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

Tecnologia 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

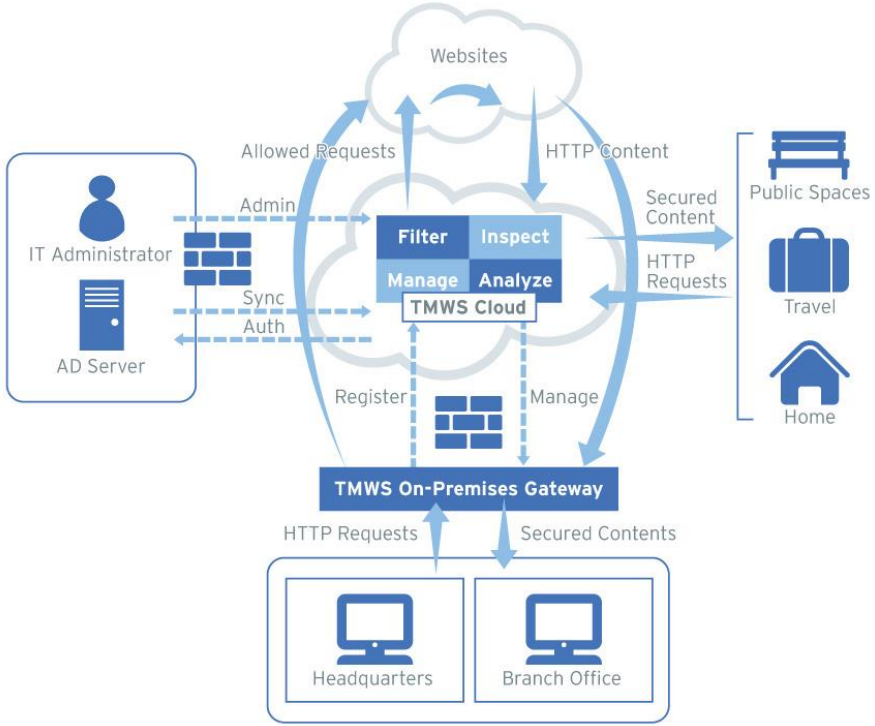
Los archivos son filtrados antes del envio a la sandbox para mayor eficiencia y menor cantidad de falsos positivos. Trackea y analiza muestras para detectar objetos sospechosos, proveer blacklists y ayudar contra malware de dia 0.

Cloud Service Filters

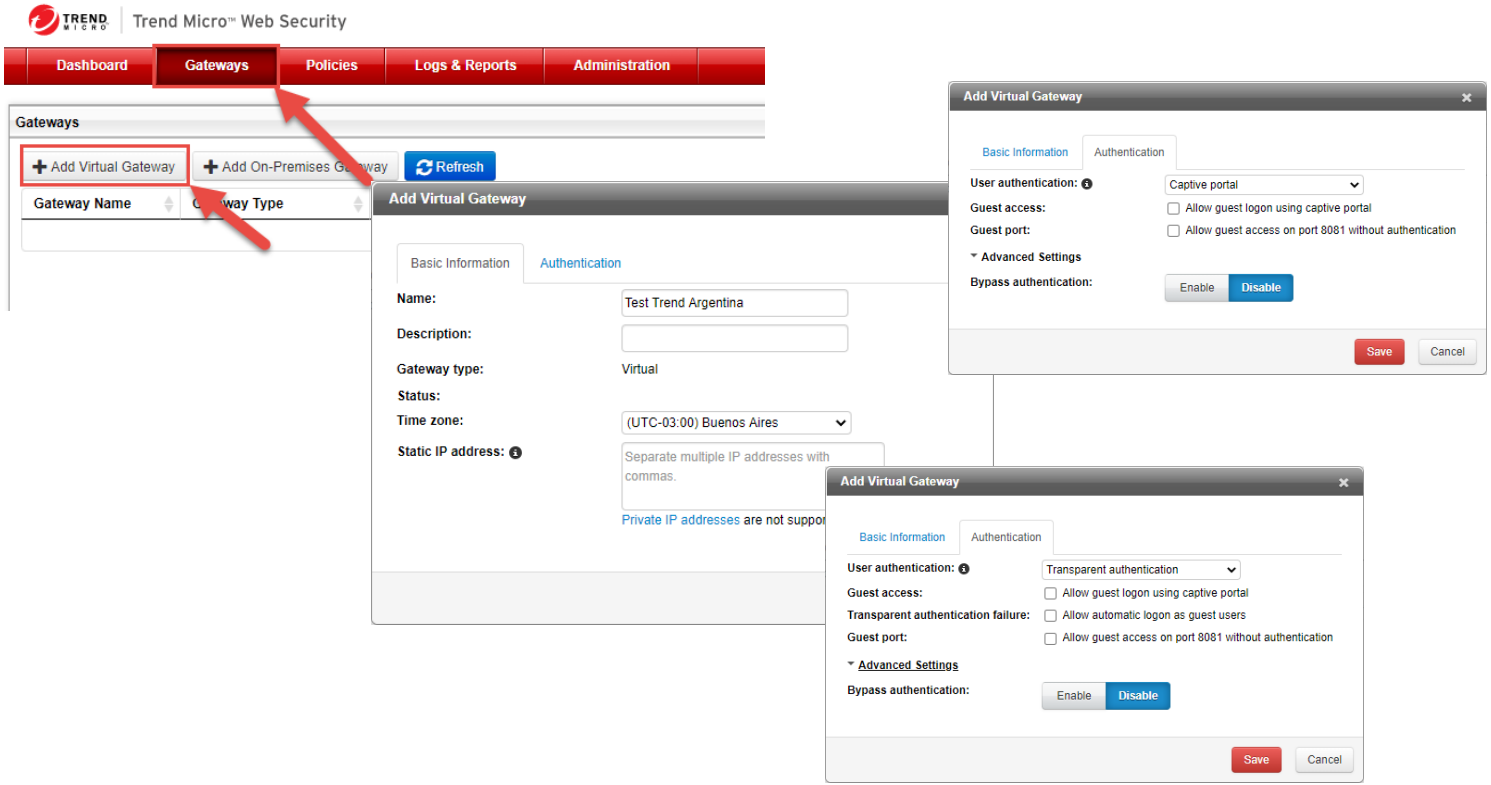
El filtrado de organización web puede ayudar a tu organización para el control de acceso sobre servicios nube.
Por ejemplo, permitiría el acceso de Office 365, G Suite y Dropbox únicamente con credenciales de dominio.

Planeamiento & Instalación de Gateway

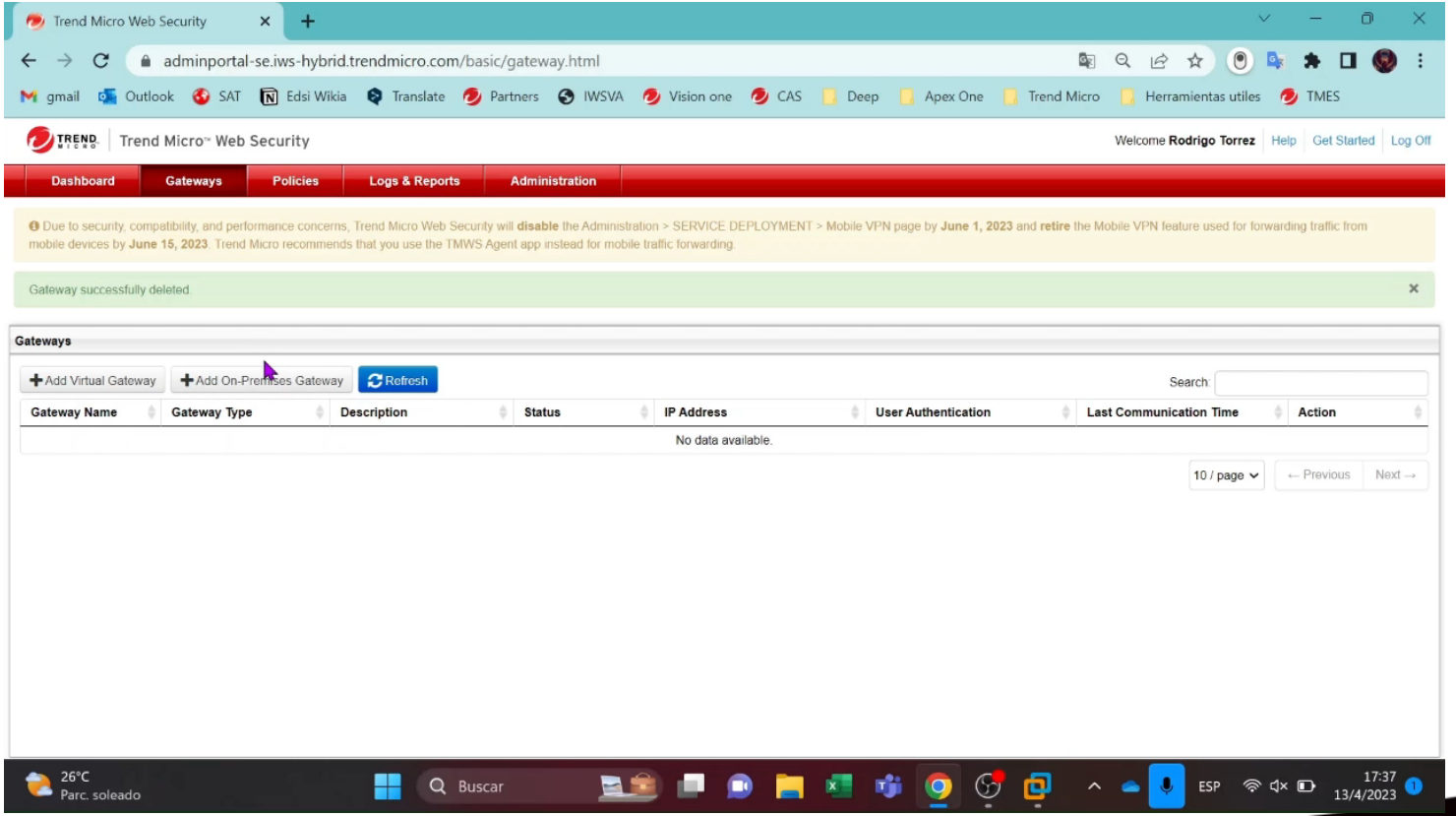
Topología de Red



Configuración de Gateway Virtual



Instalación de Gateway On-Premise

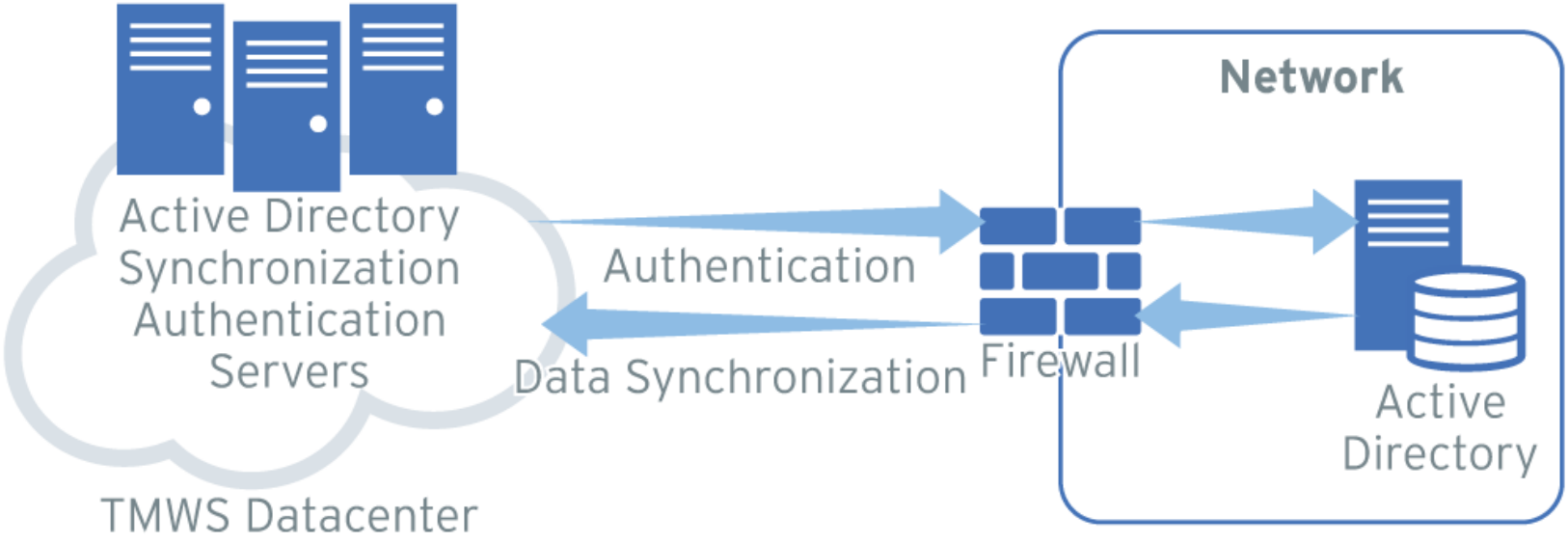


Sincronización con AD

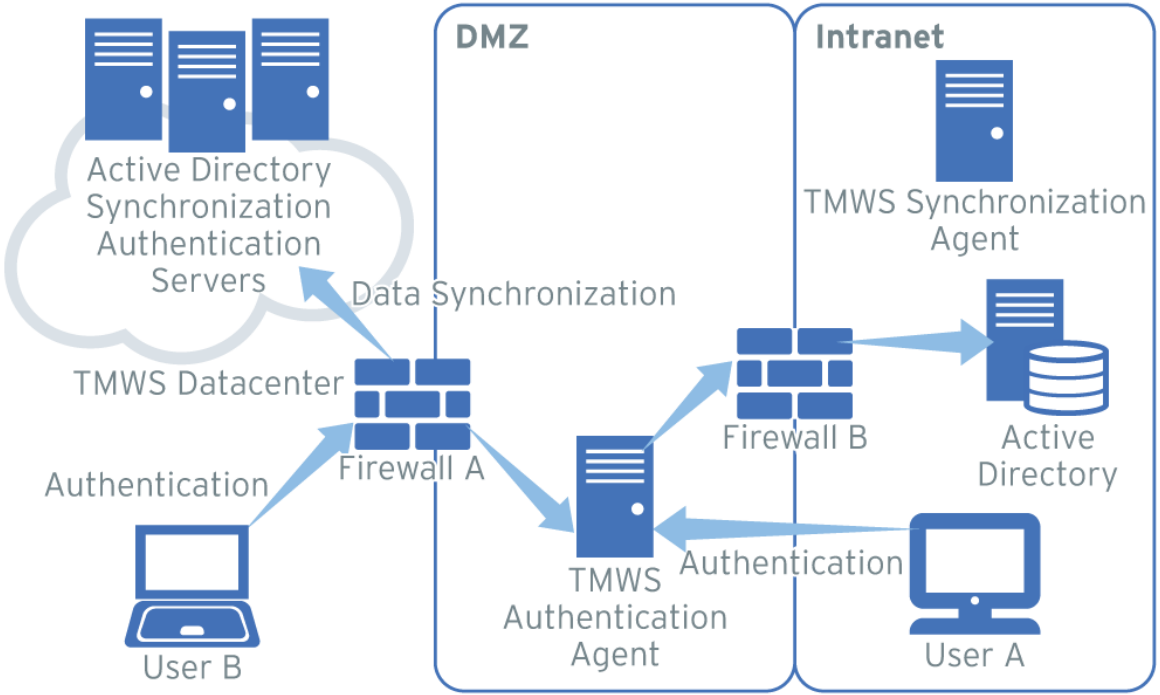
Modo de vinculación AD

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

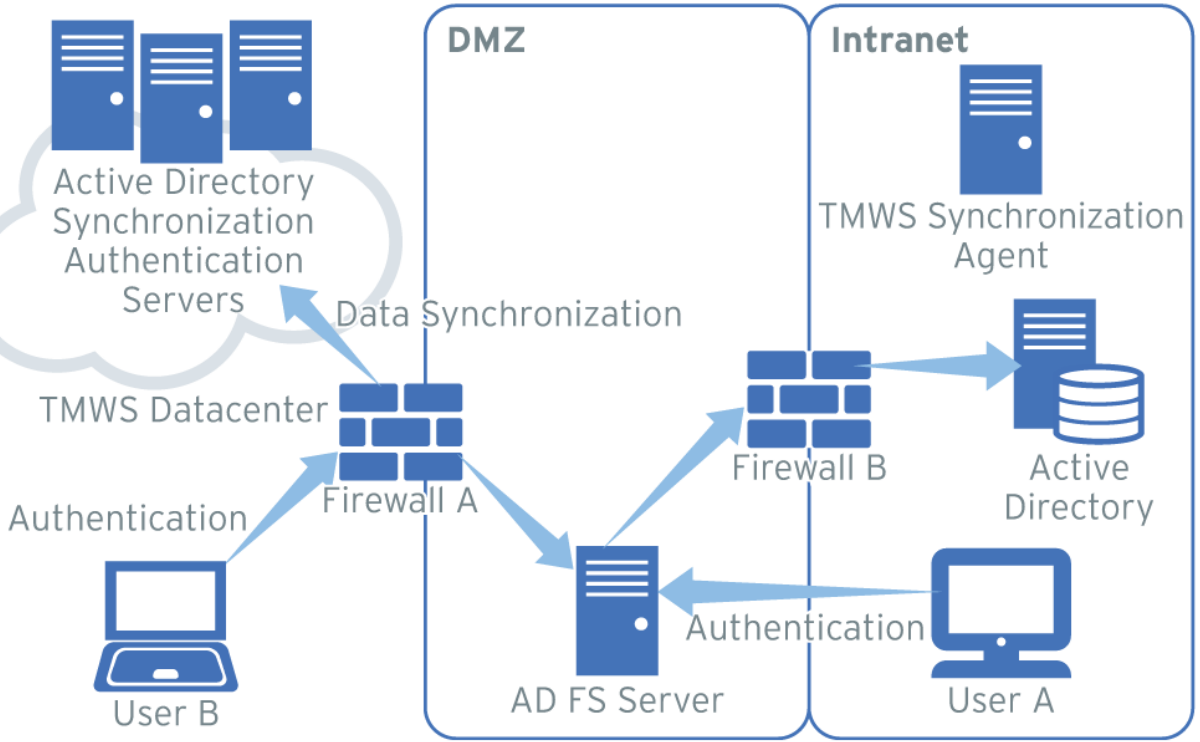
Directa


Active Directory
Synchronization
Authentication
Servers
TMWS Datacenter
Authentication
Data Synchronization
Firewall
Network
Active
Directory

Agente



AD Federation Services

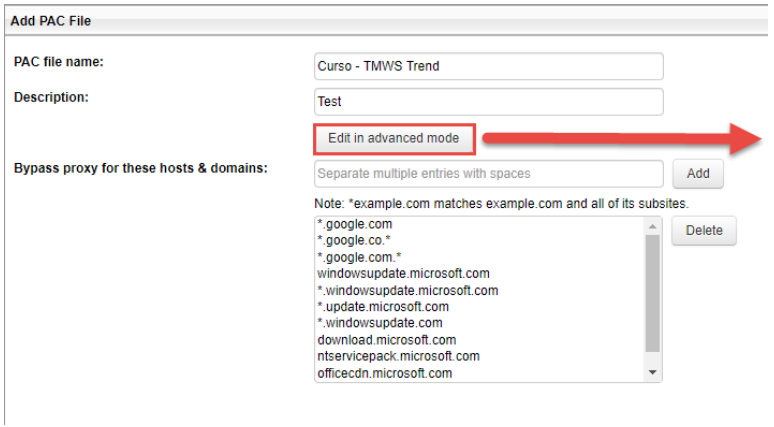


Formas de redirigir el tráfico

PAC File

Manejo de “Proxy.pac”s

- Consola de gestión básica / Opciones Avanzadas

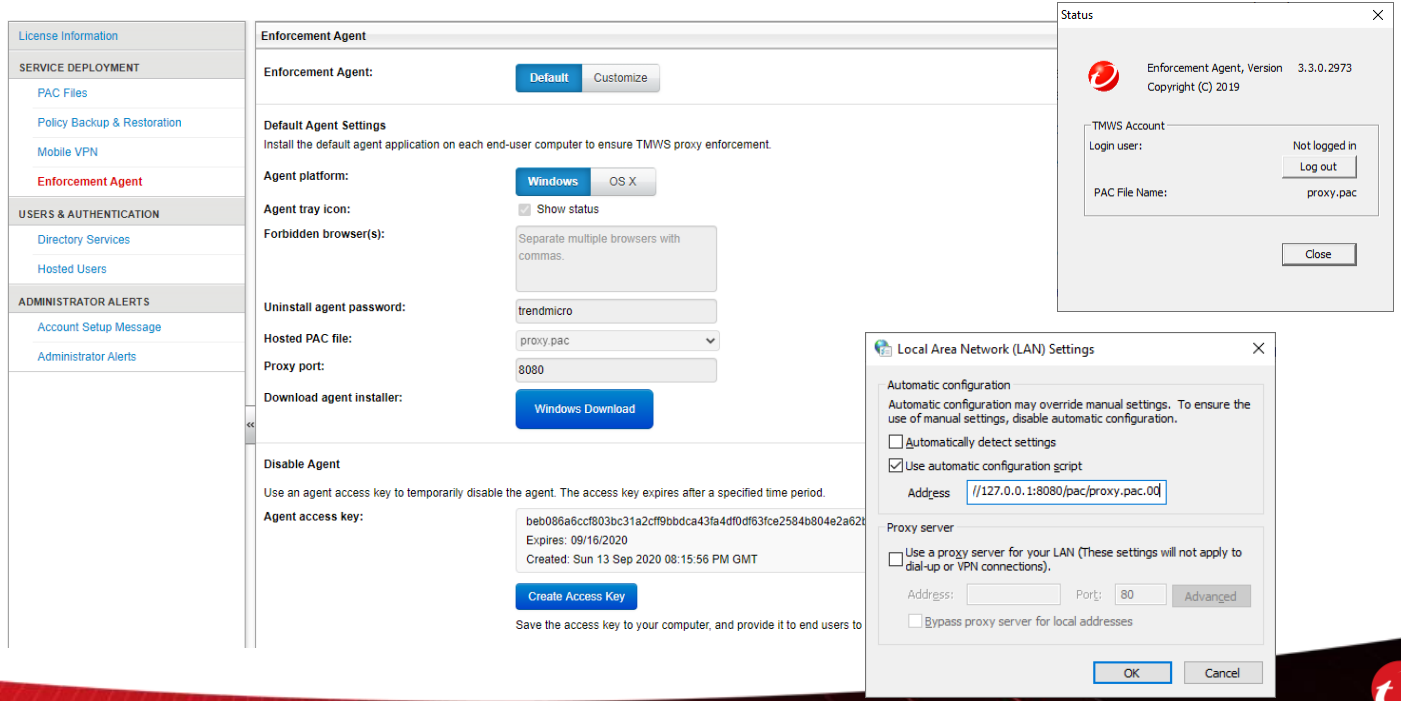



```
// TMWS pac file

function islocalip(ip) {
    return isInNet(ip, "127.0.0.0", "255.0.0.0") ||
           isInNet(ip, "169.254.0.0", "255.255.0.0") ||
           isInNet(ip, "10.0.0.0", "255.0.0.0") ||
           isInNet(ip, "192.168.0.0", "255.255.0.0") ||
           isInNet(ip, "172.16.0.0", "255.240.0.0");
}


function FindProxyForURL(url, host) {

    var DefaultScanner = "PROXY proxy.iws-hybrid.trendmicro.com:80; DIRECT";
    var HTTPSScanner   = "PROXY proxy.iws-hybrid.trendmicro.com:80; DIRECT";
    var FTPScanner     = "DIRECT";
    var DNSNeedResolve = false;
    var SkipHosts = [
        "*.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",
        "officecdn.microsoft.com.edgesuite.net"
    ];

    if (isPlainHostName(host)) {
        return "DIRECT";
    }
```

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.



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!

TREND MICRO

EDSI Trend