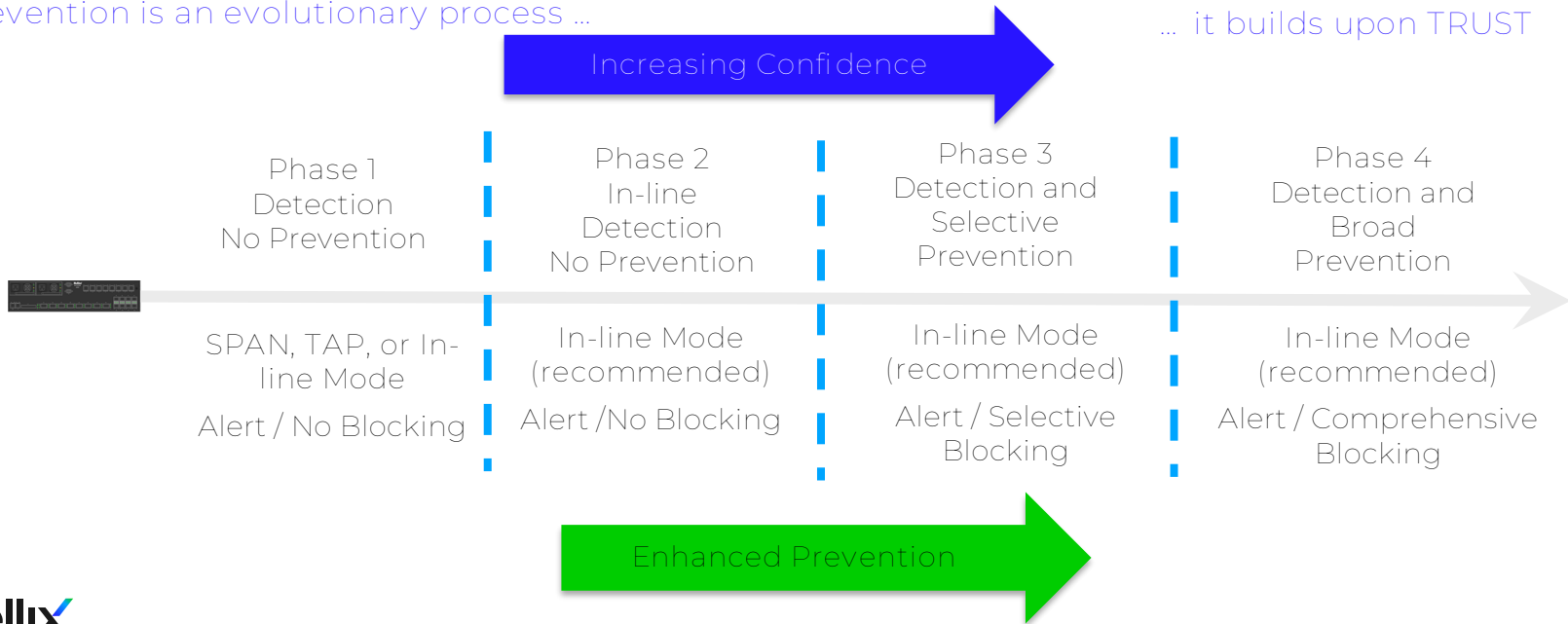
- No redundancy.
- Failure results in failed connection to the internet.

# Mejores Prácticas

Remember Sensor is Intrusion Detection System First

Prevention is an evolutionary process ...

... it builds upon TRUST



# Trellix

## Diseño de una Política IPS

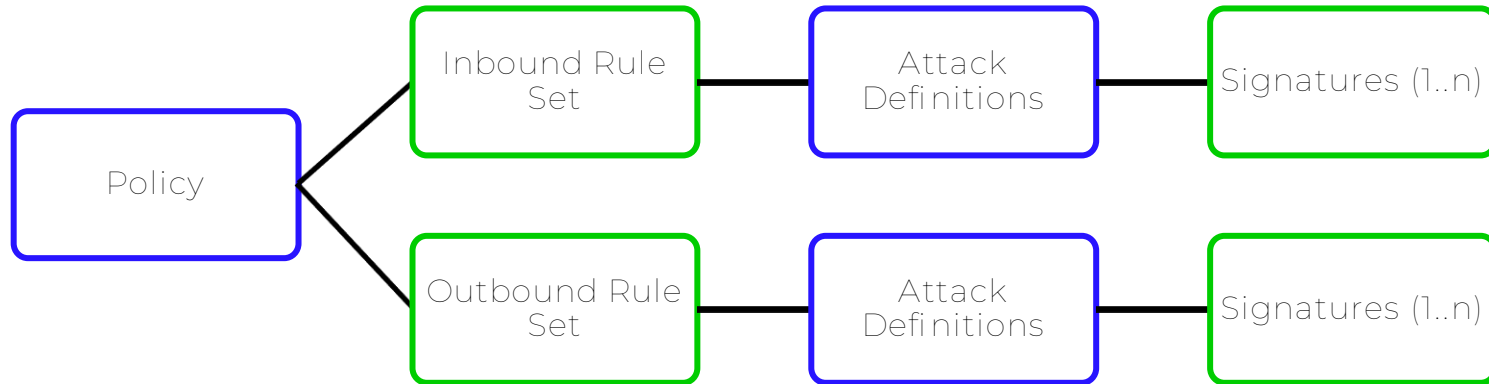
Manos a la obra



# Componentes de la Política

## KB61036

- Each policy contains inbound and outbound rule sets, attack definitions, and at least one signature set.
- The Attack database contains more than 20,000 signatures.



Note:

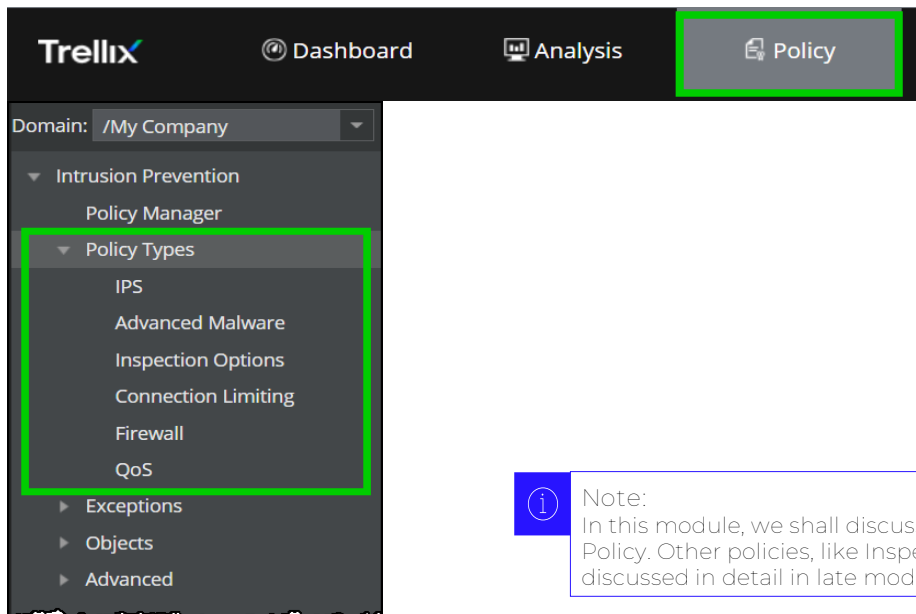
Refer to KB61036 in the company's Knowledge Base site for the list of protocols supported in the signature sets for Trellix IPS.

# Políticas de Seguridad en Trellix IPS

In Trellix IPS, all the major features, including IPS, are *Policy based*.

A Security policy in Trellix IPS is a *Set of Rules* defining:

- How you want the Sensors to behave.
- How you want the Sensors to respond when a malicious activity is detected.



The following are the types of Security Policies in Trellix IPS:

- IPS
- Advanced Malware
- Inspection Options
- Connection Limiting
- Firewall
- QoS



Note:

In this module, we shall discuss Trellix IPS Security Policies and An IPS Policy. Other policies, like Inspection policies, firewall policies, etc.; are discussed in detail in late modules.

## Conditions

- Uses pattern (string) matching and/or numeric comparisons.
- Core constructs are AND, OR, and AND THEN (Boolean operators).

Example:

```
Signature#1
  condition 1

http-rsp-INTERNAL-SWC-SWC-message-body matches
"\x39\xfa\x94\xe1\x5d\xfb\x26\x50\x0b\x14\x01\x4e\x1b\x59\x30\xe2" ( case-sensitive )

[AND] http-rsp-INTERNAL-SWC-SWC-message-body matches
"\xc4\xa1\x05\xa3\x87\x8e\x18\x5b\x56\x30\x66\xfc\xe8\x11\xe3\x0b" ( case-sensitive )

[AND] http-rsp-INTERNAL-SWC-SWC-message-body matches
"\x2b\x56\x5d\x35\x3c\x50\x1b\xa8\x0b\xd4\x37\x37\x41\xc0\x23\xa4" ( case-sensitive )
```

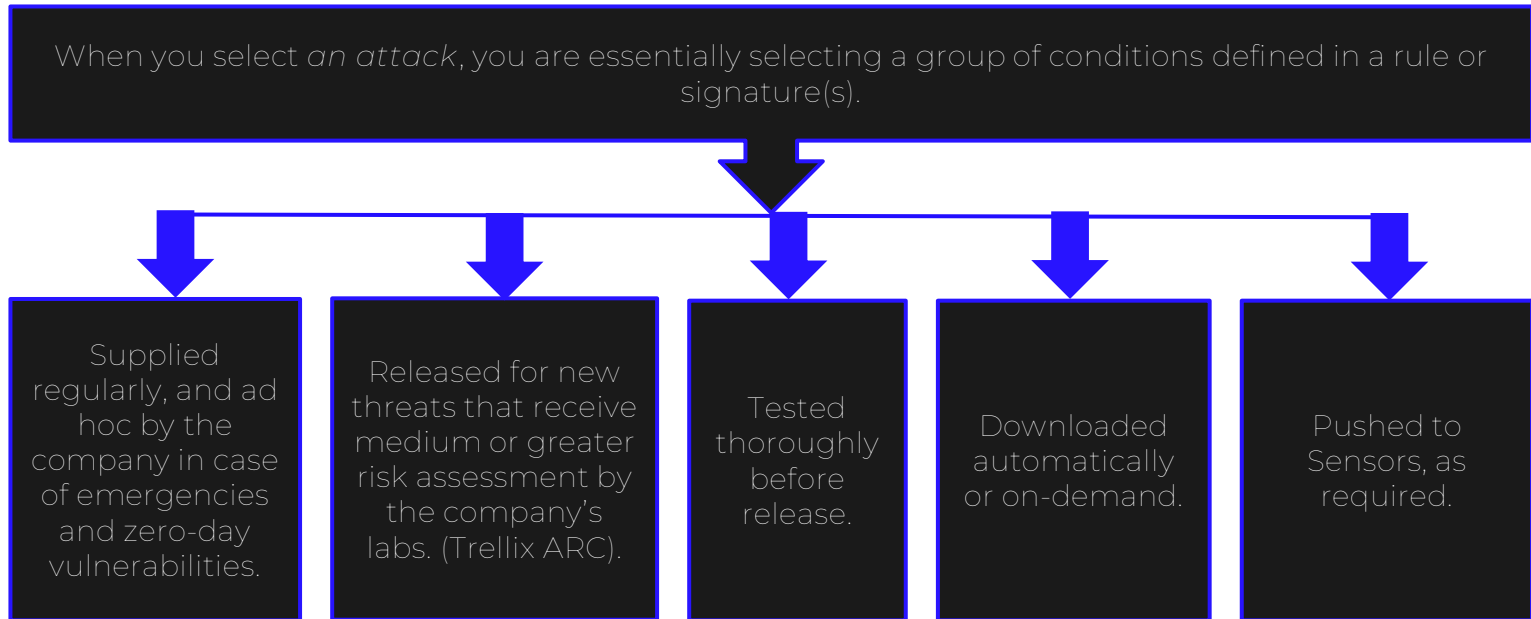
A new signature downloaded from the *Update Server* contains some default actions associated with specific attacks.

Example: Certain attacks are configured to log packets, and others are configured not to log packets.

# Definiciones de Ataques

## Aggregation of Signatures or Rules

- An Attack definition is the aggregation of the signatures (or rule) and other supporting data that can identify a specific network event.





# Clasificación de las Definiciones de Ataques

An attacker can threaten the system with an attack that affects the system. The attack categories are also known as *Attack type*. The following are the types of Attack Categories in Trellix IPS:

## Attack Categories



# Políticas Pre-Configuradas en Trellix IPS

## Default Prevention IPS

Trellix supplies a set of *preconfigured policies* for immediate application to various networks.

- Starting points to help get the System up and running.
- Available under the *Policy tab > Policy Types > IPS* in the Manager.

- Default Detection
- Default Prevention
- Default Exclude Informational
- Default Testing
- Default DoS and Reconnaissance only
- Default Prevention

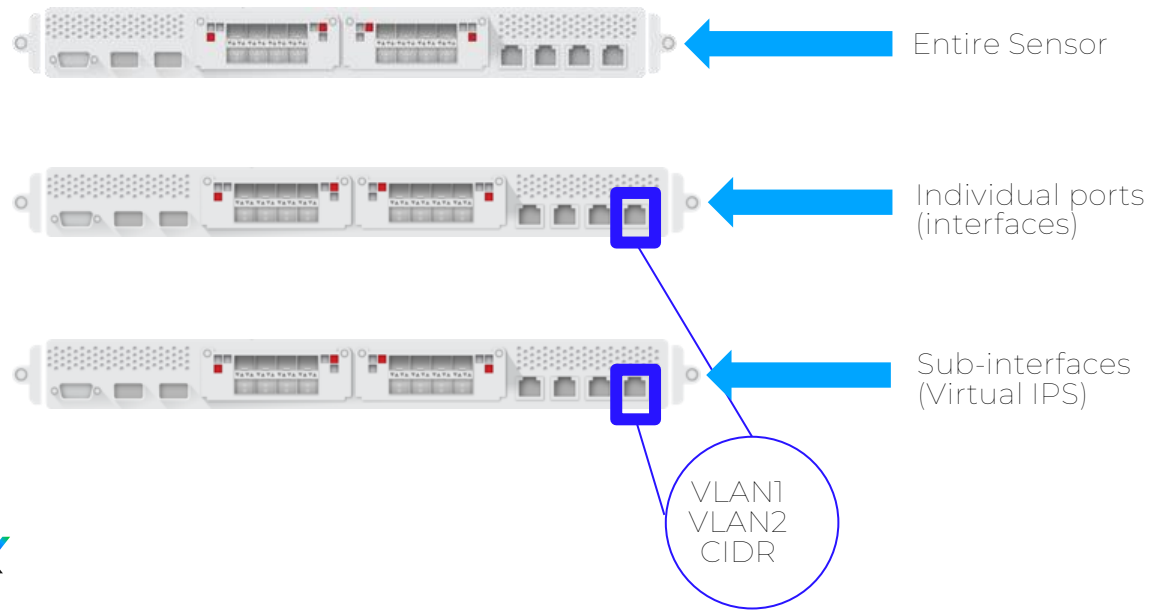
Name	Description	Attack Set Profile
Master Attack Repository	Default settings for all attack d...	Master Attack Repository
Default Detection	The standard attack set (blocki...	Default Detection
Default Exclude Informational	All attacks except informational...	Default Exclude Informational
Default Testing	All attacks (blocking disabled)	Default Testing
Default DoS and Reconnaissance Only	Threshold, learning and correlati...	Default DoS and Reconnaissance Only
Default Prevention	The standard attack set (blocki...	Default Prevention
Test Default Prevention	Test Default Prevention	Default Prevention

*Policy > [Admin Domain] > Intrusion Prevention > Policy Types > IPS*

# Asignación de Políticas

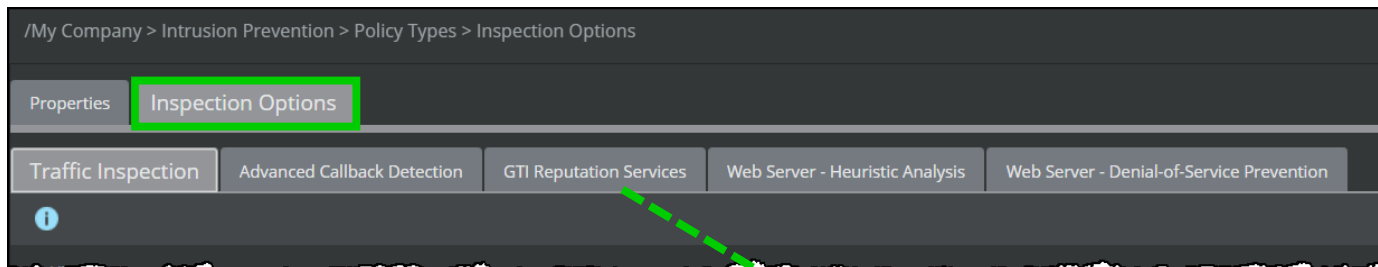
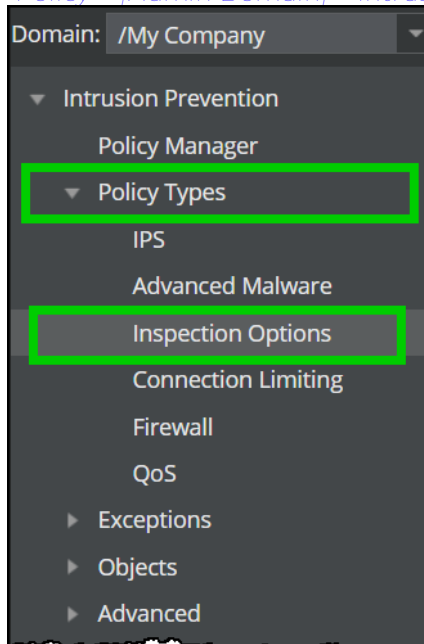
Entire Sensor, Individual Interfaces, or Sub-interfaces

You control the granularity, based on your requirements.

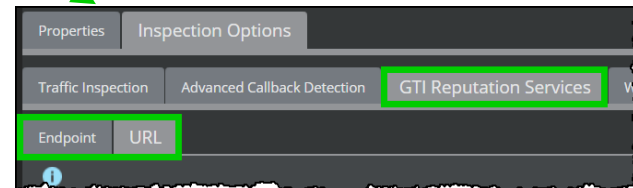


# Diferentes Opciones de Inspección

Policy > [Admin Domain] > Intrusion Prevention > Policy Types > Inspection Options



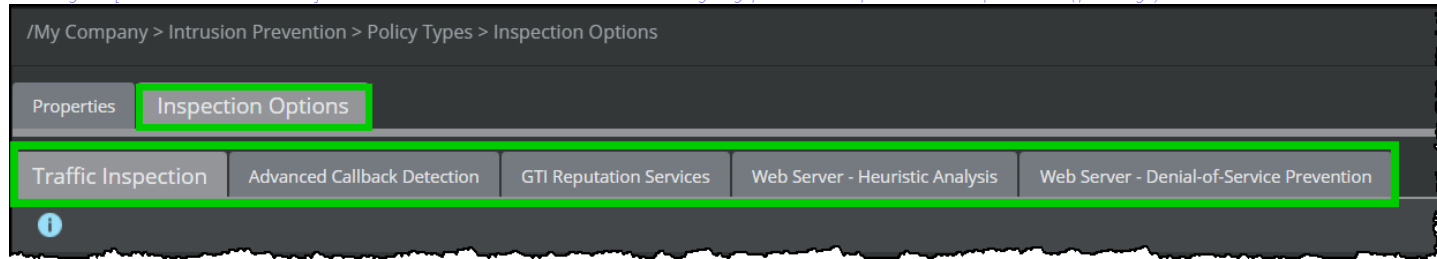
- Traffic Inspection
- Advanced Callback Detection
- GTI Reputation Services
  - Endpoint
  - URL
- Web Server – Heuristic Analysis
- Web Server – Denial-of-Service Prevention



# Tab Inspection Options

## Unique to Inspection Options Policies

*Policy > [Admin Domain] > Intrusion Prevention > Policy Types > Inspection Options (policy)*



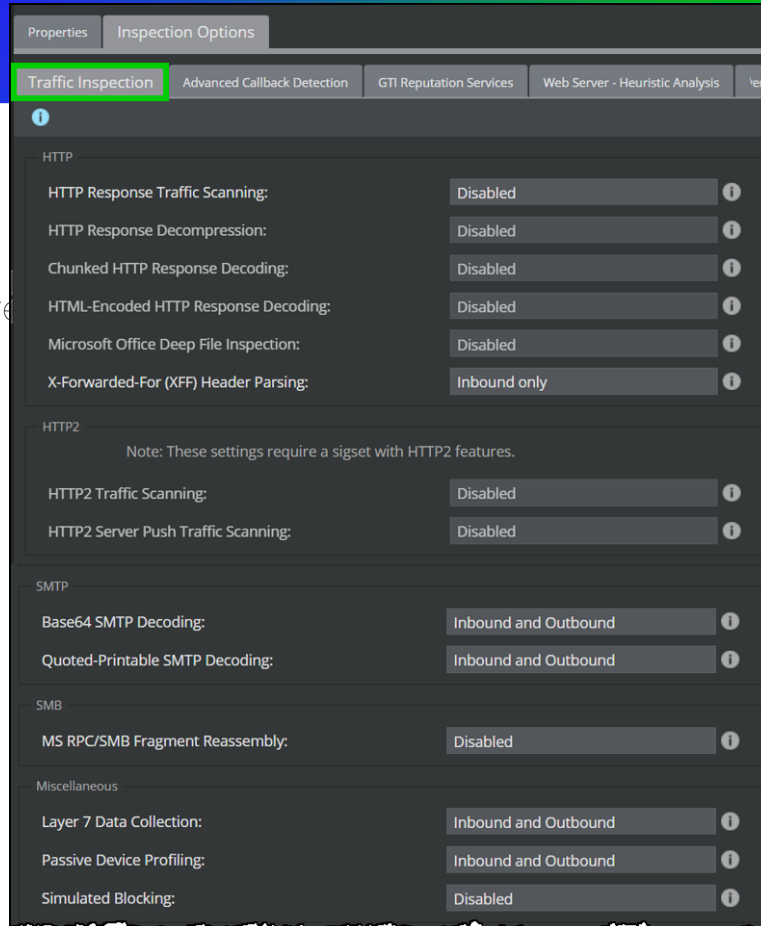
- Traffic Inspection: Control traffic decoding, reassembly and miscellaneous inspection options.
- Advanced Callback Detection: Enable advanced callback detection to take advantage of Callback Detectors, discover zero-day botnets and identify the use of DNS obfuscation techniques.
- GTI Reputation Services: Configure Global Threat Intelligence (GTI) endpoint reputation at admin domain level to influence SmartBlocking decisions and enhance connection limiting rules. Discussed separately.
- Web Server - Heuristic Analysis: Discussed separately.
- Web Server - Denial-of-Service Prevention: Discussed separately.

# Configurando la Inspección de Tráfico

- Outbound only: HTTP traffic
- Inbound only: Proxied connections
- Inbound and Outbound: SMTP, Layer 7, and Passive Device Profiling
- Disabled: MS RPC/SMB fragmentation reassembly and Simulated Blocking

**Inbound** traffic originates outside internal network is on the port designated as **Outside**.

**Outbound** traffic originate from inside internal network and is on the port designated as **Inside**.



The screenshot displays the 'Inspection Options' configuration page for 'Traffic Inspection'. The interface is dark-themed with a light grey header. The 'Traffic Inspection' tab is selected and highlighted with a green border. Below the header, there are several sections of settings, each with a list of options and their current status. Information icons (i) are present next to each setting.

Category	Setting	Value
HTTP	HTTP Response Traffic Scanning:	Disabled
	HTTP Response Decompression:	Disabled
	Chunked HTTP Response Decoding:	Disabled
	HTML-Encoded HTTP Response Decoding:	Disabled
	Microsoft Office Deep File Inspection:	Disabled
	X-Forwarded-For (XFF) Header Parsing:	Inbound only
HTTP2	Note: These settings require a sigset with HTTP2 features.	
	HTTP2 Traffic Scanning:	Disabled
	HTTP2 Server Push Traffic Scanning:	Disabled
SMTP	Base64 SMTP Decoding:	Inbound and Outbound
	Quoted-Printable SMTP Decoding:	Inbound and Outbound
SMB	MS RPC/SMB Fragment Reassembly:	Disabled
Miscellaneous	Layer 7 Data Collection:	Inbound and Outbound
	Passive Device Profiling:	Inbound and Outbound
	Simulated Blocking:	Disabled

# Configurando Advanced Callback Detection

Policy > [Admin Domain] > Intrusion Prevention > Policy Types > Inspection Options (policy)

The screenshot shows the configuration page for 'Advanced Callback Detection' within the Trellix interface. The breadcrumb path is '/My Company > Intrusion Prevention > Policy Types > Inspection Options'. The 'Advanced Callback Detection' tab is highlighted with a green box. Below the breadcrumb, there are four tabs: 'Traffic Inspection', 'Advanced Callback Detection', 'GTI Reputation Services', and 'Web Server - Heuristic Anal'. The main configuration area is divided into several sections:

- Callback Detectors and Heuristic Callback Discovery:** Set to 'Inbound and Outbound'.
- Heuristics Sensitivity:** Set to 'Low'.
- DNS Sinkholing:** Set to 'Disabled'.
- Fast Flux Detection:** Set to 'Disabled'.
- Domain Generation Algorithm Detection:** Set to 'Disabled'.
- Domain Name Exclusion List Processing:** Set to 'Enabled'.
- Export Traffic to NTBA for Additional Callback Analysis:** Set to 'Disabled'.

Below these settings is a section titled 'CIDRs Excluded from Advanced Callback Detection' with an information icon. At the bottom, there is a 'New CIDR:' field with the example '10.1.1.0/24' and an 'Add' button.

- Inbound and Outbound: Callback Heuristic Callback Discovery, Fast Flux Detection, and Domain Generation Algorithm Detection
- Heuristics Sensitivity: Low
- Disabled: DNS Sinkholing and Export to NTBA
- Enabled: Domain Name Whitelist Processing
- CIDRs Excluded: 10.1.1.0/24

# Configurando URL Reputation en el IPS Manager

## Cloning the Inspection Option Policy

Policy > [Admin Domain] > Intrusion Prevention > Policy Types > Inspection Options

Domain: /My Company

/My Company > Intrusion Prevention > Policy Types > Inspection Options

Inspection Options

Name ↑	Description	Ownership and Visibility	
		Owner Domain	Visibility
BotCC_DAT_DISABLED_AETWEB_POP	Policy with advanc...	/My Company	Owner and child domains
BotCC_DAT_INOUT_AETWEB_POP	Policy with advanc...	/My Company	Owner and child domains
BotCC_DAT_IN_AETWEB_POP	Policy with advanc...	/My Company	Owner and child domains
BotCC_DAT_OUT_AETWEB_POP	Policy with advanc...	/My Company	Owner and child domains
Default Client and Server Inspection	Inspect traffic both...	/My Company	Owner and child domains
Default Client Inspection	Inspect traffic fro...	/My Company	Owner and child domains



Note:

If you are using GTI public cloud, enable Telemetry and Domain Name Resolution (DNS).

If you are using GTI private cloud, configuring Telemetry and DNS is not mandatory.



# Configurando URL Reputation en el IPS Manager (cont.)

## Inspection Options (Properties tab)

*Policy > [Admin Domain] > Intrusion Prevention > Policy Types > Inspection Options (Properties tab)*

The screenshot displays the configuration page for 'Inspection Options' in the Trellix IPS Manager. The breadcrumb trail at the top reads: '/My Company > Intrusion Prevention > Policy Types > Inspection Options'. The 'Properties' tab is selected and highlighted with a green box. The form contains the following fields:

- Name:** Copy of Default Client Inspection
- Description:** Inspect traffic from internal endpoints as they access the Internet - DEMO
- Owner:** /My Company
- Visibility:** Owner and Child Domains (dropdown menu)
- Editable Here:** Yes
- Statistics:** (collapsed section)
- Last Updated:** Nov 16 11:23
- Last Updated By:** admin
- Assignments:** 0

At the bottom of the page, there is a navigation bar with a 'Next' button highlighted in green and a 'Cancel' button.

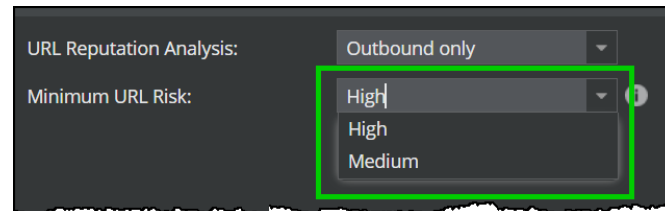
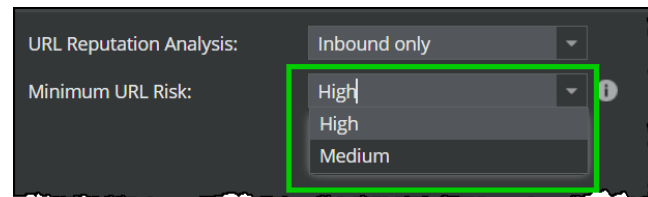
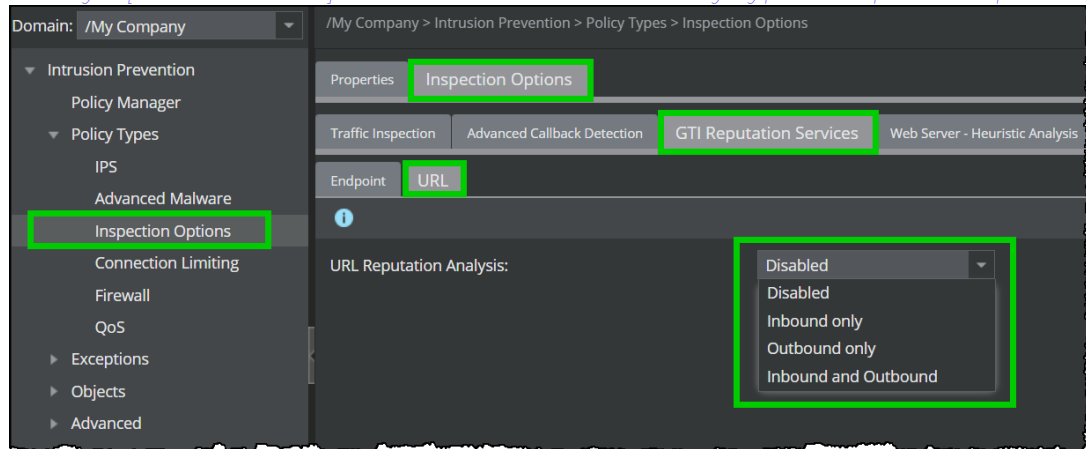
- You can edit the Name and Description.
- Click Next.

# Configurando URL Reputation en el IPS Manager (cont.)

## Inspection Options (URL tab)

- Enable / Disable URL Reputation in the Manager.

*Policy > [Admin Domain] > Intrusion Prevention > Policy Types > Inspection Options > (Inspection Options tab)*



Note:

If you are using GTI public cloud, enable Telemetry and Domain Name Resolution (DNS).  
If you are using GTI private cloud, configuring Telemetry and DNS is not mandatory.

# Configurando URL Reputation en el IPS Manager (cont.)

## Assign a Sensor

- Assign a Sensor to the new Inspection Policy created.

Inspection Options

Name ↑	Description	Ownership and Visibility		Assignments	Editable Here
		Owner Domain	Visibility		
BotCC_DAT_DISABLED_AETWEB_POP	Policy with advanc...	/My Company	Owner and child domains	0	Yes
BotCC_DAT_INOUT_AETWEB_POP	Policy with advanc...	/My Company	Owner and child domains	0	Yes
BotCC_DAT_IN_AETWEB_POP	Policy with advanc...	/My Company	Owner and child domains	0	Yes
BotCC_DAT_OUT_AETWEB_POP	Policy with advanc...	/My Company	Owner and child domains	0	Yes
<b>CLONE of Default Client Inspection</b>	<b>Inspect traffic from...</b>	<b>/My Company</b>	<b>Owner and child domains</b>	<b>0</b>	<b>Yes</b>
Default Client and Server Inspection	Inspect traffic both...	/My Company	Owner and child domains	0	No
Default Client Inspection	Inspect traffic fro...	/My Company	Owner and child domains	0	No
Default Server Inspection	Inspect traffic to e...	/My Company	Owner and child domains	0	No

Click the Assignments link

/My Company > Intrusion Prevention > Policy Types > Inspection

Assignments

Search available interfaces

Available Interfaces ↑

- /My Company/fc21\_9500/G3/1-G3/2**
- /My Company/fc21\_9500/G3/1-G3/2/Base-policy-VLA...
- /My Company/fc21\_9500/G3/1-G3/2/block-VLAN208
- /My Company/fc21\_9500/G3/1-G3/2/MATDBase-poli...
- /My Company/fc21\_9500/G3/1-G3/2/MATDblock-VLA...
- /My Company/fc21\_9500/G3/1-G3/2/MATDSendTCP...
- /My Company/fc21\_9500/G3/1-G3/2/Response Actio...
- /My Company/fc21\_9500/G3/1-G3/2/SendTCPReset...
- /My Company/fc21\_9500/G3/1-G3/2/Split-File-Downl...
- /My Company/fc21\_9500/G3/1-G3/2/Split-File-Downl...
- /My Company/fc21\_9500/G3/1-G3/2/VLAN\_40\_AIWA

Selected Interface (Policy Group) ↑

- /My Company/fc21\_9500/G0/1-G0/2**

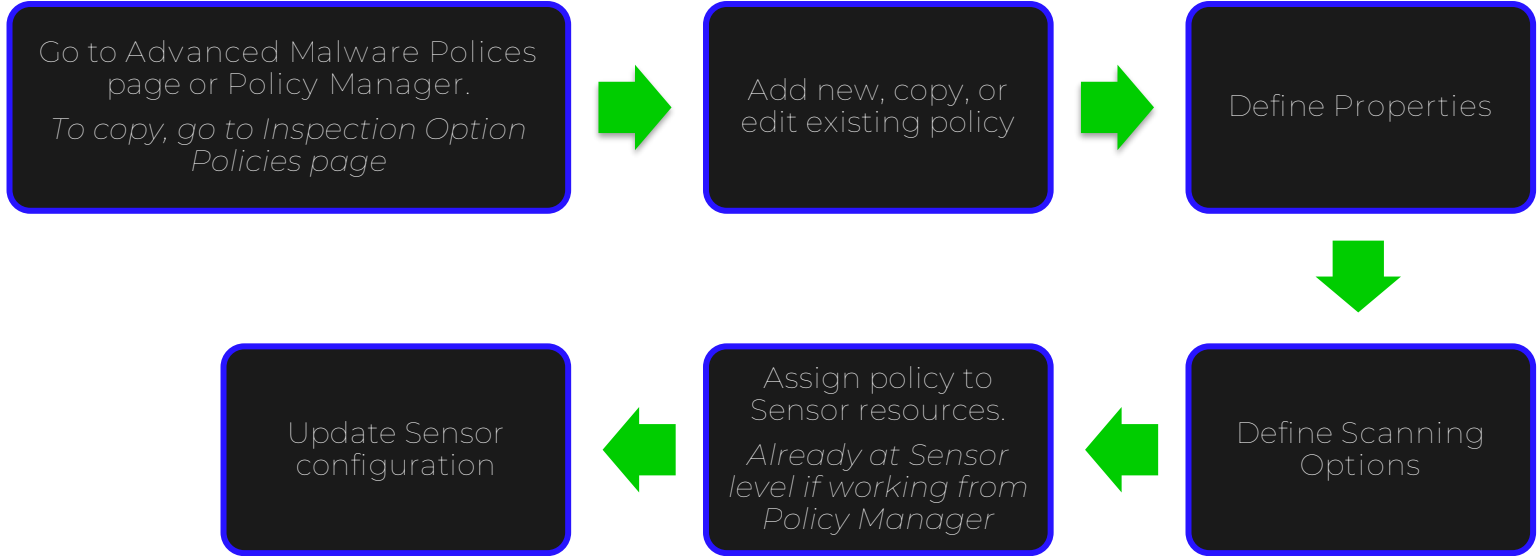
CLONE of Default Client Inspection

Save Cancel



# Flujo de Configuración de Advanced Malware Policies

## Workflow



# Usando Advanced Malware Policies

Trellix IPS provides a Default Malware Policy, which can be used as a starting point. However, the policy is configured for HTTP scanning only and cannot be edited.

[Policy > Intrusion Prevention > Policy Types > Advanced Malware](#)

/My Company > Intrusion Prevention > Policy Types > Advanced Malware

Advanced Malware

**i**

Name	Owner	Last Modified	Assignments
Default Malware Policy	/My Company	Oct 11 00:00	<b>3</b>

A default policy is included but unassigned. It scans HTTP only. It cannot be edited. Must clone or create new one.

/My Company > Intrusion Prevention > Policy Types > Advanced Malware

Properties

Name: Default Malware Policy

Description:

Owner: /My Company

Visible to Child Admin Domains?

Traffic to Inspect

HTTP:  Download **i**  Upload **i**

FTP

SMTP

# Usando Policy Manager

## Interfaces Tab

- Use the details pane for the interface when using Policy Manager.


*Policy > Intrusion Prevention > Policy Manager*

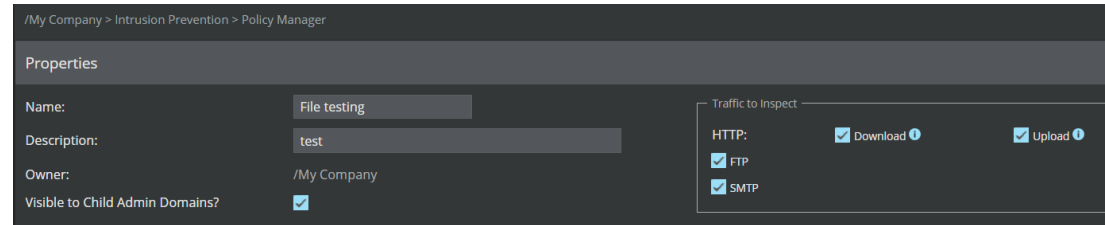
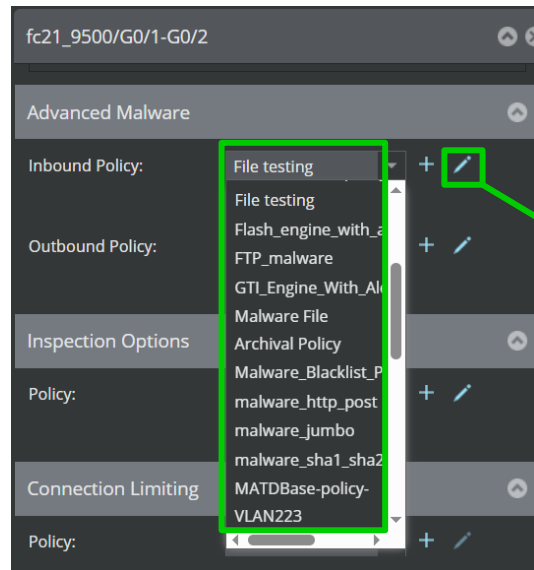
The screenshot displays the Trellix Policy Manager interface. The 'Interfaces' tab is active, showing a table of interfaces for device 'fc21\_9500'. A red box highlights the first row, and a red arrow points to the details pane on the right. A text overlay says 'Double-click an interface to display the details pane.' The details pane shows configuration for 'fc21\_9500/Base-policy-VLAN213', including Model (IPS-NS9500), Software Version (11.1.5.56), Type (VLAN), Protection Category, Policy Group (None), and Inbound Policy (NTBA-GAME-Base-...).

Device	Interface	Protection Category	Policy Group	Individual Policy Assignments			
Name	Name			IPS	Advanced Malware	Inspection Options	Connections
fc21_9500	Base-policy-VLAN213	---	---	Default Prevention	In: NTBA-GAME-Ba... Out: NTBA-GAME-...	POP_All	---
fc21_9500	G0/1-G0/2	None	---	Default Prevention	In: File testing Out: File testing	testing	---
fc21_9500	G3/1-G3/2	---	---	---	In: GTL_Engine_Wit... Out: GTL_Engine_W...	POP_All	---
fc21_9500	G3/3-G3/4	---	---	---	In: File testing Out: File testing	testing	---
fc21_9500	MATDBase-policy-VLAN223	---	---	---	In: MATDBase-poli... Out: MATDBase-p...	---	---
fc21_9500	MATDSendTCPReset-VLAN221	---	---	Default Prevention	In: MATDSendTCP... Out: MATDSendTC...	---	---
fc21_9500	MATDblock-VLAN222	---	---	Default Prevention	In: MATDblock-VLA... Out: MATDblock-V...	---	---
fc21_9500	Response Action-VLAN60	---	---	Default Prevention	---	---	---
fc21_9500	SendTCPReset-VLAN207	---	---	Default Prevention	In: NTBA-Policy-onl... Out: NTBA-Policy-b...	POP_All	---
fc21_9500	Split-File-Download-240	---	---	NSAT All-Inclusive W...	In: SFD_GAME_VLA... Out: SFD_GAME_V...	POP_All	---
fc21_9500	Split-File-Download-241	---	---	NSAT All-Inclusive W...	In: SFD_ATD_VLA... Out: SFD_ATD_VLA...	POP_All	---
fc21_9500	VLAN_40_A1WA	---	---	NSAT All-Inclusive W...	In: ATD-policy-alert... Out: ATD-policy-al...	BotCC_DAT_INOUT...	---
fc21_9500	VLAN_41_A1WOA	---	---	Default Exclude Info	In: ATD-policy-alert... Out: ATD-policy-al...	BotCC_DAT_IN_AF...	---

# Using Policy Manager (continued)

## Inbound Policy and Outbound Policy

- Select from Inbound Policy and/or Outbound Policy drop-down lists.
- Click + to add or  to edit. Opens page similar to Advanced Malware Policies page.



# Parámetros de la política de Malware

## Properties: General Settings

- Properties: General settings for policy
  - Name: Name of the policy
  - Description: Description of the policy
  - Owner: Domain to which policy belongs
  - Visible to Child Admin Domains: Whether policy is visible to owner only or owner and child admin domains

The general settings are similar to IPS policies.

/My Company > Intrusion Prevention > Policy Manager

### Properties

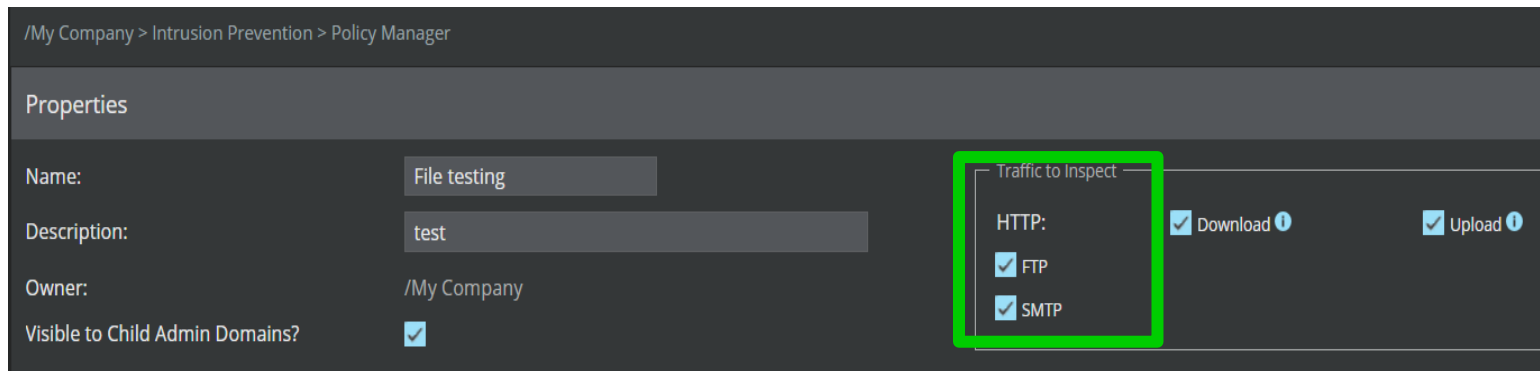
Name:	File testing
Description:	test
Owner:	/My Company
Visible to Child Admin Domains?	<input checked="" type="checkbox"/>



# Parámetros de la política de Malware (cont.)

## Properties: Protocols to Scan

- Protocols to Scan: Protocol streams Sensor monitors.
  - Sensor can extract files from Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP) traffic for scanning.
  - Files are sometimes split by browsers or download managers to speed up download.
  - Sensor can scan and analyze files downloaded as complete file or many segments.



The screenshot displays the configuration for a policy named "File testing" in the Trellix Policy Manager. The "Traffic to Inspect" section is highlighted with a green box, showing the following settings:

- HTTP:  Download ⓘ  Upload ⓘ
- FTP:
- SMTP:

Other visible settings include:

- Name: File testing
- Description: test
- Owner: /My Company
- Visible to Child Admin Domains?

# Parámetros de la política de Malware (cont.)

## Scanning Options

- File Types: File types to scan. Determine which engines to use. File support varies among engines.
- Malware Engines: One or more supported engines configured to scan specific file types. Supported file types vary among engines. (Each engine is discussed in more detail later in module).
- Action Thresholds: Specify the response based on the confidence level.

File Scanning Options												
File Type	Maximum File Size (KB) Scanned	Malware Engines						Action Thresholds				
		Allow and Block Lists	TIE / GTI File Reputation	Trellix IPS Analysis	Gateway Anti-Malware	MXV	Trellix Intelligent Sandbox	Alert	Block	Send TCP Reset	Add to Block List	Save File
Executables	5120	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High	High	High	Disabled	Disabled
MS Office Files	1024	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High	High	High	Disabled	Disabled
PDF Files	1024	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High	High	High	Disabled	Disabled
Compressed Files	5120	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High	High	High	Disabled	Disabled
Android Application Packages	2048	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High	High	High	Disabled	Disabled
Java Archives	2048	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High	High	High	Disabled	Disabled
Flash Files	2048	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High	High	High	Disabled	Disabled

Prompt for assignment after save

# Parámetros de la política de Malware (cont.)

## Scanning Options – File Types

- Executables: .exe, .dll, .scr, .ocx, .sys, .com, .drv, .cpl
- MS Office Files: .doc, .docx, .xls, .xlsx, .ppt
- Java Archive: .jar
- PDF Files: .pdf, .xdp
- Compressed Files: .zip and .rar
- Android Application: .apk
- Java Archive: .jar
- Flash Files: .flv

Files that exceed the specified maximums are not analyzed for malware by any of the engines including the block and allow lists.

File Scanning Options												
File Type	Maximum File Size (KB) Scanned	Malware Engines						Action Thresholds				
		Allow and Block Lists	TIE / GTI File Reputation	Trellix IPS Analysis	Gateway Anti-Malware	MVX	Trellix Intelligent Sandbox	Alert	Block	Send TCP Reset	Add to Block List	Save File
Executables	5120	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High	High	High	Disabled	Disabled
MS Office Files	1024	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High	High	High	Disabled	Disabled
PDF Files	1024	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High	High	High	Disabled	Disabled
Compressed Files	5120	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High	High	High	Disabled	Disabled
Android Application Packages	2048	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High	High	High	Disabled	Disabled
Java Archives	2048	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High	High	High	Disabled	Disabled
Flash Files	2048	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High	High	High	Disabled	Disabled

# Nivel de Confianza

Analysis > [Admin Domain] > Malware

/My Company > Malware Files

Malware Files

Malware Files

Hash	Actions	MD5	Overall Malware Confidence ↓	Individual Malware Confidence
1	<a href="#">Take action</a>	5db32a316f079fe7...	<b>Very High</b>	Any Malware Confidence
2	<a href="#">Take action</a>	e6568a59577670c...	<b>Very High</b>	Any Malware Confidence
3	<a href="#">Take action</a>	012ca7db8d5bae4...	<b>Very High</b>	Very High Malware Confidence
4	<a href="#">Take action</a>	4605a593579619e...	<b>Very High</b>	High+ Malware Confidence
5	<a href="#">Take action</a>	f22f09a8c4c6bac...	<b>Very High</b>	Medium+ Malware Confidence

Any Malware Confidence

- Any Malware Confidence
- Very High Malware Confidence
- High+ Malware Confidence
- Medium+ Malware Confidence
- Low+ Malware Confidence
- Very Low+ Malware Confidence

- Any
- Very High
- High+
- Medium+
- Low+



Note:

- As an example, a Very High confidence level indicates a very high probability of the file being infected.
- Multiple engines report varying confidence levels. Trellix IPS Analysis and TIE/GTI File Reputation report a low confidence level while Gateway Anti-Malware (GAM) reports a high confidence level. In such a scenario, the highest confidence level returned is considered by the Sensor for its response action.

# Umbrales de Acción

## Response Based on Returned Confidence

Determine response based on confidence returned.

- Alert: Raise alert in Attack Log.
- Block: Block packets to prevent malicious file from reaching host.
- Send TCP Reset: Disconnect connection at source, destination, or both ends.
- Add to Block List: Add file's MD5 hash to block list.
- Save File: Archive file in Manager file store based on the advanced malware policy.

File Scanning Options														
File Type	Maximum File Size (KB) Scanned	Malware Engines						Action Thresholds						
		Allow and Block Lists	TIE / GTI File Reputation	Trellix IPS Analysis	Gateway Anti-Malware	MVX	Trellix Intelligent Sandbox	Alert	Block	Send TCP Reset	Add to Block List	Save File		
Executables	5120	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High	High	High	Disabled	Disabled		
MS Office Files	1024	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High	High	High	Disabled	Disabled		
PDF Files	1024	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High	High	High	Disabled	Disabled		
Compressed Files	5120	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High	High	High	Disabled	Disabled		
Android Application Packages	2048	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High	High	High	Disabled	Disabled		
Java Archives	2048	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High	High	High	Disabled	Disabled		
Flash Files	2048	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High	High	High	Disabled	Disabled		

Default response for High and Very High confidence is Alert, Block, and Send TCP Reset.

Prompt for assignment after save

# Implementar los cambios

*Devices > [Admin Domain] > Devices tab > [Device] > Deploy Pending Changes*

The screenshot shows the Trellix interface with the following elements:

- Navigation bar: Dashboard, Analysis, Policy, **Devices** (highlighted), Manager.
- Domain: /My Company
- Global: **Devices** (highlighted)
- Device: fc21\_9500
- Left sidebar: Summary, **Deploy Pending Changes** (highlighted), Setup, Maintenance, Troubleshooting, IPS Interfaces.
- Page title: /My Company > fc21\_9500 > Deploy Pending Changes
- Message: **Changes cannot be Deployed since the Device is Disconnected from the Manager**
- Section: **Deploy Pending Changes**
- Message: **Pending changes are yet to be deployed on to the Device**
- Table:

Device Name	Last Deployment	Pending Changes	Configuration & Signature Set	SSL Key	Callback Detectors	GAM Updates
fc21_9500	2023-Dec-12 02:15:47 IST	Configuration Changed Policy Changed Global Policy Changed New Signature Set Version	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- You can Deploy Changes at the Device Level.
- Device must be active.
- Alternatively, you can also click the Deploy Changes icon on the menu bar.

# Trellix

## Configurando los Sensores para Prevención de Intrusiones

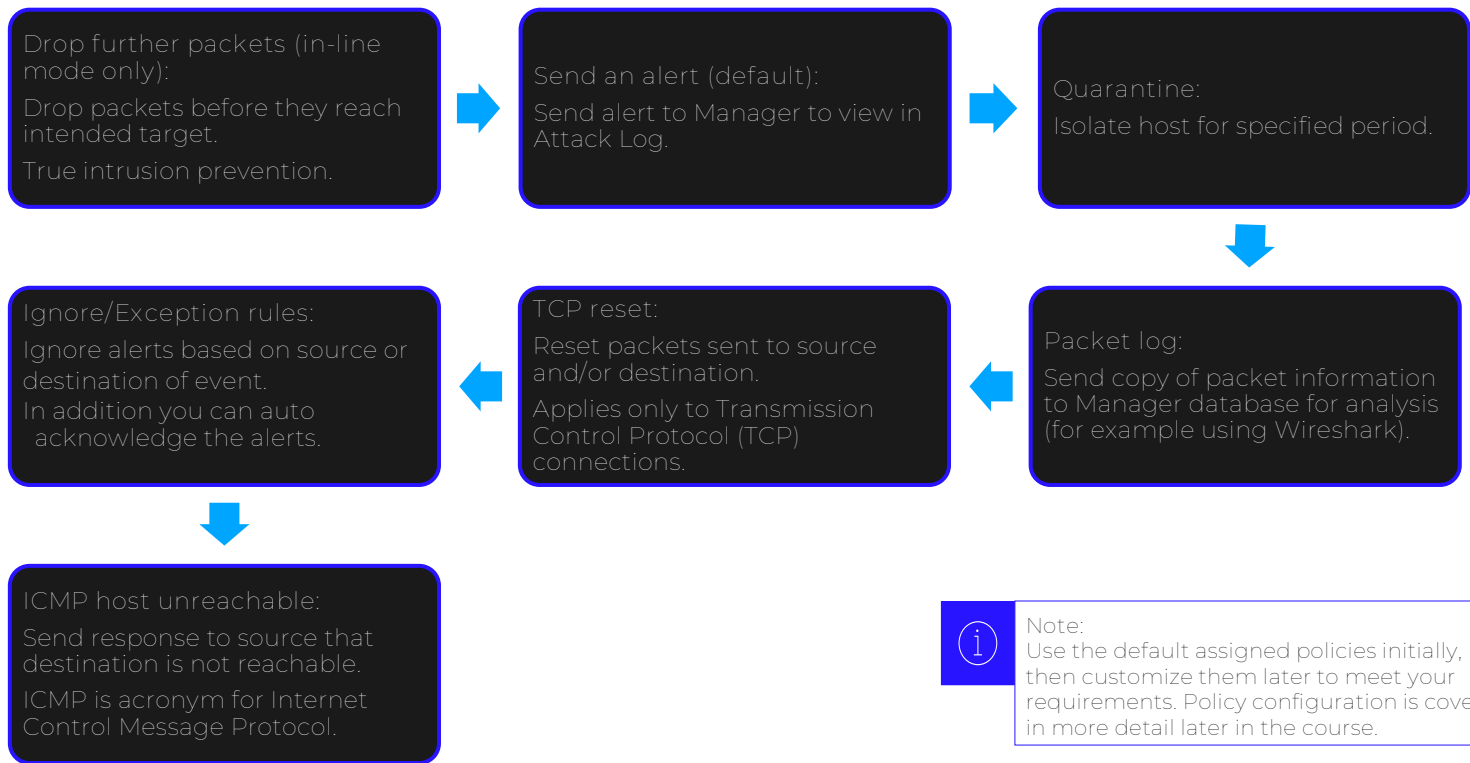
Manos a la obra





# Acciones de Respuesta del Sensor

Enacted or Sent to Prevent or Deter Subsequent Attacks



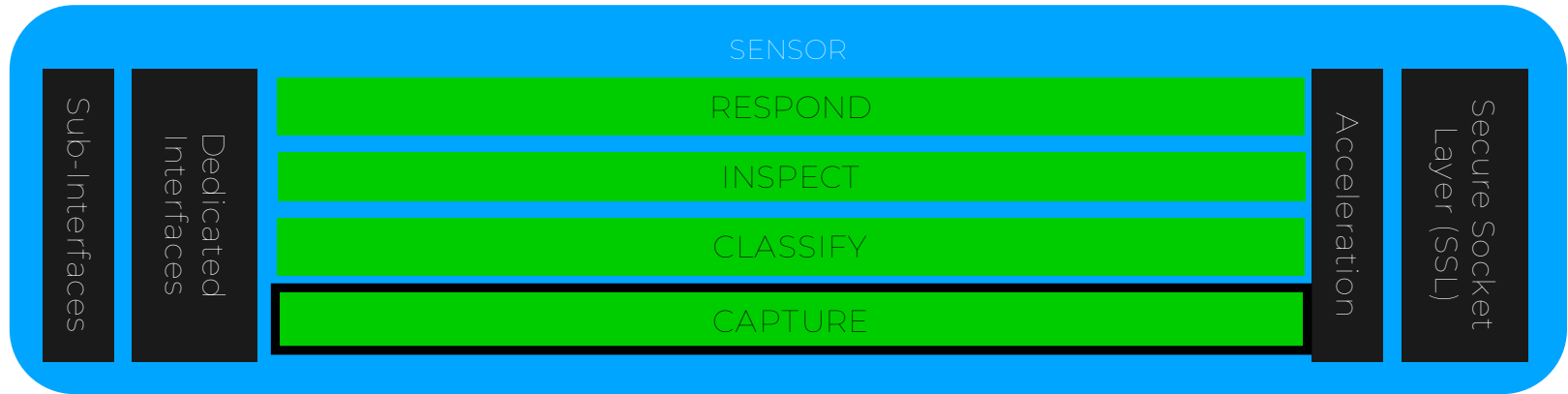
**i** Note:  
Use the default assigned policies initially, then customize them later to meet your requirements. Policy configuration is covered in more detail later in the course.



# Captura

## Analysis to Prepare for Future Attacks

- Sensor creates packet log for offending transmissions.
- Retrieved from database using Attack Log.
- Available for review using protocol analyzer (Wireshark).



### Notes:

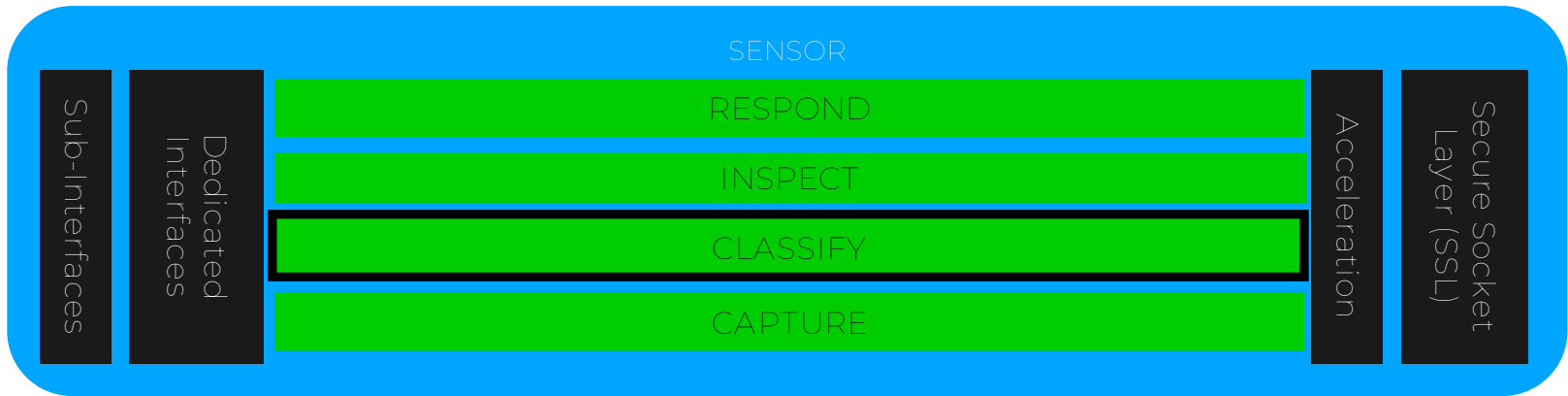
- By default, UDP and TCP protocol attacks generate a packet log for the attack and the previous 128 bytes in the flow.
- For more information about Wireshark, go to [www.wireshark.com](http://www.wireshark.com).



# Clasificación

## Categorize Traffic Based on Characteristics

- Block by Sensor's stateful firewall if connections are not permitted.
- Detect DoS attacks by TCP/SYN, UDP flood, fragments, counters.



Normal and stateful firewalls:

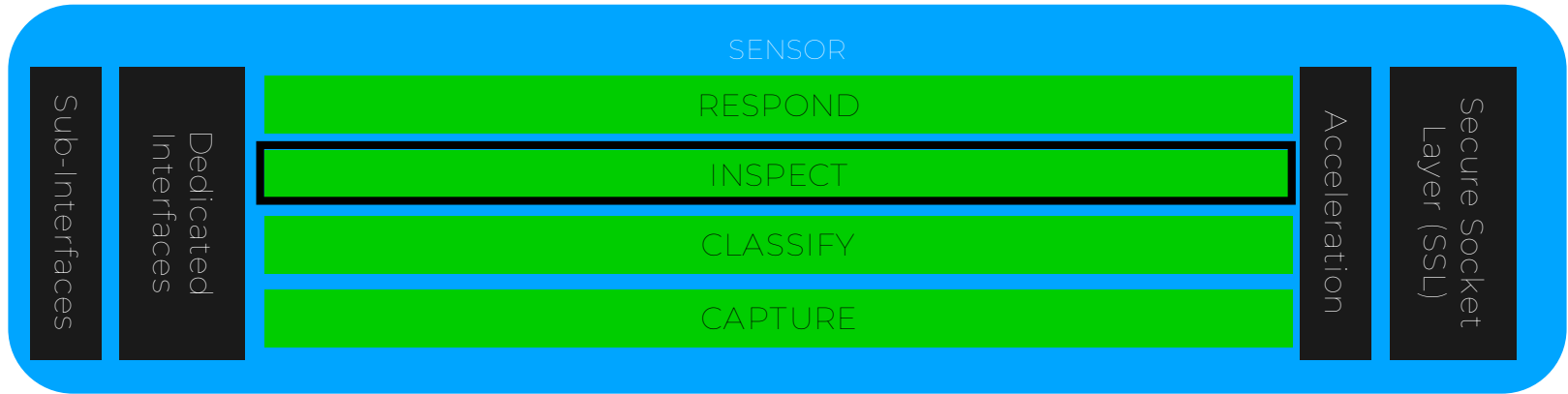
- ❑ Normal firewall is stateless because it has no memory of context for connection states.
- ❑ Stateful firewall remembers context of connections and continuously updates this state information in dynamic connection tables.



# Inspección

## Detects Deviation from Defined Baseline

- Sensor inspects traffic for various exploits and vulnerabilities using anomaly detection.
- Detects behavior that does not match normal, predefined standard, or baseline.



Features:

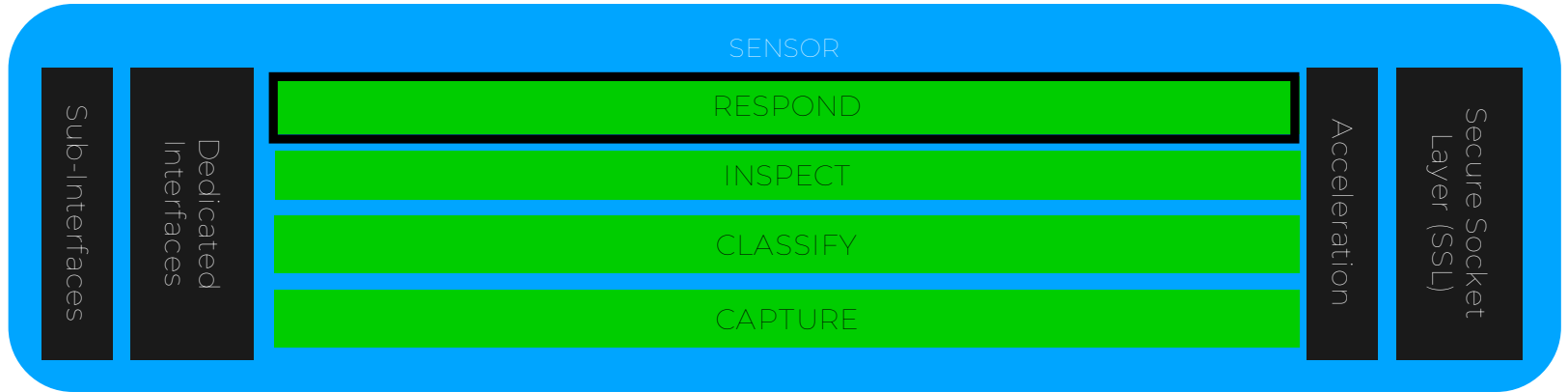
- Pre-programmed or self-learning baseline.
- Virtual patching to block vulnerability exploit.



# Respuesta

## Actions When Sensor Detects Policy Violation

- Knowing what needs to be protected helps determine response type.
- Critical attacks (buffer overflows and DoS attacks) require real-time responses.
- No-critical attacks (scans and probes) can be logged and analyzed.



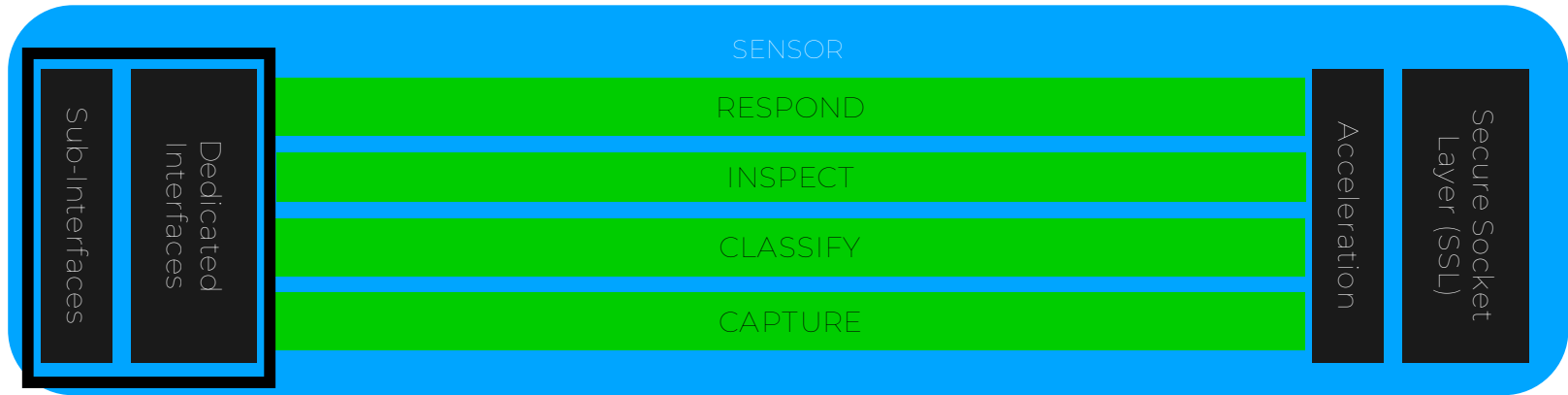
Example:

- If outside firewall, consider sending alert and responding to attack.
- For other suspicious internal traffic, consider logging alert for further analysis.

# Virtualización (sub-interfaces)

## Distinct Scanning Policies for Multiple Traffic Flows

- Intermediate-to-advanced configuration option.
- Allows interface/sub-interfaces on single Sensor.
- Configured at device level.



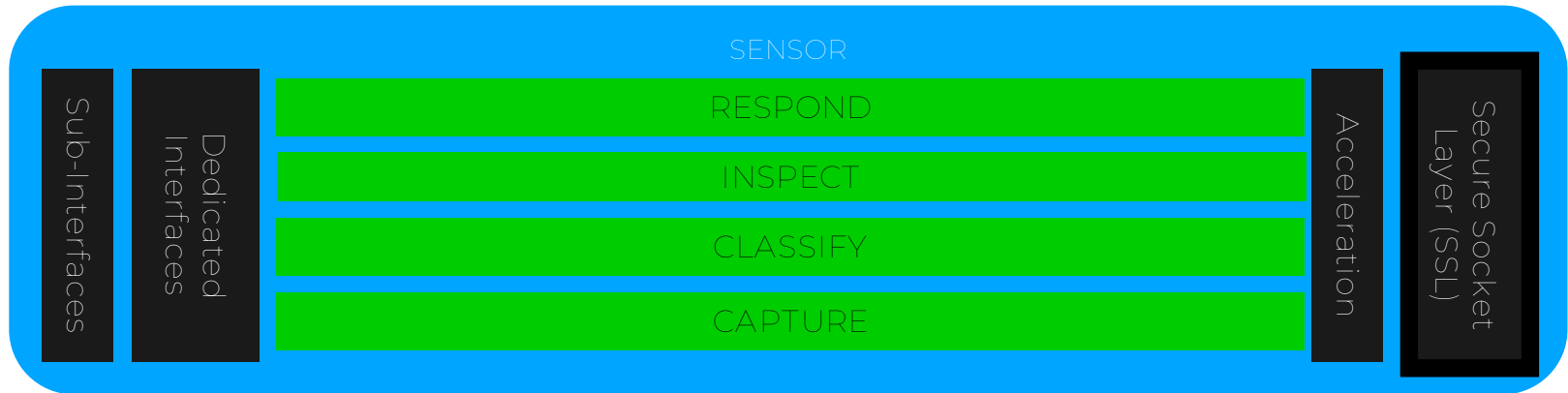
Interface types:

- Dedicated.
- Sub-interfaces: Virtual LAN (VLAN), Bridge VLAN, and Classless Inter-domain Routing (CIDR).

# Descifrado de Secure Socket Layer (SSL)

## Decryption of SSL Packets for Inspection and Response

- Allows SSL inspection of web servers and cipher suites.
- Enabled and configured at device level (packet logging, SSL flows to monitor simultaneously, and session cache time).



Note:  
Inbound SSL Decryption is not Supported: Please refer to the product guide for the details on this.

# Resolución de Nombre

- Configure DNS Server details at Domain level:

The screenshot displays the Trellix web interface for configuring DNS server details at the domain level. The breadcrumb path is `/My Company > Common Device Settings > Name Resolution`. The left sidebar shows the navigation menu with the `Global` tab selected. The main content area shows the `Name Resolution` configuration page. The settings are as follows:

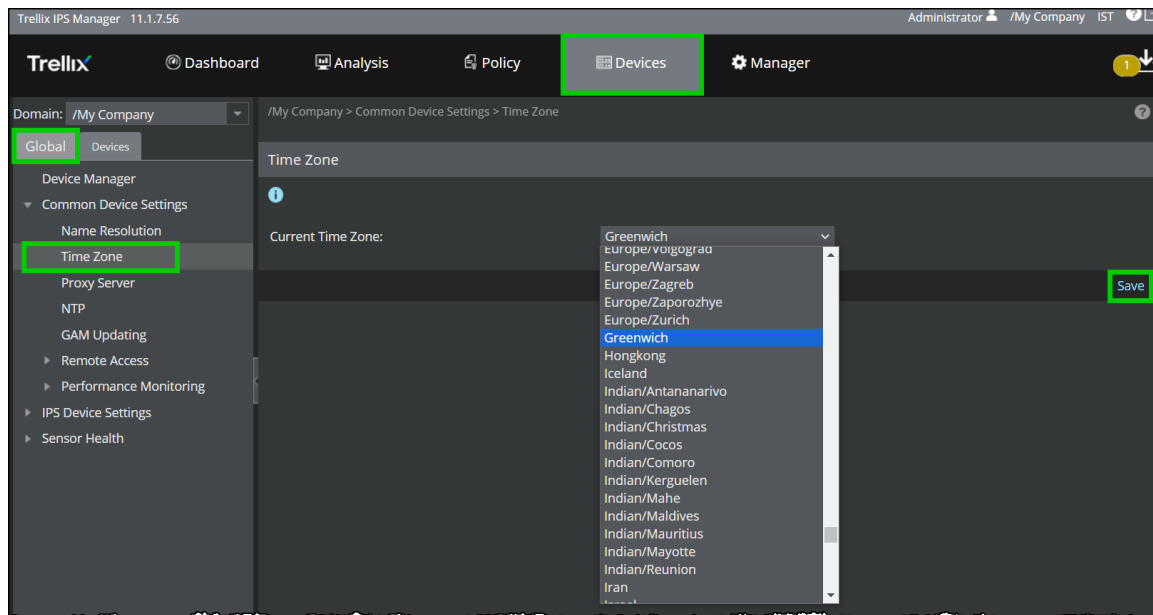
Setting	Value
Enable Name Resolution?	<input checked="" type="checkbox"/>
DNS Suffixes (e.g. trellix.com):	mycompany.com
Primary DNS Server:	10.212.24.11 *
Secondary DNS Server:	10.212.24.12 *
Refresh Interval (hours):	24 *

At the bottom of the page, there is a `Test Connection` button on the left and a `Save` button on the right.

# Configurando la Zona Horaria

## Global tab

- Selected from menu (Greenwich, Europe/London, US/Central, and so on).
- By default, the Device inherit settings on Global tab.
- Optionally, one can break inheritance and configure time zone at Device level.



*Devices > [Admin Domain] > Global tab > Common Device Settings > Time Zone*



# Configurando NTP

Global tab: Enable and configure up to two NTP servers.

*Devices > [Admin Domain] > Global tab > Common Device Settings > NTP*

The screenshot displays the Trellix web interface for configuring NTP settings. The breadcrumb path is: *Devices > [Admin Domain] > Global tab > Common Device Settings > NTP*. The interface includes a navigation menu on the left with the following items: Global, Device Manager, Common Device Settings (expanded), Name Resolution, Time Zone, Proxy Server, NTP (highlighted), GAM Updating, Remote Access, Performance Monitoring, and IPS Device Settings. The main content area shows the 'NTP Support' section with the following settings:

- Enable NTP Server:
- NTP Server-1:
- IP Address: 10.10.10.220
- Polling Interval: 6
- Authentication:

At the bottom of the configuration area, there are '+', '-' buttons and 'Test Connection' and 'Save' buttons.

- Enable NTP
- IPv4 or IPv6 (mutually exclusive)
- Polling interval 3-17 (applied as 2 seconds power x)
- Authentication (optional)



Note:

If two NTP servers are configured, the Sensor uses the one with the least Round-Trip Time (RTT).

# Servidor Proxy

Using Proxy Server for Internet connectivity (Manager tab)

Manager > [Admin Domain] > Setup > Proxy Server

The screenshot displays the Trellix Manager interface with several components highlighted in green:

- Manager Tab:** The top navigation bar has the 'Manager' tab selected.
- Domain:** The breadcrumb path shows the domain as '/My Company'.
- Setup Menu:** The left sidebar menu has 'Setup' expanded.
- Global/Devices:** The 'Global' and 'Devices' sub-menus are visible.
- Proxy Server:** The 'Proxy Server' option is selected under the 'Devices' menu.
- Device Selection:** The 'Device' dropdown is set to 'fc21\_9500'.
- Configuration Form:** The 'Proxy Server' configuration page is shown, with fields for 'Proxy Server Name or IP Address', 'Proxy Port', 'User Name', and 'Password'. A callout box points to the 'Use Device List Settings OR A Proxy Server' radio button.
- Save Button:** A 'Save' button is located at the bottom right of the configuration form.

# Monitorio de Rendimiento

Global tab: View and manage performance monitoring: Enable, Metrics, Thresholds for alarms.

*Devices > [Admin Domain] > Global tab > Common Device Settings > Performance Monitoring*

Domain: /My Company

Global Devices

Device Manager

Common Device Settings

- Name Resolution
- Time Zone
- Proxy Server
- NTP
- GAM Updating
- Remote Access
- Performance Monitoring
  - Summary
  - Enable
  - Metrics
  - Thresholds
- IPS Device Settings
- Sensor Health

/My Company > Common Device Settings > Performance Monitoring > Summary

Summary

Performance Monitoring

Metric Collection: Enabled

Threshold Analysis: Enabled

Visible to Child Admin Domains: Yes

Metrics

Metrics Collected: Device Throughput Usage, Memory Usage

Thresholds (enabled for fault generation)

Metric	Description	Direction	Threshold	Reset Threshold
CPU Usage	High Usage	Rising	90 %	70 %
Device Throughput Usage	High Usage	Rising	90 %	70 %
Memory Usage	High Usage	Rising	90 %	70 %

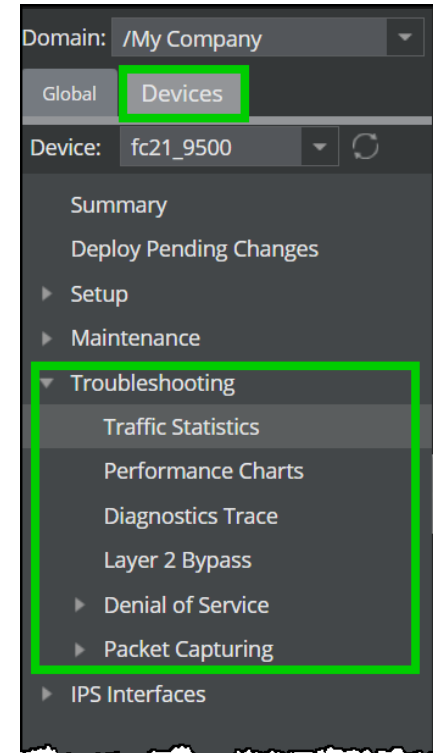
Display

Metric	Severity	Value %
Memory Usage	Medium	75
Memory Usage	High	90
Device Throughput Usage	Medium	75
Device Throughput Usage	High	90

# Solución de Problemas

- Traffic Statistics: View essential troubleshooting statistics for this device.
- Performance Charts: View throughput, flow usage, and CPU usage metrics.
- Diagnostics Trace: encrypted archive containing essential device debugging information and logs, which can be sent to the Support for analysis.
- Layer 2 Bypass: Enable device to bypass the scanning process if critical faults occur and to enable ARP spoofing.
- Denial of Service: Manage DoS Profile learning, upload and restore DoS Profiles, and copy DoS packets externally for further analysis.
- Packet Capturing: Capture data packets on ingress traffic in your network to perform forensics analysis. (Not supported on NS9300, NS9200, NS9100, IPS-VM600 and IPS-VM100 Sensors).

*Devices > [Admin Domain] > Global tab > [Device] > Troubleshooting*



# Trellix

## Ajuste fino de Políticas

Manos a la obra



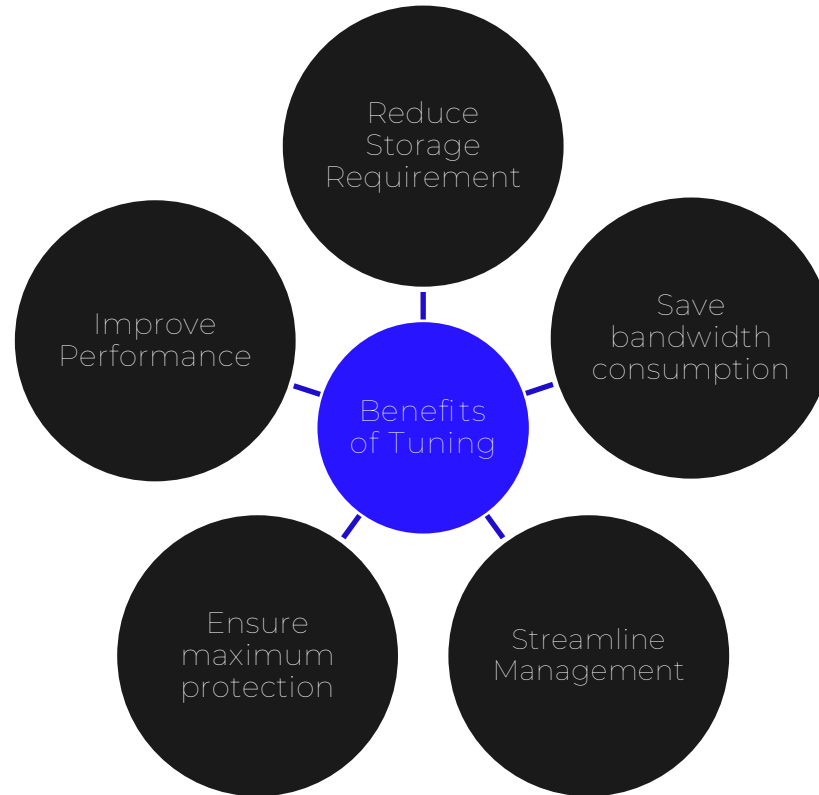
# ¿Qué es Ajuste Fino (Tuning)?

## Limiting Display of Alerts in the Attack Log

- Too many alerts become noise that can result in overlooking or missing critical information.
- Too many alerts can clog the database and slow resources.
- To tune, begin with the IPS policy templates.
- Identify those templates that most meet your security requirements.
- Copy and customize templates to meet your network requirements.
- Pay attention to false positives. Disabling alerts that are not applicable to your network.

# ¿Por qué implementar Ajuste Fino?

## Benefits



# Previo al Ajuste Fino

- Set expectations.:
  - False positives are normal in the beginning.
  - It takes a few weeks to fully identify network requirements and tune appropriately.
- Choose where to install:
  - Do not install in the busiest part of the network just to see what is detected.
  - Focus on policy hot spots.
- Determine sources known false positive offenders:
  - For example, SNMP Managers, Vulnerability Scanners, and so forth.
- Have Wireshark installed and ready on the client PC.



# Fases del Ajuste Fino de Políticas en Trellix IPS

## Phase 1 – Security Design

- Owned by the security architecture team
- Place the IPS Sensors in the right locations
- Select the correct policy
- Review the IPS security architecture

## Phase 2 – Day to Day Operations

- Owned by security operations team
- How many alerts per day?
- Review repetitive alerts
- Block attacks
- Find a way to reduce the attack reporting
- 70% or more of repeating alerts can be eliminated

# Falsos Positivos y Ruido

- To better manage the security risks, it is pivotal to understand the exact meaning of different types of alerts so that appropriate response can be applied.
- With Trellix IPS, there are three types of alerts that are often taken as "*false positives*":
  - Incorrectly identified events
  - Correctly identified events subject to interpretation by usage policy
  - Correctly identified events uninteresting to the user

# Falsos Positivos y Ruido (cont.)

## Incorrectly Identified Events

Signifies “Alerts” resulting from overly aggressive signature design, special characteristics of the user environment, or system bugs.



## Correctly Identified Events - significant to the usage of a Policy

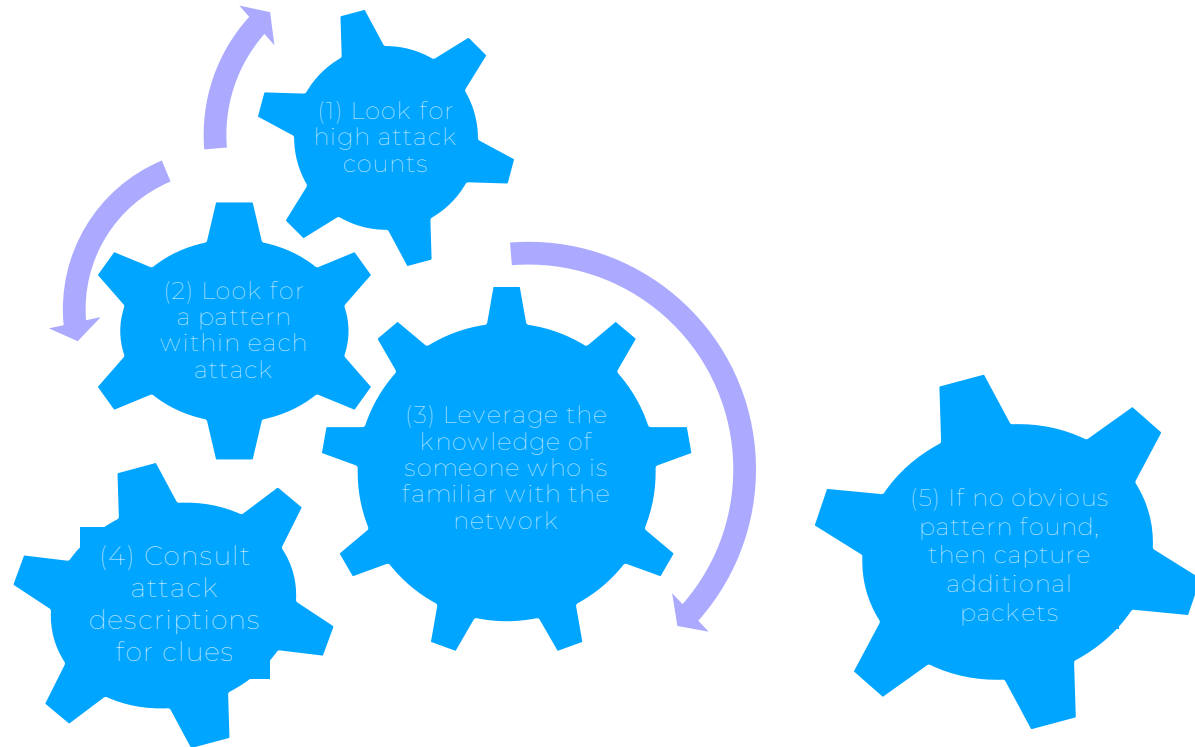
Example: Some environments allow the usage of Instant Messaging, Internet relay chat (IRC), and peer-to-peer programs (P2P); while others do not.



## Correctly Identified Event but significant to User sensitivity (also known as noise)

An Alert classified as noise due to the perceived severity of the event.

# Identificando Falsos Positivos



# Pasos para Reducir Falsos Positivos

Sources	Details
Hosts with special functions tend to create false positives.	Such hosts often include: <ul style="list-style-type: none"><li>▪ DNS servers</li><li>▪ Windows domain controllers</li><li>▪ HTTP cache servers</li><li>▪ SMTP relays</li></ul>
Use ignore rules to eliminate false positives in a granular fashion.	Ignore rules eliminate specific alerts when a specific IP address (or range) is the source or destination of the attack.
Use firewall rules to eliminate false positives in a general fashion.	Firewall rules can be used to bypass the intrusion engine when a specific combination of IP address (or range) and protocol.
If an alert is (too unpredictable) i.e. coming from too many hosts.	The more customized a network, the more potential for false positives. If a given signature produces false positives from an unpredictable set of hosts, the best approach is to disable the alert.

# Prevencción de Falsos Positivos

- Apply a scanning policy that is specific to the network.
- Consider virtual IPS to break down traffic into meaningful segments.
- Noise-to-incorrect-identification ratio can be high if,
  - The configured policy includes a lot of Informational alerts, or scan alerts which are based on request activities (such as the Default Testing (Attack Set Profile) policy).
  - Deployment links where there is a lot of hostile traffic, such as in front of a firewall.
  - Overly coarse traffic VIDS definition that contains very disparate applications. For example, a highly aggregated link in dedicated interface mode.

# Iniciar con Alto Volumen de Ataques

- Threat Explorer - Consolidated View – Top 10
- Use Wireshark to discover the packet level characteristics of a data flow
- False positives more common during initial tuning
- Attack
- Signatures Sets
- Thresholds
- Anomaly profiles
- Correlation rules



# Buscando por Patrones

Type of Pattern	How to Tune
1 to Many	Ignore rule
1 to 1	Ignore rule
Subnet to Subnet	Ignore rule or consider Disable
Many to Many	Disable



# Prevencción Futura de Falsos Positivos

## Options available with Trellix IPS

1. Use an ignore rule
  - Create an ignore rule
    - In the Attack Log
    - Select the attack
    - Select 'Other Actions > Create Exception > Add Ignore Rule
    - Name the rule
    - Select Secondary Action
    - Customized any settings
    - Assign to Scope (Sensor, Interface or sub-interface)
    - Save
2. Disable an Attack
3. Disable an Alert

# Deshabilitando Ataques en Trellix IPS

## Policy tab

- Change the Status to Disabled

Policy > [Domain] > Intrusion Prevention > Policy Types > IPS

The screenshot shows the Trellix IPS configuration interface. The breadcrumb path is "/My Company > Intrusion Prevention > Policy Types > IPS". The "Attack Definitions" tab is selected. A table lists various attack definitions with their states and severities. A specific attack, "(Inbound) 32BITFTP: 32bit FTP Client Stack Bu...", is selected, and its settings are shown in a panel on the right. The "Settings" button is highlighted, and the "State" dropdown menu is open, showing options: "Inherit (Enabled)", "Inherit (Enabled)", "Enabled", and "Disabled". A green arrow points to the "Disabled" option. The "Update" button is also highlighted.

State	Name	Severity	Industry IDs
Enabled	32BITFTP: 32bit FTP Client Stack Buffer Overflow	Medium (5)	
Enabled	32BITFTP: 32bit FTP Client Stack Buffer Overflow	Medium (5)	
Enabled	AASync: AASync LIST Command Response Filename	Medium (5)	
Enabled	AASync: AASync LIST Command Response Filename	Medium (5)	
Enabled	ABB: ABB MicroSCADA Wserver.exe Remote Code Ex	High (7)	CVE-2019-5620
Enabled	ABB: ABB MicroSCADA Wserver.exe Remote Code Ex	High (7)	CVE-2019-5620
Enabled	ABB: WebWare RobNetScanHost.exe Remote Code	High (7)	CVE-2012-0245
Enabled	ABB: WebWare RobNetScanHost.exe Remote Code	High (7)	CVE-2012-0245
Enabled	AbsoluteFTP: AbsoluteFTP LIST Command Remote	Medium (5)	CVE-2011-5164
Enabled	AbsoluteFTP: AbsoluteFTP LIST Command Remote	Medium (5)	CVE-2011-5164
Enabled	ACCELLION: Accellion File Transfer Appliance MPIPEZ	Medium (5)	

Settings panel for "(Inbound) 32BITFTP: 32bit FTP Client Stack Bu...":

- State: Inherit (Enabled) (dropdown menu open, "Disabled" selected)
- Severity: Inherit (Enabled)
- Sensor Actions: Disabled
- Response: Block: Inherit (Disabled), Quarantine: Inherit (Disabled), TCP Reset: Inherit (Disabled), ICMP Message: Inherit (Disabled)

Reduce false positives by *Disabling Alerts*.  
For example, all alerts with severity level lower than 4.

Disable attacks = Do not detect

# Deshabilitando Alerts

## Policy tab

Policy > [Admin Domain] > Intrusion Prevention > Policy Types > IPS

The screenshot shows the Trellix interface with the 'Attack Definitions' tab selected. A table lists various attack definitions, including '32BITFTP: 32bit FTP Client Stack Buffer Overflow' and 'AASync: AASync LIST Command Response Filename Handling C...'. The 'Sensor Actions' configuration for the selected alert is shown on the right, with the 'Alert' dropdown menu set to 'Disabled'.

State	Name ↑
1 Enabled	32BITFTP: 32bit FTP Client Stack Buffer Overflow
2 Enabled	32BITFTP: 32bit FTP Client Stack Buffer Overflow
3 Enabled	AASync: AASync LIST Command Response Filename Handling C...
4 Enabled	AASync: AASync LIST Command Response Filename Handling C...
5 Enabled	ABB: ABB MicroSCADA Wserver.exe Remote Code Execution
6 Enabled	ABB: ABB MicroSCADA Wserver.exe Remote Code Execution
7 Enabled	ABB: WebWare RobNetScanHost.exe Remote Code Execution VU...
8 Enabled	ABB: WebWare RobNetScanHost.exe Remote Code Execution VU...
9 Enabled	AbsoluteFTP: AbsoluteFTP LIST Command Remote Buffer OverP...
10 Enabled	AbsoluteFTP: AbsoluteFTP LIST Command Remote Buffer OverP...

**Sensor Actions**

Response

Block: **Enable SmartBlocking**

Quarantine: **Inherit (Disabled)**

TCP Reset: **Inherit (Disabled)**

ICMP Message: **Inherit (Disabled)**

Alert: **Disabled**

Capture Packets  
This option requires alerts to be sent to the Manager.

Edit the *Sensor Actions* for the Alert: (Response)

Block:

- Select Enable SmartBlocking

Alert is set to Disabled:

- No alert is sent to the Manager

# Agregando Ataques Low Severity Attacks al Proceso

## Automated blocking of attacks: Exceptions

Creating or editing an attack set profile: You can create one or more rules with the categories, subcategories and minimum severity level of attacks that you want to be blocked by the Sensor.

Use a blocking strategy that suits your network environment and use the same profile during any IPS policy configuration.

Enforce the IPS policy at the interfaces and sub-interfaces of the required Sensor(s)

When the policy and rule updates are applied to the required Sensor(s), they automatically block all attacks that match your blocking criteria and send an alert to the Manager.

# Alertas Excesivas

## Categories

Valid Alerts

- These are actual attacks.
- Impact may be critical, or moderate, or none.

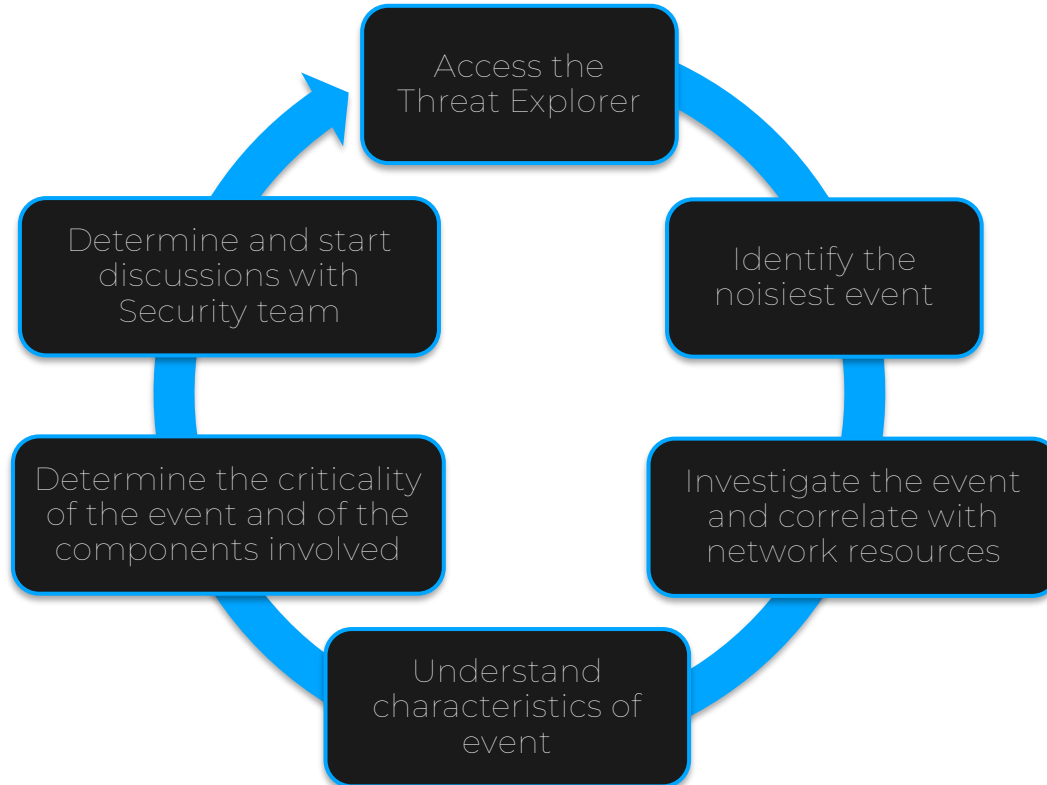
Irrelevant Alerts

- What is the company policy for allowed communication?

False Positives

- These are incorrectly-identified events.

# Acercamiento de Arriba hacia Abajo



# Analizando Eventos

## Threat Explorer

Displays:

- The attacks that have *happened the most*.
- The IP addresses *responsible for most of the attacks*.
- The IP addresses *that are mostly attacked*.
- The applications used to *perform most of these attacks*.
- The most downloaded or uploaded *malware to perform these attacks*.

Analysis > [Admin Domain] > Threat Explorer

The screenshot shows the Trellix Threat Explorer interface. The navigation menu on the left includes 'Attack Log', 'Threat Explorer', 'Malware Files', 'Callback Activity', 'High-Risk Endpoints', 'Network Forensics', 'Endpoint Executables', 'Quarantine', 'MITRE ATTACK View', and 'Event Reporting'. The main content area displays a summary of attacks, including 'Top Attacks', 'Top Attackers', 'Top Targets', 'Top Attack Applications', and 'Top Attack Executables'. The 'Top Attack Executables' section is expanded, showing a table with columns for Executable Hash, File Name, Executable Malware Confidence, Executable Classification, and Attack Count.

# Analizando Eventos (continued)

## Attack Log

Analysis > [Admin Domain] > Attack Log

The screenshot shows the Trellix Analysis console. The top navigation bar includes 'Dashboard', 'Analysis' (highlighted with a green box), 'Policy', 'Devices', and 'Manager'. The left sidebar contains various tool categories, with 'Attack Log' highlighted. The main area displays a table of events with columns for Name, Time, Direction, Result, Attack Count, CVE ID, and Packet Capture. A table with 12 rows is visible, showing various network events like SMB traffic and DCERPC calls.

	Name	Event	Direction	Result	Attack Count	CVE ID	Packet Capture
1	NETBIOS-SS: SMB V1 Traff...	Nov 30, 2023 09:34:41	Inbound	Inconclusive	1	---	Export
2	NETBIOS-SS: SMB V1 Traff...	Nov 30, 2023 09:34:41	Outbound	Inconclusive	29,085	---	Export
3	NETBIOS-SS: Metasploit En...	Nov 30, 2023 09:33:11	Inbound	Inconclusive	1	---	Export
4	NETBIOS-SS: Metasploit En...	Nov 30, 2023 09:33:11	Inbound	Inconclusive	1	---	Export
5	DCERPC: Microsoft Plug an...	Nov 30, 2023 09:33:11	Inbound	Attack Blo...	1	CVE-2005-1983	Export
6	DCERPC: Suspicious PnP Call	Nov 30, 2023 09:33:11	Inbound	Inconclusive	1	CVE-2005-1983	Export
7	NETBIOS-SS: SMB Write Tr...	Nov 30, 2023 09:33:11	Inbound	Inconclusive	1	---	Export
8	NETBIOS-SS: SMB V1 Traff...	Nov 30, 2023 09:32:55	Outbound	Inconclusive	1	---	Export
9	NETBIOS-SS: SMB V1 Traff...	Nov 30, 2023 09:32:55	Outbound	Inconclusive	1	---	Export
10	NETBIOS-SS: SMB V1 Traff...	Nov 30, 2023 09:32:55	Outbound	Inconclusive	1	---	Export
11	NETBIOS-SS: SMB V1 Traff...	Nov 30, 2023 09:32:55	Outbound	Inconclusive	1	---	Export
12	NETBIOS-SS: SMB V1 Traff...	Nov 30, 2023 09:32:55	Outbound	Inconclusive	1	---	Export

This screenshot shows the 'Other Actions' dropdown menu for a selected event. The menu items are: Update Policy, Create Exception, Quarantine Endpoint, Tag Endpoint, Terminate Connection, Perform Network Forensics, Assign Alert, Acknowledge All Matching Alerts, Unacknowledge All Matching Alerts, Delete All Matching Alerts, and Save Attack Log as. The 'Other Actions' button in the main interface is also highlighted with a green box.

- Update Policy
- Create Exception
- Quarantine Endpoint
- Tag Endpoint
- Terminate Connection
- Perform Network Forensics
- Assign Alert
- Acknowledge All Matching Alerts
- Unacknowledge All Matching Alerts
- Delete All Matching Alerts
- Save Attack Log as





# Alerta de ICMP Unsolicited Echo Reply

## Investigation

- This environment has asymmetric routing, but the Sensors are not configured for an asymmetric routing configuration.
- One Sensor port only sees the ICMP reply from a server but does not see the ICMP request from the client. Another Sensor port may see the ICMP request.
- The Sensor alerts for an unmatched ICMP echo reply.

## Solution Adopted

- The Sensor is configured to use an “Interface Group”, and the alerts are no longer generated.
- If the request/response traffic passes through two different Sensors (geographically distributed), then the recommendation is to enable the “Permit out-of-order” feature.
- This tells the Sensor to pass a response if the flow did not exist in the state table

## Best Practice

- Verify whether this alert is generated due to loading balancing, asymmetric routing or other hardware related configuration

# Microsoft DNS Services Resolver Overflow

## Investigation

- This vulnerability exists on un-patched versions of Microsoft Exchange 2000 Server, Microsoft Exchange Server 2003, Windows XP 64-Bit Edition, or Windows Server 2003 prior to MS04-035.
- This environment does not have SMTP services installed on DNS servers.
- In this case, the exploit is harmless, as the servers are either patched or hardened.

## Solution Adopted

- Either configure an ignore rule (any-to-1) or exclude the attack from the associated policy.

## Best Practice

- Customize the associated policy, excluding irrelevant attacks.
- Use a unique policy and VIPS provide more granularity if required.

# ICMP: Nachi Like Ping Attack

## Investigation

- Lots of Nachi Ping alerts from one source to one destination in the internal network.
- After analyzing the traffic, temporarily configuring and reviewing Forensic Packet Logging, it was found that the source of this alert is from legitimate ICMP polling done via a control center deployment. The agent of SRM software is running on the source host and keeps polling to the manager software on destination host.
- It is determined that this is a valid management action, and the ICMP traffic has a similar pattern to Nachi Ping.

## Solution Adopted

- A one-to-one ignore rule was configured.
- Alternatives considered included Auto-Acknowledgement for the attack.

## Best Practice

- Customize the policy and exclude irrelevant attacks.
- Use a unique policy and VIPS provide more granularity if required.



# Alertas de Backdoor: Back Orifice Trojan

Investigation	Solution Adopted	Best Practice
<ul style="list-style-type: none"><li>• This alert was triggered in over 6,000 user network segments.</li><li>• The third-party NAC server was scanning for open ports including the Back Orifice server port to determine if the hosts were active and/or unhealthy.</li></ul>	<ul style="list-style-type: none"><li>• Configure ignore rules to filter the Vulnerability Scanner server to any IP.</li><li>• Alternative approaches included Auto-Acknowledge alerts.</li><li>• Whitelist the Vulnerability Scanner server using the ACL (bypass IPS) feature.</li></ul>	<ul style="list-style-type: none"><li>• Review the environment and document Management servers (systems management, security management, vulnerability scanners etc.). Consider excluding them from IPS inspection or create unique policies and disable the attack following the appropriate approval process and sign off.</li></ul>



# HTTP Login Brute Force Detected

## Investigation

- This is a correlated attack, and it detects any HTTP login authentication errors. By default, if there are 5 login errors within 120 seconds from a single source host, it will trigger the alert.
- After review it was understood that this event was appropriate behavior in the network and no alert was required for this specific attack.

## Solution Adopted

- Attack disabled in the appropriate policy if the event is expected behavior.
- Alternative options include increasing the threshold or increasing the alert suppression time.

## Best Practice

- Customize the correlated alert parameters (Threshold and Suppress time) as needed.
- Review the requirement to detect this attack and either disable in the policy for environments where this is common or enable auto-acknowledge if reporting is required.

# ARP Spoofing Detected

## Investigation

- The Sensor is located adjacent to a Linux based clustered device such as a Firewall or Web Server.
- The clustering solution uses gratuitous ARP's or ARP Spoofing to fail over the cluster.

## Solution Adopted

- The attack was disabled in the appropriate policy as this event is expected behavior in that environment.

## Best Practice

- Disable the attack in the policy for those environments where clustering is expected.
- This attack could also indicate the presence of a captive portal.
- Review the environment to ensure a captive portal is expected & take appropriate actions.



# ARP: MAC Address Flip-Flop Events

## Investigation

- The Sensor is located adjacent to a Linux based clustered device such as a Firewall or Web Server.
- The clustering solution uses gratuitous ARP's reverse ARPs to share traffic between the cluster members.
- Servers protected by the Sensor are dual homed.

## Solution Adopted

- Attack was disabled in the appropriate policy as this event is expected behavior in that environment.

## Best Practice

- Disable the attack in the policy for those environments where clustering is expected.
- Disable this attack in the policy for DHCP environments with many hosts joining and leaving the network.



# P2P Events including P2P: Bit Torrent Meta-Info Retrieving

## Investigation

- The firewall is blocking Peer-to-Peer (P2P) traffic but only on non-HTTP ports.
- Users have installed P2P applications and are attempting to share files via P2P.
- Corporate Policy does not allow un-authorized applications including P2P.

## Solution Adopted

- The attack was blocked and auto-acknowledged.
- Alternatives considered included.
- Rate-Limit P2P on the Sensor.
- Ignore and disable Attack in the policy.

## Best Practice

- If P2P is allowed, then disable this category of attack.
- If P2P is not allowed, then block and auto-acknowledge.
- Allow ignore rules such as Skype.
- Where certain P2P applications are allowed ensure that these are not blocked (e.g. Universities often share research material via BitTorrent).





# IM: Yahoo Messenger Server Lookup Events

## Investigation

- The firewall is not blocking IM traffic.
- Corporate Policy allows the unrestricted use of IM.

## Solution Adopted

- The attack was auto-acknowledged.
- Additional controls were considered such as limiting certain IM features like file transfers via IM protocols.

## Best Practice

- If all IM is allowed, then disable this category of attack.
- If only corporate IM is allowed, then block all IM except the corporate IM protocol (e.g., Office Communicator uses the MSN protocol).
- Either use existing controls to limit IM functionality or use the NSP to block only unwanted IM activities such as file transfers.



# Host and Port Sweep Events Including UDP: Host Sweep

## Investigation

- Multiple Host Sweeps and Port scan events coming from a few servers directed at multiple hosts.
- Source IP addresses were determined to be Domain Controllers.
- Port Scans were found to be coming from a Vulnerability Management solution, implemented by the IT Security team.

## Solution Adopted

- Events are classed as reconnaissance events and do not necessarily indicate attacks.
- Because behavior is expected with Domain Controllers authenticating hosts and users the reconnaissance policy was modified for Sensor protecting the domain controllers.
- IP addresses for the Vulnerability Management solution were whitelisted using the ACL feature of the Sensor (bypass IPS).

## Best Practice

- Reconnaissance policies apply to the entire Sensor.
- Disable these attacks if the Sensor is protecting internal servers only.
- If the Sensor is protecting internal servers and other environments, consider either adjusting the alert threshold settings and/or modifying the severity to allow for auto acknowledgement.
- Use ACL bypass or selective Layer-2 scanning ignore rules (where available) for Vulnerability Management solutions.

# Gestión de Respuestas

- A preset response from the Sensor is integral to the protection or prevention process.
- Critical attacks like buffer overflows and DoS attacks require responses in real time, while scans and probes can be logged and researched to determine compromise potential and the source of the attack.
- If the Sensor is monitoring the network outside of the firewall in in-line mode, preventing DoS attacks and attacks against the firewall is crucial.
- Other suspicious traffic intended for the internal network, such as scans and low-impact well-known exploits, are best logged and analyzed as the impact is not immediate.
- Remember that response actions are decoupled from alerting.
- Pay particular attention to this with the SmartBlocking status.

# Acciones de Respuesta del Sensor

Multiple Sensor Actions that are Available for Configuration per Attack

## Dropping Alert Packets

Only works in in-line mode. Will drop a detected attack packet and all subsequent packets in the same flow.



## IPS Quarantine

Sensor will quarantine/remediate a host as per the configurations in Manager and the Sensor monitoring ports. IPS Quarantine can be enabled per attack in the Policy Editors.



**Trellix**