



EDSI Trend

Trend Micro Web Security

# Temario

- Web Security: Standard vs. Advanced
- Planeamiento & Instalación de Gateway
- Sincronización con AD
- Formas de redirigir el tráfico
  - PAC File
  - Enforcement Agent
- Primeros pasos
- Políticas y sus mejores prácticas
- Recapitulación



## **TMWS: Standard vs. Advanced**

---

# Trend Micro Web Security Standard/Advanced

## Web Security Standard

- On-premises, cloud o ambos
- Descifrado HTTPS
- Filtro de URLs
- Control de Aplicaciones
- Servicio de Web Reputation
- Antimalware
- Anti-botnet
- Logeo/Reportes

## Web Security Advanced

- Predictive ML
- Cloud sandboxing
- DLP
- Cloud app access control\*
- Filtros de servicios en la nube
- Control de cuentas basado en funciones
- Syslog/SIEM

# Versión Advanced



## Predictive Machine Learning

Tecnología nube de para la detección de amenazas de ejecución local. Utiliza algoritmos matemáticos para predecir si un archivo es malicioso o no.



## Data Loss Prevention

Utiliza templates para resguardar bienes digitales contra descuidos o fuga de datos deliberados.



## Cloud Sandboxing

Los archivos son filtrados antes del envío a la sandbox para mayor eficiencia y menor cantidad de falsos positivos. Trackea y analiza muestras para detectar objetos sospechosos, proveer blacklists y ayudar contra malware de día 0.



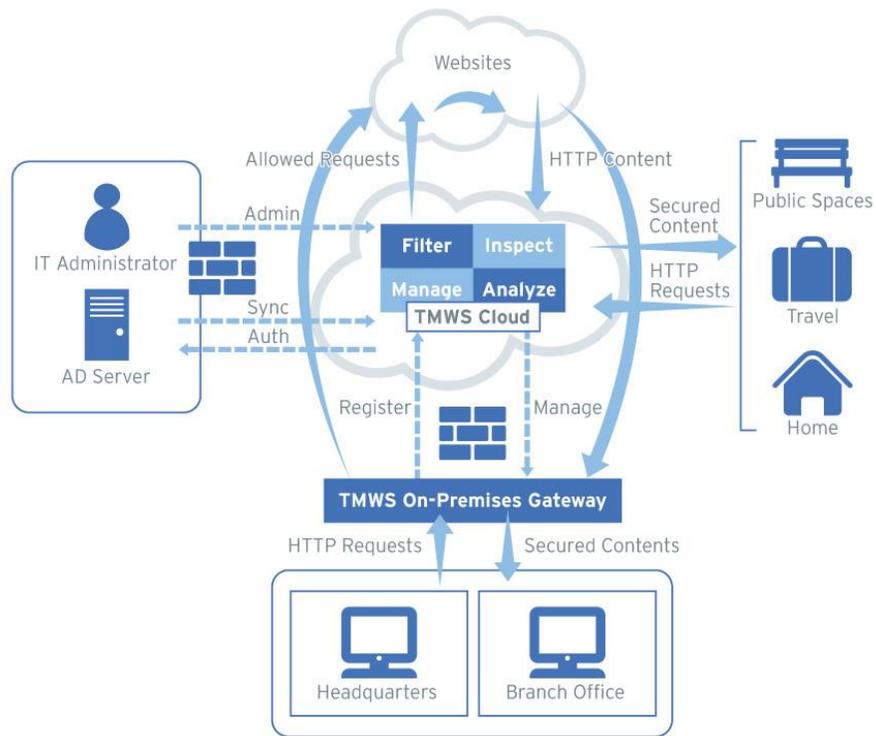
## Cloud Service Filters

El filtrado de organización web puede ayudar a tu organización para el control de acceso sobre servicios nube. Por ejemplo, permitiría el acceso de Office 365, G Suite y Dropbox únicamente con credenciales de dominio.



# Planeamiento & Instalación de Gateway

# Topología de Red



# Configuración de Gateway Virtual

The screenshot displays the Trend Micro Web Security console interface. At the top, the navigation menu includes Dashboard, Gateways, Policies, Logs & Reports, and Administration. The 'Gateways' tab is selected, and a red arrow points to it. Below the navigation, the 'Gateways' section contains a table with columns for Gateway Name and Gateway Type. A red box highlights the '+ Add Virtual Gateway' button, and another red arrow points to it. To the right, two 'Add Virtual Gateway' dialog boxes are shown. The top dialog is in the 'Basic Information' tab, with fields for Name (Test Trend Argentina), Description, Gateway type (Virtual), Status, Time zone (UTC-03:00 Buenos Aires), and Static IP address. The bottom dialog is in the 'Authentication' tab, showing options for User authentication (Captive portal), Guest access, Guest port, and Bypass authentication (Enable/Disable).

# Instalación de Gateway On-Premise

The screenshot shows the Trend Micro Web Security admin portal. The browser address bar displays `adminportal-se.iws-hybrid.trendmicro.com/basic/gateway.html`. The navigation menu includes Dashboard, Gateways, Policies, Logs & Reports, and Administration. A notification banner states: "Due to security, compatibility, and performance concerns, Trend Micro Web Security will disable the Administration > SERVICE DEPLOYMENT > Mobile VPN page by June 1, 2023 and retire the Mobile VPN feature used for forwarding traffic from mobile devices by June 15, 2023. Trend Micro recommends that you use the TMWS Agent app instead for mobile traffic forwarding." Below this, a green message box says "Gateway successfully deleted". The main content area is titled "Gateways" and contains buttons for "+ Add Virtual Gateway", "+ Add On-Premises Gateway", and "Refresh". A search bar is present. Below the buttons is a table with columns: Gateway Name, Gateway Type, Description, Status, IP Address, User Authentication, Last Communication Time, and Action. The table is currently empty, displaying "No data available." at the bottom. The Windows taskbar at the bottom shows the date and time as 17:37 on 13/4/2023.



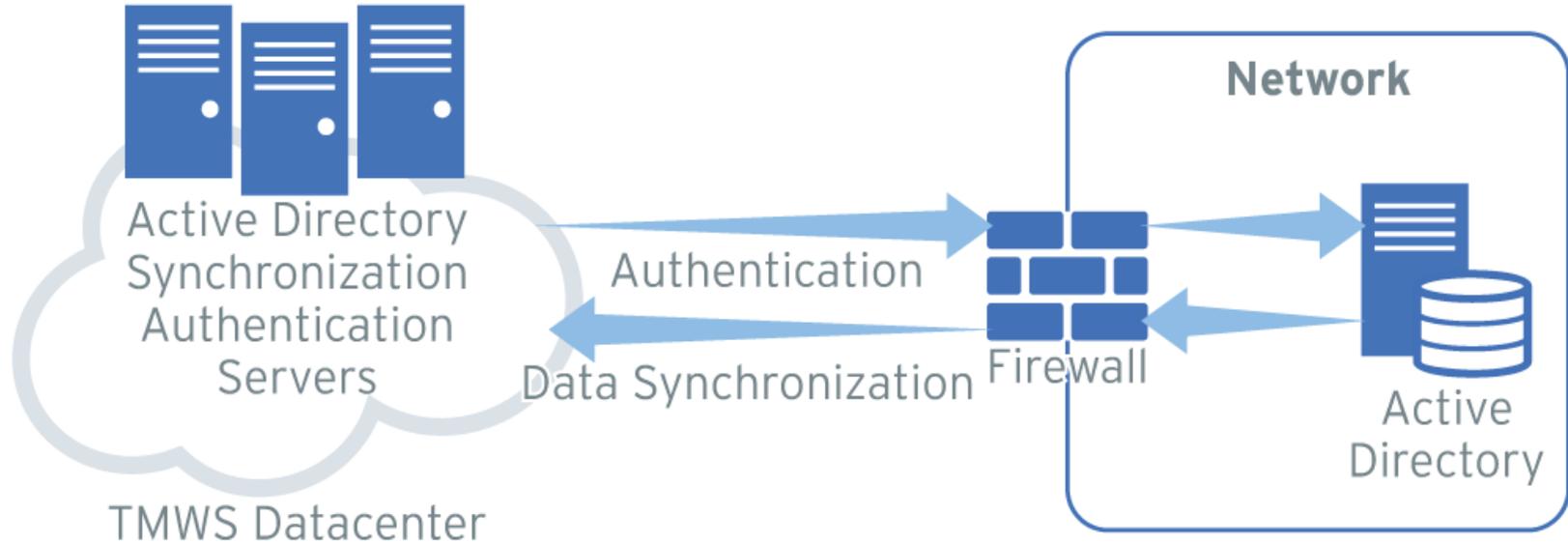
## Sincronización con AD

---

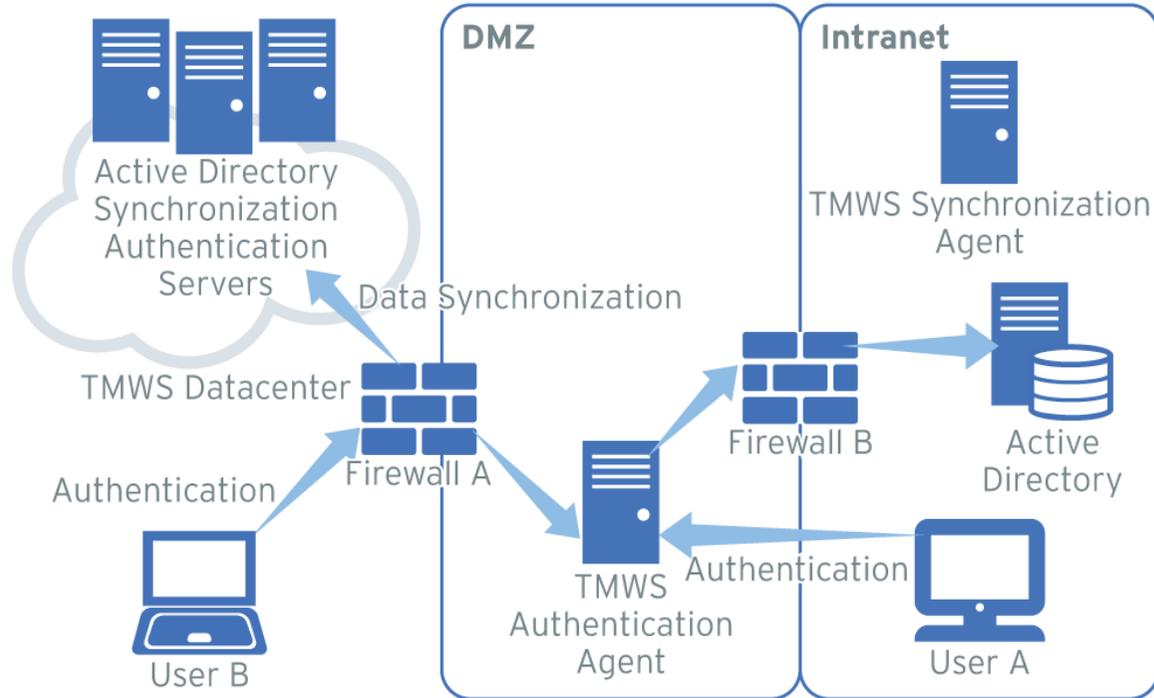
# Modo de vinculación AD

- Directa
- Agentes
- Microsoft AD FS
- Azure
- Okta

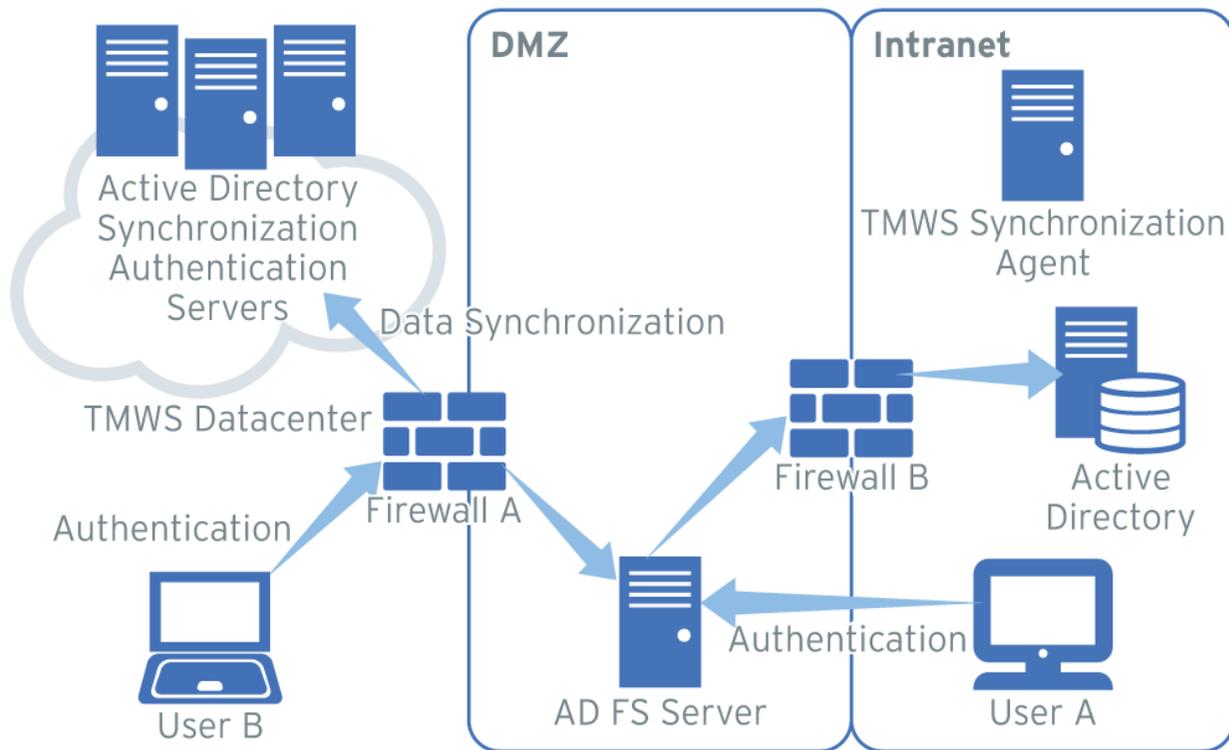
# Directa



# Agente



# AD Federation Services



# Formas de redirigir el tráfico



# PAC File

---

# Manejo de "Proxy.pac"s

- Consola de gestión básica / Opciones Avanzadas

### Add PAC File

PAC file name:

Description:



Bypass proxy for these hosts & domains:

Note: \*example.com matches example.com and all of its subsites.

- \*.google.com
- \*.google.co.\*
- \*.google.com.\*
- windowsupdate.microsoft.com
- \*.windowsupdate.microsoft.com
- \*.update.microsoft.com
- \*.windowsupdate.com
- download.microsoft.com
- ntservicepack.microsoft.com
- officecdn.microsoft.com

```
1 // TMWS pac file
2
3 function islocalip(ip) {
4     return isInNet(ip, "127.0.0.0", "255.0.0.0") ||
5            isInNet(ip, "169.254.0.0", "255.255.0.0") ||
6            isInNet(ip, "10.0.0.0", "255.0.0.0") ||
7            isInNet(ip, "192.168.0.0", "255.255.0.0") ||
8            isInNet(ip, "172.16.0.0", "255.240.0.0");
9 }
10
11
12 function FindProxyForURL(url, host) {
13
14     var DefaultScanner = "PROXY proxy.iws-hybrid.trendmicro.com:80; DIRECT";
15     var HTTPSScanner = "PROXY proxy.iws-hybrid.trendmicro.com:80; DIRECT";
16     var FTPScanner = "DIRECT";
17     var DNSNeedResolve = false;
18     var SkipHosts = [
19         "*.google.com",
20         "*.google.co.*",
21         "*.google.com.*",
22         "windowsupdate.microsoft.com",
23         "*.windowsupdate.microsoft.com",
24         "*.update.microsoft.com",
25         "*.windowsupdate.com",
26         "download.microsoft.com",
27         "ntservicepack.microsoft.com",
28         "officecdn.microsoft.com",
29         "officecdn.microsoft.com.edgesuite.net"
30     ];
31
32     if (isPlainHostName(host)) {
33         return "DIRECT";
34     }
35 }
```



# Enforcement Agent

---

# Enforcement Agent

- Este agente fuerza al usuario final a utilizar el “proxy.pac” designado, tanto por configuración de Windows, como por diferentes navegadores.

The screenshot displays the Enforcement Agent configuration interface. The left sidebar contains navigation links: License Information, SERVICE DEPLOYMENT (PAC Files, Policy Backup & Restoration, Mobile VPN, Enforcement Agent), USERS & AUTHENTICATION (Directory Services, Hosted Users), and ADMINISTRATOR ALERTS (Account Setup Message, Administrator Alerts). The main panel is titled 'Enforcement Agent' and includes a 'Default' button and a 'Customize' button. Below this, the 'Default Agent Settings' section provides instructions and configuration options: Agent platform (Windows selected, OS X available), Agent tray icon (Show status checked), Forbidden browser(s) (text input), Uninstall agent password (trendmicro), Hosted PAC file (proxy.pac), Proxy port (8080), and a Windows Download button. The 'Disable Agent' section includes an Agent access key (beb086a6ccf803bc31a2c1f9bbdca43fa4df0df63fce2584b804e2a62c) with expiration and creation dates, and a Create Access Key button.

Two dialog boxes are overlaid on the interface. The 'Status' dialog shows the Enforcement Agent version (3.3.0.2973), TMWS Account information (Not logged in), and the PAC File Name (proxy.pac). The 'Local Area Network (LAN) Settings' dialog shows the 'Use automatic configuration script' option checked, with the address set to //127.0.0.1:8080/pac/proxy.pac.0d.



# Primeros pasos

---

# Implementación

- Registrar Dominio y verificarlo
- Crear un usuario administrador
- Registrar usuarios
- Creación de políticas



# Creación de políticas

---

# Consola



# Logs & Reports

---

# ¿Qué registros vamos a ver?

- El cumplimiento de políticas
- Navegación por usuario/dominio
- El análisis de los objetos sospechosos
- El ingreso y modificaciones a la consola

¡Muchas gracias!



EDSI Trend