Escuela Politécnica Superior de Jaén

Máster Universitario en Seguridad Informática

UNIVERSIDAD DE JAÉN
Escuela Politécnica Superior (Jaén)

Trabajo Fin de Máster

ANÁLISIS TEÓRICO PRÁCTICO DE LA MATRIZ MITRE ATT&CK

Alumno/a: **Fernández-Piñar Padial, Jose Luis**

Tutor/a: Prof. D. Miguel Ángel García Cumbreras

Dpto.: Departamento de Informática

Universidad de Jaén

Escuela Politécnica Superior de Jaén
Departamento de Informática

Don Miguel Ángel García Cumbreras , tutor del Proyecto Fin de Máster titulado *Análisis teórico práctico de la matriz MITRE ATT&CK*, que presenta Jose Luis Fernández-Piñar Padial, autoriza su presentación para defensa y evaluación en la Escuela Politécnica Superior de Jaén.

Jaén, Julio de 2022

El alumno:

FERNANDEZ-PIÑAR PADIAL, JOSE LUIS (FIRMA)

Firmado digitalmente por FERNANDEZ-PIÑAR PADIAL, JOSE LUIS (FIRMA)
Nombre de reconocimiento (DN): c=ES, serialNumber=75146461X, sn=FERNANDEZ-PIÑAR, givenName=JOSE LUIS, cn=FERNANDEZ-PIÑAR PADIAL, JOSE LUIS (FIRMA)
Fecha: 2022.07.28 17:22:30 +02'00'

Jose Luis Fernández-Piñar Padial

Los tutores:

GARCIA CUMBRERAS MIGUEL ANGEL - 52871272E

Firmado digitalmente por GARCIA CUMBRERAS MIGUEL ANGEL - 52871272E
Fecha: 2022.07.28 11:14:42 +02'00'

Miguel Ángel García Cumbreras

RESUMEN

En el presente documento se describe un estudio teórico-práctico de la matriz MITRE ATT&CK Enterprise, aplicado a una empresa. En el estudio teórico se hace uso de la matriz como analizador de fallas defensivas. En el estudio práctico se aplican soluciones técnicas para mitigar las fallas defensivas analizadas a lo largo del estudio teórico.

ABSTRACT

This document describes a theoretical and practical study of the MITRE ATT&CK Enterprise matrix, applied to a company. In the theoretical study, the matrix is used for defensive gap assessment. In the practical study, technical solutions are applied to mitigate the defensive gaps analyzed throughout the theoretical study.

ANÁLISIS TEÓRICO PRÁCTICO DE LA MATRIZ MITRE ATT&CK

1. INTRODUCCIÓN 15
1.1. Motivación 16
1.2. Objetivos 17
1.3. Estructura del documento 17
2. MITRE ATT&CK ENTERPRISE 19
2.1. Definición y características 19
2.2. Modelo de Relaciones 21
2.3. Casos de uso 22
2.4. Herramientas para trabajar con MITRE ATT&CK Enterprise 23
3. ESTUDIO TEÓRICO 25
3.1. Empresa caso de estudio 25
3.2. Descripción y características de la empresa 25
3.3. Diagrama de redes e IT 26
3.4. Primeras conclusiones y propuestas 27
3.5. Desarrollo del Estudio Teórico 28
3.5.1. Caso de estudio y objetivos 28
3.5.2. Estructura del Estudio Teórico 28
3.5.3. Reconocimiento 30
3.5.3.1. Phising for Information 31
3.5.4. Desarrollo de Recursos 31
3.5.5. Acceso Inicial 32
3.5.5.1. Exploit Public Facing Applications 33
3.5.5.2. External Remote Services 33
3.5.5.3. Valid Accounts 34
3.5.6. Ejecución 35
3.5.6.1. JavaScript 36
3.5.6.2. PowerShell 37
3.5.7. Persistencia 37
3.5.7.1. Additional Cloud Credentials 38
3.5.7.2. Addional Cloud Roles 39
3.5.8. Escalado de Privilegios 39
3.5.8.1. Create or Modify System Process 40
3.5.9. Evasión de defensas 41

3.5.9.1. File and directory Permissions Modification 41
3.5.10. Acceso a Credenciales 42
3.5.10.1. Brute Force 42
3.5.10.2. Explotation for Credential Access 43
3.5.11. Descubrimiento 44
3.5.11.1. Cloud Account 45
3.5.11.2. Network Sniffing 45
3.5.12. Movimiento Lateral 46
3.5.12.1. Remote Desktop Protocol 47
3.5.12.2. SSH 48
3.5.13. Colección 48
3.5.13.1. Browser Session Hijacking 49
3.5.14. Comando y Control 50
3.5.14.1. Application Layer Protocol 50
3.5.14.2. Web Service 51
3.5.15. Exfiltración 52
3.5.15.1. Exfiltration Over Physical Medium 52
3.5.15.2. Exfiltration Over Web Service 53
3.5.16. Impacto 53
3.5.16.1. Data Destruction 54
3.5.16.2. Network Denial of Service 54
3.6. Tabla resumen de mitigaciones a implementar 55
3.7. Tabla resumen de detecciones a implementar 56
3.8. Conclusiones 57
3.9. A implementar en Estudio Práctico 58
3.9.1. Diagrama de redes e IT propuesto para Estudio Práctico 59
4. ESTUDIO PRÁCTICO 60
4.1. Objetivos 60
4.2. Mitigaciones 60
4.2.1. M1054: Software Configuration 60
4.2.2. M1017: User Training 61
4.2.3. M1050: Exploit Protection 62
4.2.4. M1021: Restrict Web-Based Content 63

4.2.5. M1026: Privileged Account Management 65
4.2.6. M1035: Limit Access to Resource Over Network 66
4.2.7. M1032: Multi-factor Authentication 66
4.2.8. M1030: Network Segmentation 68
4.2.9. M1049: Antivirus/Antimalware 69
4.2.10. M1018: User Account Management 69
4.3. Detecciones 71
4.3.1. DS0015: Application Log - Application Log Content 71
4.3.2. DS0029: Network Traffic - Network Connection Creation 71
4.3.3. DS0029: Network Traffic - Network Traffic Content 72
4.4. Conclusiones 73
5. PLIEGO DE CONDICIONES 74
5.1. Web Application Firewall 74
5.2. Firewall Palo Alto (capacidades firewall, IPS y VPN) 74
6. ESTUDIO ECONÓMICO 75
7. LÍNEAS DE FUTURO 76
7.1. Masterizar las herramientas implementadas 76
7.2. Implementación de un SIEM 76
7.3. Revisiones periódicas de la matriz 77
8. REFERENCIAS, BIBLIOGRAFÍA Y RECURSOS 78
ANEXO I: USANDO ATT&CAK NAVIGATOR 83
ANEXO II: AMPLIACIÓN ESTUDIO TEÓRICO 90
ANEXO III: AMPLIACIÓN ESTUDIO PRÁCTICO 113
ANEXO IV: IMPLEMENTACIÓN DE UN WAF EN AWS 119
ANEXO V: IMPLEMENTACIÓN DE VPN CON 2FA USANDO KEYCLOAK Y GOOGLE AUTHENTICATOR 138

INDICE DE FIGURAS

Figura 1 ATT&CK Matrix for Enterprise.Fuente: https://attack.mitre.org/ 21
Figura 2 Diagrama de relaciones general. Fuente: MITRE ATT&CK: Design and Philosophy..... 21
Figura 3: Diagrama de relaciones aplicado 22
Figura 4 Diagrama redes e IT 26
Figura 5 Sistema de Puntuación 29
Figura 6 Táctica Reconocimiento 30
Figura 7 Táctica Acceso Inicial..... 32
Figura 8 Táctica Ejecución 36
Figura 9 Táctica Persistencia 38
Figura 10 Táctica Escalado de Privilegios..... 40
Figura 11 Táctica Evasión de defensas 41
Figura 12 Táctica Acceso a Credenciales 42
Figura 13 Táctica Descubrimiento..... 45
Figura 14 Táctica Movimiento Lateral 47
Figura 15 Táctica Colección..... 49
Figura 16 Táctica Comando y Control..... 50
Figura 17 Táctica Exfiltración 52
Figura 18 Táctica Impacto..... 54
Figura 19 Diagrama Redes e IT para Estudio Práctico 59
Figura 20 Protección ante Phising mail..... 61
Figura 21 Configuración borrado de cookies al cerrar el navegador..... 61
Figura 22 Detección ejecución de archivo durante la navegación 63
Figura 23 Bloqueo de acceso a web maliciosa 64
Figura 24 Reporte bloque acceso a web maliciosa..... 64
Figura 25 Listas dinámicas Firewall Palo Alto 65
Figura 26 Usario raíz AWS sin 2FA 67
Figura 27 Solicitud 2FA consola AWS..... 67
Figura 28 Usuario raíz en AWS con 2FA configurado..... 67
Figura 29 2FA en dispositivo móvil para acceso a consola de AWS..... 67
Figura 30 VPCs independientes en AWS..... 68
Figura 31 Subredes de distintas VPCs en AWS 69
Figura 32 Bloqueo de web phising 69
Figura 33 Establecimiento de permisos para usuario IAM en AWS 70
Figura 34 Permisos relacionados con Route 53 en AWS..... 71
Figura 35 Controles de Selección 83
Figura 36 Controles de capa..... 84
Figura 37 Controles de Técnicas 84
Figura 38 Mitigación Antivirus y técnicas y subtécnicas afectadas 85
Figura 39 Técnicas y subtécnicas conocidas del grupo Blue MockingBird 86
Figura 40 Técnicas afectadas por mitigaciones 'Política de contraseñas'..... 87
Figura 41 Valores numéricos y color asociado..... 87

Figura 42 Capa ‘MFA’ 88
Figura 43 Sumado de capas 88
Figura 44 Política de contraseñas + MFA 89
Figura 45 Advanced Threat Protection Firewall Palo Alto 114
Figura 46 Inspección de ficheros en Firewall Palo Alto 114
Figura 47 Detalles instancia LightSail 119
Figura 48 Menú Account 120
Figura 49 Habilitar VPC Peering 120
Figura 50 Interconexión de VPCs 120
Figura 51 Crear VPC 121
Figura 52 Parámetros VPC 121
Figura 53 Subredes de una VPC 121
Figura 54 Elemento Grupo de destino 122
Figura 55 Tipo destino: IP adresses 122
Figura 56 Parámetros Target Group 123
Figura 57 IP y Puertos 123
Figura 58 Puertos 124
Figura 59 Objetivo correctamente detectado 124
Figura 60 Elemento Balanceador de carga 124
Figura 61 Elemento menú para LB 125
Figura 62 Parámetros Balanceador de Carga 125
Figura 63 Panel configuración LB 126
Figura 64 Seleccionar Grupos de Seguridad 126
Figura 65 Configurar Listener 127
Figura 66 Asociación de Recursos 128
Figura 67 Añadir reglas 128
Figura 68 Seleccionar reglas 129
Figura 69 Zonas alojadas 130
Figura 70 Crear Registros 130
Figura 71 configuración registro 130
Figura 72 Registros creados 131
Figura 73 JuiceShop accedido desde TOR 132
Figura 74 JuiceShop tras WAF accedido desde TOR 132
Figura 75 Formulario Login vulnerable 133
Figura 76 Cuenta Admin 133
Figura 77 Bloqueo inyección SQL 134
Figura 78 Payloads Usuario 135
Figura 79 Payloads Contraseñas 135
Figura 80 Credenciales detectadas 136
Figura 81 Credenciales no detectadas 137
Figura 82 Creación de un Realm 138
Figura 83 Creando el realm 139
Figura 84 Creación de usuario en un Realm 139

Figura 85 Creación cliente SAML 140
Figura 86 Configuración cliente SAML 141
Figura 87 Descargar fichero de configuración SAML 141
Figura 88 Flujo de autenticación 142
Figura 89 Añadir Google OTP 142
Figura 90 Elementos flujo de autenticación 142
Figura 91 Otros parámetros configurables 143
Figura 92 Requerir OTP para el usuario 144
Figura 93 Sincronización dispositivo móvil 145
Figura 94 Creación certificado como CA 146
Figura 95 Creación de Certificado firmado por nuestra CA 147
Figura 96 SSL/TLS profile 148
Figura 97 Carga de configuración SAML 148
Figura 98 Configuración SAML 149
Figura 99 Authentication Profile 150
Figura 100 Usuarios Authentication Profile 151
Figura 101 Interface Túnel 152
Figura 102 Configuración General Portal 153
Figura 103 Configuración Autenticación 153
Figura 104 Client Authentication 154
Figura 105 Resumen configuración 154
Figura 106 Configuración Agente Portal 155
Figura 107 External Gateway 155
Figura 108 Resumen Configuración 156
Figura 109 Configuración APP 156
Figura 110 Configuración General Gateway 157
Figura 111 Client Authentication Gateway 158
Figura 112 Configuración Agente Gateway 158
Figura 113 Autenticación Portal 159
Figura 114 Pool de IPs para clietes de la VPN 159
Figura 115 Inicio de conexión con cliente VPN (Global Protect) 160
Figura 116 Redirección hacia Keycloak 160
Figura 117 2FA con Google OTP en Keycloak 161
Figura 118 Cliente VPN Conectado 161
Figura 119 Ping a red Interna tras conexión con VPN 161
Figura 120 Añadir certificado de confianza en Windows 162
Figura 121 Error de autenticación en Keycloak 162
Figura 122 Deshabilitar requerimiento firma 163
Figura 123 Requerimientos flujo de autenticación 163
Figura 124 Habilitar autenticación en Zona del firewall 164
Figura 125 Generar y aceptar cookies entre gatewy y portal 164

INDICE DE TABLAS

Tabla 1 Mitigaciones Phising for information (Reconocimiento) 31
Tabla 2 Detecciones Phising for information (Reconocimiento) 31
Tabla 3 Mitigaciones Exploit Public Facing Applications (Acceso Inicial) 33
Tabla 4 Detecciones Exploit Public Facing Applications (Acceso Inicial) 33
Tabla 5 Mitigaciones External Remote Services (Acceso Inicial) 34
Tabla 6 Detecciones External Remote Services (Acceso Inicial) 34
Tabla 7 Mitigaciones Valid Accounts (Acceso Inicial) 35
Tabla 8 Detecciones Valid Accounts (Acceso Inicial) 35
Tabla 9 Mitigaciones JavaScript (Ejecución) 36
Tabla 10 Mitigaciones Powershell (Ejecución) 37
Tabla 11 Mitigaciones Additional Cloud Credentials (Persistencia) 38
Tabla 12 Detecciones Additional Cloud Credentials (Persistencia) 39
Tabla 13 Mitigaciones Addional Cloud Roles (Persistencia) 39
Tabla 14 Detecciones Addional Cloud Roles (Persistencia) 39
Tabla 15 Mitigaciones File and Directory Permissions Modification (Evasión de Defensas) 41
Tabla 16 Mitigaciones y Detecciones Fuerza Bruta (Acceso a Credenciales) 43
Tabla 17 Mitigaciones Explotation for Credential Access (Acceso a Credenciales) 44
Tabla 18 Detecciones Explotation for Credential Access (Acceso a Credenciales) 44
Tabla 19 Mitigaciones Cloud Account (Descubrimiento) 45
Tabla 20 Mitigaciones Network Sniffing (Descubrimiento) 46
Tabla 21 Mitigaciones y Detecciones Remote Desktop Protocol (Movimiento Lateral) 47
Tabla 22 Mitigaciones SSH (Movimiento Lateral) 48
Tabla 23 Detecciones SSH (Movimiento Lateral) 48
Tabla 24 Mitigaciones Browser Session Hijacking 49
Tabla 25 Mitigaciones Application Layer Protocol (Comando y Control) 51
Tabla 26 Detecciones Application Layer Protocol (Comando y Control) 51
Tabla 27 Mitigaciones Web Service (Comando y Control) 51
Tabla 28 Detecciones Web Service (Comando y Control) 51
Tabla 29 Mitigaciones Exfiltration Over Physical Medium (Exfiltración) 53
Tabla 30 Mitigaciones Exfiltration Over Web Service (Exfiltración) 53
Tabla 31 Exfiltration Over Web Service (Exfiltración) 53
Tabla 32 Mitigaciones Data Destruction (Impacto) 54
Tabla 33 Mitigaciones Network Denial of Service (Impacto) 55
Tabla 34 Detecciones Network Denial of Service (Impacto) 55
Tabla 35 Tabla resumen de mitigaciones a implementar 56
Tabla 36 Tabla resumen de detecciones a implementar 57
Tabla 37 Presupuesto 75
Tabla 38 Mitigaciones Drive-by compromise (Acceso Inicial) 93
Tabla 39 Detecciones Drive-by compromise (Acceso Inicial) 93
Tabla 40 Mitigaciones Phising (Acceso Inicial) 94
Tabla 41 Detecciones Phising (Acceso Inicial) 94

Tabla 42 Mitigaciones Python (Ejecución) 95
Tabla 43 Mitigaciones User Execution (Ejecución) 95
Tabla 44 Detecciones User Execution (Ejecución) 95
Tabla 45 Mitigaciones Browser Extensions (Persistencia) 97
Tabla 46 Detecciones Browser Extensions (Persistencia) 97
Tabla 47 Mitigaciones Compromise Client Software Binary (Persistencia) 98
Tabla 48 Mitigaciones Cloud Account (Persistencia) 98
Tabla 49 Detecciones Cloud Account (Persistencia)..... 98
Tabla 50 Mitigaciones Local Account (Persistencia) 99
Tabla 51 Detecciones Local Account (Persistencia) 99
Tabla 52 Mitigaciones External Remote Services (Persistencia) 100
Tabla 53 Detecciones External Remote Services (Persistencia) 100
Tabla 54 Mitigaciones Valid Accounts (Persistencia)..... 101
Tabla 55 Detecciones Valid Accounts (Persistencia)..... 101
Tabla 56 Mitigaciones Valid Accounts (Escalado de Privilegios) 103
Tabla 57 Detecciones Valid Accounts (Escalado de Privilegios)..... 103
Tabla 58 Mitigaciones Valid Accounts (Evasión de Defensas)..... 104
Tabla 59 Detecciones Valid Accounts (Evasión de Defensas)..... 104
Tabla 60 Mitigaciones Adversary in the Middle (Credential Access)..... 105
Tabla 61 Detecciones Adversary in the Middle (Credential Access) 105
Tabla 62 Mitigaciones Credentials from Password Stores (Credential Access)..... 106
Tabla 63 Mitigaciones Forced Authentication (Acceso a Credenciales)..... 106
Tabla 64 Detecciones Forced Authentication (Acceso a Credenciales)..... 107
Tabla 65 Mitigaciones Forge Web Credentials (Acceso a Credenciales)..... 107
Tabla 66 Detecciones Forge Web Credentials (Acceso a Credenciales) 107
Tabla 67 Mitigaciones Multi-Factor Authentication Request Generation (Acceso a Credenciales)..... 108
Tabla 68 Mitigaciones Network Service Discovery (Descubrimiento) 110
Tabla 69 Detecciones Network Service Discovery (Descubrimiento)..... 111
Tabla 70 Mitigaciones Exploitation of Remote Services (Movimiento Lateral) 111
Tabla 71 Detecciones Exploitation of Remote Services (Movimiento Lateral) 111
Tabla 72 Mitigaciones Exfiltration Over alternative Protocol (Exfiltración)..... 112
Tabla 73 Detecciones Exfiltration Over Alternative Protocol (Exfiltración) 112

1. INTRODUCCIÓN

Que vivimos en una sociedad digitalizada es un hecho ante el que ya nadie se sorprende. El nivel de simbiosis del ser humano con las capacidades informáticas actuales no sólo no tiene marcha atrás, sino que avanza a pasos agigantados.

Estas capacidades informáticas, a muy grandes rasgos, serían la ejecución de tareas de manera automática, atendiendo a una lógica programada para trabajar con la información que recibe y/o genera, y su almacenado y presentación.

Cualquier avance en campos como medicina, arquitectura o mecánica (y un largo etcétera) está ligado actualmente a capacidades informáticas que ayudan a su progreso. Por otro lado, tenemos aquellos campos que directamente nacen y se soportan íntegramente gracias a estas capacidades informáticas, como las telecomunicaciones modernas o la inteligencia artificial.

Dentro de esta realidad en la que prácticamente cualquier ámbito está relacionado de alguna manera con la informática, uno de los actores principales son las empresas. Ya quedaron atrás aquellos tiempos en los que las empresas se pensaban dar o no el salto digital. Ahora la pregunta es ¿cómo voy a digitalizar mi empresa? ¿qué tecnologías debo usar? O incluso ¿puede mi negocio estar basado íntegramente en estas capacidades informáticas? ¿qué oportunidades me brinda la informática para crear un negocio y vivir de él?

Tras estas observaciones, nos encontramos inevitablemente con el concepto de la seguridad informática. Si tan estrecha es la relación de las empresas con la informática, el concepto de seguridad informática, ¿afecta a las empresas? La respuesta es clara, rotundamente sí. (Por definición, se considerará que la seguridad informática pretende garantizar [1] la confidencialidad, integridad y disponibilidad de la información y, además, en cuanto a su relación con los usuarios, esta información podrá ser autenticada, autorizada y no repudiable).

Cualquier empresa que actualmente cuente con sistemas informáticos debería proteger dichos sistemas y su información. Dependiendo del grado de informatización de

la empresa, la totalidad de su ejercicio podría estar en peligro si no se toman las medidas de seguridad necesarias.

Ante esta situación de riesgo o incluso catástrofe, surgen preguntas como ¿qué pueden hacer las empresas para protegerse? ¿cómo pueden aplicarse medidas de seguridad informática? ¿qué deben proteger? O preguntas para los profesionales del sector de la seguridad como ¿qué medidas pueden aplicarse para proteger a una empresa y cómo? ¿Qué garantías se tiene de que esas medidas funcionan? ¿Pueden justificarse al empresario para que tenga confianza en las mismas?

Por suerte, existe respuesta a estas y otras preguntas relacionadas que pudieran surgir. Esta respuesta es el uso de marcos de trabajo (frameworks) de seguridad, los cuales están especialmente diseñados para ayudar a la implantación de la seguridad informática en diferentes ámbitos, como por ejemplo gobiernos, administraciones públicas o empresas. Y aunque nunca se puede o se debe considerar un sistema informático como 100% seguro, el uso de estos frameworks ayudará a implantar medidas de seguridad que bien pueden permitirnos cierto grado de fiabilidad y garantías en cuanto a resultados obtenidos tras su aplicación.

Una lista muy completa y actualizada de los frameworks más utilizados en la actualidad, sus diferentes aplicaciones y una breve descripción de estos puede encontrarse en [2].

1.1. Motivación

Las empresas son hoy por hoy uno de los principales objetivos de los atacantes informáticos. El robo o exposición de la información de las empresas puede suponer ventajas de mercado para los competidores y un daño considerable a la actividad y reputación de una empresa.

Dada la importancia de aplicar medidas de defensa, resulta motivador ser capaz de estudiar y aplicar alguno de estos frameworks y conseguir que una empresa esté protegida ante las amenazas existentes en la mayor medida posible.

De entre todos los frameworks disponibles, llama la atención por su enfoque el framework MITRE ATT&CK Enterprise, que basa sus capacidades defensivas atendiendo a las acciones que realizan los atacantes y los objetivos de estos cuando atacan empresas. Esto nos permite enfocarnos no sólo en cómo debería protegerse una empresa, si no en cómo se puede detectar y responder frente a ataques, puesto que contamos con una base de datos que describe de manera minuciosa cómo actúa un atacante a lo largo de todo el ciclo de vida de un ataque.

1.2. Objetivos

Los objetivos del presente Trabajo Fin de Máster, de acuerdo con las competencias requeridas por la titulación, son:

- Estudiar la matriz Mitre ATT&CK Enterprise, su estructura, funcionamiento y aplicación.
- Realizar un estudio teórico de la aplicación de la Mitre ATT&CK Enterprise en una empresa.
- Aplicar de manera práctica en la empresa el estudio teórico realizado o parte del mismo.
- Realizar un informe en el que se documenten los resultados de los estudios realizados y su aplicación práctica.

1.3. Estructura del documento

El presente documento cuenta con la siguiente estructura, en orden de aparición:

a) Una descripción del framework MITRE ATT&CK Enterprise que pretende ayudar al lector a comprender el funcionamiento y la estructura de este.
b) Un estudio teórico aplicado a una empresa en el que se aplicará el framework MITRE ATT&CK para analizar las fallas defensivas de la empresa.
c) Un estudio práctico en el que se aplicarán medidas defensivas y de detección, basándose en las fallas descubiertas en el estudio teórico previo.
d) Un Pliego de Condiciones reflejando las herramientas utilizadas para el desarrollo de este TFM.

e) Un Estudio Económico reflejando el coste de este TFM.
f) Un apartado exponiendo las Líneas de Futuro aplicables y/o recomendadas tras la realización de este TFM.
g) Un apartado de referencias, bibliografía y recursos utilizados.
h) Finalmente, se adjuntan un conjunto de anexos que profundizan la información expuesta en determinados puntos del documento, complementando su información tanto teórica como práctica.

2. MITRE ATT&CK ENTERPRISE

En este apartado se describe brevemente el framework MITRE ATT&CK Enterprise, su estructura, casos de uso y algunas herramientas que permiten su aplicación.

2.1. Definición y características

MITRE ATT&CK es una base de conocimiento y marco de trabajo globalmente accesible que se basa en las tácticas, técnicas y subtécnicas empleadas por ciber atacantes. ATT&CK se centra en cómo los ciber atacantes operan y comprometen sistemas y redes de información, reflejando las fases del ciclo de vida de los ataques y las plataformas comúnmente atacadas.

Está desarrollada y mantenida de forma activa por la organización MITRE, toda una eminencia dentro del mundo de la ciberseguridad que, entre otras actividades relevantes, destacan por ser los responsables del mantenimiento de las CVE (Common Vulnerabilities and Exposures). Una base de datos en la que se pueden encontrar prácticamente todas las vulnerabilidades actuales conocidas [3].

La aplicación de tácticas, técnicas y subtécnicas permite desarrollar un modelo de amenazas y metodologías aplicable al sector privado, gobiernos y a toda la comunidad de productos y servicios de ciberseguridad. ATT&CK proporciona una taxonomía común para ataque y defensa, y se ha convertido en una herramienta conceptual muy útil en múltiples disciplinas de la seguridad informática, proporcionando inteligencia para el modelado de amenazas, realización de pruebas de red teaming o emulación de adversarios y para mejorar las defensas de redes y sistemas frente a intrusiones.

A grandes rasgos y considerando los más importantes, ATT&CK consta de los siguientes componentes:

- **Tácticas**: Los objetivos de un atacante. Una descripción más detallada de todas las tácticas se presentará en el estudio teórico.
- **Técnicas**: Los métodos usados por un atacante para desarrollar y conseguir aplicar las tácticas. Una descripción más detallada de las técnicas vistas se presentará en el estudio teórico.

- **Subtécnicas**: Describen métodos más específicos dentro de las propias técnicas usadas. Una descripción más detallada de las subtécnicas vistas se presentará en el estudio teórico.
- **Procedimientos**: Hacen referencia a las implementaciones específicas que los atacantes han usado para usar las técnicas y las subtécnicas.
- **Grupos**: Representan a atacantes conocidos que son rastreados por organizaciones públicas y privadas y reportados en informes de inteligencia de amenazas.
- **Software**: Herramientas y Malware de código abierto, de pago o propias, que los atacantes usan durante las intrusiones.
- **Mitigaciones**: Conceptos de seguridad o tecnologías que pueden ser usadas para evitar la ejecución exitosa de técnicas o subtécnicas. Las mitigaciones en ATT&CK tienen la siguiente estructura:
  - ID: Identificador de mitigación.
  - Mitigación: Nombre de la mitigación.
  - Descripción: Descripción de la acción o concepto a implementar.
- **Detecciones**: Conceptos que pueden ser monitorizados y que ayudan a detectar, prevenir y actuar frente a ataques. Las detecciones en ATT&CK tienen la siguiente estructura:
  - ID: Identificador de detección.
  - Data Source: La fuente de datos a monitorizar o detectar.
  - Data Component: Componente específico dentro de la fuente de datos.
  - Detects: Descripción concreta del aspecto a monitorizar y/o detectar.

Se muestra a continuación una imagen la matriz MITRE ATT&CK Enterprise para dar una idea de su magnitud. Cabe mencionar que en la imagen todas las técnicas se encuentran plegadas, por lo que no se muestran las subtécnicas de cada técnica. Toda la información relativa a la matriz puede encontrarse en [4].

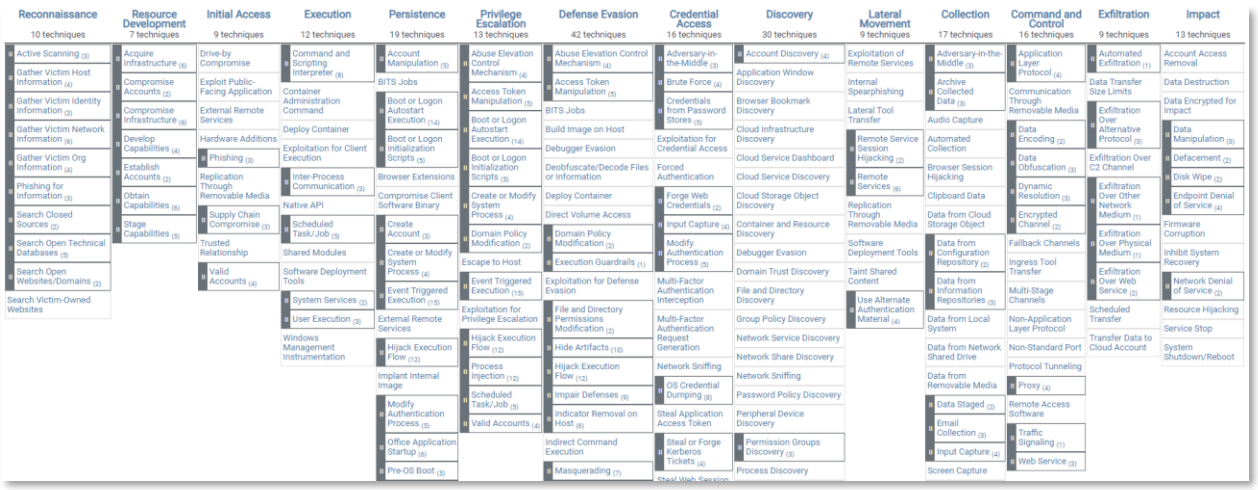


Figura 1 ATT&CK Matrix for Enterprise. Fuente: https://attack.mitre.org/

2.2. Modelo de Relaciones

Todos los componentes previamente vistos, están relacionados entre sí atendiendo al siguiente diagrama de relaciones:

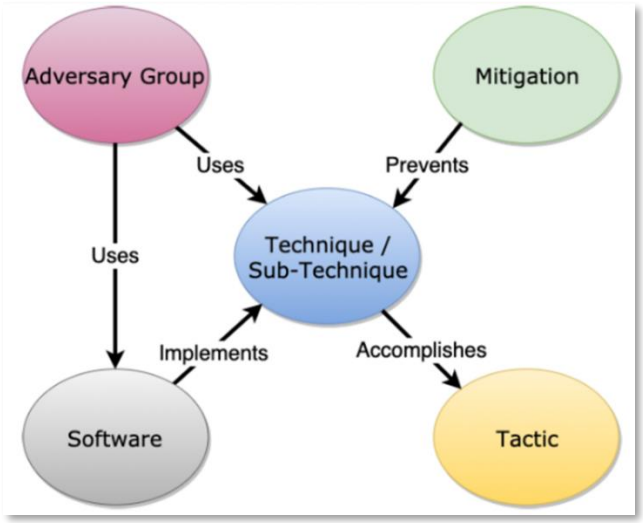


Figura 2 Diagrama de relaciones general. Fuente: MITRE ATT&CK: Design and Philosophy

Un ejemplo de aplicación de este diagrama sería el siguiente:

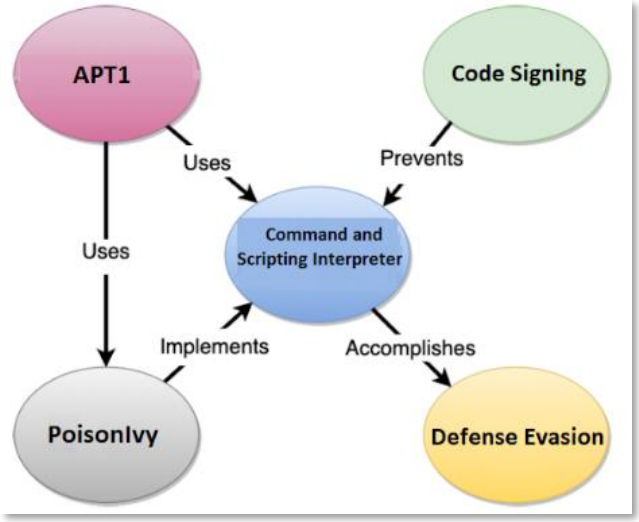


Figura 3: Diagrama de relaciones aplicado

2.3. Casos de uso

Ante la pregunta de para qué o cómo puede usarse la MITRE ATT&CK, tenemos que los casos de uso más comunes son:

a) **Emulación de adversarios**: Consiste en realizar una evaluación de la seguridad en un dominio tecnológico aplicando inteligencia de ciber amenazas. Se trata de replicar las acciones de uno o varios grupos de atacantes y la forma en la que operan. Se pretende así poner el foco en la habilidad de una organización para detectar y/o mitigar las acciones de los atacantes a lo largo del ciclo de vida del ataque.

b) **Red teaming**: Aplicar el modus operandi de determinados grupos de adversarios a la hora de realizar los ejercicios de red teaming.

c) **Desarrollo de analíticas de comportamiento**: Detectar comportamientos potencialmente maliciosos dentro de un sistema o de una red, de los cuales se podría o no tener conocimiento previo.

d) **Evaluación de fallas defensivas**: Permite a una organización evaluar y/o detectar sus puntos débiles y potenciales vectores de entrada para los adversarios. La identificación de estos puntos débiles ayudará a priorizar las

mitigaciones o detecciones que se decidan implementar para la defensa y por tanto también a la hora de decidir en aquello en lo que la empresa va a invertir.

e) **Evaluación de madurez de un SOC**: Permite determinar cuán efectivo es el SOC de una compañía en cuanto a detecciones, análisis y respuesta ante intrusiones.
f) **Enriquecimiento de inteligencia sobre ciber amenazas**: Permite reconocer cuál es la situación de una compañía frente a un determinado grupo de amenazas o frente a amenazas concretas (malware, determinadas herramientas, etc.).

2.4. Herramientas para trabajar con MITRE ATT&CK Enterprise

Se describen en este apartado algunas herramientas útiles a la hora de trabajar con el framework MITRE ATT&CK Enterprise:

a) **ATT&CK Navigator**: Es una aplicación web que se usa para anotaciones y exploración de la matriz ATT&CK. Puede utilizarse para visualizar las defensas que se pretenden implementar o las vulnerabilidades que se pretenden cubrir, para planificar ejercicios de red/blue teaming, realizar un modelado de amenazas y/o para visualizar la frecuencia de técnicas detectadas, entre otras utilidades. Todo ello con el objetivo de facilitar la exploración de la matriz de una manera sencilla y visual (codificar con colores, añadir comentarios, asignar valores numéricos, etc.). Puede adquirirse para descarga o para trabajar online en [5].
   Es la única herramienta que usaremos para este trabajo, siendo esta suficiente para alcanzar los objetivos propuestos.
   Una ampliación de información sobre ATT&CK Navigator y algunos ejemplos de uso puede encontrarse en el ‘ANEXO I: Usando ATT&CK Navigator’.
b) **DeTTECT**: Comúnmente conocido como MITRE DeTTECT. Aunque oficialmente no es una herramienta desarrollada por MITRE, sí que está diseñada para ser usada en conjunto con MITRE ATT&CK y servir de complemento. DeTTECT tiene como objetivo servir de ayuda a los blue teams a la hora de usar ATT&CK, permitiendo puntuar y comparar fuentes de datos de logs, visibilidad de la cobertura de amenazas, cobertura de detecciones y comportamiento de adversarios. Está desarrollado en Python y usa archivos YAML. Estos archivos

YAML pueden convertirse en archivos JSON que son interpretados por MITRE Navigator. Más información relacionada y los archivos de descarga pueden encontrarse en [6], la página oficial del proyecto.

c) **MITRE CALDERA**: Es un framework desarrollado por MITRE y basado en MITRE ATT&CK que permite ejecutar ejercicios de simulación de brechas de seguridad. También se usa para realizar ejercicios de red y blue teaming y de respuesta ante incidentes. Está formado por el core del sistema (código del framework incluyendo una API REST y una interfaz web) y diversos Plugins (repositorios que pueden acoplarse en el core añadiendo funcionalidades adicionales). Puede encontrarse más información y los elementos necesarios para su implementación en [7], la página oficial del proyecto.

d) **Atomic Red Team**: Es una librera open-source para pruebas que puede ser usada por los equipos de seguridad para simular actividad de atacantes en sus redes o entornos en general. Puede encontrarse más información y la librería misma en [8], la página oficial del proyecto.

3. ESTUDIO TEÓRICO

En este apartado se desarrolla un estudio teórico de la MITRE ATT&CK Enterprise aplicado a una empresa y usando el framework como evaluador de fallas defensivas. Se comenzará con una descripción de la empresa y sus características para conocer así su situación actual y facilitar la identificación de fallas y necesidades.

Posteriormente se continuará con el estudio teórico en si mismo, en el cual se estudiarán las tácticas, técnicas y subtécnicas para comprender cómo la empresa se ve afectada por estas.

3.1. Empresa caso de estudio

Se describen a continuación las características y situación actual de la empresa, el objetivo es tener una visión general que permita justificar ante los responsables de la empresa las observaciones que se hagan a lo largo del estudio teórico y facilitar a la empresa la toma de decisiones a la hora de la implementación de medidas.

3.2. Descripción y características de la empresa

Para la aplicación del estudio teórico y práctico del presente trabajo, hemos elegido una empresa a la que llamaremos XYZ. Las principales características de la empresa se describen a continuación:

- Entre 10 y 20 empleados.
- Trabajo en oficina y necesidad de implementación de trabajo remoto. Las conexiones remotas se realizarán desde equipos propiedad de la empresa en la mayoría de los casos, pero habrá ocasiones en las que se deban de permitir conexiones desde equipos que no están bajo control de la empresa (algunos empleados, clientes, socios, etc.).
- Se dedica al desarrollo de aplicaciones web (en cuanto a la parte que nos interesa para este estudio teórico-práctico).
- Aplicaciones web alojadas en la nube. Concretamente usando los servicios de AWS (Amazon Web Services).

- En las oficinas cuentan con varios servidores para el alojamiento de información y existen 10 PCs que cuentan con el sistema operativo Windows 10.
- Todos los clientes residen en España y las aplicaciones web sólo esperan conexiones desde el territorio nacional.
- Conexión a Internet mediante proveedor local de servicios. La conexión a la red se realiza mediante el router proporcionado por el Proveedor de Servicios de Internet (ISP).
- Las aplicaciones alojadas en la nube permiten conexiones HTTP y HTTPS.
- Las máquinas virtuales en las que se alojan las aplicaciones son instancias de LightSail (servicio de AWS) que permiten conexiones HTTP, HTTPS y SSH.

3.3. Diagrama de redes e IT

En la imagen siguiente se describe la situación actual de la empresa en cuanto al uso de redes e Internet.

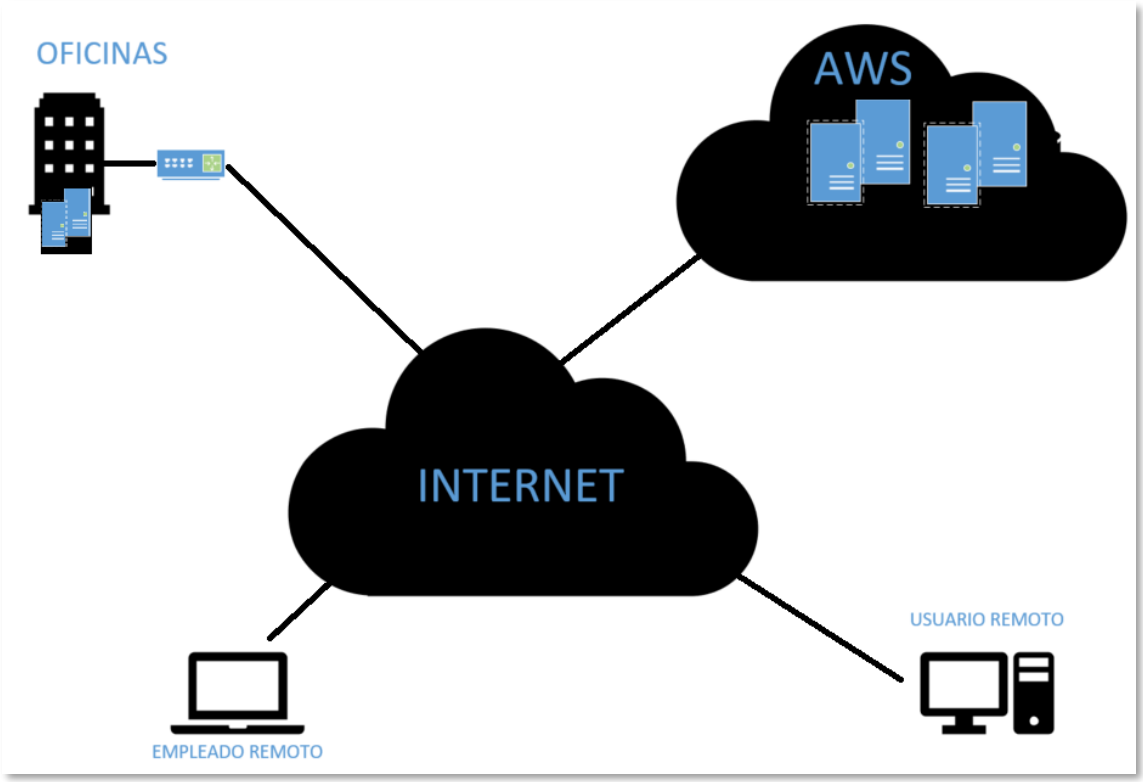


Figura 4 Diagrama redes e IT

El entorno de red actual en el que opera la empresa se describe como:

- Conexión a Internet desde la oficina de la empresa usando como puerta de enlace el router que proporciona el ISP.
- Los empleados no pueden acceder a la red de la oficina de manera remota.
- Cuando los empleados acceden a AWS o a cualquier otro lugar de Internet sin estar en la oficina, lo hacen usando sus propias conexiones a Internet (en casa, hotspot de datos móviles) y trabajan con información de la empresa.
- En la oficina se almacena información.
- El entorno de gestión de servicios en la nube de AWS en el que se alojan las aplicaciones web y con el que se conecta para todo lo relacionado con las mismas, es accesible públicamente mediante credenciales.
- Las aplicaciones web alojadas en AWS son accesibles públicamente mediante credenciales.

3.4. Primeras conclusiones y propuestas

Del análisis de las características, requisitos y situación actual de la empresa, se deducen diferentes necesidades de seguridad con diferentes prioridades que han de ser expuestas a los responsables de la empresa. Estas pueden resumirse en:

- Proteger las aplicaciones web. Prioridad: Muy urgente.
- Protección de credenciales. Prioridad: Muy Urgente.
- Proteger la red de la oficina y los datos almacenados en los servidores de la oficina. Prioridad: Urgente.
- Proteger los equipos de trabajo de la oficina y los equipos usados para conexiones remotas con la oficina. Prioridad: Urgente.
- Implementar y proteger las capacidades de conexiones remotas, con vistas principalmente a capacidades de trabajo remoto. Prioridad: Urgente.

Para nuestro estudio teórico, debemos tener en cuenta estas primeras necesidades detectadas y tratar de relacionarlas con las tácticas, técnicas y subtécnicas a medida que se vayan estudiando.

3.5. Desarrollo del Estudio Teórico

En este punto se describe el estudio teórico realizado sobre la matriz MITRE ATT&CK Enterprise, aplicado a la empresa descrita previamente.

3.5.1. Caso de estudio y objetivos

Para el presente estudio teórico, se usará la matriz MITRE ATT&CK Enterprise como **evaluador de fallas defensivas** en la empresa propuesta.

Los objetivos a la hora de usar la matriz MITRE ATT&CK Enterprise como el caso de estudio propuesto, son:

a) Evaluar la eficiencia de la Matriz MITRE ATT&CK Enterprise como evaluador de fallas defensivas.
b) Evaluar características de la matriz MITRE ATT&CK Enterprise tales como:

- Complejidad de uso.
- Alcance, profundidad y detalle de la matriz.
- Conocimientos obtenidos con su uso.

c) Evaluar el framework en general a través del caso de estudio particular.
d) Obtener conclusiones firmes sobre el uso de la matriz como evaluador de fallas defensivas y como framework de trabajo para ciberseguridad en general.

3.5.2. Estructura del Estudio Teórico

En este estudio teórico, se han repasado todas las tácticas y sus correspondientes técnicas y subtécnicas, pretendiendo conocer cuáles son las que más afectan a la empresa y cuáles deberían ser las medidas a aplicar. Para ello, se ha definido un sistema sencillo de puntuación que se irá aplicando a lo largo del recorrido de la matriz. El sistema de puntuación definido es el siguiente:

Importancia	Color	Puntuación	Mitigaciones	Detecciones
Muy Alta		1	Sí	Sí o todas las posibles
Alta		2	Sí o parcialmente	Sí o parcialmente
Media		3	Parcialmente	Parcialmente
Baja		4	Parcialmente / No	No
Muy Baja		5	No	No

Figura 5 Sistema de Puntuación

Para el análisis de cada táctica se mostrará:

- Descripción de la táctica.
- Una imagen de la táctica en la matriz mostrando las técnicas y/o subtécnicas seleccionadas para su tratamiento, con el color de la puntuación dada.
- Una breve descripción de la técnica o subtécnica.
- La puntuación dada a las técnicas y/o subtécnicas.
- Justificación de la puntuación dada a cada técnica y/o subtécnicas.
- Una tabla incluyendo las Mitigaciones, su ID y mitigación aplicable.
- Una tabla incluyendo las detecciones su ID, fuente de datos y el componente.

Si se marca una técnica significa que se incluyen con la misma puntuación todas las subtécnicas y se incluirán justificaciones y decisiones generales para el grupo técnica/subtécnicas.

Es una primera toma de contacto, y muchas cosas se desconocían al momento de realizar el estudio, por lo que marcarlas como baja o muy baja sigue siendo importante, ya que será en algunos casos la primera toma de contacto con, por ejemplo, determinadas herramientas de detección, y quizás estás herramientas de detección sirvan para completar muchísimas detecciones en unas futuras revisiones de la matriz.

Por cuestiones de coherencia con la matriz original, únicamente se ha traducido al español el nombre de las tácticas. Todas las técnicas y subtécnicas se muestran en inglés, facilitando así la comprensión y cualquier actividad comparativa, de búsqueda o de cualquier otra índole que pudiese realizar el lector de este documento.

NOTA: Por cuestiones de espacio y con el objetivo de mantener una extensión adecuada de este documento, para cada táctica se mostrará el análisis realizado sobre algunas de sus técnicas y/o subtécnicas. El estudio teórico al completo, incluyendo todas las técnicas y subtécnicas estudiadas que no se muestran en este punto, puede encontrarse en el 'ANEXO II: Ampliación Estudio Teórico'.

3.5.3. Reconocimiento

El atacante intenta recopilar información que será de utilidad en las operaciones que se realizarán posteriormente. Consiste en técnicas de recopilación de información sobre el objetivo a atacar. Dichas técnicas, podrán ser tanto activas como pasivas.

La información recopilada por el atacante incluye detalles de la organización a atacar, su infraestructura, IPs, empleados, socios, relaciones, etc. Esta información será usada por el atacante para planear la ejecución del Acceso Inicial, priorizar objetivos a comprometer o incluso para servir de guía para profundizar más en la fase de reconocimiento.

Figura 6 Táctica Reconocimiento

3.5.3.1. Phising for Information

Los atacantes realizan actividades de Phishing sobre sus víctimas con el objetivo de obtener información de valor (credenciales, direcciones de correo, nombres, etc.).

Puntuación: 2. Importancia Alta. Es un riesgo real y que se enfrenta diariamente.

Justificación

Los intentos de Phishing en la actualidad por parte de los atacantes son una de las técnicas más usadas y en caso de resultar exitosas (Ej: robo de credenciales), pueden tener consecuencias muy graves.

MITIGACIONES	
ID	Mitigación
M1054	Software Configuration
M1017	User Training

Tabla 1 Mitigaciones Phising for information (Reconocimiento)

DETECCIONES		
ID	Fuente de datos	Componente
DS0029	Network Traffic	Network Traffic Content
		Network Traffic Flow

Tabla 2 Detecciones Phising for information (Reconocimiento)

3.5.4. Desarrollo de Recursos

El atacante trata de establecer recursos que serán usados para dar soporte a sus operaciones.

Para ello el atacante usará técnicas que le permitan crear, adquirir, comprometer o apropiarse ilegalmente de recursos que serán usados para dar soporte a las actividades de ataque. Estos recursos pueden ser infraestructura, cuentas de usuario o capacidades. Todos los recursos desarrollados y/o adquiridos serán usados en otras fases del ciclo de vida del ataque.

Frente a esta táctica no va a tomarse ningún tipo de medida frente a técnicas o subtécnicas.

Justificación

La mayoría de las mitigaciones y detecciones suponen un esfuerzo que la empresa no está dispuesta a asumir dado que los beneficios de hacerlo no están claros o no se prevé que vayan a ser significativos.

Las técnicas y subtécnicas de esta táctica están fuera del alcance de la empresa, tanto a la hora de su mitigación como de su detección.

3.5.5. Acceso Inicial

El atacante intenta ganar acceso a la red interna.

Consiste en técnicas que usan diferentes vectores de entrada que permitan obtener un punto de apoyo inicial dentro de la red atacada. De un acceso inicial pueden derivarse la adquisición de un punto de entrada fijo, cómo credenciales de cuentas, puertas traseras o uso de servicios remotos.

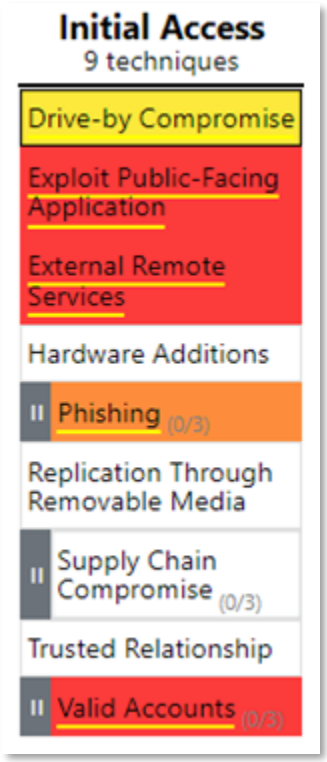


Figura 7 Táctica Acceso Inicial

3.5.5.1. Exploit Public Facing Applications

Los atacantes tratan de tomar ventaja y explotar posibles debilidades en equipos o aplicaciones que estén expuestos en Internet.

Puntuación: 1. Importancia Muy Alta. La empresa cuenta con Aplicaciones expuestas públicamente.

Justificación

Una de las actividades principales de la empresa se basa en el desarrollo de aplicaciones web, y en la actualidad estas cuentan únicamente con la protección que brinda el código en el que están codificadas y el propio firewall que ofrece el vendedor AWS. Este firewall únicamente impide conexiones en puertos que no sean el 22 (SSH), 80 (HTTP) y 443 (HTTPS), pero no está realizando un análisis del tráfico que entra en la red por esos puertos.

Dada la actividad de la empresa y la situación actual, medidas de mitigación y detección frente a esta técnica se consideran imprescindibles.

MITIGACIONES	
ID	Mitigación
M1050	Exploit Protection
M1026	Privileged Account Management
M1051	Update Software
M1016	Vulnerability Scanning

Tabla 3 Mitigaciones Exploit Public Facing Applications (Acceso Inicial)

DETECCIONES		
ID	Fuente de datos	Componente
DS0015	Application Log	Application Log Content
DS0029	Network Traffic	Network Traffic Content

Tabla 4 Detecciones Exploit Public Facing Applications (Acceso Inicial)

3.5.5.2. External Remote Services

Los atacantes tratan de aprovechar el uso de servicios expuestos en Internet y que podrían dar acceso a redes internas.

Puntuación: 1. Importancia Muy Alta. Se pretende en la empresa implementar capacidades de acceso remoto.

Justificación

Abrir los puertos en el router de la oficina y redirigir conexiones a equipos en la red interna para tener acceso a los equipos de la oficina no es una opción que se contemple de ninguna manera. Esto supondría una invitación al desastre más absoluto.

Si se necesitan accesos remotos a equipos y ficheros en la oficina, por causas de teletrabajo o accesos fuera del horario de trabajo normal, esto se hará bajo conexiones protegidas y cifradas mediante el uso de VPNs.

MITIGACIONES	
ID	Mitigación
M1035	Limit Access to Resource Over Network
M1032	Multi-factor Authentication
M1030	Network Segmentation

Tabla 5 Mitigaciones External Remote Services (Acceso Inicial)

DETECCIONES		
ID	Fuente de datos	Componente
DS0015	Application Log	Application Log Content
DS0029	Network Traffic	Network Traffic Flow

Tabla 6 Detecciones External Remote Services (Acceso Inicial)

3.5.5.3. Valid Accounts

Los atacantes tratan de ganar acceso usando cuentas válidas y/o credenciales comprometidas.

Puntuación: 1. Importancia Muy Alta. Se tratará de evitar a toda costa que atacantes consigan credenciales válidas.

Justificación

Por la actividad de la empresa, el uso de credenciales y la existencia de formularios de acceso público están muy presentes y son ampliamente usados:

Las aplicaciones web son accesibles previa autenticación y los formularios de login están expuestos públicamente al acceder a las aplicaciones.

El acceso a la consola de AWS se realiza mediante credenciales. Este acceso es público y es el mismo para todos los usuarios de AWS.

El acceso a la VPN se realizará mediante autenticación usando credenciales en el cliente VPN.

MITIGACIONES	
ID	Mitigación
M1013	Application Developer Guidance
M1027	Password Policies
M1026	Privileged Account Management
M1018	User Account Management
M1017	User Training

Tabla 7 Mitigaciones Valid Accounts (Acceso Inicial)

DETECCIONES		
ID	Fuente de datos	Componente
DS0028	Logon Session	Logon Session Creation
DS0002	User Account	User Account Authentication

Tabla 8 Detecciones Valid Accounts (Acceso Inicial)

3.5.6. Ejecución

El atacante intenta ejecutar código malicioso.

Consiste en técnicas mediante las cuales ejecutar código malicioso, controlado y definido por el atacante, en sistemas locales o remotos. La ejecución de este código permitirá al atacante alcanzar otros objetivos tales como la exploración de la red objetivo de ataque o el robo/exfiltración de información, entre otros.

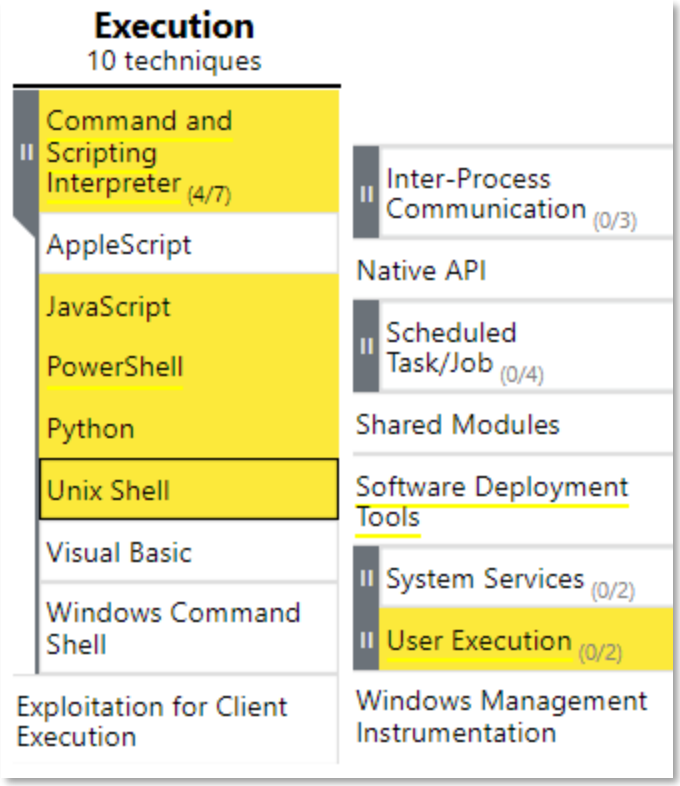


Figura 8 Táctica Ejecución

3.5.6.1. JavaScript

Los atacantes realizan acciones que implican el uso del lenguaje JavaScript, lenguaje que puede ser utilizado tanto en navegadores como entornos fuera de los mismos.

Puntuación: 3. Importancia Media. Subtécnica para tener en cuenta y algunas mitigaciones de fácil implementación.

Justificación

Los desarrolladores de la empresa utilizan JavaScript en sus tareas de desarrollo diarias y además es un lenguaje ampliamente usado en los navegadores actuales.

MITIGACIONES	
ID	Mitigación
M1021	Restrict Web-Based Content

Tabla 9 Mitigaciones JavaScript (Ejecución)

Detecciones: No. La implementación de las detecciones necesarias no se contempla por el momento debido a sus requisitos técnicos.

3.5.6.2. PowerShell

Los atacantes podrían usar la herramienta PowerShell (en equipos Windows) para ejecutar acciones determinadas.

Puntuación: 3. Importancia Media. Subtécnica para tener en cuenta y algunas mitigaciones de fácil implementación.

Justificación

Es una herramienta incluida en los Sistemas Windows, por lo que está presente en todos los ordenadores de la oficina.

MITIGACIONES	
ID	Mitigación
M1049	Antivirus/Antimalware

Tabla 10 Mitigaciones Powershell (Ejecución)

Detecciones: No. La implementación de las detecciones necesarias no se contempla por el momento debido a sus requisitos técnicos.

3.5.7. Persistencia

El atacante intenta mantener su posición dentro la red atacada una vez ha conseguido accederla.

Consiste en técnicas que permiten al atacante mantener su acceso a los sistemas atacados y comprometidos, incluso cuando estos sean reiniciados, se cambien credenciales de acceso o se produzca cualquier otro tipo de interrupción que pueda suponer la pérdida del acceso ganado.

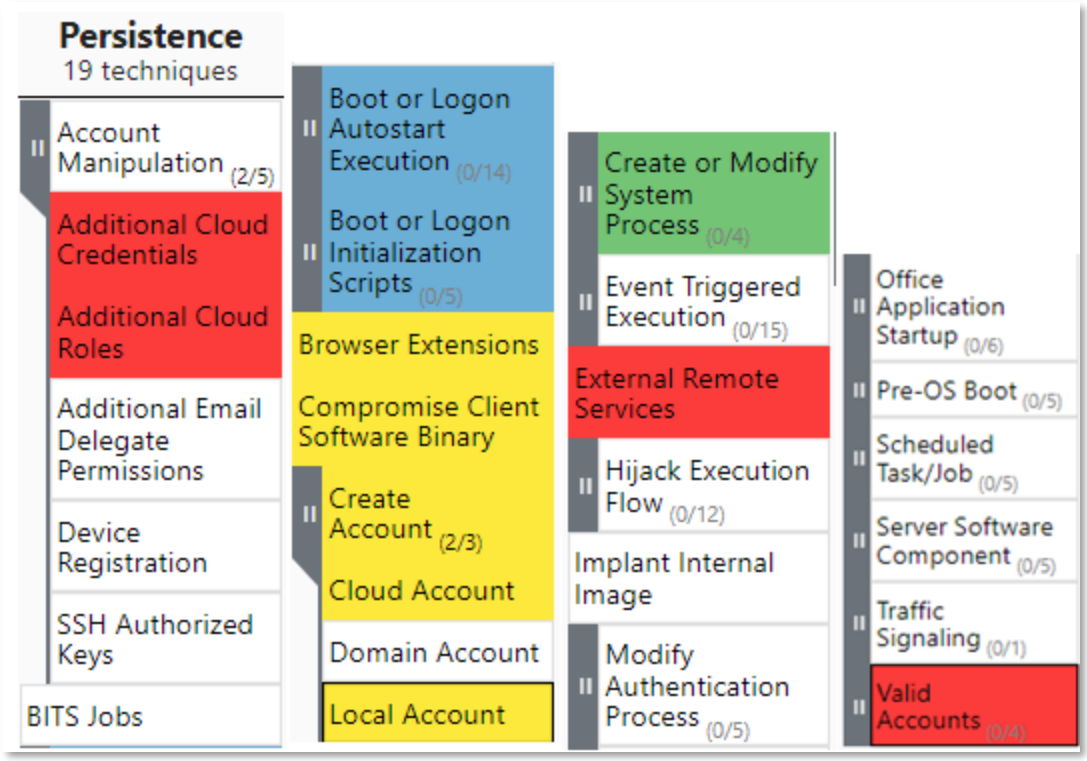


Figura 9 Táctica Persistencia

3.5.7.1. Additional Cloud Credentials

Los atacantes podrían crear cuentas adicionales que les permitiesen asegurar su acceso a la plataforma correspondiente.

Puntuación: 1. Importancia Muy Alta. Formularios de login públicos y posibilidad de consecuencias nefastas.

Justificación

La consola de AWS está disponible y es la misma para todos los usuarios. Si se averiguan o consiguen las credenciales, los atacantes tendrían acceso a la gestión de las aplicaciones web y de todos los elementos utilizados dentro del entorno AWS.

MITIGACIONES	
ID	Mitigación
M1032	Multi-factor Authentication
M1026	Privileged Account Management

Tabla 11 Mitigaciones Additional Cloud Credentials (Persistencia)

DETECCIONES		
ID	Fuente de datos	Componente
DS0002	User Account	User Account Modification

Tabla 12 Detecciones Additional Cloud Credentials (Persistencia)

3.5.7.2. Addional Cloud Roles

Los atacantes podrían dar permisos adicionales a una cuenta bajo su control para realizar acciones más significativas.

Puntuación: 1. Importancia Muy Alta. Se necesita control y revisión sobre las cuentas y sus permisos.

Justificación

Todos los empleados tendrán una cuenta en la consola de AWS. Durante la gestión de las cuentas pueden darse errores que permitan a algunos empleados con determinados roles acceder a más permisos de los debidos.

MITIGACIONES	
ID	Mitigación
M1032	Multi-factor Authentication
M1026	Privileged Account Management

Tabla 13 Mitigaciones Addional Cloud Roles (Persistencia)

DETECCIONES		
ID	Fuente de datos	Componente
DS0002	User Account	User Account Modification

Tabla 14 Detecciones Addional Cloud Roles (Persistencia)

3.5.8. Escalado de Privilegios

El atacante intenta conseguir permisos de más alto nivel.

Consiste en técnicas que permiten al atacante ganar privilegios en una red o en un sistema, y de este modo ejecutar operaciones sólo al alcance de usuarios privilegiados, todo ello mediante el aprovechamiento de vulnerabilidades de los sistemas, configuraciones erróneas o incompletas. La escalada de privilegios incluye por ejemplo la adquisición de roles como usuario root, administrador local, cuentas de administrador

o cuentas que permitan la ejecución de determinadas operaciones no permitidas para usuarios por defecto.

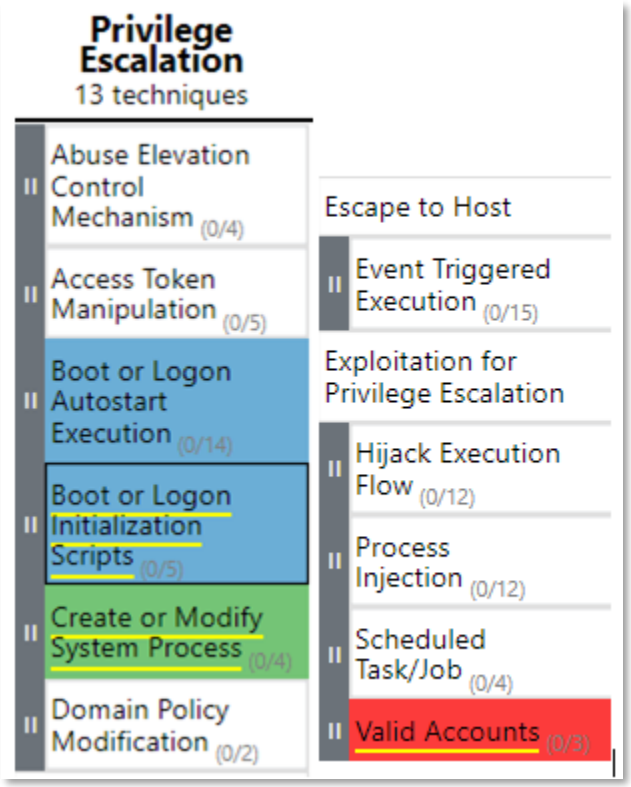


Figura 10 Táctica Escalado de Privilegios

3.5.8.1. Create or Modify System Process

Los atacantes podrían crear o modificar procesos a nivel de sistema que les permitiesen ejecutar repetidamente código malicioso. A efectos prácticos sería persistencia en la ejecución.

Puntuación: 4. Importancia Baja. No se considera una amenaza preocupante pero sí como digna de tener en cuenta.

Justificación

Aunque ahora no supone una de las técnicas más preocupantes, sí que son una de las técnicas que desde la empresa se ha decidido tener en el punto de mira para futuras revisiones de la matriz.

Mitigaciones: No.

Detecciones: No.

3.5.9. Evasión de defensas

El atacante intenta que sus actividades no sean detectadas.

Consiste en técnicas mediante las cuales el atacante evita ser detectado. Algunas de estas técnicas incluyen desinstalar o deshabilitar software de seguridad o encriptar u ofuscar datos o scripts.

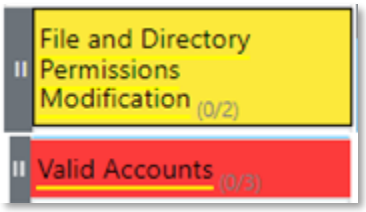


Figura 11 Táctica Evasión de defensas

3.5.9.1. File and directory Permissions Modification

Los atacantes podrían modificar los permisos de ficheros y/o directorios para evadir listas de control de acceso y acceder así archivos protegidos.

Puntuación: 3. Importancia Media. Subtécnica para tener en cuenta y algunas mitigaciones de fácil implementación.

Justificación

En el día a día de la empresa se trabaja con sistemas Windows y Linux, por lo que es importante y además es posible establecer cierto control sobre los ficheros y directorios de estos sistemas.

MITIGACIONES	
ID	Mitigación
M1022	Restrict File and Directory Permissions

Tabla 15 Mitigaciones File and Directory Permissions Modification (Evasión de Defensas)

3.5.10. Acceso a Credenciales

El atacante intenta conseguir credenciales (nombre de usuario y contraseñas válidas de acceso a la red o sistemas).

Consiste en técnicas como Keylogging o volcado de credenciales. Si el atacante consigue credenciales válidas, se dificulta su detección y el atacante podría incluso tener acceso a la creación de más cuentas válidas que le permitan alcanzar sus objetivos.

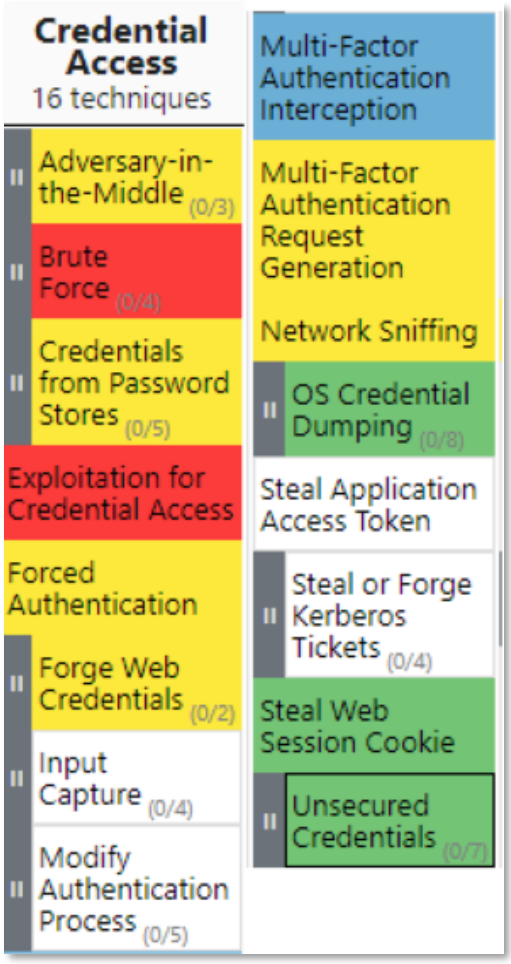


Figura 12 Táctica Acceso a Credenciales

3.5.10.1. Brute Force

Los atacantes podrían usar técnicas de fuerza bruta para ganar acceso a cuentas de las que no conocen las credenciales o cuando han obtenido el hash de alguna contraseña.

Puntuación: 1. Importancia Muy Alta. La empresa cuenta con elementos que pueden ser objetivos de ataques de fuerza bruta que, de ser exitosos, tendrían consecuencias nefastas.

Justificación

La protección de las credenciales es esencial, más aún cuando se cuenta con aplicaciones web que están expuestas públicamente y a las que se accede mediante credenciales. Evitar el descubrimiento y segurizar las aplicaciones frente a acceso no autorizadas son objetivos principales.

MITIGACIONES		
ID	Mitigación	
M1036	Account Use Policies	
M1032	Multi-factor Authentication	
M1027	Password Policies	
M1018	User Account Management	
DETECCIONES		
ID	Fuente de datos	Componente
DS0015	Application Log	Application Log Content
DS0002	User Account	User Account Authentication

Tabla 16 Mitigaciones y Detecciones Fuerza Bruta (Acceso a Credenciales)

3.5.10.2. Explotation for Credential Access

Los atacantes podrían explotar vulnerabilidades software para intentar obtener credenciales.

Puntuación: 1. La empresa cuenta con elementos que pueden ser objetivos de intentos de explotación que, de ser exitosos, tendrían consecuencias nefastas.

Justificación

La protección de las credenciales es esencial, más aún cuando se cuenta con aplicaciones web que están expuestas públicamente y a las que se accede mediante

credenciales. Evitar el descubrimiento y segurizar las credenciales para evitar accesos no autorizados son objetivos principales.

MITIGACIONES	
ID	Mitigación
M1050	Exploit Protection

Tabla 17 Mitigaciones Explotation for Credential Access (Acceso a Credenciales)

DETECCIONES		
ID	Fuente de datos	Componente
DS0015	Application Log	Application Log Content
DS0002	User Account	User Account Authentication

Tabla 18 Detecciones Explotation for Credential Access (Acceso a Credenciales)

3.5.11. Descubrimiento

El atacante trata de averiguar cómo es la red y qué sistemas se encuentran en ella.

Consiste en técnicas que permite al atacante conocer el entorno en el que se está moviendo de manera que pueda tener una orientación correcta en su modo de actuar y/o mejorar sus decisiones.

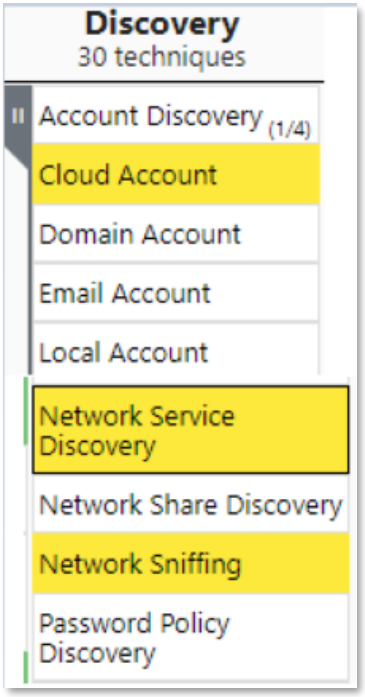


Figura 13 Táctica Descubrimiento

3.5.11.1. Cloud Account

Los atacantes podrían obtener una lista de cuentas de acceso a servicios en la nube.

Puntuación: 3. Importancia Media. Existencia de cuentas para servicios en la nube.

Justificación

Los empleados usan diariamente sus cuentas de AWS.

MITIGACIONES	
ID	Mitigación
M1047	Audit
M1018	User Account Management

Tabla 19 Mitigaciones Cloud Account (Descubrimiento)

Detecciones: No. No se contempla por el momento la implementación de detecciones frente a esta subtécnica.

3.5.11.2. Network Sniffing

Los atacantes podrían capturar tráfico y obtener información sobre un determinado entorno y sobre material de autenticación.

Puntuación: 3. Importancia Media. El riesgo no es alto, pero existe y es importante prevenirlo.

Justificación

En las oficinas hay red Wifi con una señal que por su propia naturaleza podrá alcanzar espacios colindantes o cercanos a las oficinas. Ganado el acceso a la red Wifi se podría acceder a sistemas que pertenezcan a la red cableada.

MITIGACIONES	
ID	Mitigación
M1041	Encrypt Sensitive Information
M1032	Multi-factor Authentication
M1018	User Account Management

Tabla 20 Mitigaciones Network Sniffing (Descubrimiento)

Detecciones: No. No se considera que merezca el esfuerzo de la implementación y las mitigaciones se consideran suficientes.

3.5.12. Movimiento Lateral

El atacante intenta moverse a través del entorno atacado, una vez ha conseguido acceso a algún sistema.

Consiste en técnicas que permite al atacante entrar en sistemas remotos y controlarlos, de manera que pueda ganar acceso a otros sistemas y moverse entre todos ellos.

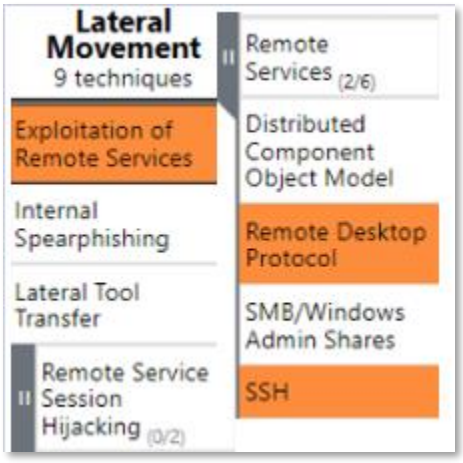


Figura 14 Táctica Movimiento Lateral

3.5.12.1. Remote Desktop Protocol

Los atacantes podrían usar cuentas válidas para acceder a ordenadores de manera remota usando RDP (Remote Desktop Protocol).

Puntuación: 2. Importancia Alta. Se plantea el uso de RDP.

Justificación

Se usará la aplicación Remote Desktop de Windows cuando se conecte desde el exterior con equipos de la oficina (mediante VPN).

MITIGACIONES		
ID	Mitigación	
M1035	Limit Access to Resource Over Network	
M1032	Multi-factor Authentication	
M1030	Network Segmentation	
M1028	Operating System Configuration	
DETECCIONES		
ID	Fuente de datos	Componente
DS0029	Network Traffic	Network Connection Creation
		Network Traffic Flow

Tabla 21 Mitigaciones y Detecciones Remote Desktop Protocol (Movimiento Lateral)

3.5.12.2. SSH

Los atacantes podrían usar cuentas válidas para acceder a equipos de manera remota usando SSH (Secure Shell).

Puntuación: 2. Importancia Alta. La empresa cuenta con servicios SSH que están expuestos públicamente.

Justificación

Las instancias de AWS son accesibles mediante SSH a través de IPs (previa autenticación mediante uso de claves) públicas y cualquier protección adicional es importante.

MITIGACIONES	
ID	Mitigación
M1032	Multi-factor Authentication

Tabla 22 Mitigaciones SSH (Movimiento Lateral)

DETECCIONES		
ID	Fuente de datos	Componente
DS0029	Network Traffic	Network Connection Creation

Tabla 23 Detecciones SSH (Movimiento Lateral)

3.5.13. Colección

El atacante trata de conseguir datos de su interés o que le permitan alcanzar sus objetivos.

Consiste en técnicas que permiten conseguir datos y establecerse en las fuentes de las que se recogen esos datos. Estas fuentes pueden ser distintos tipos de unidades de información o de almacenamiento de información, navegadores, audio, vídeo y/o correo electrónico.

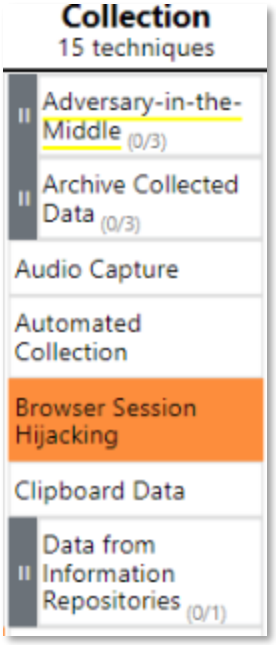


Figura 15 Táctica Colección

3.5.13.1. Browser Session Hijacking

Los atacantes podrían aprovechar las vulnerabilidades de seguridad y la funcionalidad inherente en el software del navegador para cambiar el contenido, modificar el comportamiento de los usuarios e interceptar información como parte de varias técnicas de browser session hijacking.

Puntuación: 2. Importancia Alta. Necesidad de uso seguro de navegadores.

Justificación.

El extensivo uso de los navegadores por parte de los empleados.

MITIGACIONES	
ID	Mitigación
M1017	User Training

Tabla 24 Mitigaciones Browser Session Hijacking

Detecciones: No. Se considera suficiente con las mitigaciones.

3.5.14. Comando y Control

El atacante trata de comunicarse con sistemas comprometidos para conseguir controlarlos.

Consiste en técnicas que el atacante usa para tomar el control de sistemas previamente comprometidos, para que estos estén bajo su control.

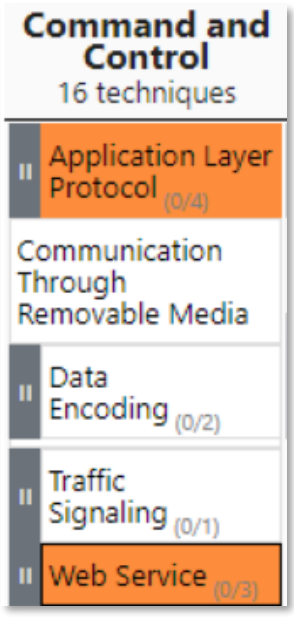


Figura 16 Táctica Comando y Control

3.5.14.1. Application Layer Protocol

Los atacantes podrían comunicarse utilizando protocolos de capa de aplicación para evitar la detección/filtrado de red mezclándose con el tráfico existente.

Puntuación: 2. Importancia Alta. Servicios usados y que deben de permitirse en su mayoría.

Justificación

Los trabajadores hacen uso intensivo de los protocolos de aplicación (protocolos web, transferencia de ficheros, mail y DNS) y por lo tanto se necesita permitir y a la vez segurizar dichos servicios tanto en entorno de oficina como de cloud.

MITIGACIONES	
ID	Mitigación
M1031	Network Intrusion Prevention

Tabla 25 Mitigaciones Application Layer Protocol (Comando y Control)

DETECCIONES		
ID	Fuente de datos	Componente
DS0029	Network Traffic	Network Traffic Content
		Network Traffic Flow

Tabla 26 Detecciones Application Layer Protocol (Comando y Control)

3.5.14.2. Web Service

Los atacantes podrían usar servicios web legítimos a los que podrían enviar o desde los que recibir información.

Puntuación: 2. Importancia Alta. Inevitablemente se hará uso de muchos de estos servicios.

Justificación

Cualquier servicio web que pueda ser usado por los empleados puede suponer un riesgo debido a la actividad que los atacantes pueden realizar en los mismos.

MITIGACIONES	
ID	Mitigación
M1031	Network Intrusion Prevention

Tabla 27 Mitigaciones Web Service (Comando y Control)

DETECCIONES		
ID	Fuente de datos	Componente
DS0029	Network Traffic	Network Traffic Content
		Network Traffic Flow

Tabla 28 Detecciones Web Service (Comando y Control)

3.5.15. Exfiltración

El atacante intenta robar datos y hacerlos de su posesión.

Consiste en técnicas que permiten exportar datos fuera de la red atacada, evitando ser detectados durante el proceso.

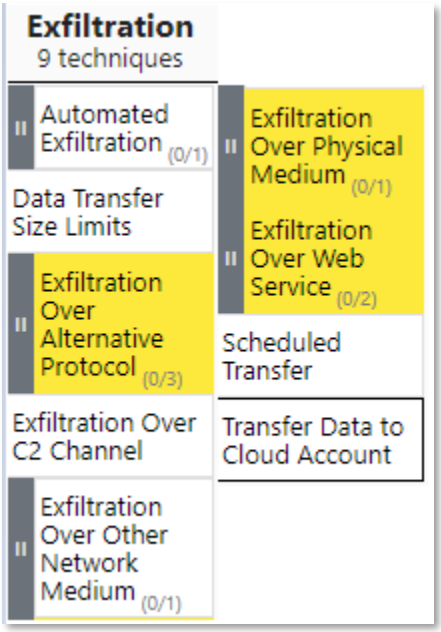


Figura 17 Táctica Exfiltración

3.5.15.1. Exfiltration Over Physical Medium

Los atacantes podrían exfiltrar datos usando dispositivos de almacenamiento físico, como una memoria USB.

Puntuación: 3. Importancia Media. Todos los PCs cuentan con puertos USB.

Justificación

Actualmente cualquier empleado puede insertar un USB en los PCs de la oficina y salvar la información presente en dichos PCs.

MITIGACIONES	
ID	Mitigación
M1042	Disable or Remove Feature or Program
M1034	Limit Hardware Installation

Tabla 29 Mitigaciones Exfiltration Over Physical Medium (Exfiltración)

Detecciones: No. Se considera suficiente con las mitigaciones.

3.5.15.2. Exfiltration Over Web Service

Los atacantes podrían exfiltrar datos haciendo uso de servicios web legítimos.

Puntuación: 3. Importancia Media. Servicios web usados y que deben ser permitidos.

Justificación

Los empleados usan gran cantidad de servicios web que pueden servir para enmascarar tráfico hacia el exterior.

MITIGACIONES	
ID	Mitigación
M1021	Restrict Web-Based Content

Tabla 30 Mitigaciones Exfiltration Over Web Service (Exfiltración)

DETECCIONES		
ID	Fuente de datos	Componente
DS0029	Network Traffic	Network Traffic Content
		Network Traffic Flow

Tabla 31 Exfiltration Over Web Service (Exfiltración)

3.5.16. Impacto

El atacante intenta manipular, interrumpir o destruir los datos y/o los sistemas.

Consiste en técnicas que el atacante usa para romper la disponibilidad de los sistemas y su información, así como comprometer su integridad mediante la manipulación de información en si misma o de los procesos mediante los que se genera.

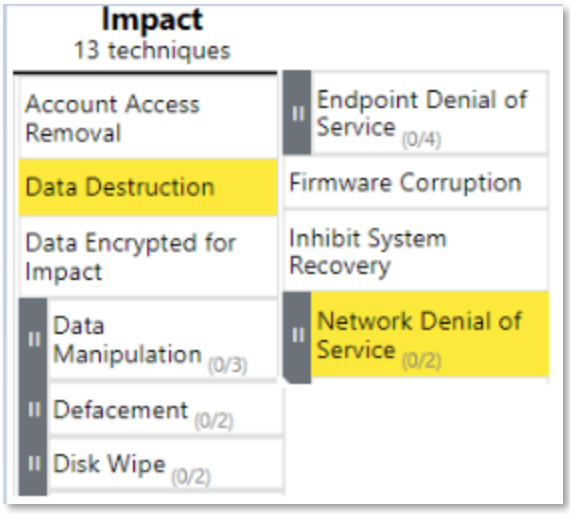


Figura 18 Táctica Impacto

3.5.16.1. Data Destruction

Los atacantes podrían destruir datos y archivos en sistemas específicos o en grandes cantidades en una red para interrumpir la disponibilidad de los sistemas, servicios y recursos de la red.

Puntuación: 3. Importancia Media. Necesidad de proteger los datos.

Justificación

Es imprescindible, en cualquier empresa, estar protegido ante la pérdida o destrucción de datos.

MITIGACIONES	
ID	Mitigación
M1053	Data Backup

Tabla 32 Mitigaciones Data Destruction (Impacto)

Detecciones: No. Se considera suficiente con las mitigaciones.

3.5.16.2. Network Denial of Service

Los atacantes pueden realizar ataques de denegación de servicio (DDoS) de red para degradar o bloquear la disponibilidad de los recursos específicos para los usuarios.

Puntuación: 3. Importancia Media. Se cuenta con elementos que pueden ser objeto de dichos ataques.

Justificación

Tanto las aplicaciones web como la oficina (Portal para la VPN) tendrán IPs públicas que podrían ser víctimas de un ataque DDoS.

MITIGACIONES	
ID	Mitigación
M1037	Filter Network Traffic

Tabla 33 Mitigaciones Network Denial of Service (Impacto)

DETECCIONES		
ID	Fuente de datos	Componente
DS0029	Network Traffic	Network Traffic Flow
DS0013	Sensor Health	Host Status

Tabla 34 Detecciones Network Denial of Service (Impacto)

3.6. Tabla resumen de mitigaciones a implementar

Se muestra en la siguiente tabla la recopilación de todas las mitigaciones que van a implementarse. Se muestran las mitigaciones por orden de aparición a lo largo del estudio teórico.

MITIGACIONES	
ID	Mitigación
M1054	Software Configuration
M1017	User Training
M1050	Exploit Protection
M1021	Restrict Web-Based Content
M1026	Privileged Account Management
M1051	Update Software
M1016	Vulnerability Scanning
M1035	Limit Access to Resource Over Network
M1032	Multi-factor Authentication

M1030	Network Segmentation
M1049	Antivirus/Antimalware
M1031	Network Intrusion Prevention
M1013	Application Developer Guidance
M1027	Password Policies
M1018	User Account Management
M1040	Behavior Prevention on Endpoint
M1038	Execution Prevention
M1047	Audit
M1033	Limit Software Installation
M1045	Code Signing
M1042	Disable or Remove Feature or Program
M1036	Account Use Policies
M1041	Encrypt Sensitive Information
M1028	Operating System Configuration
M1053	Data Backup
M1037	Filter Network Traffic
M1022	Restrict File and Directory Permissions
M1034	Limit Hardware Installation

Tabla 35 Tabla resumen de mitigaciones a implementar

3.7. Tabla resumen de detecciones a implementar

Se muestra en la siguiente tabla la recopilación de todas las detecciones que van a implementarse.

DETECCIONES		
ID	Fuente de datos	Componente
DS0015	Application Log	Application Log Content
DS0029	Network Traffic	Network Connection Creation
		Network Traffic Content
		Network Traffic Flow

DS0028	Logon Session	Logon Session Creation
		Logon Session Metadata
DS0002	User Account	User Account Modification
		User Account Creation
		User Account Authentication
DS0017	Command	Command Execution
DS0013	Sensor Health	Host Status

Tabla 36 Tabla resumen de detecciones a implementar

3.8. Conclusiones

Las conclusiones obtenidas tras estudiar la matriz MITRE ATT&CK Enterprise como un evaluador de fallas defensivas son:

- La matriz aporta una eficiencia de grandes magnitudes en cuanto a la evaluación de fallas defensivas. Esto se debe a su alto nivel de detalle y minuciosidad, que le permite cubrir prácticamente cualquier aspecto existente.
- Su uso no es excesivamente complejo, aunque puede resultar tedioso dependiendo de la profundidad que se pretenda alcanzar.
- El uso del framework aporta a sus usuarios una gran cantidad de información muy relevante y de gran utilidad en lo que a la ciberseguridad respecta.
- Independientemente del caso de uso o de estudio para el que se utilice el framework, su minuciosidad y detalle hace que inevitablemente repercuta de manera positiva sobre otros casos de uso o estudio. Esto se debe a que a pesar de contener una cantidad de información que podría parecer ingobernable, la propia estructura de la matriz aporta coherencia y hace que sea un framework compacto en el que, a pesar de su volumen, los usuarios puedan moverse sabiendo lo que se está haciendo en todo momento.
- En líneas generales, es probablemente uno de los frameworks más potentes que existen en la actualidad en cuanto a ciberseguridad.

3.9. A implementar en Estudio Práctico

Tras el análisis de las fallas defensivas de la empresa usando la matriz MITRE ATT&CK Enterprise, se ha llegado a la conclusión de que actualmente lo que más interesa implementar son mitigaciones, dado el preocupante estado de desprotección en algunos aspectos. Tendría poco sentido implementar un SIEM para detecciones, por ejemplo, mientras que las aplicaciones web se encuentran expuestas en Internet a merced de cualquier atacante.

Sobre las detecciones, se implementarán aquellas que estén al alcance y no requieran demasiada inversión adicional, tanto económica como temporal.

Tomada una decisión por los responsables de la empresa, se ha decidido implementar:

a) Un WAF para proteger las aplicaciones web alojadas en las instancias de AWS.
b) Un firewall en la oficina que permita la conexión con los equipos de la red de la oficina mediante VPN y a la vez proteja la red de la oficina y las conexiones de los empleados remotos durante sus horas de trabajo.
c) Factor de doble autenticación para la conexión con la VPN y con la consola de AWS.

3.9.1. Diagrama de redes e IT propuesto para Estudio Práctico

Se muestra en la siguiente imagen el diagrama de red deseado tras la implementación práctica.

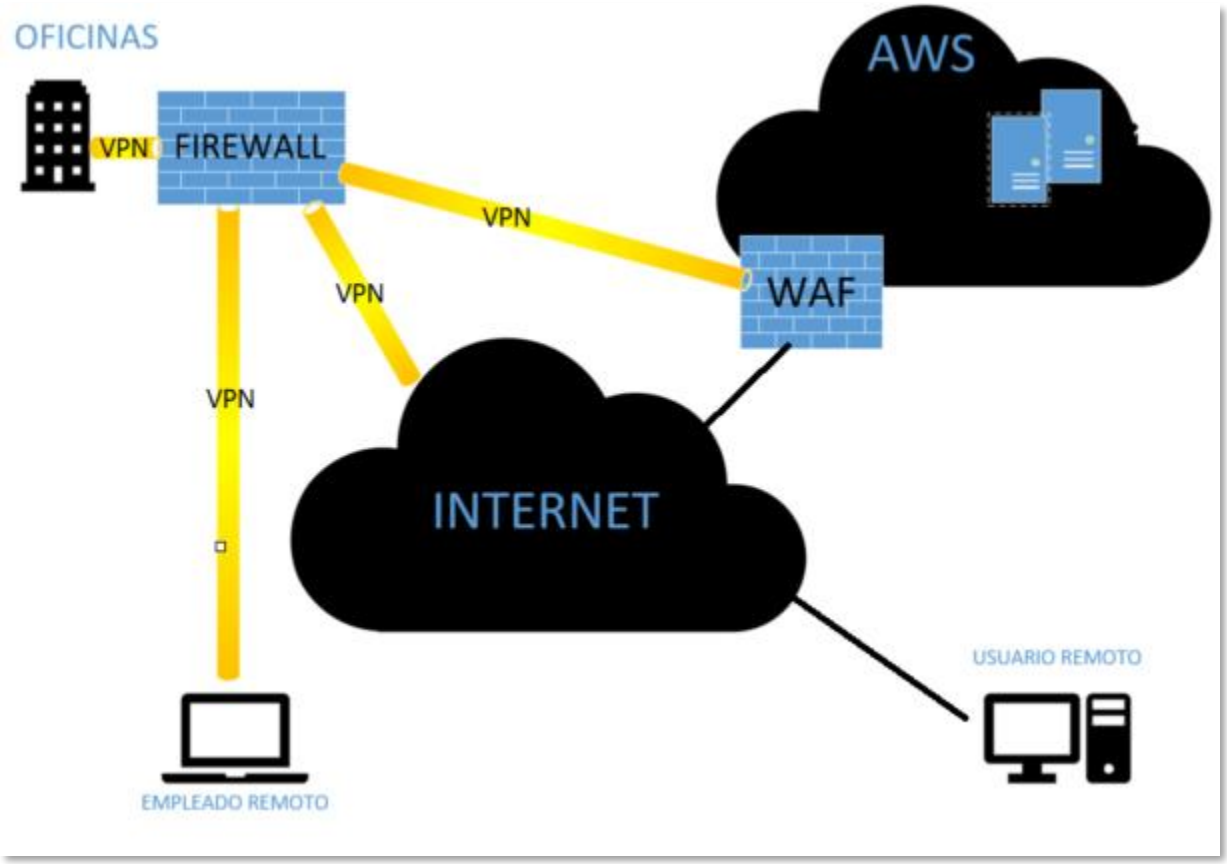


Figura 19 Diagrama Redes e IT para Estudio Práctico

Con la propuesta realizada para la implementación se consigue:

- Que cuando los empleados conecten con la oficina o naveguen por Internet para realizar su trabajo, lo hagan siempre bajo conexión cifrada y atendiendo a los criterios de seguridad establecidos por la empresa (políticas de tráfico, inspección de descargas, filtrado de URLs, comprobación de aplicaciones y el tráfico de estas, etc.).
- Que cualquier usuario remoto (posible atacante) se encuentre con un Firewall o con un WAF siempre que trata de conectar con las redes o servicios de la empresa.

4. ESTUDIO PRÁCTICO

En este apartado se llevarán a cabo las implementaciones necesarias para cubrir las mitigaciones y detecciones propuestas.

A lo largo del desarrollo de este punto se incluirán capturas que muestren brevemente la implementación de algunas mitigaciones. Para aquellas mitigaciones que han requerido mayor extensión documental por su naturaleza técnica, se incluirán anexos reflejando todo el proceso a seguir para realizar la implementación (*'Anexo IV: Implementación de un WAF en AWS'* y '*Anexo V: Implementación de VPN con 2FA usando Keycloack y Google Authenticator'*).

Los diferentes apartados de este punto serán las propias mitigaciones y detecciones a implementar. Para cada una de ellas se indicarán las técnicas y subtécnicas afectadas y la táctica en la que se aplican, así como una descripción de la mitigación que se pretende implementar. Las técnicas y subtécnicas se mostrarán agrupadas en listas si la mitigación a implementar es similar o idéntica, o de manera independiente si la mitigación es única para una determinada técnica o subtécnica.

NOTA: Por cuestiones de espacio y con el objetivo de mantener una extensión adecuada de este documento, se muestran únicamente en este punto algunas de las mitigaciones y detecciones implementadas. El estudio práctico al completo puede encontrarse en el 'ANEXO III: Ampliación Estudio Práctico'.

4.1. Objetivos

Los objetivos del estudio práctico son aplicar de manera práctica el estudio teórico realizado, y por tanto cubrir de manera real las fallas defensivas detectadas.

4.2. Mitigaciones

4.2.1. M1054: Software Configuration

- Phising for information (Reconocimiento).
- Phising (Acceso Inicial).

La empresa de hosting que proporciona el servicio de webmail, cuenta con filtros antivirus y antispam. Se seleccionará el nivel de protección más alto (recomendado).

Figura 20 Protección ante Phising mail

- Forge Web Credentials (Acceso a Credenciales).

Configurar los navegadores para que eliminen regularmente credenciales almacenadas, como cookies.

En Chrome, por ejemplo, es muy sencillo configurar la opción de borrar cookies al cerrar el navegador o incluso añadir URLs en las que se impida el almacenamiento de cookies.

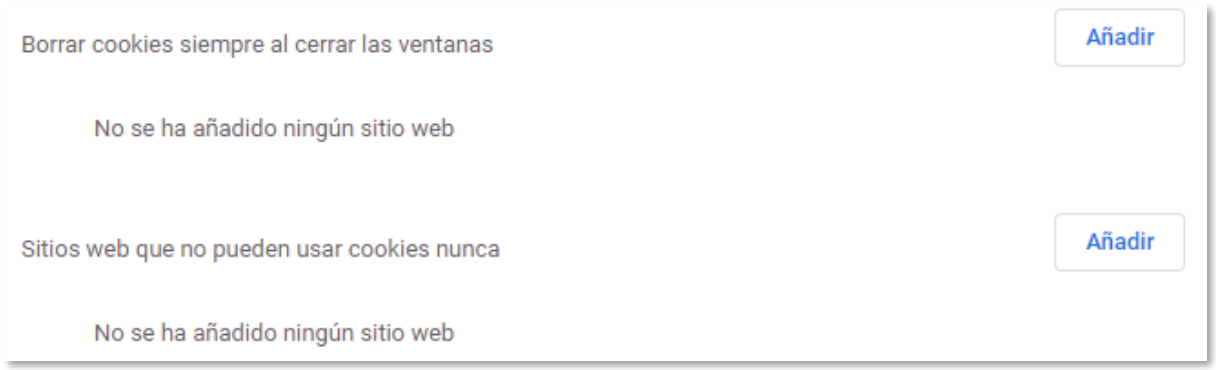


Figura 21 Configuración borrado de cookies al cerrar el navegador

4.2.2. M1017: User Training

- Phising for information (Reconocimiento).
- Phising (Acceso Inicial).
- User Execution (Execution).

Todos los empleados recibirán un curso formativo que les permita identificar técnicas de ingeniería social e intentos de phishing en cualquiera de sus variantes (mail, teléfono, sms, etc.). Además de las técnicas de phishing.

- Valid Accounts (Acceso Inicial).
- Valid Accounts (Persistencia).
- Valid Accounts (Escalado de Privilegios).
- Multi - Factor Authentication Request Generation (Acceso a Credenciales).

En los cursos formativos se incluirá un apartado sobre la importancia de las credenciales de usuario y la confidencialidad de estas, del uso de contraseñas seguras y su almacenamiento, autenticación multifactor y otros temas que aporten valor y ayuden al entendimiento.

- Browser Extensions (Persistencia).
- Browser Session Hijacking (Colección).

En los cursos formativos se incluirá un apartado educacional sobre navegadores y extensiones de navegadores, cómo instalarlas y/o desinstalarlas y cómo sospechar de extensiones de dudosa confiabilidad.

También se educará a los empleados en cerrar las sesiones en los navegadores si no se están utilizando.

4.2.3. M1050: Exploit Protection

Se incluye toda la mitigación posible que aporta el Antivirus. Con el Antivirus actual, siempre que se intenta ejecutar algún archivo durante la navegación, se muestran alertas indicando el resultado del análisis. Si el archivo es seguro, se muestra un aviso y se ejecuta. Si se detecta como malicioso, se bloquea y se muestra un aviso que permite acceder a todos los detalles.

A continuación, se muestra una captura de los detalles de un archivo ejecutado y clasificado como seguro.

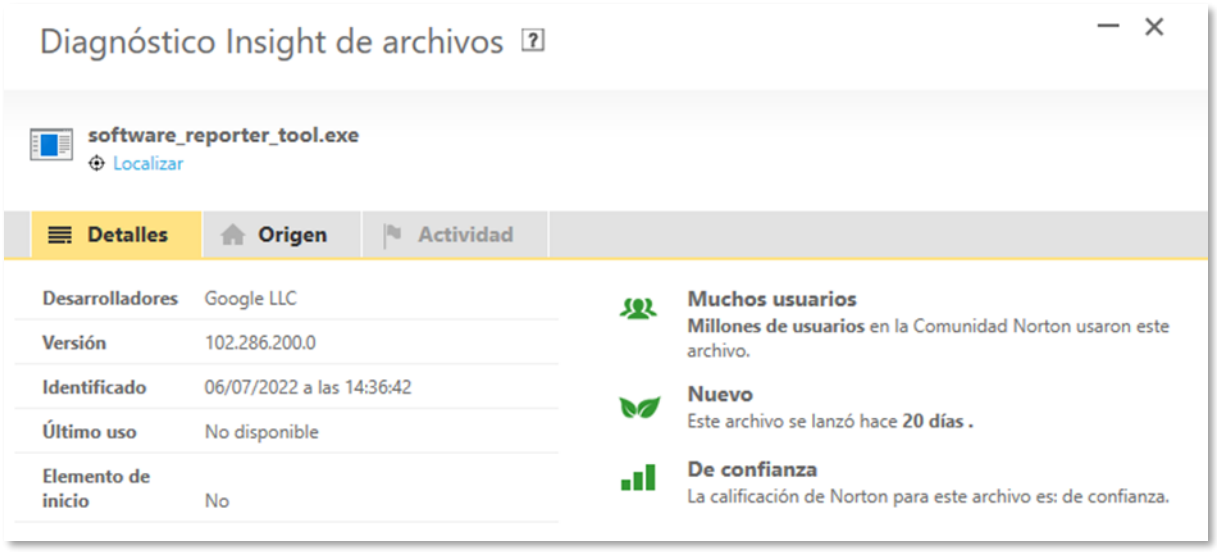


Figura 22 Detección ejecución de archivo durante la navegación

- Explotación de Servicios Remotos (Movimiento Lateral).

El AntiVirus en principio debería de detectar la ejecución de archivos catalogados como peligrosos.

- Exploit Public Facing Application (Acceso Inicial).
- Exploitation for Credential Access (Acceso a Credenciales).

Se implementará un WAF para proteger las aplicaciones web. El proceso detallado de implementación del WAF en AWS se describe en el '*ANEXO IV: Implementación de un WAF en AWS*'.

4.2.4. M1021: Restrict Web-Based Content

- Drive by Compromise (Acceso Inicial).
- Phising (Acceso Inicial).
- Command and Scripting Interpreter - JavaScript (Ejecución).

Se utilizará la extensión para navegadores que incluye el Antivirus (Norton Safe Web). Esta extensión permite detectar páginas web no seguras y bloquear y/o advertir cuando se intenta acceder a las mismas.

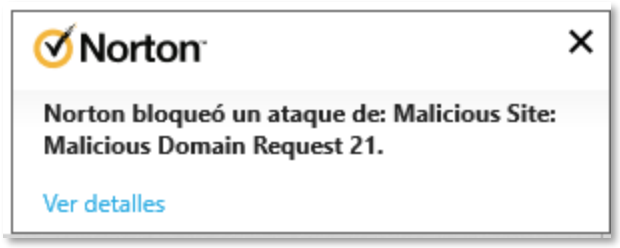


Figura 23 Bloqueo de acceso a web maliciosa

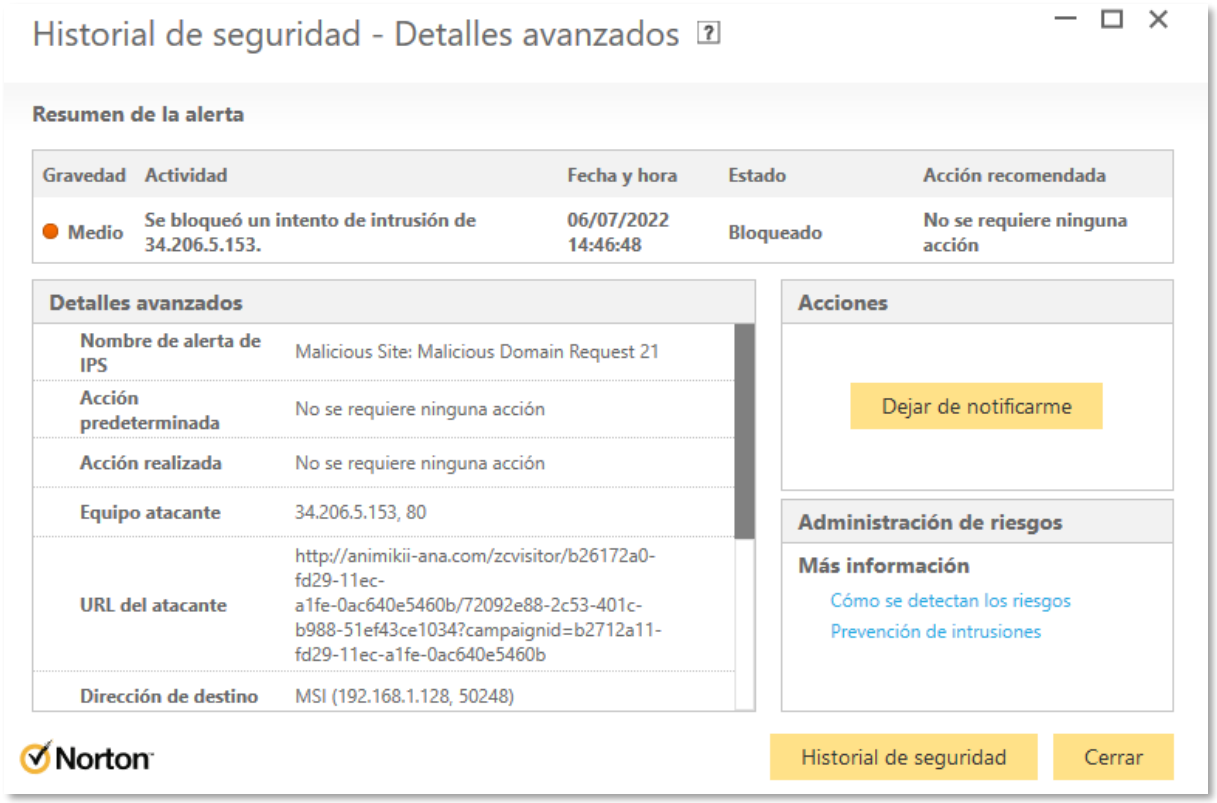
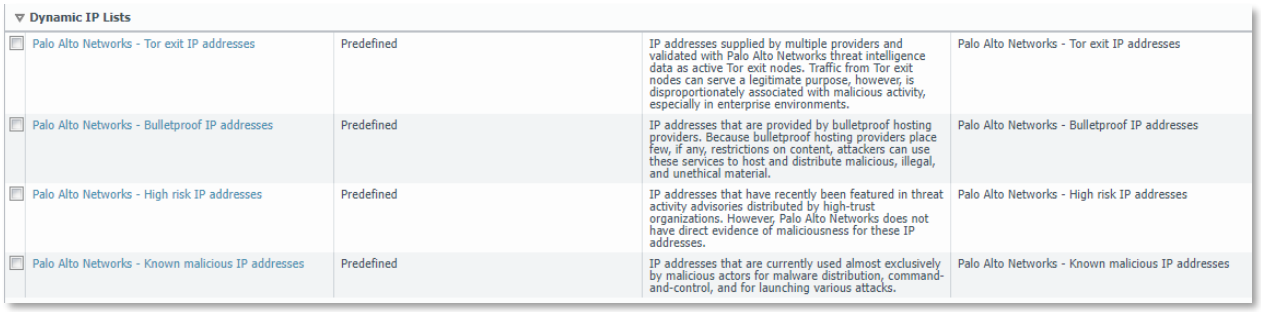


Figura 24 Reporte bloque acceso a web maliciosa

Se usarán también bloqueadores de anuncios de confiabilidad reconocida.

- User Execution (Ejecución).

El firewall bloqueará los intentos de acceso a links categorizados como maliciosos. La categorización de los links se hace atendiendo a listas dinámicas, categorías, aplicaciones, etc.



Dynamic IP Lists

Palo Alto Networks - Tor exit IP addresses	Predefined	IP addresses supplied by multiple providers and validated with Palo Alto Networks threat intelligence data as active Tor exit nodes. Traffic from Tor exit nodes can serve a legitimate purpose, however, is disproportionately associated with malicious activity, especially in enterprise environments.	Palo Alto Networks - Tor exit IP addresses
Palo Alto Networks - Bulletproof IP addresses	Predefined	IP addresses that are provided by bulletproof hosting providers. Because bulletproof hosting providers place few, if any, restrictions on content, attackers can use these services to host and distribute malicious, illegal, and unethical material.	Palo Alto Networks - Bulletproof IP addresses
Palo Alto Networks - High risk IP addresses	Predefined	IP addresses that have recently been featured in threat activity advisories distributed by high-trust organizations. However, Palo Alto Networks does not have direct evidence of maliciousness for these IP addresses.	Palo Alto Networks - High risk IP addresses
Palo Alto Networks - Known malicious IP addresses	Predefined	IP addresses that are currently used almost exclusively by malicious actors for malware distribution, command-and-control, and for launching various attacks.	Palo Alto Networks - Known malicious IP addresses

Figura 25 Listas dinámicas Firewall Palo Alto

4.2.5. M1026: Privileged Account Management

- Exploit Public Facing Application (Acceso Inicial).

Las aplicaciones muestran diferentes vistas y permiten determinadas acciones dependiendo del usuario que se loguea. Para ello se usan las capacidades de los frameworks y lenguajes de programación utilizados en la programación de las aplicaciones.

- Valid Accounts (Acceso Inicial).
- Valid Accounts (Persistencia).
- Create Account - Local Account (Persistencia).
- Valid Accounts (Escalado de Privilegios).
- Forge Web Credentials (Acceso a Credenciales).
- Explotación de Servicios Remotos (Movimiento Lateral).

El uso de cuentas privilegiadas ha de mantenerse reducido al máximo posible y siempre controlado.

Si se crean cuentas adicionales, minimizar los permisos en la medida de lo posible y otorgar los permisos justos y necesarios para que los empleados realicen sus tareas.

- Command and Scripting Interpreter - PowerShell (Ejecución).

Finalmente, no se va a restringir el uso de PowerShell.

- Account Manipulation - Additional Cloud Credentials (Persistencia).
- Account Manipulation - Additional Cloud Roles (Persistence).
- Create Account - Cloud Account (Persistencia).

Restringir el uso de la cuenta raíz en AWS y crear cuentas IAM con los permisos estrictamente necesarios.

4.2.6. M1035: Limit Access to Resource Over Network

- External Remote Services (Acceso Inicial).
- External Remote Services (Persistencia).

Se implementará una VPN que conectará al firewall de la oficina previa autenticación usando el software cliente del vendedor.

La implementación completa de la VPN, que además usará 2FA, se describe en el '*Anexo V: Implementación de VPN con 2FA usando Keycloak y Google Authenticator'*.

- Remote Services - Remote Desktop Protocol (Movimiento Lateral).

Se permitirá el uso de conexiones RDP únicamente desde la zona del Portal de la VPN y en la medida de lo posible, sólo desde IPs conocidas.

4.2.7. M1032: Multi-factor Authentication

- External Remote Services (Acceso Inicial).
- Create Account - Local Account (Persistencia).
- External Remote Services (Persistencial).
- Fuerza Bruta (Acceso a Credenciales).
- Multi - Factor Authentication Request Generation (Acceso a Credenciales).
- Network Sniffing (Descubrimiento).
- Remote Services - Remote Desktop Protocol (Movimiento Lateral).

Se implementará 2FA para la autenticación en la VPN.

- Account Manipulation - Additional Cloud Credentials (Persistencia).
- Account Manipulation - Additional Cloud Roles (Persistence).
- Create Account - Cloud Account (Persistencia).
- Fuerza Bruta (Acceso a Credenciales).
- Multi - Factor Authentication Request Generation (Acceso a Credenciales).

Agregar MFA a todas las cuentas de AWS de todos los empleados, ya sea cuenta Raíz o cuenta IAM. El proceso es bastante sencillo, y se pueden usar aplicaciones gratuitas como ‘Microsoft Authenticator’.

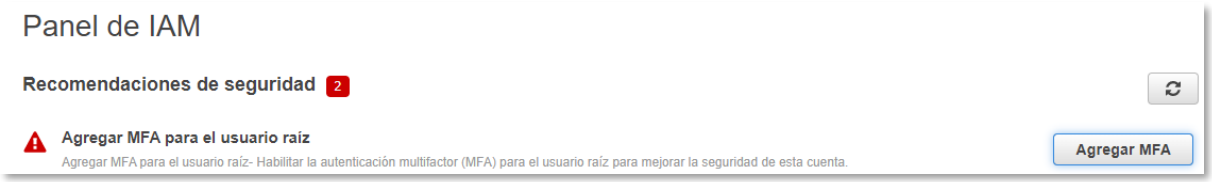


Figura 26 Usario raíz AWS sin 2FA

Figura 27 Solicitud 2FA consola AWS

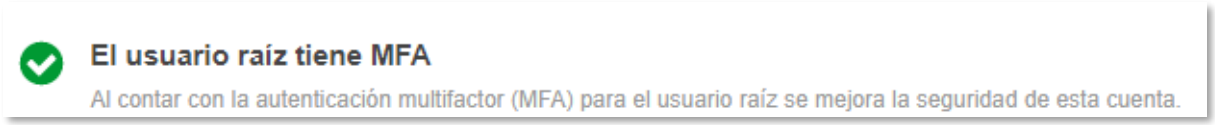


Figura 28 Usuario raíz en AWS con 2FA configurado

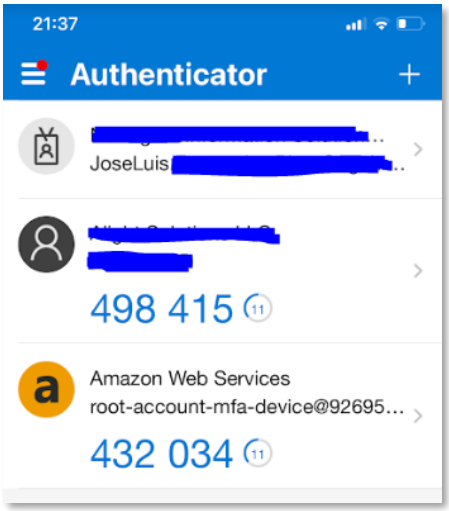


Figura 29 2FA en dispositivo móvil para acceso a consola de AWS

- Remote Services - SSH (Movimiento Lateral).

Implementar 2FA para la autenticación en conexiones mediante SSH con las instancias en AWS.

4.2.8. M1030: Network Segmentation

- External Remote Services (Acceso Inicial).
- External Remote Services (Persistencial).
- Network Service Discovery (Descubrimiento).
- Explotación de Servicios Remotos (Movimiento Lateral).
- Remote Services - Remote Desktop Protocol (Movimiento Lateral).
- Exfiltration Over Alternative Protocol (Exfiltración)

La red de la oficina estará segmentada en zonas y se aplicarán políticas de tráfico, filtrado, inspección de paquetes, etc. atendiendo a estas zonas.

- Create Account - Cloud Account (Persistencia).

El entorno de red configurado en la nube ha de estar correctamente segmentado, impidiendo la comunicación entre equipos y aplicaciones que no necesitan comunicar. Para ello se usarán VPCs (Virtual Private Clouds), subredes, grupos de seguridad, interfaces virtuales, etc.

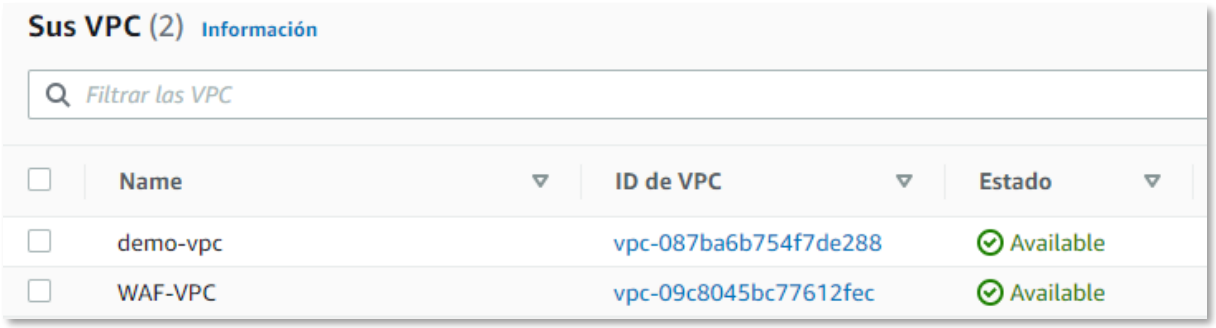


Figura 30 VPCs independientes en AWS

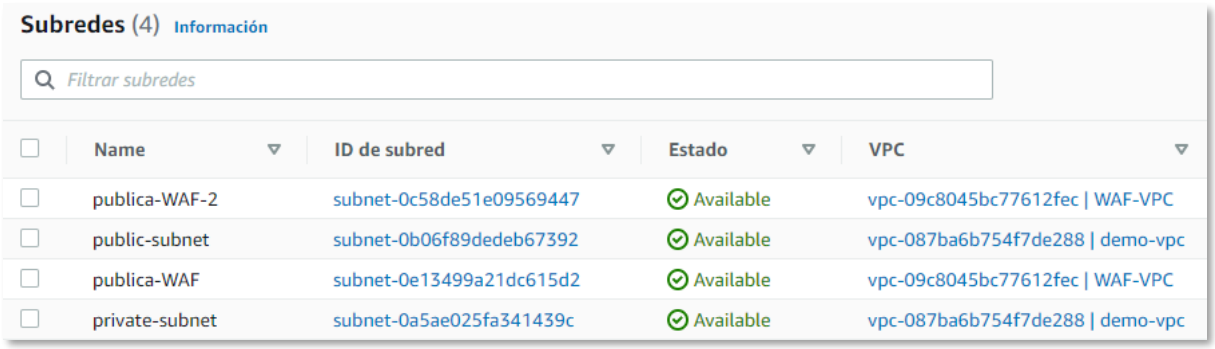


Figura 31 Subredes de distintas VPCs en AWS

4.2.9. M1049: Antivirus/Antimalware

- Phishing (Acceso Inicial).

Todos los ordenadores de la oficina contarán con un Antivirus con licencia que permita bloquear la ejecución de ficheros maliciosos y ponerlos en cuarentena para que sean investigados.

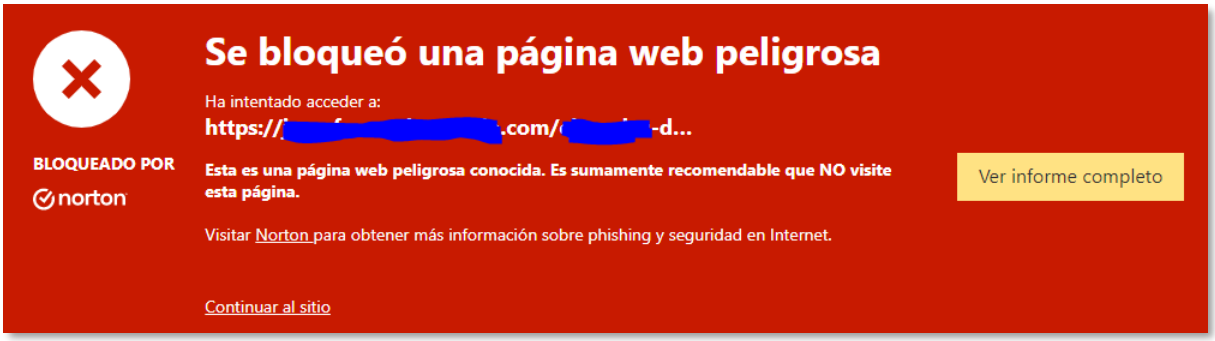


Figura 32 Bloqueo de web phising

- Command and Scripting Interpreter - PowerShell (Ejecución).

El Antivirus debe de detectar intentos de ejecución maliciosos de la herramienta PowerShell.

- Command and Scripting Interpreter - Python (Ejecución).

El Antivirus debe de detectar intentos de ejecución de archivos maliciosos que usen Python.

4.2.10. M1018: User Account Management

- Valid Accounts (Acceso Inicial).
- Valid Accounts (Persistencia).

- Valid Accounts (Escalado de Privilegios).
- Fuerza Bruta (Acceso a Credenciales).
- Forge Web Credentials (Acceso a Credenciales).
- Account Discovery - Cloud Account (Descubrimiento).

Todas las cuentas, independientemente de a lo que den acceso, tendrán definidas las acciones permitidas que pueden realizar, otorgando los privilegios justos y necesarios para el desempleo de las tareas adjudicadas a cada empleado.

Las cuentas con mayor cantidad de privilegios se mantendrán reducidas al máximo y sólo se otorgarán a usuarios con la autoridad necesaria.

Se eliminarán todas las cuentas que no se usan y las de empleados que dejen de formar parte de la empresa.

En AWS, se pueden crear nuevos usuarios y el nivel de permisos asignables es extremadamente detallado.

En las siguientes imágenes se muestra un ejemplo de creación de usuario IAM en AWS y algunos de los posibles permisos que se le podrían dar con respecto al uso del servicio Route 53, usado para la gestión de dominios en AWS.

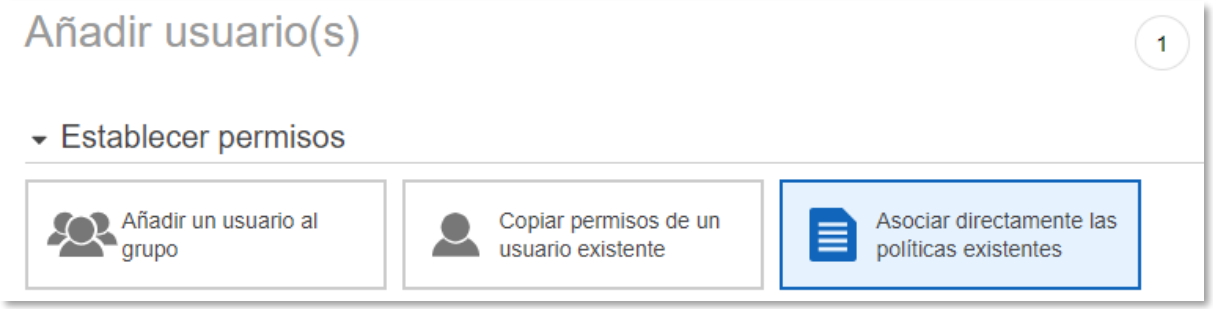


Figura 33 Establecimiento de permisos para usuario IAM en AWS

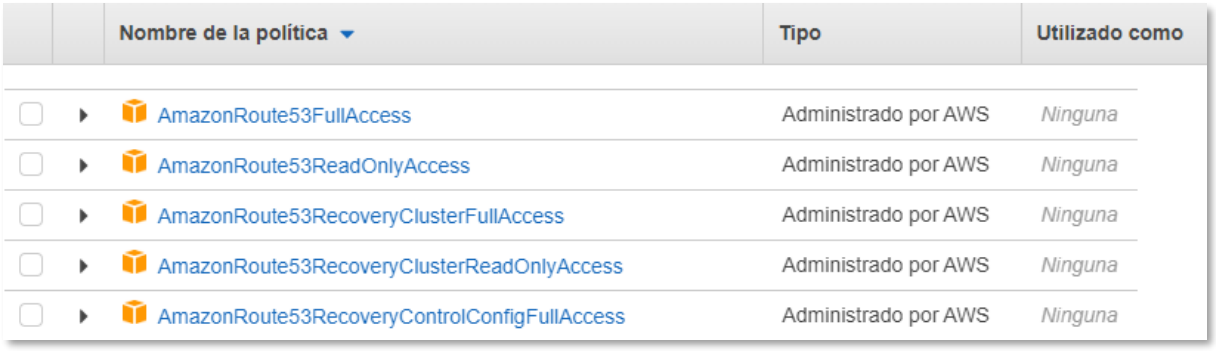


Figura 34 Permisos relacionados con Route 53 en AWS

- Fuerza Bruta (Acceso a Credenciales).

Si se detectan intentos de fuerza bruta sobre una cuenta, eliminar dicha cuenta.

4.3. Detecciones

4.3.1. DS0015: Application Log - Application Log Content

- Drive by Compromise (Acceso Inicial).
- Phishing (Acceso Inicial).
- Fuerza Bruta (Acceso a Credenciales).

El firewall de las oficinas logueará todo el tráfico y es capaz de detectar la aplicación en uso en la mayoría de los casos.

- Exploit Public-Facing Application (Acceso Inicial).
- Explotación de Servicios Remotos (Movimiento Lateral).

El WAF puede loguear intentos de ejecución de exploits o uso de herramientas que pudiesen implicar la aplicación de alguna técnica maliciosa.

- External Remote Services (Acceso Inicial).
- External Remote Services (Persistencial).

El firewall contra el que se establecerán las VPNs monitorizará y logueará todas las conexiones (exitosas o no) realizadas.

4.3.2. DS0029: Network Traffic - Network Connection Creation

- Drive by Compromise (Acceso Inicial).
- Phishing (Acceso Inicial).
- User Execution (Ejecución).

- Browser Extensions (Persistencia).
- Remote Services - Remote Desktop Protocol (Movimiento Lateral).
- Remote Services - SSH (Movimiento Lateral).
- Exfiltration Over Alternative Protocol (Exfiltración)

El firewall deberá monitorizar, detectar y bloquear conexiones de red recibidas desde host o IPs no confiables. Para ello podrá hacer uso de listas dinámicas o filtrado de URLs.

4.3.3. DS0029: Network Traffic - Network Traffic Content

- Phising for Information (Reconocimiento).
- Drive by Compromise (Acceso Inicial).
- Phishing (Acceso Inicial).

Tanto el Firewall como el WAF deben detectar en principio escaneos de vulnerabilidades, puertos, de solicitud de información, etc.

- Exploit Public-Facing Application (Acceso Inicial).

El WAF puede detectar en las peticiones que se realizan a las aplicaciones intentos de inyecciones SQL o intentos de logueo por fuerza bruta, por ejemplo, y bloquearlos.

- User Execution (Ejecución).

El firewall puede realizar inspección de paquetes en busca de malware.

- Application Layer Protocol (Comando y Control).
- Web service (Comando y Control).
- Exfiltration Over Alternative Protocol (Exfiltración).
- Exfiltration over Web Service (Exfiltración).

Monitorizar y analizar patrones de tráfico y realizar inspección de paquetes asociados a determinados protocolos.

Realizar inspección SSL/TLS para tráfico cifrado que no siga los estándares del protocolo o los flujos de tráfico esperados (por ejemplo, paquetes extraños que no pertenezcan a flujos establecidos).

4.4. Conclusiones

Tras aplicar las medidas que se propusieron en el estudio teórico, puede concluirse que el uso de la matriz MITRE ATT&CK Enterprise como framework de ciberseguridad es altamente efectivo.

El uso de la matriz nos ha ayudado a comprender cuáles eran las fallas defensivas de la empresa y cuáles eran las medidas necesarias para cubrir dichas fallas. Además, ha servido para conocer con alto grado de confianza la situación actual de la empresa en cuanto a seguridad y cuáles han de ser los siguientes movimientos y las líneas de futuro a seguir para no volver a dejar de lado un asunto tan importante. Gracias a la matriz, ahora la empresa tiene las ideas claras, sabe dónde está y cuáles serán sus próximos pasos.

Cabe mencionar que el nivel de detalle de la matriz es tan minucioso, que no se han podido cubrir todas las fallas, aunque sí que se han cubierto las más importantes y las que más preocupación generaban por su alto riesgo. Con la ayuda de la matriz, el objetivo ahora es seguir mejorando y mantenerse siempre activos de ahora en adelante frente a las ciber amenazas que pueden afectar a la empresa.

En el punto 6 de este documento puede encontrarse el estudio económico que refleja el precio de las implementaciones propuestas en el Estudio Práctico.

5. PLIEGO DE CONDICIONES

Al momento de realización de este documento, las medidas a implementar no se han aplicado de manera real en la empresa. Para poder implementarlas, se han simulado entornos usando los servicios de AWS. Esto no supone ninguna diferencia en cuanto a una implementación en un entorno real, pues las configuraciones son exactamente las mismas independientemente del entorno.

5.1. Web Application Firewall

Para la implementación del WAF se han usado los siguientes servicios de AWS:

- Instancia Ubuntu en LightSail alojando la aplicación 'OWASP Juice Shop', haciendo las veces de aplicación a proteger.
- ACL web.
- Reglas gratuitas para la ACL.
- Otros elementos necesarios por defecto para trabajar con los servicios de AWS: VPCs, subredes, grupos de seguridad, IPs elásticas, etc.

5.2. Firewall Palo Alto (capacidades firewall, IPS y VPN)

- Instancia Virtualizada del firewall con la licencia Bundle 2, que incluye: Global Protect VPN, Threat Prevention (IPS), URL Filtering, DNS Security, WildFire y Premium Support.
- Instancia EC2 situada tras el firewall simulando la red interna de la oficina.
- Otros elementos necesarios por defecto para trabajar con los servicios de AWS: Interfaces virtuales, VPCs, subredes, grupos de seguridad, IPs elásticas, etc.

6. ESTUDIO ECONÓMICO

Para la estimación económica se han incluido los gastos asociados a la creación y mantenimiento de laboratorios para la implementación del estudio práctico y las horas de trabajo empleadas.

El precio de la hora de trabajo se ha tomado, de manera lo más aproximada posible de https://www.linkedin.com/salary/explorer?countryCode=es&geoId=105646813&titleId=109

Concepto	Cantidad	Coste	Horas	TOTAL €
Mano de obra	**1**	**12,24 € / Hora**	**300**	**3672**
Instancia Virtual Firewall Palo Alto Bundle 2 (m4.xlarge)	**1**	**1,55 € / Hora**	**95**	**147,25**
ACL Web	**1**	**5 € / Mes**	**Precio mensual**	**5**
Direcciones IP elásticas	**5**	**3,528 € / Mes**	**5**	**17,64**
Amazon Elastic Compute Cloud running Linux/Unix (t2 medium)	**4**	**0,0464 € / hora**	**120**	**22,27**
Route 53 Registered domain	**1**	**11 € / Dominio**	**Precio fijo por Dominio Registrado**	**11**
GigaBytes of Elastic Block Store (m4.xlarge)	**20**	**0,20 €/GB per month**	**Precio mensual**	**4**
			SUBTOTAL	**3879,16**
			I.V.A	**814,62**
			TOTAL	**4693,78**

Tabla 37 Presupuesto

El presupuesto asciende a **CUATRO MIL SEISCIENTOS NOVENTA Y TRES EUROS CON SETENTA Y OCHO CÉNTIMOS**.

7. LÍNEAS DE FUTURO

Cómo ya se ha mencionado previamente, el uso de la matriz MITRE ATT&CK Enterprise ha servido para conocer de manera clara la situación actual de la empresa y los siguientes pasos que se han de tomar en esta en cuanto a ciberseguridad.

Tras el estudio minucioso de la matriz y las medidas adoptadas, las líneas de futuro que se hacen más evidentes e importantes se describen en los puntos a continuación.

7.1. Masterizar las herramientas implementadas

Tanto El WAF de AWS y el firewall Palo Alto (o de otro vendedor que se pudiese elegir finalmente) aportan más capacidades de las que uno puede esperarse y de las que en un principio se han implementado. Cabe decir que por ejemplo el firewall Palo Alto cuenta con su propia certificación de administrador, lo que nos da una idea del potencial de esta herramienta. Si se ha hecho la inversión, el paso siguiente es tener a alguien en la empresa que sea capaz de masterizar las capacidades de esta herramienta. No basta con crear zonas, asignar políticas y bloquear el acceso a determinados puertos. Podemos analizar minuciosamente cada paquete, trabajar y desgranar las aplicaciones que generan flujos en nuestra red, realizar filtrado de URLs con alto nivel de granularidad, crear políticas complejas, crear redundancia entre interfaces, establecer políticas entre zonas, crear VLANs y aplicar políticas sobre las mismas y/o entre diferentes VLANs y un largo, muy largo etcétera.

7.2. Implementación de un SIEM

A pesar de que se ha realizado un trabajo extenso y la situación de la empresa en cuanto a ciberseguridad ha mejorado considerablemente, se han quedado en el camino la implementación de muchas detecciones.

Ya que la matriz nos ha permitido conocer todos los flancos que pueden cubrirse, ignorarlos no es una opción.

La implementación de un SIEM ayudaría no sólo con las detecciones, si no con la respuesta ante incidentes y en las fases posteriores de análisis.

Algunas de las detecciones y/o monitorizaciones más destacadas que podrían incluirse en el SIEM, serían:

- Monitorización de ficheros: monitorizar y loguear la creación, modificación y borrado de ficheros, sus extensiones y sus metadatos.
- Monitorización de procesos: monitorizar y loguear la ejecución de procesos, en busca de procesos poco habituales o inesperados y registrando las ejecuciones de todos aquellos que se consideren importantes o potencialmente útiles en ataques.
- Monitorización de servicios: monitorizar y loguear los servicios que se ejecutan y las llamadas a los mismos.
- El registro de Windows: monitorizar y loguear la creación, modificación, consultas, etc. de registros del sistema operativo.
- Considerar no sólo la monitorización, logueo y creación de alertas, sino también la posibilidad de bloquear determinadas ejecuciones.

7.3. Revisiones periódicas de la matriz

Vistos y comprobados los buenos resultados que ofrece el uso y aplicación de este framework, considerar revisiones periódicas de la matriz para no dejar nunca de mejorar las capacidades defensivas y de detección y mantener activa siempre las actividades de la empresa en cuanto a ciberseguridad.

8. REFERENCIAS, BIBLIOGRAFÍA Y RECURSOS

[1] Linda Pesante. Introduction to information security [Online]. Disponible en: https://www.cisa.gov/uscert/sites/default/files/publications/infosecuritybasics.pdf [PDF].

[2] Security Scorecoard. Top 25 Cybersecurity Frameworks to Consider [Online]. https://securityscorecard.com/blog/top-cybersecurity-frameworks-to-consider

[3] CVE. Common Vulneravilities and Exposures [Online]. Disponible en: https://cve.mitre.org/

[4] MITRE ATT&CK Enterprise [Online]. Disponible en: https://attack.mitre.org/matrices/enterprise/

[5] MITRE ATT&CK Navigator [Online]. Disponible en: https://mitre-attack.github.io/attack-navigator/

[6] DeTTECT [Online]. Disponible en: https://github.com/rabobank-cdc/DeTTECT

[7] MITRE CALDERA [Online]. Disponible en: https://caldera.mitre.org/

[8] Atomic Red Team [Online]. Disponible en: https://atomicredteam.io/

[8] MITRE ATT&CK [Online]. Disponible en: https://attack.mitre.org/

[9] Paul A. Grassi, James L. Fenton, Elaine M. Newton, Ray A. Perlner, Andrew R. Regenscheid, William E. Burr, Justin P. Richer. Digital Identity Guidelines [Online]. Disponible en: https://pages.nist.gov/800-63-3/sp800-63b.html

[11] Blake E. Strom, Andy Applebaum, Doug P. Miller, Kathryn C. Nickels, Adam G. Pennington, Cody B. Thomas. MITRE ATT&CK: Design and Philosophy [PDF].

[12] Palo Alto Networks. External Dynamic List [Online]. Disponible en: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/external-dynamic-list

[13] Palo Alto Networks. Threat Prevention [Online]. Disponible en: https://docs.paloaltonetworks.com/threat-prevention

[14] Palo Alto Networks. Set Up SAML Authentication [Online]. Disponible en: https://docs.paloaltonetworks.com/globalprotect/9-0/globalprotect-admin/authentication/set-up-external-authentication/set-up-saml-authentication#idd0ddf3b8-127a-4e6e-af3b-624c532ee44c

[15] Palo Alto Networks. Create Interfaces and Zones for GlobalProtect [Online]. Disponible en: https://docs.paloaltonetworks.com/globalprotect/9-1/globalprotect-admin/get-started/create-interfaces-and-zones-for-globalprotect

[16] Palo Alto PA-220. Ficha Técnica [Online]. Disponible en: https://www.paloaltonetworks.es/resources/datasheets/pa-220-specsheet

[17] Palo Alto Networks. Configure SAML SSO for GlobalProtect [Online]. Disponible en: https://live.paloaltonetworks.com/t5/instructor-led-training/configure-saml-sso-for-globalprotect/td-p/254049

[18] Palo Alto Networks. Getting Started: Packet Capture [Online]. Disponible en: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClTJCA0

[19] Palo Alto Networks. Default System Browser for SAML Authentication [Online]. Disponible en: https://docs.paloaltonetworks.com/globalprotect/5-2/globalprotect-app-new-features/new-features-released-in-gp-app/default-browser-for-saml-authentication

[20] Palo Alto Networks. Cookie Authentication on the Portal or Gateway [Online]. Disponible en: https://docs.paloaltonetworks.com/globalprotect/8-1/globalprotect-admin/authentication/about-globalprotect-user-authentication/how-does-the-app-know-what-credentials-to-supply/cookie-authentication-on-the-portal-or-gateway

[21] Palo Alto Networks. Set Up Two-Factor Authentication [Online]. Disponible en: https://docs.paloaltonetworks.com/globalprotect/8-1/globalprotect-admin/authentication/set-up-two-factor-authentication#id8ab40bac-d17f-412b-8a15-a41603b19253

[22] Udemy. Mastering Palo Alto Networks. Plataforma de aprendizaje Udemy [Online]. Disponible en (curso de pago): https://www.udemy.com/course/mastering-palo-alto-networks/

[23] Udemy. Palo Alto Firewalls Configuration By Example PCNSE Prep [Online]. Plataforma de aprendizaje Udemy. Disponible en (curso de pago): https://www.udemy.com/course/draft/591298/

[24] Keycloak [Online]. Disponible en: https://www.keycloak.org/

[25] Keycloak. Getting Started [Online]. Disponible en: https://www.keycloak.org/guides#getting-started

[26] Install Docker Engine on Ubuntu [Online]. Disponible en: https://docs.docker.com/engine/install/ubuntu/

[27] Install Docker Compose [Online]. Disponible en: https://docs.docker.com/compose/install/

[28] AWS Multi-Factor Authentication [Online]. Disponible en: https://aws.amazon.com/es/iam/features/mfa/

[29] AWS Respuesta ante eventos DDoS [Online]. Disponible en: https://docs.aws.amazon.com/es_es/waf/latest/developerguide/ddos-responding.html

[30] AWS Precios de Elastic Load Balancing [Online]. Disponible en: https://aws.amazon.com/es/elasticloadbalancing/pricing/?nc=sn&loc=3

[31] AWS Precios de AWS WAF [Online]. Disponible en: https://aws.amazon.com/es/waf/pricing/

[32] AWS Crear una ACL web [Online]. Disponible en: https://docs.aws.amazon.com/es_es/waf/latest/developerguide/web-acl-creating.html

[33] AWS AWS Load Balancer not reaching LightSail instance [Online]. Disponible en: https://repost.aws/questions/QUiBmA9NGBS0urxsokexscOA/aws-load-balancer-not-reaching-light-sail-instance

[34] OWASP Top 10 Vulnerabilities in 2022 [Online]. Disponible en: https://www.spiceworks.com/it-security/vulnerability-management/articles/owasp-top-ten-vulnerabilities/

[35] SniferL4bs. Curso Burpsuite desde 0. Plataforma de vídeo YouTube [Online]. Disponible en: https://www.youtube.com/watch?v=G6crkGwS8mQ&list=PL4TbrTdoQBY_dZQ9XI9NKwb5evvyfYQNQ&ab_channel=SniferL4bs

[36] HackerSploit. How to install OWASP Juice Shop. Plataforma de vídeo YouTube [Online]. Disponible en: https://www.youtube.com/watch?v=tvNKp1QXV_8&t=275s&ab_channel=HackerSploit

[37] NamrataHShah. Hands on Lab - AWS WAF and AWS ALB. Plataforma de vídeo YouTube [Online]. Disponible en: https://www.youtube.com/watch?v=8G97_8id-NI&ab_channel=NamrataHShah

[38] NamrataHShah. AWS Tutorial - Setup an Application Load Balancer over Http with Linux EC2 webservers. Plataforma de vídeo YouTube [Online]. Disponible en: https://www.youtube.com/watch?v=5PeVd23zAOE&ab_channel=NamrataHShah

[39] Stian Thorgersen. Keycloak Intro. Plataforma de vídeo YouTube [Online]. Disponible en: https://www.youtube.com/watch?v=duawSV69LDI&ab_channel=StianThorgersen

[40] Krish Dinesh. Single sign on (SSO) with Keycloak + Active Directory + Angular | Microservice Security Practical. Plataforma de vídeo YouTube [Online]. Disponible en: https://www.youtube.com/watch?v=ZUpIGxEDz4k&ab_channel=KrishDinesh

[41] CodeLens. Keycloak Tutorial Series - Authenticator Part 1. Plataforma de vídeo YouTube [Online]. Disponible en: https://www.youtube.com/watch?v=BCklDn5K6C4&ab_channel=CodeLens

[42] Niko Köbler (@dasniko). 2FA with Keycloak and SMS based OTP text messages | Niko Köbler (@dasniko). Plataforma de vídeo YouTube [Online]. Disponible en: https://www.youtube.com/watch?v=GQi19817fFk&t=383s&ab_channel=NikoK%C3%B6bler%28%40dasniko%29

[43] StackOverflow. "HTTPS required" while logging in to Keycloak as admin [Online]. Disponible en: https://stackoverflow.com/questions/30622599/https-required-while-logging-in-to-keycloak-as-admin

ANEXO I: USANDO ATT&CAK NAVIGATOR

En este anexo se dará una visión general de las principales utilidades que ofrece Navigator y que nos serán de utilidad posteriormente en nuestro análisis teórico y práctico.

Controles de selección

Permiten establecer el comportamiento a la hora de seleccionar técnicas; buscar técnica y subtécnicas; seleccionar de una sola vez todas las técnicas que estén relacionadas con un grupo de amenazas, un determinado software o una determinada mitigación y limpiar todas las selecciones realizadas. Los controles de selección se muestran en la siguiente figura

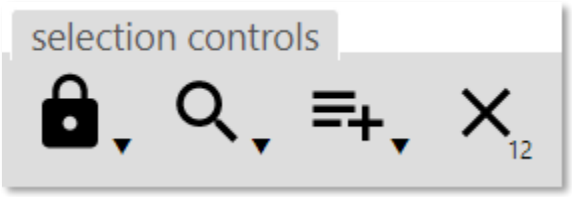


Figura 35 Controles de Selección

Controles de capa

Con los controles de capa podemos:

- Configurar la información de la capa: Nombre, descripción y metadatos (pares clave y valor).
- Descargar el estado actual del Navigator en formato json, excel o svg. El formato json puede ser leído y representa en Navigator mediante programación.
- Seleccionar la plataforma sobre la que se va a trabajar: Windows. Linux, macOS, AWS, GCP, Azure, Azure AD, Office 365, SaaS. Seleccionando o deseleccionando plataformas, la cantidad de técnicas y subtécnicas presentes para cada táctica puede aumentarse o reducirse.
- Seleccionar la etapa: preparación o actuación.
- Mostrar ocultar elementos, ordenar por orden alfabético creciente o decreciente, expandir/contraer técnicas y subtécnicas y cambiar la visualización de la matriz (layout).

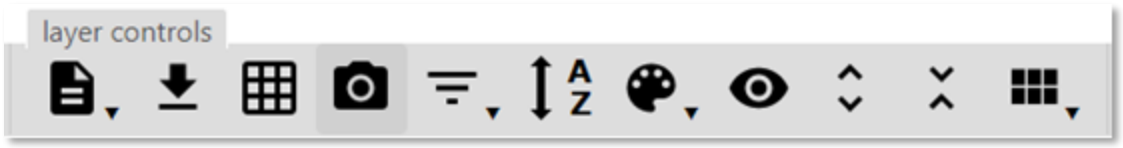


Figura 36 Controles de capa

Control de técnicas

Para trabajar con las técnicas y/o subtécnicas seleccionadas, permitiendo: Resaltar o apagar su visualización, asignarles diferentes colores, asignarles puntuación y/o incluir comentarios.

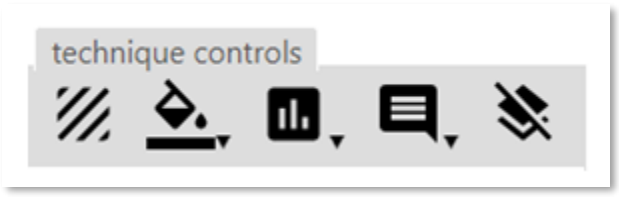


Figura 37 Controles de Técnicas

Algunos ejemplos de uso

Se muestran a continuación algunos ejemplos de uso y se describe cómo realizarlos.

a) Seleccionar todas las técnicas y subtécnicas que pueden mitigarse usando un Antivirus/Antimalware.

En los controles de selección navegamos a *Multi Select* < *Mitigations* y seleccionamos *Antivirus/Antimalware*. Una vez seleccionados, Con los controles de técnicas le damos el color verde.

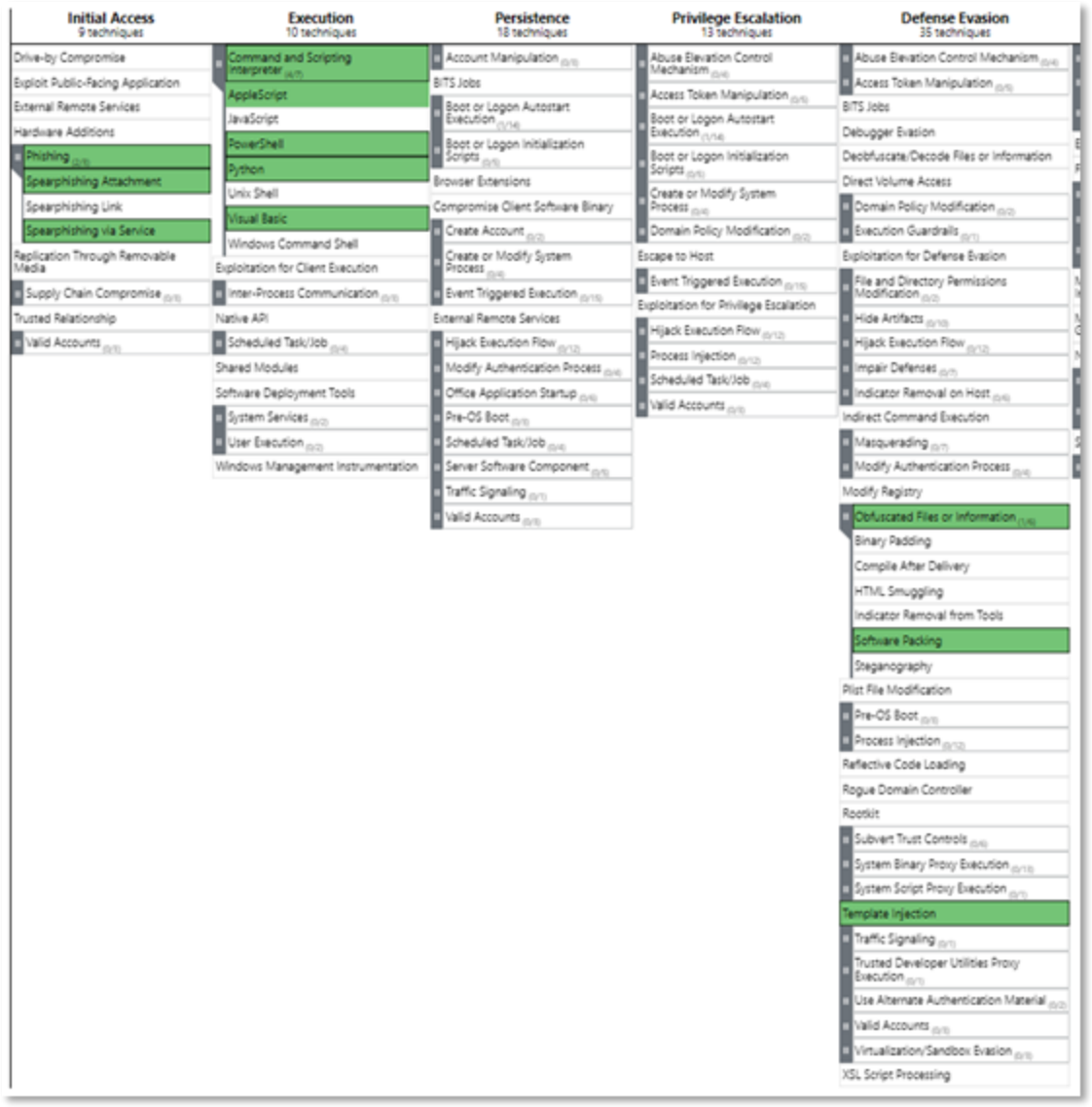


Figura 38 Mitigación Antivirus y técnicas y subtécnicas afectadas

b) Crear una capa que muestre las técnicas y subtécnicas de un determinado Threat Group, por ejemplo Blue MockingBird.

Cómo ya se vió en ‘2.1. Definición y características’, los grupos representan a atacantes conocidos que son rastreados por organizaciones públicas y privadas y reportados en informes de inteligencia de amenazas. Concretamente el grupo Blue MockingBird es un grupo relacionado, entre otras actividades, con el minado de la

criptomoneda Monero haciendo uso de payload en DLLs (Dinamic-Link Libraries) en sistemas Windows.

En los controles de selección navegamos a *Multi Select* < *Threat Groups* y seleccionamos *Blue MockingBird*. Una vez seleccionados, Con los controles de técnicas le damos el color azul.

Figura 39 Técnicas y subtécnicas conocidas del grupo Blue MockingBird

c) Descubrir qué técnicas y subtécnicas quedarían más cubiertas si usamos las mitigaciones 'Política de contraseñas' y ‘Autenticación Multi-factor' (a efectos de mejor visualización, se muestra sólo una parte de la matriz).

Creamos una capa a la que llamaremos 'Políticas', seleccionamos todas las técnicas y subtécnicas relacionadas con esta mitigación (*Multi Select* < *Mitigations* y seleccionamos *Password Policies*).

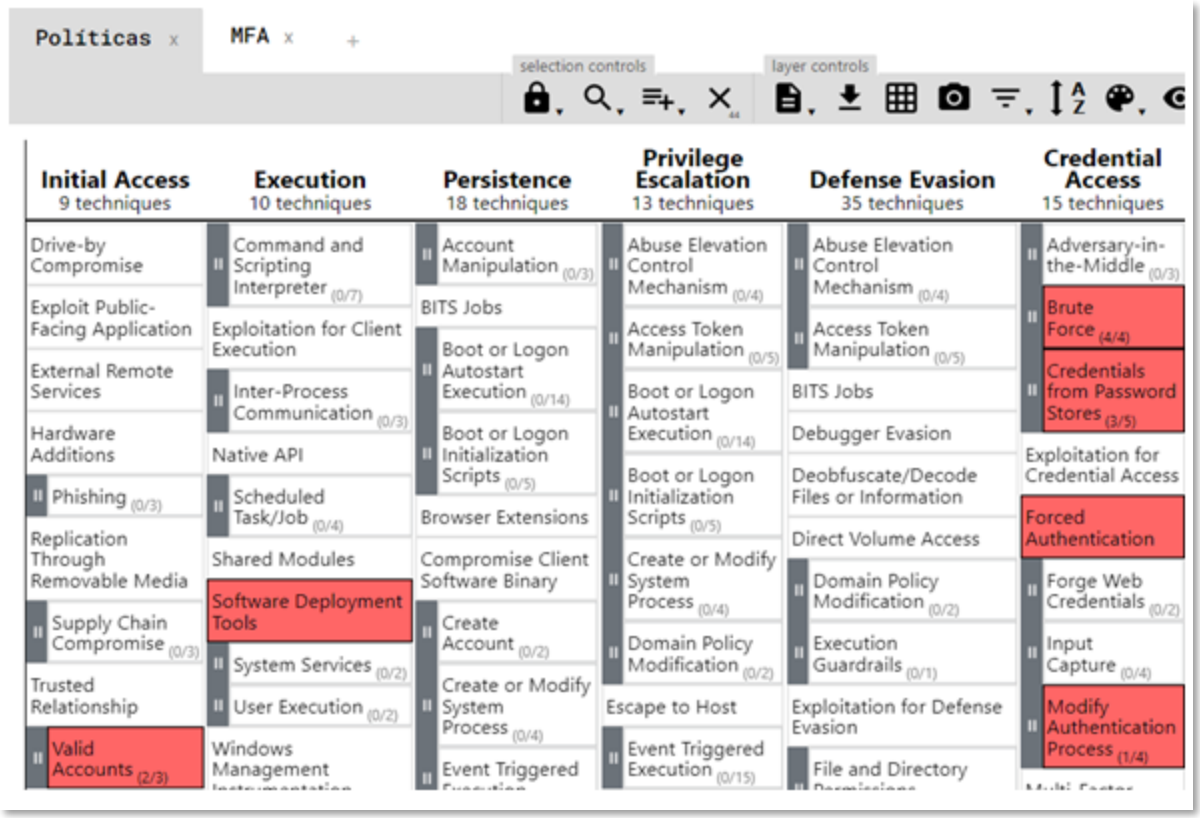


Figura 40 Técnicas afectadas por mitigaciones 'Política de contraseñas'

En Control de Técnicas le damos una puntuación de 1 (este valor se da con el objetivo de sumar capas hasta un valor máximo de 3) y en Control de Capa configuramos los colores para que el valor mínimo sea 1 y el máximo 3.

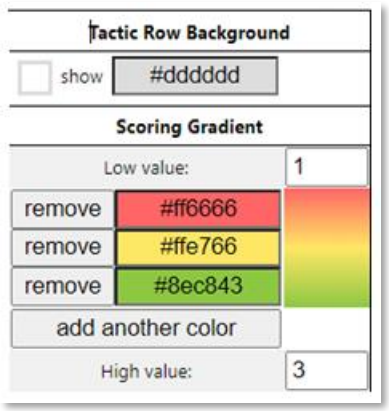


Figura 41 Valores numéricos y color asociado

Creamos otra capa llamada 'MFA' y seleccionamos todas las técnicas y subtécnicas relacionadas con esta mitigación (*Multi Select* < *Mitigations* y seleccionamos

Multi-factor Authentication). En control de técnicas le damos una puntuación de 2 (este valor se da con el objetivo de sumar capas hasta un valor máximo de 3) y en Control de Capa configuramos los colores para que el valor mínimo sea 1 y el máximo 3.

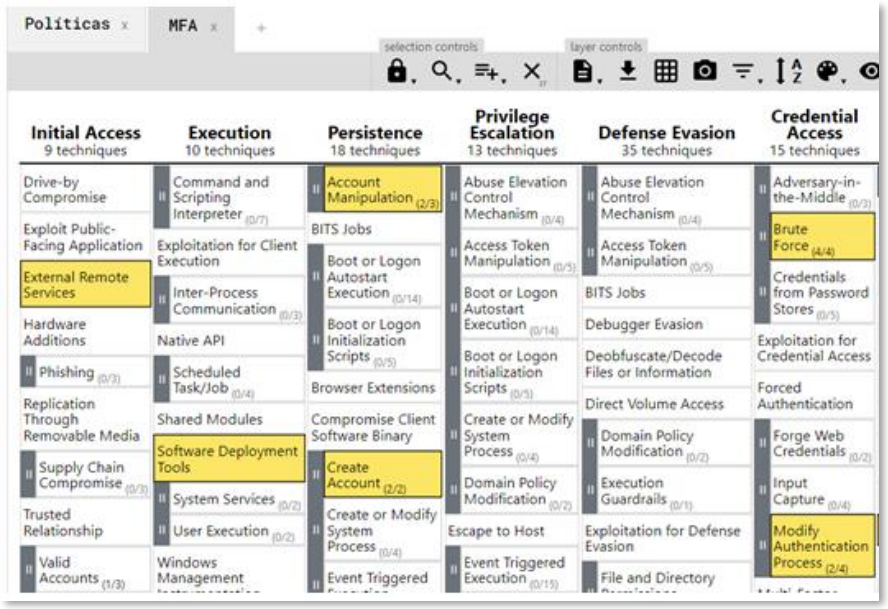


Figura 42 Capa 'MFA'

Creamos una tercera capa del tipo 'Create Layer from other Layers' y sumamos las capas 'a' y 'b' creadas previamente.

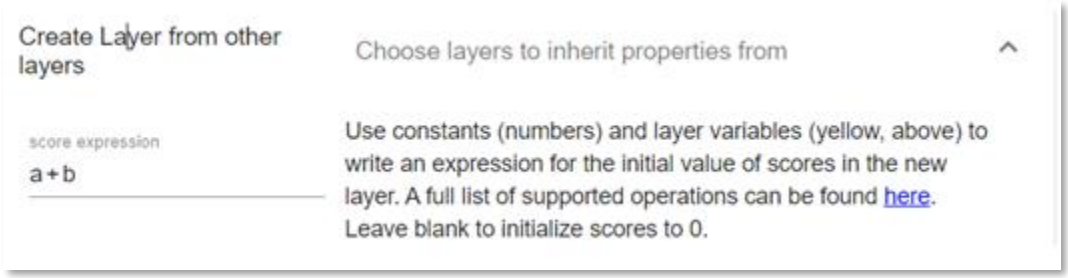


Figura 43 Sumado de capas

Como resultado, obtenemos una tercera capa (que hemos llamado 'PP+MFA') en la que las técnicas y subtécnicas afectadas por ambas mitigaciones presentan una puntuación de 3 (la suma de los valores 1 y 2 dados en las capas previas) y aparecen coloreadas en verde (esto es totalmente customizable).

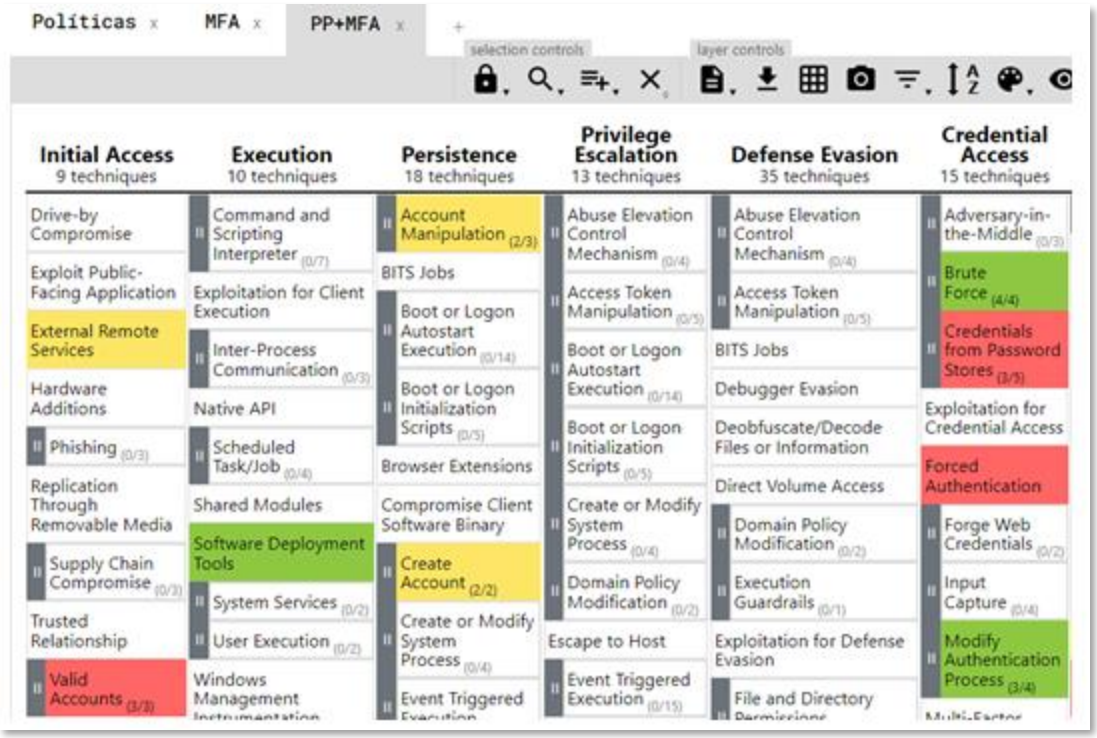


Figura 44 Política de contraseñas + MFA

Con unas simples configuraciones, sabemos que técnicas como 'Software Development Deployment', 'Brute Force' o 'Modify Authentication Procces' quedarán más cubiertas en cuanto a mitigación si aplicamos las mitigaciones propuestas Password Policies y Multi Factor-Authentication.

ANEXO II: AMPLIACIÓN ESTUDIO TEÓRICO

En este anexo se incluyen todas aquellas técnicas y subtécnicas estudiadas durante el estudio teórico y que no se incluyeron en el mismo por cuestiones de extensión del documento. Se muestran nuevamente las tácticas (sin descripción) y las técnicas y subtécnicas no incluidas previamente.

Táctica: Reconocimiento

Active Scanning

Los atacantes realizan actividades de reconocimiento para obtener información que puede ser usada a la hora de fijar objetivos. Estas actividades de reconocimiento, al ser activas, implican de alguna forma interacción con la empresa objetivo.

Puntuación: 5. No merece el esfuerzo ni el coste para los resultados que se prevén obtener.

Justificación

No pueden tomarse mitigaciones ni detecciones considerables o que vayan a suponer una diferencia notable debido a:

- La información está disponible en Internet y no se tiene control sobre la misma. Ej. No hay control sobre lo que muestra la herramienta WHOIS si se ejecuta sobre una IP de las instancias en AWS, ya que va a mostrar información sobre el vendedor AWS.
- La empresa no cuenta con un rango considerable de IPs. Tiene IP pública que le proporciona el proveedor de servicios en la oficina y en las aplicaciones web se toman las IPs (elásticas o no) que proporciona el vendedor AWS.

A pesar de lo anterior, se ha considerado que es importante que la empresa reconozca esta técnica y comience a ser consciente de su exposición en la red.

Mitigaciones: No.

Detecciones: No.

Gather Victim Host Information

Los atacantes tratan de obtener información sobre los posibles host objetivo: IPs, funcionalidad, sistema operativo, etc.

Puntuación: 5. No merece el esfuerzo ni el coste para los resultados que se preveen obtener.

Justificación

No pueden tomarse mitigaciones ni detecciones considerables o que vayan a suponer una diferencia notable debido a:

- Información está disponible en Internet y no se tiene control sobre la misma. Ej. Podría ocultarse información sobre nuestro servidor (Server: Nginx o Server: Apache), pero los atacantes podrían extraer esta información usando herramientas potentes que obtengan esta información por como el servidor responde a determinadas peticiones.

A pesar de lo anterior, se ha considerado que es importante que la empresa reconozca esta técnica y comience a ser consciente de su exposición en la red.

Mitigaciones: No.

Detecciones: No.

Gather Victim Identity Information

Los atacantes tratan de obtener información sobre sus víctimas tal como nombres de empleados, direcciones de correo, direcciones postales, credenciales, etc.

Puntuación: 5.

Justificación

No pueden tomarse mitigaciones ni detecciones considerables o que vayan a suponer una diferencia notable debido a:

Información está disponible en Internet (o de otra forma, pero públicamente) y no se tiene control sobre la misma. Ej: Redes sociales como LinkedIn se exponen las

direcciones de correo de miembros de la empresa. Están expuestas conscientemente y además desde la empresa se pretende que lo sean ya que suponen una herramienta para que otros profesionales puedan iniciar contacto.

A pesar de lo anterior, se ha considerado que es importante que la empresa reconozca esta técnica y comience a ser consciente de su exposición en la red.

Mitigaciones: No.

Detecciones: No.

Gather Victim Network Information

Los atacantes tratan de obtener información sobre la red de sus víctimas. Esta información puede ser IPs y/o rangos de IPs, DNS, topología, etc.

Puntuación: 5.

Justificación

No pueden tomarse mitigaciones ni detecciones considerables o que vayan a suponer una diferencia notable debido a:

Información está disponible en Internet y no tenemos control sobre la misma. Ej: No podemos evitar que alguien haga un NSLOOKUP sobre el dominio de nuestras aplicaciones web públicas en Internet y obtenga la IP asociada a nuestro dominio. Obtenida la IP comprobará que corresponde a AWS en incluso podrá saber la zona de disponibilidad en la que se encuentran los servidores que alojan las aplicaciones.

A pesar de lo anterior, se ha considerado que es importante que la empresa reconozca esta técnica y comience a ser consciente de su exposición en la red.

Mitigaciones: No.

Detecciones: No.

Táctica: Acceso Inicial

Drive-by Compromise

Los atacantes tratan de ganar acceso al equipo de su víctima haciendo, por ejemplo, que este visite un determinado sitio web. Es muy común que el elemento atacado sea el navegador web de la víctima.

Puntuación: 3. Importancia Media. Cualquier usuario en Internet es víctima potencial para esta técnica

Justificación

En el día a día de los trabajadores, estos pueden visitar determinados sitios webs que podría estar infectados o se podría hacer uso de navegadores con vulnerabilidades conocidas. Aunque no es una de las prioridades, algunas de las mitigaciones o detecciones son sencillas de implementar.

MITIGACIONES	
ID	Mitigación
M1050	Exploit Protection
M1021	Restrict Web-Based Content

Tabla 38 Mitigaciones Drive-by compromise (Acceso Inicial)

DETECCIONES		
ID	Fuente de datos	Componente
DS0015	Application Log	Application Log Content
DS0029	Network Traffic	Network Connection Creation

Tabla 39 Detecciones Drive-by compromise (Acceso Inicial)

Phising

Los atacantes podrían enviar mensajes de phishing con el objetivo de ganar acceso al equipo de la víctima.

Puntuación: 2. Importancia Alta. Cualquier usuario en Internet es víctima potencial de phishing.

Justificación

Se ha comentado previamente y se ha confirmado que los intentos de phishing suponen una amenaza grave para la empresa dadas las nefastas consecuencias que puede tener en caso de resultar exitosos.

MITIGACIONES	
ID	Mitigación
M1049	Antivirus/Antimalware
M1031	Network Intrusion Prevention
M1021	Restrict Web-Based
M1054	Software Configuration
M1017	User Training

Tabla 40 Mitigaciones Phising (Acceso Inicial)

DETECCIONES		
ID	Fuente de datos	Componente
DS0015	Application Log	Application Log Content
DS0029	Network Traffic	Network Connection Creation
		Network Traffic Content

Tabla 41 Detecciones Phising (Acceso Inicial)

Táctica: Ejecución

Python

Los atacantes usarían el lenguaje Python para cumplir sus objetivos. Podrían usarlo mediante scripts o en la línea de comandos, por ejemplo.

Puntuación: 3. Importancia Media. Se contempla el uso de Python.

Justificación

Los desarrolladores de la empresa utilizan Python en sus tareas de desarrollo diarias.

Muchas de las mitigaciones no pueden aplicarse ya que los trabajadores necesitan que el uso de Python no esté denegado en ninguna de sus formas.

MITIGACIONES	
ID	Mitigación
M1049	Antivirus/Antimalware

Tabla 42 Mitigaciones Python (Ejecución)

Detecciones: No. Se considera suficiente con las mitigaciones.

User Execution

Los atacantes esperan o aprovechan determinadas acciones de las víctimas para realizar determinadas acciones.

Puntuación: 3. Importancia Media. Guarda relación con intentos de phishing.

Justificación

Ya que se ha dado bastante importancia a las mitigaciones frente al phishing, se debe hacer lo mismo con los pasos posteriores a un phishing exitoso.

MITIGACIONES	
ID	Mitigación
M1031	Network Intrusion Prevention
M1021	Restrict Web-Based Content
M1017	User Training

Tabla 43 Mitigaciones User Execution (Ejecución)

DETECCIONES		
ID	Fuente de datos	Componente
DS0017	Command	Command Execution
DS0029	Network Traffic	Network Connection Creation
		Network Traffic Content

Tabla 44 Detecciones User Execution (Ejecución)

Táctica: Persistencia
Boot or Logon Autostart Execution

Los atacantes podrían configurar elementos en un sistema para que se ejecute un determinado programa en el momento de iniciar dicho sistema.

Puntuación: 5. Importancia Baja. No se considera una técnica a la que dedicar recursos por el momento.

Justificación

Aunque por el momento no se pretende implementar mitigaciones o detecciones, desde los responsables de la empresa se ha decidido que se tendrá en cuenta para futuras revisiones de la matriz.

Mitigaciones: No.

Detecciones: No.

Boot or Logon Initialization Scripts

Los atacantes podrían configurar elementos en un sistema para que se ejecute un determinado script en el momento de iniciar dicho sistema.

Puntuación: 5. Importancia Baja. No se considera una técnica a la que dedicar recursos por el momento.

Justificación

Aunque por el momento no se pretende implementar mitigaciones o detecciones, desde el personal de la empresa se ha decidido que se tendrá en cuenta para futuras revisiones de la matriz.

Mitigaciones: No.

Detecciones: No

Browser Extensions

Los atacantes podrían usar extensiones del navegador para ganar persistencia en el acceso al sistema o sistemas víctima.

Puntuación: 3. Importancia Media. El uso de navegadores es imprescindible.

Justificación

Los navegadores son una herramienta fundamental de todos los empleados de la empresa. Es amplia y frecuentemente usada.

MITIGACIONES	
ID	Mitigación
M1047	Audit
M1033	Limit Software Installation
M1051	Update Software
M1017	User Training

Tabla 45 Mitigaciones Browser Extensions (Persistencia)

DETECCIONES		
ID	Fuente de datos	Componente
DS0029	Network Traffic	Network Connection Creation

Tabla 46 Detecciones Browser Extensions (Persistencia)

Compromise Client Software Binary

Los atacantes podrían usar binarios modificados y ganar así persistencia en los equipos víctima.

Puntuación: 3. Importancia Media. Se contempla la descarga y uso de software.

Justificación

En el día a día de la empresa es normal descargar y utilizar software cliente (Ej. Software cliente para conectar con la VPN).

MITIGACIONES	
ID	Mitigación
M1045	Code Signing

Tabla 47 Mitigaciones Compromise Client Software Binary (Persistencia)

Cloud Account

Los atacantes podrían crear cuentas adicionales en los servicios en la nube de manera que ganasen persistencia a la hora de acceder a los equipos víctima.

Puntuación: 3. Importancia Media. Existencia de cuentas en la nube.

Justificación

Se ha de tener un control absoluto sobre las cuentas en las plataformas de servicios en la nube, en este caso AWS.

MITIGACIONES	
ID	Mitigación
M1032	Multi-factor Authentication
M1030	Network Segmentation
M1026	Privileged Account Management

Tabla 48 Mitigaciones Cloud Account (Persistencia)

DETECCIONES		
ID	Fuente de datos	Componente
DS0002	User Account	User Account Creation

Tabla 49 Detecciones Cloud Account (Persistencia)

Local Account

Los atacantes podrían crear cuentas locales adicionales de manera que ganasen persistencia a la hora de acceder a los equipos víctima.

Puntuación: 3. Importancia Media. Existencia de cuentas locales.

Justificación

Se ha de tener un control absoluto sobre las cuentas locales de las aplicaciones, de los equipos de la oficina, de las cuentas de acceso a la VPN y de la cuenta de gestión del firewall de la oficina.

También se tendrá control absoluto sobre otras posibles cuentas que den acceso a herramientas autorizadas por la empresa y usadas en la misma.

MITIGACIONES	
ID	Mitigación
M1032	Multi-factor Authentication
M1026	Privileged Account Management

Tabla 50 Mitigaciones Local Account (Persistencia)

DETECCIONES		
ID	Fuente de datos	Componente
DS0002	User Account	User Account Creation

Tabla 51 Detecciones Local Account (Persistencia)

Create or Modify System Processes

Los atacantes podrían crear o modificar procesos a nivel de sistema que les permitiesen ejecutar repetidamente código malicioso. A efectos prácticos sería persistencia en la ejecución.

Puntuación: 4. Importancia Media. De momento no se van a destinar recursos frente a esta técnica.

Justificación

Aunque ahora no supone una de las técnicas más preocupantes, sí que son una de las técnicas que desde la empresa se ha decidido tener en el punto de mira para futuras revisiones de la matriz.

Mitigaciones: No.

Detecciones: No.

External Remote Services

Los atacantes tratan de aprovechar el uso de servicios expuestos en Internet y que podrían dar acceso a redes internas.

Puntuación: 1. Importancia Muy Alta. Se pretende implementar la capacidad de acceso remoto.

Justificación

Abrir los puertos en el router de la oficina y redirigir conexiones a equipos en la red interna para tener acceso a los equipos de la oficina no es una opción que se contemple de ninguna manera. Esto supondría una invitación al desastre más absoluto.

Si se necesitan accesos remotos a equipos y ficheros en la oficina, por causas de teletrabajo o accesos fuera del horario de trabajo normal, esto se hará bajo conexiones protegidas y cifradas mediante el uso de VPNs.

MITIGACIONES	
ID	Mitigación
M1035	Limit Access to Resource Over Network
M1032	Multi-factor Authentication
M1030	Network Segmentation
M1042	Disable or Remove Feature or Program

Tabla 52 Mitigaciones External Remote Services (Persistencia)

DETECCIONES		
ID	Fuente de datos	Componente
DS0015	Application Log	Application Log Content
DS0029	Network Traffic	Network Traffic Flow
DS0028	Logon	Logon Session Metadata

Tabla 53 Detecciones External Remote Services (Persistencia)

Valid Accounts

Los atacantes tratan de ganar acceso usando cuentas válidas y/o credenciales comprometidas.

Puntuación: 1. Importancia Muy Alta. Proteger las credenciales es uno de los principales objetivos.

Justificación

Por la actividad de la empresa, el uso de credenciales y la existencia de formularios de acceso público están muy presentes y son ampliamente usados:

Las aplicaciones web son accesibles previa autenticación y los formularios de login están expuestos públicamente al acceder a las aplicaciones.

El acceso a la consola de AWS se realiza mediante credenciales. Este acceso es público y es el mismo para todos los usuarios de AWS.

El acceso a la VPN se realiza mediante autenticación en el cliente VPN.

MITIGACIONES	
ID	Mitigación
M1013	Application Developer Guidance
M1027	Password Policies
M1026	Privileged Account Management
M1018	User Account Management
M1017	User Training

Tabla 54 Mitigaciones Valid Accounts (Persistencia)

DETECCIONES		
ID	Fuente de datos	Componente
DS0028	Logon Session	Logon Session Creation
DS0002	User Account	User Account Authentication

Tabla 55 Detecciones Valid Accounts (Persistencia)

Táctica: Escalado de Privilegios
Boot or Logon Autostart Execution

Los atacantes podrían configurar elementos en un sistema para que se ejecute un determinado programa en el momento de iniciar dicho sistema.

Puntuación: 5. Importancia Baja. No se considera una técnica a la que dedicar recursos por el momento.

Justificación

Aunque por el momento no se pretende implementar mitigaciones o detecciones, desde los responsables de la empresa se ha decidido que se tendrá en cuenta para futuras revisiones de la matriz.

Mitigaciones: No.

Detecciones: No.

Boot or Logon Initialization Scripts

Los atacantes podrían configurar elementos en un sistema para que se ejecute un determinado script en el momento de iniciar dicho sistema.

Puntuación: 5.

Justificación

Aunque por el momento no se pretende implementar mitigaciones o detecciones, desde el personal de la empresa se ha decidido que se tendrá en cuenta para futuras revisiones de la matriz.

Mitigaciones: No.

Detecciones: No

Valid Accounts

Los atacantes tratan de ganar acceso usando cuentas válidas y/o credenciales comprometidas.

Puntuación: 1. Importancia Muy alta. La protección de cuentas y credenciales es uno de los objetivos principales.

Justificación

Por la actividad de la empresa, el uso de credenciales y la existencia de formularios de acceso público están muy presentes y son ampliamente usados:

Las aplicaciones web son accesibles previa autenticación y los formularios de login están expuestos públicamente al acceder a las aplicaciones.

El acceso a la consola de AWS se realiza mediante credenciales. Este acceso es público y es el mismo para todos los usuarios de AWS.

El acceso a la VPN se realiza mediante autenticación en el cliente VPN.

MITIGACIONES	
ID	Mitigación
M1013	Application Developer Guidance
M1027	Password Policies
M1026	Privileged Account Management
M1018	User Account Management
M1017	User Training

Tabla 56 Mitigaciones Valid Accounts (Escalado de Privilegios)

DETECCIONES		
ID	Fuente de datos	Componente
DS0028	Logon Session	Logon Session Creation
DS0002	User Account	User Account Authentication

Tabla 57 Detecciones Valid Accounts (Escalado de Privilegios)

Táctica: Evasión de defensas
Valid Accounts

Los atacantes tratan de ganar acceso usando cuentas válidas y/o credenciales comprometidas.

Puntuación: 1. Importancia Muy alta. La protección de cuentas y credenciales es uno de los objetivos principales.

Justificación

Por la actividad de la empresa, el uso de credenciales y la existencia de formularios de acceso público están muy presentes y son ampliamente usados:

Las aplicaciones web son accesibles previa autenticación y los formularios de login están expuestos públicamente al acceder a las aplicaciones.

El acceso a la consola de AWS se realiza mediante credenciales. Este acceso es público y es el mismo para todos los usuarios de AWS.

El acceso a la VPN se realiza mediante autenticación en el cliente VPN.

MITIGACIONES	
ID	Mitigación
M1013	Application Developer Guidance
M1027	Password Policies
M1026	Privileged Account Management
M1018	User Account Management
M1017	User Training

Tabla 58 Mitigaciones Valid Accounts (Evasión de Defensas)

DETECCIONES		
ID	Fuente de datos	Componente
DS0028	Logon Session	Logon Session Creation
DS0002	User Account	User Account Authentication

Tabla 59 Detecciones Valid Accounts (Evasión de Defensas)

Táctica: Acceso a Credenciales
Adversary in the Middle

Los atacantes podrían posicionarse entre dos o más dispositivos de red y capturar el tráfico o incluso modificarlo.

Puntuación: 3. Importancia Media. Cualquier usuario de Internet o de una red local es víctima en potencia.

Justificación

La protección de las credenciales y ante accesos no autorizados es uno de los objetivos principales de la empresa.

MITIGACIONES	
ID	Mitigación
M1041	Encrypt Sensitive Information
M1035	Limit Access to Resource Over Network
M1037	Filter Network Traffic
M1031	Network Intrusion Prevention
M1030	Network Segmentation
M1017	User Training

Tabla 60 Mitigaciones Adversary in the Middle (Credential Access)

DETECCIONES		
ID	Fuente de datos	Componente
DS0015	Application Log	Application Log Content
DS0029	Network Traffic	Network Traffic Content
		Network Traffic Flow

Tabla 61 Detecciones Adversary in the Middle (Credential Access)

Credentials from Password Stores

Los atacantes podrían buscar en lugares en los que comúnmente se suelen almacenar credenciales.

Puntuación: 3. Importancia Media. Se usan gestores de contraseñas (ej. Keepass).

Justificación

La mayoría de las mitigaciones son sencillas de aplicar y pueden ser implementadas, añadiendo un plus de seguridad.

MITIGACIONES	
ID	Mitigación
M1027	Password Policies
M1054	Software Configuration
M1051	Update Software

Tabla 62 Mitigaciones Credentials from Password Stores (Credential Access)

Detecciones: No. Se considera suficiente con las mitigaciones.

Forced Authentication

Los adversarios pueden recopilar material de credenciales invocando u obligando a un usuario a proporcionar automáticamente información de autenticación a través de un mecanismo que pueden interceptar.

Puntuación: 3. Importancia Media. Uso extensivo de credenciales y herramientas/plataformas que requieren autenticación.

Justificación

Debido al continuo uso de credenciales por parte de los empleados para acceder a la nube y a otros servicios, dichas credenciales están en tránsito de manera frecuente.

MITIGACIONES	
ID	Mitigación
M1037	Filter Network Traffic
M1027	Password Policies

Tabla 63 Mitigaciones Forced Authentication (Acceso a Credenciales)

DETECCIONES		
ID	Fuente de datos	Componente
DS0029	Network Traffic	Network Traffic Content
		Network Traffic Flow

Tabla 64 Detecciones Forced Authentication (Acceso a Credenciales)

Forge Web Credentials

Los atacantes podrían falsificar material de credenciales para acceder a servicios. Este material podrían ser cookies, tokens o cualquier otro elemento usado para autenticar y autorizar usuarios.

Puntuación: 3. Importancia Media. La empresa cuenta con aplicaciones web.

Justificación

Se necesita imperantemente proteger las credenciales web ante cualquier intento de falsificación de estas.

MITIGACIONES	
ID	Mitigación
M1047	Audit
M1026	Privileged Account Management
M1054	Software Configuration
M1018	User Account Management

Tabla 65 Mitigaciones Forge Web Credentials (Acceso a Credenciales)

DETECCIONES		
ID	Fuente de datos	Componente
DS0028	Logon Session	Logon Session Creation
DS0002	Web Credential	Web Credential Creation
		Web Credential Usage

Tabla 66 Detecciones Forge Web Credentials (Acceso a Credenciales)

Multi-Factor Authentication Interception

Los atacantes podrían interceptar u obtener mecanismos que podrían proporcionar credenciales (generadores de token, Smart cards, etc.).

Puntuación: 5. Importancia Muy Baja.

Justificación

Puesto que vamos a usar al menos 2FA es importante tener en cuenta este aspecto. Las soluciones que se pretenden implementar ya incorporan las mitigaciones necesarias y/o no se ven afectadas (Ej. no se van a implementar tokens físicos o tarjetas).

Mitigaciones: No

Detecciones: No.

Multi-Factor Authentication Request Generation

Los atacantes podrían intentar saltarse un proceso de MFA y ganar acceso a cuentas generando falsas solicitudes de MFA.

Puntuación: 3. Importancia Media. El riesgo no es alto, pero existe.

Justificación

Aunque se pretende usar sistemas de 2FA o MFA seguros o que no tienen vulnerabilidades conocidas, es conveniente mitigar esta técnica. Además, las mitigaciones son fácilmente aplicables.

MITIGACIONES	
ID	Mitigación
M1036	Account Use Policies
M1032	Multi-factor Authentication
M1017	User Training

Tabla 67 Mitigaciones Multi-Factor Authentication Request Generation (Acceso a Credenciales)

Detecciones: No. Se considera suficiente con las mitigaciones.

OS Credential Dumping

Los atacantes podrían intentar un volcado de credenciales para obtener información sobre cuentas o credenciales.

Puntuación: 4. Importancia Baja. Merece la pena ser tenida en cuenta para el futuro.

Justificación

Aunque no se van a implementar mitigaciones o detecciones para esta técnica y sus subtécnicas, se ha marcado para ser tenida en cuenta en futuras revisiones de la matriz.

Mitigaciones: No.

Detecciones: No.

Steal Web Session Cookie

Los atacantes podrían robar cookies de sesiones de servicios o aplicaciones web y usarlas para obtener acceso a aplicaciones web o servicios de Internet como un usuario autenticado sin necesidad de credenciales.

Puntuación: 4. Importancia Baja. Merece la pena ser tenida en cuenta para el futuro.

Justificación

Aunque no se van a implementar mitigaciones o detecciones para esta técnica y sus subtécnicas, se ha marcado para ser tenida en cuenta en futuras revisiones de la matriz.

Mitigaciones: No.

Detecciones: No.

Unsecured Credentials

Los atacantes podrían buscar equipos que comprometer y que pudiesen contener contraseñas almacenadas de manera insegura.

Puntuación: 4. Importancia Baja. Merece la pena ser tenida en cuenta para el futuro.

Justificación

Aunque no se van a implementar mitigaciones o detecciones para esta técnica y sus subtécnicas, se ha marcado para ser tenida en cuenta en futuras revisiones de la matriz.

Mitigaciones: No.

Detecciones: No.

Táctica: Descubrimiento
Network Service Discovery

Los atacantes podrían intentar obtener una lista de servicios que se ejecutan en hosts remotos y dispositivos de infraestructura de red local, incluidos aquellos que pueden ser vulnerables a la explotación remota de software.

Puntuación: 3. Importancia Media. Se cuenta con infraestructura de red local y en la nube.

Justificación

Tanto en la empresa como en la nube, se utilizan servicios de red que pueden o podrían estar expuestos públicamente.

MITIGACIONES	
ID	Mitigación
M1042	Disable or Remove Feature or Program
M1031	Network Intrusion Prevention
M1030	Network Segmentation

Tabla 68 Mitigaciones Network Service Discovery (Descubrimiento)

DETECCIONES		
ID	Fuente de datos	Componente
DS0025	Cloud Service	Cloud Service Enumeration
DS0017	Command	Command Execution
DS0029	Network	Network Traffic Flow

Tabla 69 Detecciones Network Service Discovery (Descubrimiento)

Táctica: Movimiento Lateral
Exploitation of Remote Services

Los atacantes podrían explotar servicios remotos para ganar acceso no autorizado a sistemas internos una vez se encuentre dentro de la red atacada.

Puntuación: 2. Importancia Alta. Se cuenta con servicios expuestos públicamente.

Justificación

Los servicios que se ejecutan en la nube podrían ser vulnerables al estar expuestos públicamente.

MITIGACIONES	
ID	Mitigación
M1042	Disable or Remove Feature or Program
M1050	Exploit Protection
M1030	Network Segmentation
M1026	Privileged Account Management
M1051	Update Software
M1016	Vulnerability Scanning

Tabla 70 Mitigaciones Exploitation of Remote Services (Movimiento Lateral)

DETECCIONES		
ID	Fuente de datos	Componente
DS0015	Application Log	Application Log Content
DS0029	Network Traffic	Traffic Content

Tabla 71 Detecciones Exploitation of Remote Services (Movimiento Lateral)

Táctica: Exfiltración
Exfiltration Over Alternative Protocol

Los atacantes podrían robar datos exfiltrándolos a través de un protocolo diferente al del canal de comando y control existente.

Puntuación: 3. Importancia Media. Uso extensivo de protocolos de comunicación.

Justificación

En las tareas diarias de la empresa se hace uso de protocolos alternativos como FTP, HTTP/S, DNS, etc. Si los atacantes pueden usarlos para exfiltrar información, sería conveniente tenerlos controlados en la medida de lo posible.

MITIGACIONES	
ID	Mitigación
M1037	Filter Network Traffic
M1031	Network Intrusion Prevention
M1030	Network Segmentation

Tabla 72 Mitigaciones Exfiltration Over alternative Protocol (Exfiltración)

DETECCIONES		
ID	Fuente de datos	Componente
DS0029	Network Traffic	Network Traffic Content
		Network Connection Creation
		Network Traffic Flow

Tabla 73 Detecciones Exfiltration Over Alternative Protocol (Exfiltración)

ANEXO III: AMPLIACIÓN ESTUDIO PRÁCTICO

En este anexo se incluyen todas las mitigaciones y detecciones que se pretenden implementar y que por cuestiones de extensión del documento no se incluyeron en el punto ‘4. Estudio Teórico’. La estructura es igual a la mostrada en dicho apartado.

Mitigaciones

M1051: Update Software

- Exploit Public Facing Application (Acceso Inicial).
- Explotación de Servicios Remotos (Movimiento Lateral).

Los desarrolladores deberán conocer los tipos y versiones del software (servidores, frameworks de lenguajes, etc.) utilizado en el desarrollo de las aplicaciones y aplicar los parches necesarios si se detectan vulnerabilidades.

Los parches se aplicarán siempre que sea posible y siempre se testearán previamente en las réplicas de las aplicaciones en un entorno de no producción.

- Browser Extensions (Persistencia).

Los navegadores estarán siempre actualizados a las versiones más recientes.

M1016: Vulnerability Scanning

- Exploit Public Facing Application (Acceso Inicial).
- Explotación de Servicios Remotos (Movimiento Lateral).

En este caso se usarán herramientas de escaneo gratuitas para el análisis de código (Sonarqube) y para el análisis de aplicaciones web (OWAS ZAP) y detectar así posibles vulnerabilidades. Se podrían usar herramientas de pago como Nessus o Accunetix si se tiene la oportunidad o se decide hacer la inversión (no es necesario comprar el producto, pero se podría pagar a una empresa para que realice el ejercicio de escaneo).

M1031: Network Intrusion Prevention

- Phishing (Acceso Inicial).
- Application Layer Protocol (Comando y Control).
- Web service (Comando y Control).
- Exfiltration Over Alternative Protocol (Exfiltración).

Las capacidades incluidas en el firewall Palo Alto permiten identificar enlaces maliciosos, basándose por ejemplo en listas dinámicas externas que se actualizan continuamente. El propio vendedor se encarga de mantener actualizadas estas listas usando diferentes métodos, como tomar información de otros vendedores como Symantec Norton o McAfee.

El firewall también incluye capacidades Antivirus, Anti-Spyware, protección frente a vulnerabilidades, inspección de paquetes, etc. Por ejemplo, podría inspeccionar paquetes en busca de firmas maliciosas conocidas o sospechosas.

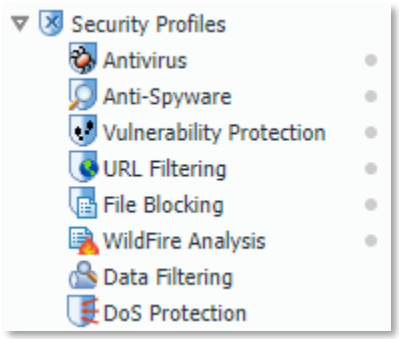


Figura 45 Advanced Threat Protection Firewall Palo Alto

- User Execution (Execution).

El firewall analizará las descargas en busca de ficheros maliciosos y también podrá detectar y actuar ante el acceso a links maliciosos.

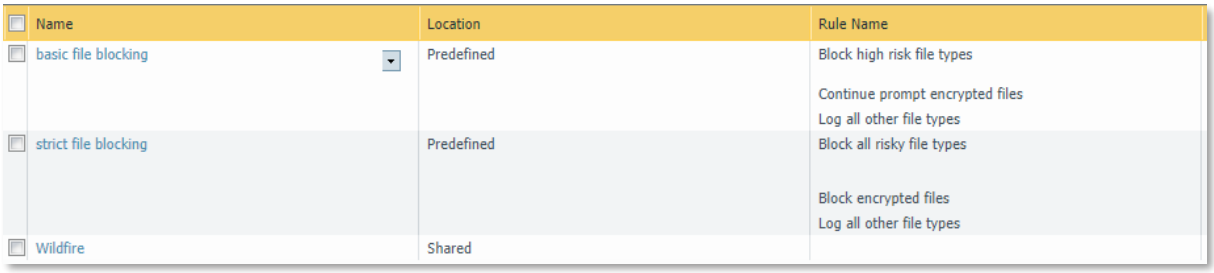


Figura 46 Inspección de ficheros en Firewall Palo Alto

- Network Service Discovery (Descubrimiento).

El sistema Threat Prevention de Palo Alto podría detectar escaneos de puertos y/o vulnerabilidades y bloquearlos.

M1013: Application Developer Guidance

- Valid Accounts (Acceso Inicial).
- Valid Accounts (Persistencia).
- Valid Accounts (Escalado de Privilegios).

Las aplicaciones han de incorporar en su código las herramientas que aporte el lenguaje de programación o el framework que permitan la creación y validación segura de formularios de autenticación.

Las credenciales que se almacenen en las bases de datos se cifrarán o hashearán usando siempre algoritmos sin vulnerabilidades conocidas.

M1027: Password Policies

- Valid Accounts (Acceso Inicial).
- Valid Accounts (Persistencia).
- Valid Accounts (Escalado de Privilegios).
- Fuerza Bruta (Acceso a Credenciales).
- Forced Authentication (Acceso a Credenciales).

No se usarán credenciales por defecto.

Las contraseñas deberán tener un mínimo de complejidad para asegurar que son fuertes. Se recomienda seguir las reglas NIST [https://pages.nist.gov/800-63-3/sp800-63b.html].

Se aplicará en la medida de lo posible el uso de diferentes contraseñas para diferentes aplicaciones.

Las contraseñas se renovarán cada cierto periodo de tiempo.

M1040: Behavior Prevention on Endpoint

- User Execution (Execution).

No va a implementarse mitigación para esta técnica en esta táctica.

M1038: Execution Prevention

- User Execution (Execution).

No va a implementarse mitigación para esta técnica en esta táctica.

M1047: Audit

- Browser Extensions (Persistencia).

Cada empleado y de manera general el responsable o responsables de seguridad en la empresa confirmarán la no existencia de extensiones no deseadas en los navegadores.

- Forge Web Credentials (Acceso a Credenciales).
- Account Discovery - Cloud Account (Descubrimiento).

Se deben revisar todas las cuentas existentes en las aplicaciones web y en la consola o CLI de AWS.

Eliminar todas aquellas cuentas que no se usen o se desconozcan.

Sólo el usuario raíz puede tener los permisos necesarios para crear otras cuentas.

M1033: Limit Software Installation

- Browser Extensions (Persistencia).

En la medida de lo posible todo el personal de la empresa evitará la instalación de programas y/o extensiones de navegador desconocidas, y se consultará al responsable de seguridad designado en caso de duda.

M1045: Code Signing

- Compromise Client Software Binary (Persistencia).

Asegurar siempre que el software se descarga de las fuentes correctas y que está firmado por los desarrolladores reales.

También es conveniente contrastar los hashes de los archivos con los que se indican en las páginas de descarga oficial.

M1042: disable or Remove Feature or Program

- External Remote Services (Persistencia).
- Network Service Discovery (Descubrimiento).
- Explotación de Servicios Remotos (Movimiento Lateral).

En la medida de lo posible, restringir el acceso a puertos que no necesiten ser accedidos remotamente.

- Exfiltration Over Physical Medium (Exfiltración).

Podría deshabilitarse el arranque automático en los puertos USB de los ordenadores de la oficina.

M1036: Account Use Policies

- Fuerza Bruta (Acceso a Credenciales).
- Multi - Factor Authentication Request Generation (Acceso a Credenciales).

Se limitará siempre la autenticación a un determinado número de intentos.

M1041: Encrypt Sensitive Information

- Network Sniffing (Acceso a Credenciales).
- Network Sniffing (Descubrimiento).

En la oficina, la red WiFi usará únicamente protocolos seguros (WPA2 ó WPA3).

M1028: Operating System Configuration

- Remote Services - Remote Desktop Protocol (Movimiento Lateral).

Configurar la herramienta Remote Desktop de Windows para que cierre las sesiones tras un cierto periodo de inactividad.

M1053: Data Backup

- Destrucción de Datos (Impacto).

Realizar copias de seguridad de las aplicaciones.

Considerar la realización de ejercicios de recuperación de desastre (Disaster Recovery) para poner a prueba las copias de seguridad.

M1037: Filter Network Traffic

- Denegación de Servicio (Impacto).

AWS detecta y bloquea de manera automática ataques DDoS realizados contra su infraestructura.

El firewall de la oficina puede configurarse para que, superado un umbral de tráfico y/o conexiones en un periodo de tiempo determinado, se considere DDoS y bloquee dicho tráfico.

- Exfiltration Over Alternative Protocol (Exfiltración).

Podría considerarse la implantación de un proxy para salir a Internet bajo determinadas reglas. El volumen de tráfico actual en la empresa hace que se descarte esta opción y que el firewall aporta sobradamente estas capacidades.

M1022: Restrict file and Directory Permissions

- File and directory Permissions Modification (Evasión de Defensas)

En los sistemas Linux que almacenan las aplicaciones web, otorgar a los ficheros y directorios los permisos necesarios. Si durante el desarrollo se necesita ampliar permisos, reconfigurar estos a su estado previo una vez se realizan las actividades necesarias.

M1034: Limit Hardware Installation

- Exfiltration Over Physical Medium (Exfiltración)

Limitar el uso de memorias USB o cualquier otro tipo de memorias portátiles en el entorno de red de la empresa.

ANEXO IV: IMPLEMENTACIÓN DE UN WAF EN AWS

En este punto se describe el proceso a seguir para configurar un Web Application Firewall (WAF) para proteger aplicaciones web alojadas en instancias de AWS LightSail.

Una vez descrito el proceso de implementación del WAF, se muestran algunos ejemplos de su funcionamiento.

Permitir el Peering de la VPC de LightSail con la VPC de AWS

Permitir el Peering entre VPCs permite conectar recursos de AWS con recursos de LightSail.

La VPC de AWS y la VPC de LightSail han de estar obligatoriamente en la misma zona de disponibilidad. Para todo el proceso descrito en este anexo la zona de disponibilidad en la que se trabaja es Irlanda (eu-west-1). El proceso puede ser replicado independientemente de la zona de disponibilidad, siempre que dicha zona sea compatible con VPC peering y AWS/WAF.

Para nuestro ejemplo, la instancia está en la zona de disponibilidad eu-west-1a y tiene como IP privada 172.26.6.141.

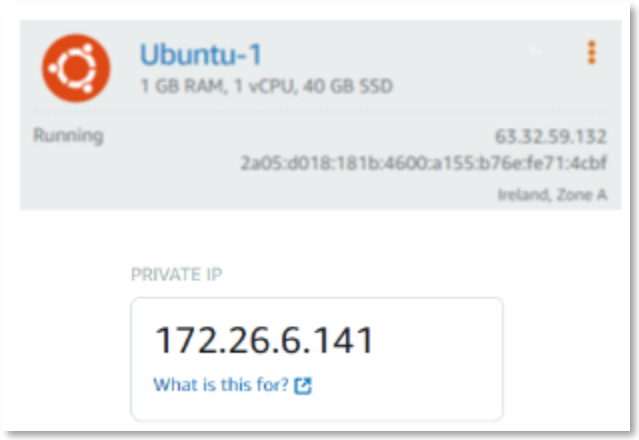


Figura 47 Detalles instancia LightSail

Para habilitar el VPC peering, en la consola de LightSail, nos dirigimos a *Account* < *Account*.

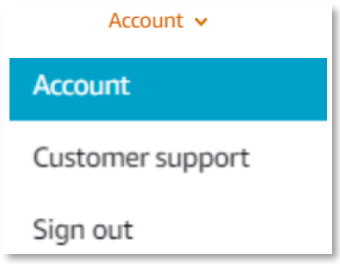


Figura 48 Menú Account

En la pestaña *Advanced* se muestran las zonas de disponibilidad en las que haya instancias de LightSail creadas. Para la zona en la que se desea habilitar el peering de VPC, marcamos la casilla para habilitar el peering.

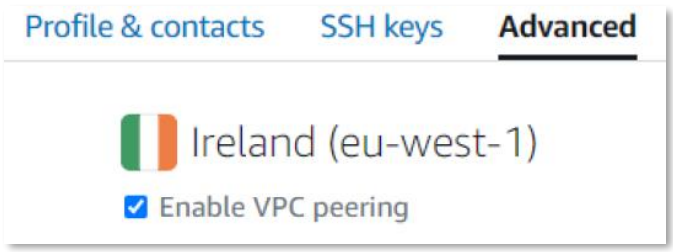


Figura 49 Habilitar VPC Peering

Habilitar el peering de VPC es posible únicamente si se dispone de una VPC por defecto en la misma zona en la que se encuentra la instancia de LightSail, de lo contrario obtendremos un error al tratar de habilitar el peering. Si no se dispone de una VPC por defecto, crearla (se describe el proceso en el punto siguiente).

Si ya disponemos de una VPC por defecto en AWS en la zona correspondiente, podemos comprobar que el peering se ha realizado de manera exitosa en *VPC* < *Interconexiones*.

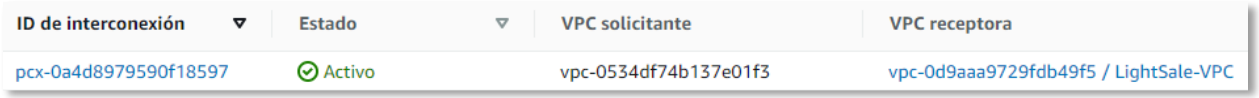


Figura 50 Interconexión de VPCs

Crear una VPC por defecto en AWS

Normalmente cuando se empieza a trabajar en una zona de AWS, esta zona ya suele incluir una VPC por defecto, que a su vez incorpora subredes por defecto. En caso de que no esté habilitada o haya sido borrada, seguir los pasos que se describen a continuación. Añadir que sólo se permite una única VPC por defecto por cada zona de disponibilidad.

Para crear una VPC por defecto, en la consola de AWS, dirigirse a *VPC < Acciones < Crear VPC predeterminada.*

Figura 51 Crear VPC

Configuramos los parámetros necesarios (nombre y rango de IPs privadas).

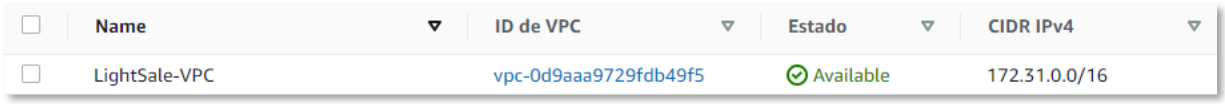


Figura 52 Parámetros VPC

Las subredes deben de crearse automáticamente al crear la VPC.

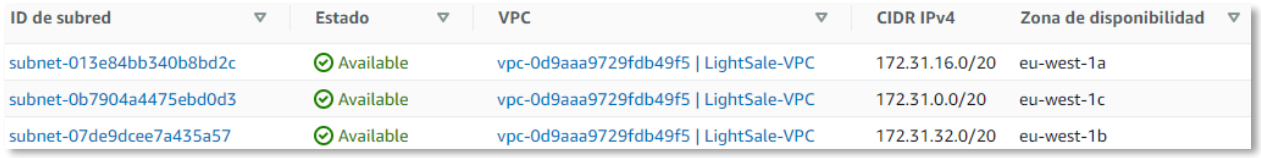


Figura 53 Subredes de una VPC

Si las subredes no se crean automáticamente o han sido borradas, siempre pueden volver a crearse y asociarse a la VPC por defecto.

Es imprescindible tener al menos 2 subredes en diferentes zonas de disponibilidad ya que el Balanceador de Carga necesita 2 zonas a las que balancear el tráfico (aunque posteriormente se dirija el tráfico sólo a una de estas zonas). En nuestro ejemplo vamos a trabajar posteriormente con las zonas *eu-west-1a* y *eu-west-1b.*

Crear un Target Group

El Target Group es el conjunto de instancias sobre las que se hará el balanceo de carga. Puede indicarse únicamente una instancia.

Para crear un Target Group, en la consola de AWS - EC2, nos dirigimos a *Equilibrio de Carga < Grupos de destino < Create Target Group*.

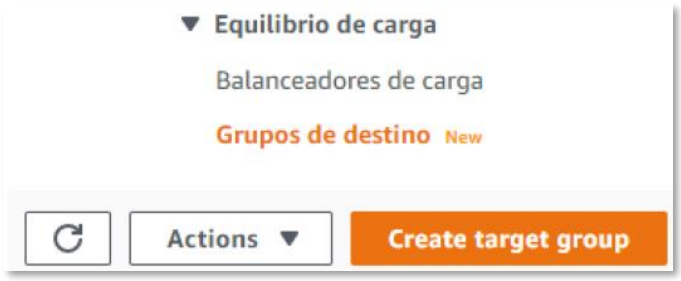


Figura 54 Elemento Grupo de destino

Tipo de destino: IP Addresses.

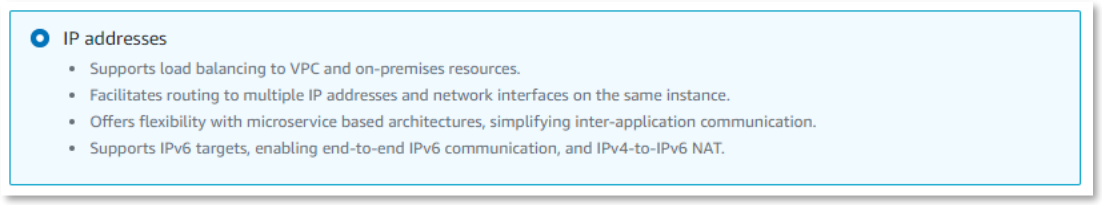


Figura 55 Tipo destino: IP adresses

Dar nombre a nuestro Target Group, seleccionar el protocolo y el puerto en el que escucha nuestra instancia de LightSail (en este caso, en nuestra instancia de LightSail tenemos un servidor web corriendo en el puerto 3000) y seleccionar la VPC por defecto previamente creada (o previamente existente).

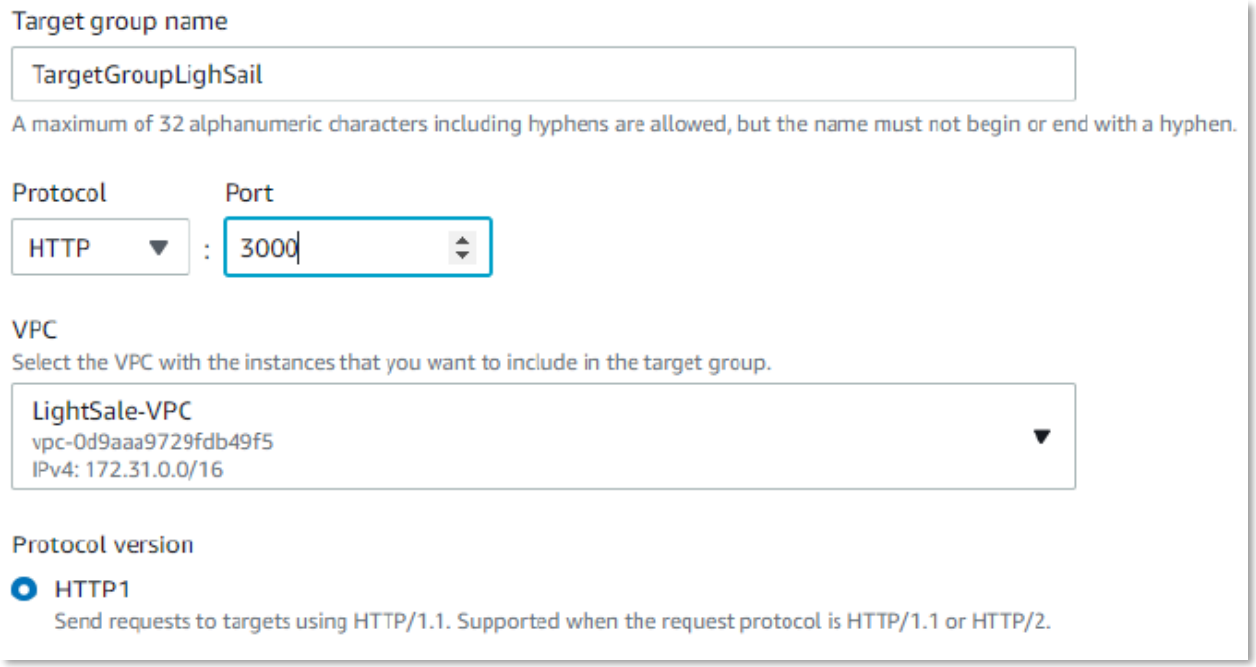


Figura 56 Parámetros Target Group

Pulsamos *Next* para continuar. En el siguiente paso, seleccionamos el tipo de Network *Other private IP address* y le indicamos la IP privada de nuestra instancia de LightSail (172.26.6.141).

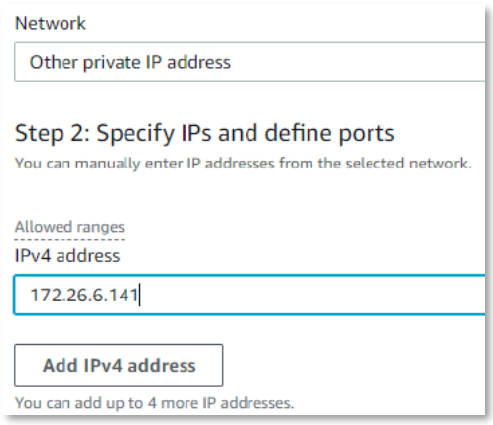


Figura 57 IP y Puertos

Pulsamos sobre *Include as pending below* para que el Target Group comience a sincronizarse con nuestra instancia de LightSail.

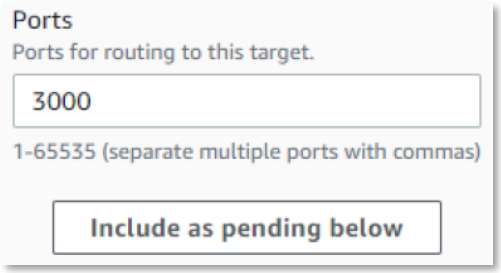


Figura 58 Puertos

Si nuestra instancia de LightSail está efectivamente escuchando en el puerto 3000, pasados unos segundos se mostrará el indicador Health Status como *healthy*, el cual nos indica que nuestro Target Group ha conectado exitosamente con nuestra instancia de LightSail.

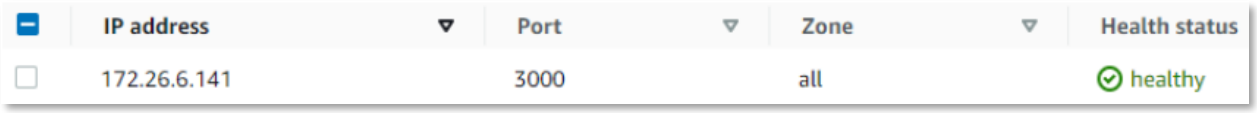


Figura 59 Objetivo correctamente detectado

Crear un balanceador de carga

Las características necesarias para nuestro Balanceador de Carga son: Ha de estar en la VPC por defecto, debe tener asignado el Target Group creado previamente y deben proporcionarse al menos 2 zonas de disponibilidad (aunque posteriormente sólo se utilice una de ellas, que será en la que se encuentre nuestra instancia de LightSail, en este caso eu-west-1a).

Para crear un Balanceador de Carga, en la consola de AWS - EC2, nos dirigimos a *Equilibrio de carga* < *Balanceadores de carga* < *Crear Balanceador de carga*.

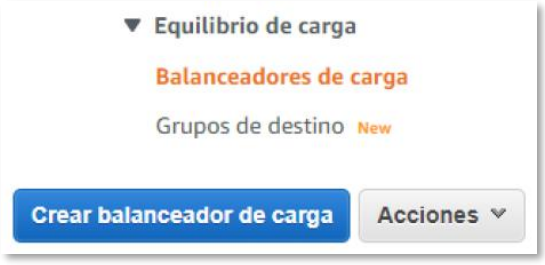


Figura 60 Elemento Balanceador de carga

Tipo de Balanceador de Carga: *Application Load Balancer*.

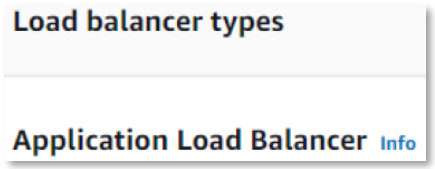


Figura 61 Elemento menú para LB

Le damos nombre, lo configuramos como *Internet-facing* y tipo de IP IPv4.

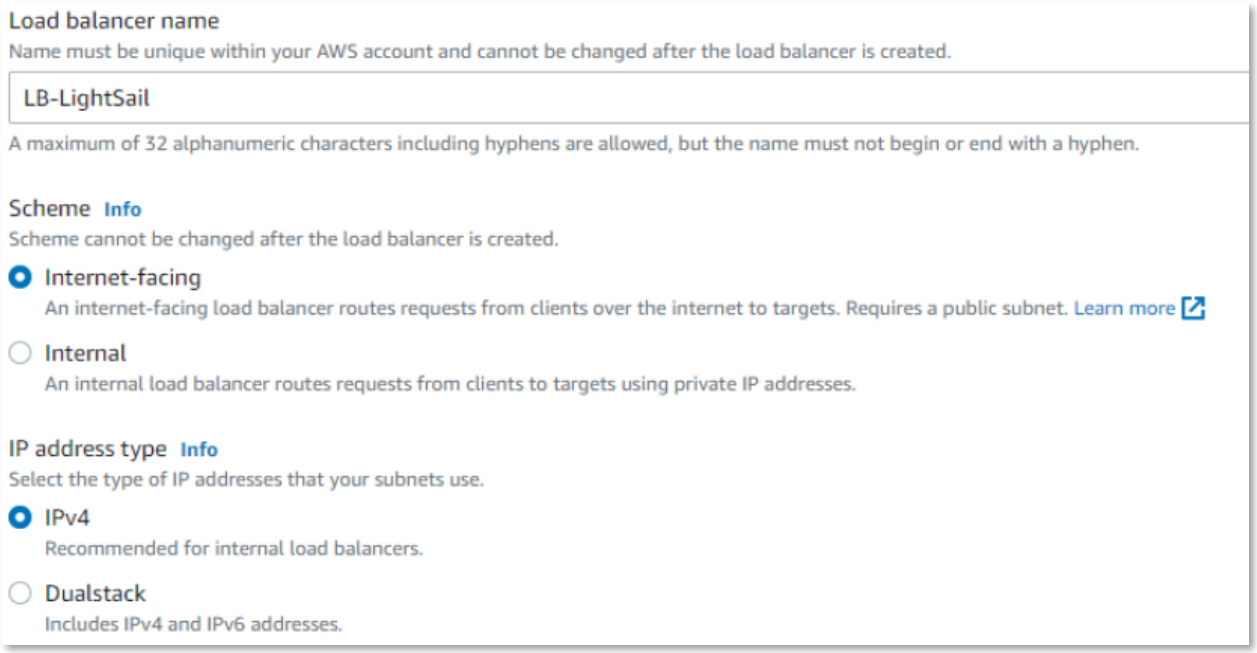


Figura 62 Parámetros Balanceador de Carga

Lo incluimos en nuestra VPC por defecto y seleccionamos las zonas de disponibilidad y las subredes de cada zona de disponibilidad. Una de las zonas de disponibilidad ha de ser obligatoriamente la misma en la que se encuentra nuestra instancia de LightSail, en este caso eu-west-1a.

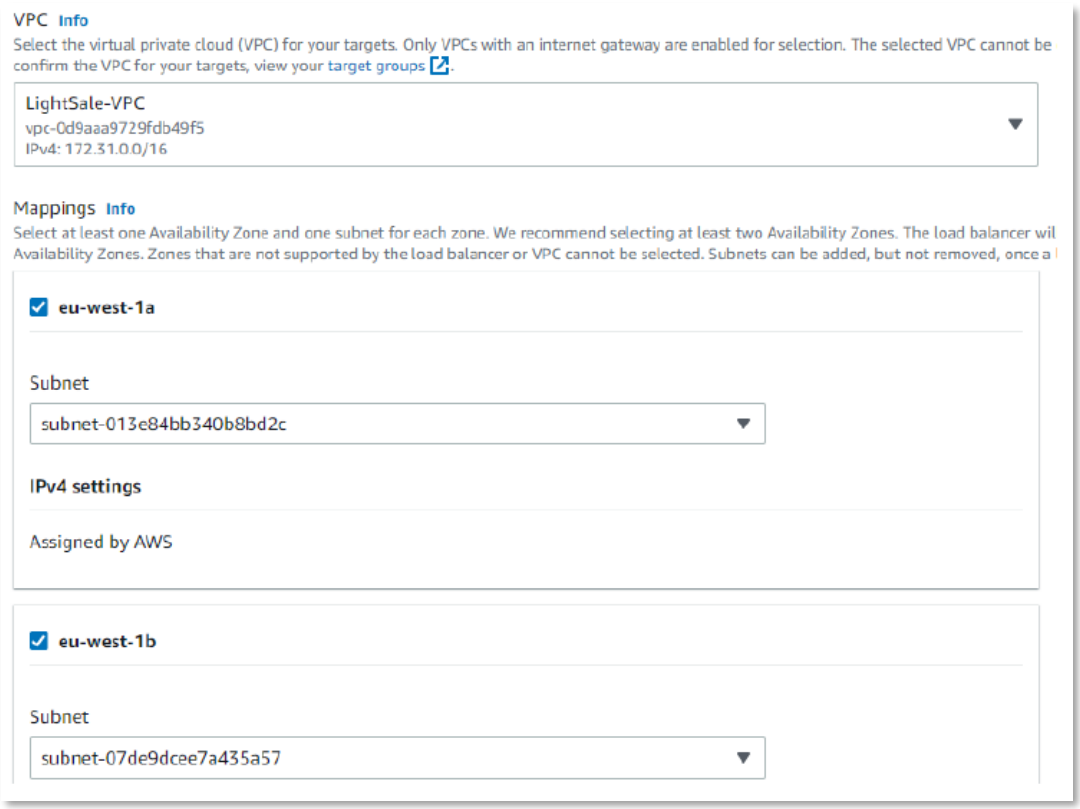


Figura 63 Panel configuración LB

Seleccionamos el Grupo de Seguridad. En este caso seleccionamos el grupo de seguridad por defecto. Este grupo de seguridad puede configurarse posteriormente, y deberá configurarse de manera que sólo permita conexiones en los puertos en los que corren nuestros servicios en la instancia de LightSail.

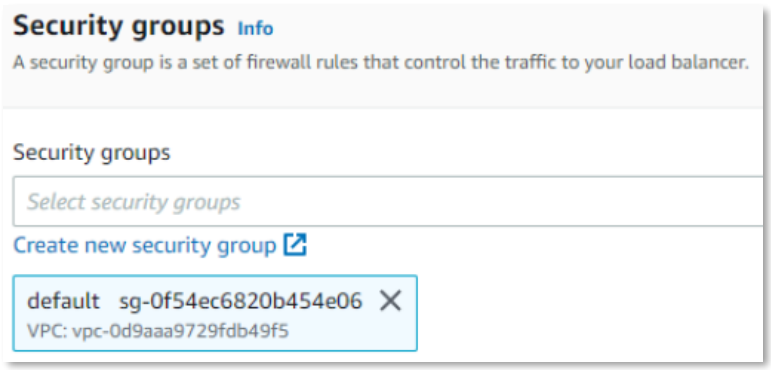


Figura 64 Seleccionar Grupos de Seguridad

Añadimos el Listener y el Target Group creado previamente y pulsamos sobre *Create Load Balancer*.

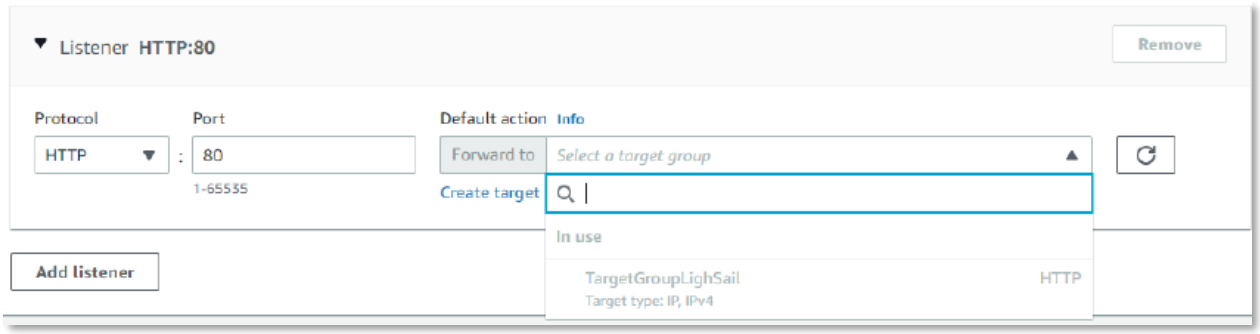


Figura 65 Configurar Listener

En este caso el Listener se configura en el puerto 80. Si se requiere que el acceso sea mediante SSL, deberá de indicarse el puerto 443 (HTTPS).

Crear el WAF: Access Control List (ACL) y Reglas

Para crear el WAF que protegerá las aplicaciones alojadas en las instancias de LightSail ha de crearse una ACL e incluir las reglas correspondientes en la misma.

Para crear una ACL dirigirse a la consola de AWS-WAF, una vez en la consola, dirigirse a *Web ACLs* < *Crear Web ACL*.

Damos nombre a nuestra ACL y le añadimos un recurso de tipo Balanceador de Carga. Al seleccionar *Application Load Balancer* se nos mostrará automáticamente nuestro Balanceador de Carga creado previamente.

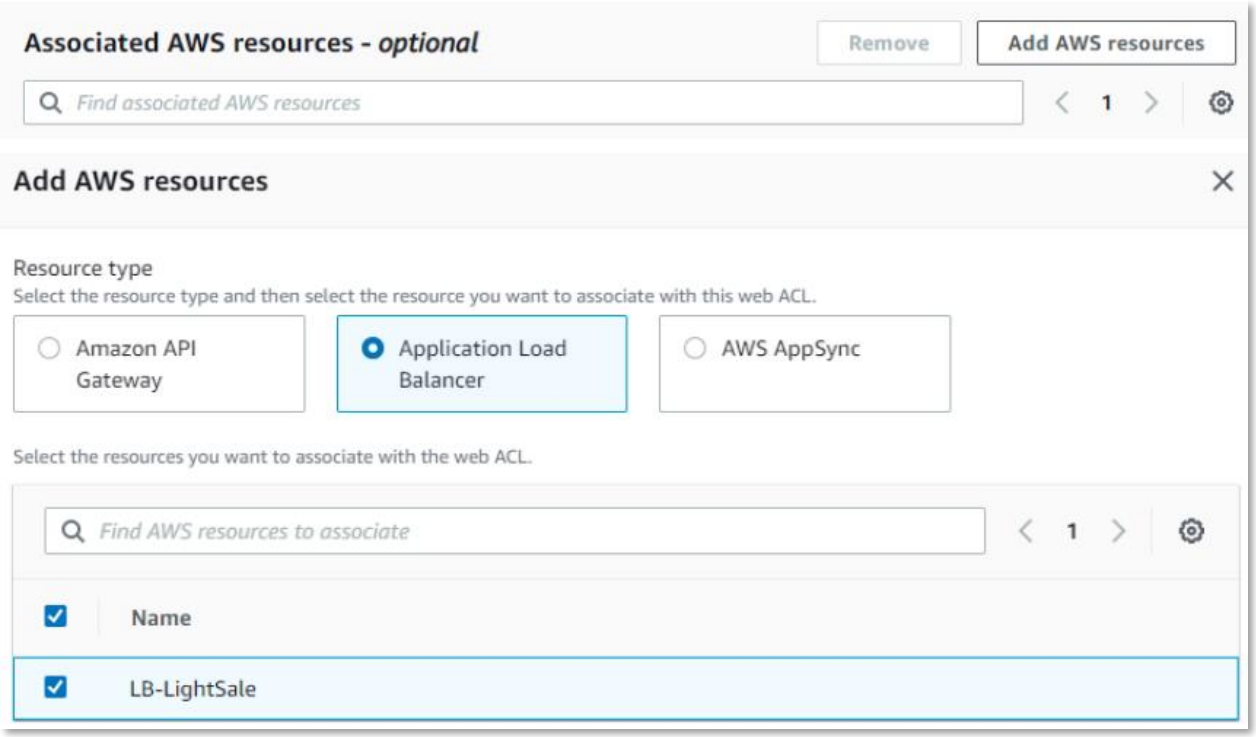


Figura 66 Asociación de Recursos

El paso siguiente es añadir reglas a nuestra ACL recién creada. Disponemos de diferentes reglas (gratuitas y de pago) e incluso podemos crear nuestras propias reglas. Entre las opciones disponibles están reglas de pago implementadas por empresas de seguridad altamente confiables. Para nuestro caso, son destacables aquellas reglas que protegen contra la *OWASP Top 10 Web Application Threats list (https://owasp.org/www-project-top-ten/).*

Figura 67 Añadir reglas

Para nuestro caso y a modo de ejemplo, añadimos varias reglas gratuitas y posteriormente comprobaremos su funcionamiento (*Probando el WAF. Algunos ejemplos de protección*).

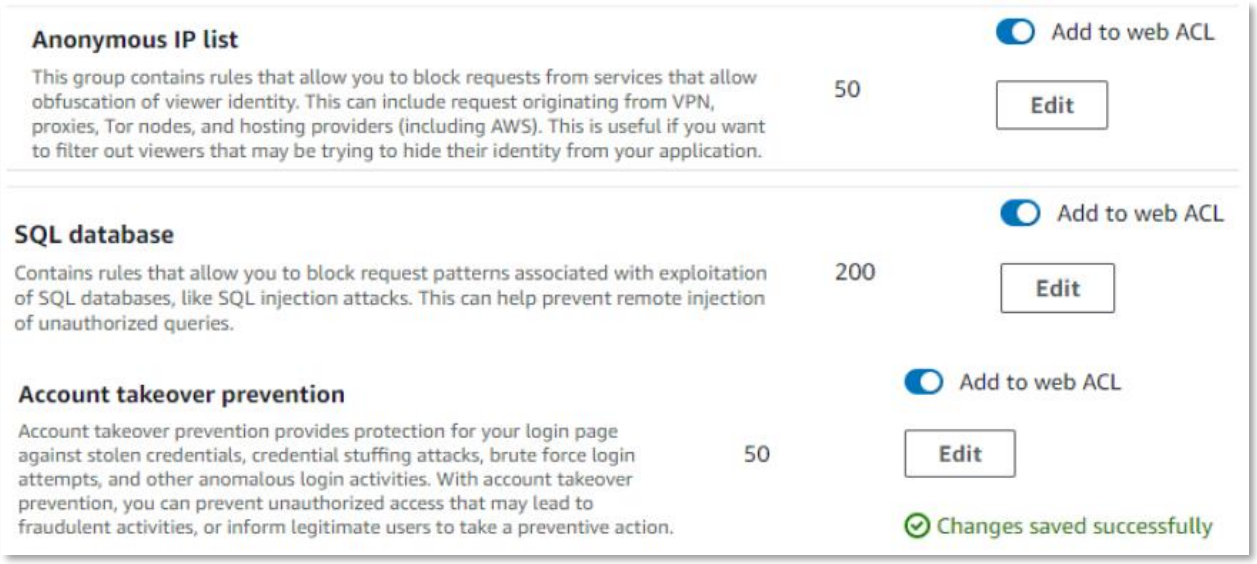


Figura 68 Seleccionar reglas

Nota: Se han incluido estas 3 reglas a modo de ejemplo para probar el funcionamiento del WAF. Hay más reglas y se puede proteger la aplicación frente a más tipos de ataques o vulnerabilidades. Esto es sólo un pequeño ejemplo ilustrativo.

Crear una zona alojada mediante el servicio AWS – Route 53 y apuntar un registra A al DNS del Balanceador de carga

Para este apartado se ha usado un dominio registrado directamente con AWS Route53. Si el dominio está registrado con otro proveedor de dominios, es recomendable portarlo a AWS - Route 53.

Si el dominio se ha registrado con Route 53, la zona alojada se crea de manera automática. En caso contrario, una vez portado el dominio, crear la zona alojada desde la consola de Route 53.

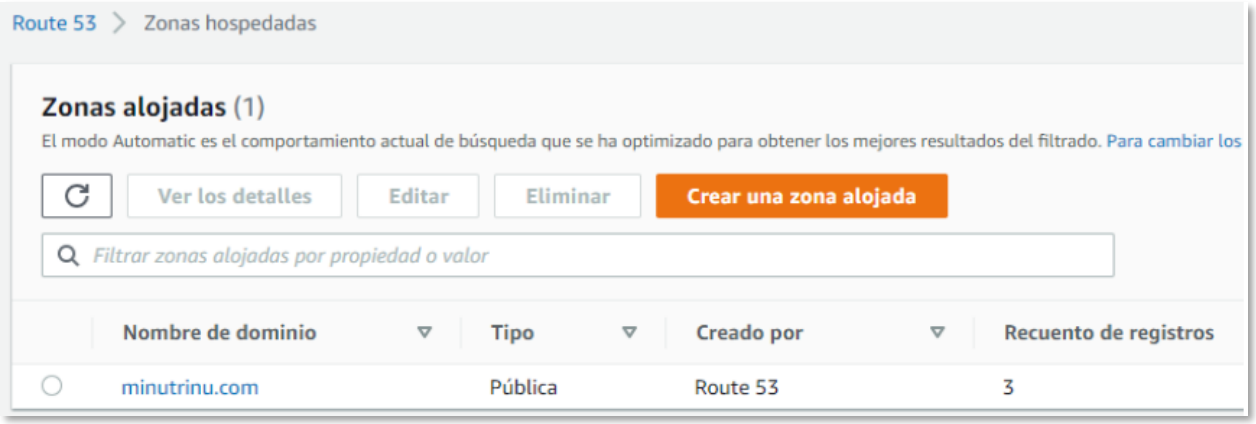


Figura 69 Zonas alojadas

Una vez creada nuestra zona alojada con el dominio correspondiente, el siguiente paso es crear un registro de tipo A que apunte al DNS de nuestro Balanceador de Carga. Para ello, dentro de nuestra zona alojada, seleccionamos *Crear Registro*.

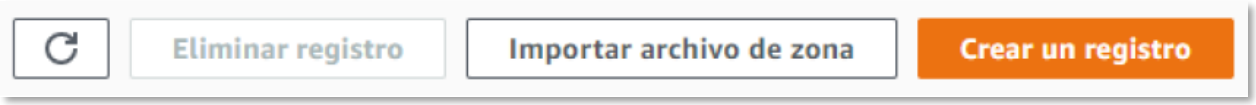


Figura 70 Crear Registros

Creamos un registro de tipo A, dirigimos el tráfico al Alias del Balanceador de Carga de Aplicaciones, en la zona correspondiente (eu-west-1) y apuntando al DNS de nuestro Balanceador de Carga. Seleccionamos *Direccionamiento Sencillo* como política de direccionamiento.

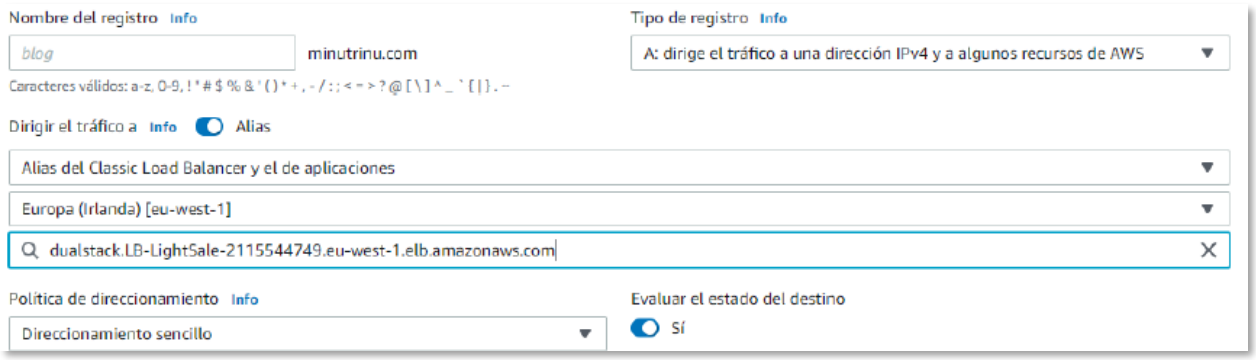
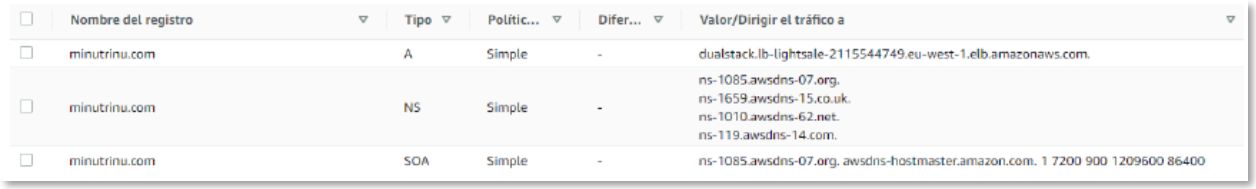


Figura 71 configuración registro

Route 53 añade *dualstack*. al nombre de nuestro Balanceador de Carga.

Una vez creado nuestro registro A, tendremos 3 registros. Los registros NS y SOA se crean por defecto al crear la zona alojada y no pueden modificarse ni borrarse.



Nombre del registro	Tipo	Politic...	Difer...	Valor/Dirigir el tráfico a
minutrinu.com	A	Simple	-	dualstack.lb-lightsale-2115544749.eu-west-1.elb.amazonaws.com.
minutrinu.com	NS	Simple	-	ns-1085.awsdns-07.org. ns-1659.awsdns-15.co.uk. ns-1010.awsdns-62.net. ns-119.awsdns-14.com.
minutrinu.com	SOA	Simple	-	ns-1085.awsdns-07.org. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400

Figura 72 Registros creados

Pasos adicionales

En la instancia de LightSail eliminar todos los accesos a cualquier puerto. Los accesos a los puertos que se permitan se configuran en los grupos de seguridad del balanceador de carga. Esto es muy importante ya que, si se permiten accesos a puertos directamente en LightSail, cualquier usuario podrá acceder a la aplicación alojada en LightSail mediante la IP pública de la instancia, saltándose el WAF.

Configurar los grupos de seguridad del Balanceador de Carga para que sólo permita el acceso en los puertos necesarios, normalmente el 443.

Probando el WAF: Algunos ejemplos de protección

Para poner a prueba el WAF implementado usaremos la aplicación web *OWASP Juice Shop*. Es una aplicación creada por la compañía OWASP, la cual contiene de manera intencionada una gran cantidad de vulnerabilidades y cuyo objetivo principal es el estudio y práctica de actividades de Hacking Ético.

La aplicación OWASP Juice Shop está corriendo en el puerto 3000 de la instancia de LightSail descrita en este anexo.

Regla Anonymous IP List

El objetivo de esta regla es impedir el acceso a la aplicación desde orígenes anónimos, es decir, IPs que no están reconocidas o que pueden ser peligrosas. Un buen ejemplo de este tipo de IPs son los nodos de salida de la red TOR (The Onion Ring).

Veamos qué ocurre si tratamos de acceder a nuestra aplicación web desde el navegador de TOR sin que nuestra regla *Anonymous IP List* esté activada:

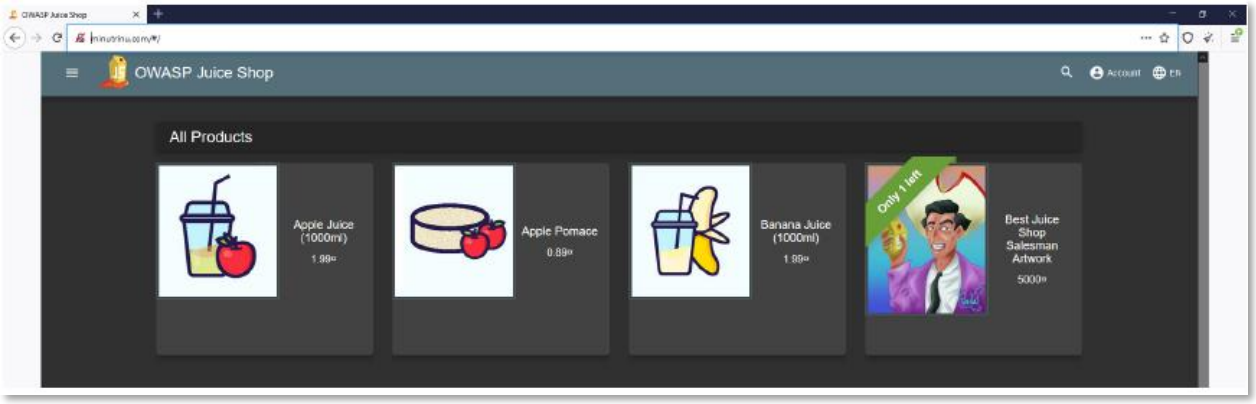


Figura 73 JuiceShop accedido desde TOR

Sin la regla activada, accedemos a la aplicación desde los nodos de salida de TOR. A continuación, activemos nuestra regla y comprobemos si funciona:

Figura 74 JuiceShop tras WAF accedido desde TOR

Al activar la regla y tratar de acceder a nuestra aplicación desde el navegador de TOR, nuestro WAF detecta que es un nodo de salida de la red TOR y bloquea el acceso devolviendo un *403 Forbidden*.

Regla Managed Rules SQLi RuleSet

Esta regla protege contra inyecciones SQL. Sin la regla activada, en el formulario de login de Juice Shop, podemos inyectar código SQL y loguearnos con la cuenta de administrador. Probemos con la regla desactivada:

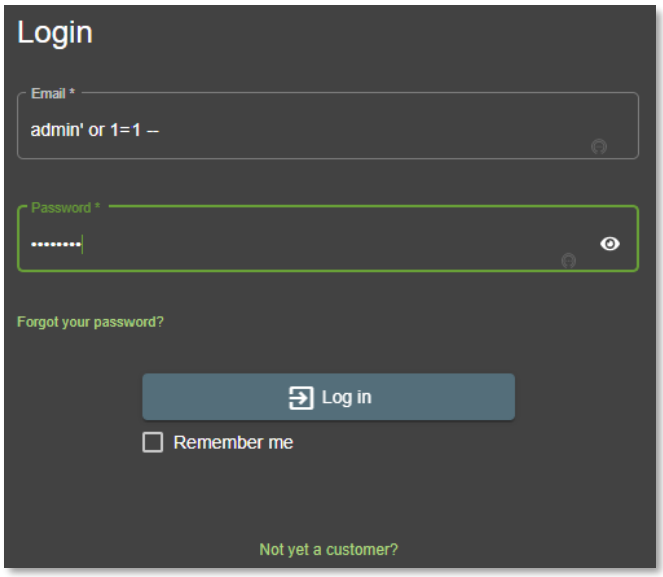


Figura 75 Formulario Login vulnerable

Mediante inyección SQL nos hemos logueado con la cuenta de administrador:

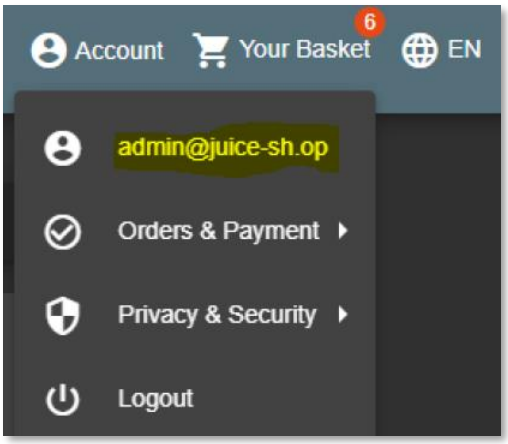


Figura 76 Cuenta Admin

Activamos la regla y probamos la misma inyección SQL:

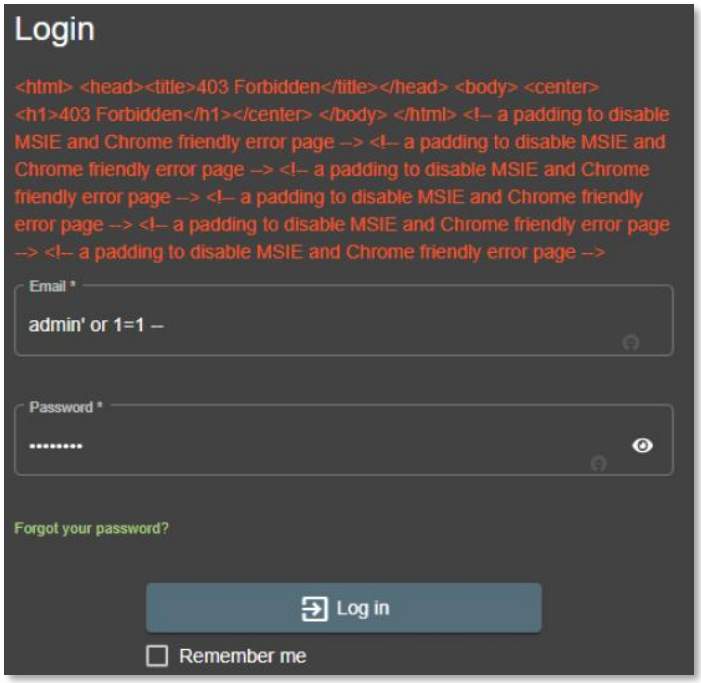


Figura 77 Bloqueo inyección SQL

El WAF ha detectado el código SQL inyectado y ha bloqueado el intento de login.

Regla Account Takover Prevention

Esta regla permite a la aplicación protegerse ante ataques de fuerza bruta para, por ejemplo, loguearse en la aplicación probando una gran cantidad de combinaciones posibles de nombre de usuario y password.

Para el ejemplo hemos creado en JuiceShop una cuenta con nombre de *usuario=jose@gmail.com* y *password=usuario.*

Usaremos la herramienta BurpSuite para configurar el ataque y sus payloads, es decir, diferentes nombres de usuario y diferentes contraseñas, las cuáles BurpSuite irá combinando para tratar de encontrar la combinación correcta. A efectos de ejemplo, los payloads se han mantenido reducidos. Configuramos los payloads para el nombre de usuario:

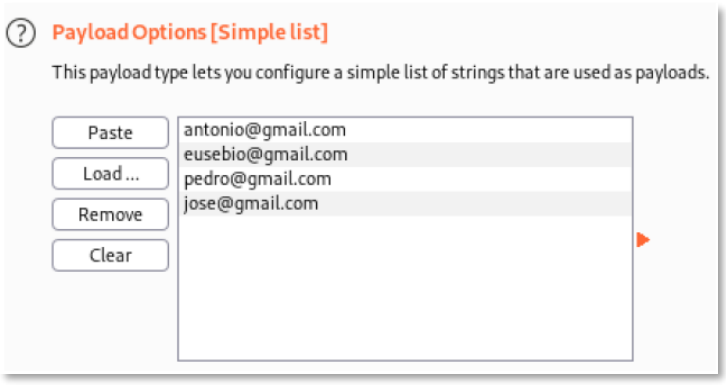


Figura 78 Payloads Usuario

Configuramos los payloads para el campo password:

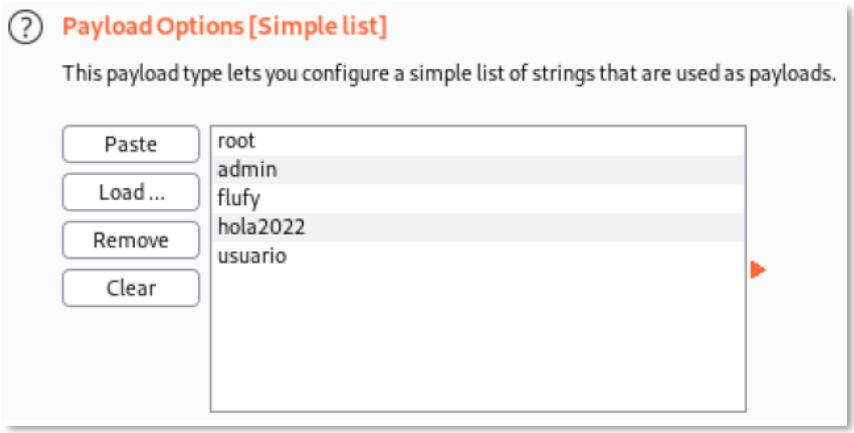


Figura 79 Payloads Contraseñas

Lanzamos el ataque sin tener la regla activada y comprobamos los resultados de las solicitudes realizadas. Vemos que, tras el ataque, BurpSuite nos ha devuelto en primera posición una línea que se diferencia de las demás. Esta línea tiene una respuesta 200 (respuesta positiva desde el servidor) y además tiene una longitud de 1162 bytes. El resto de solicitudes tienen código 401 (credenciales inválidas) y longitud 362 bytes. Si comprobamos los campos de la solicitud indicada, vemos que efectivamente es la respuesta que contiene las credenciales válidas.

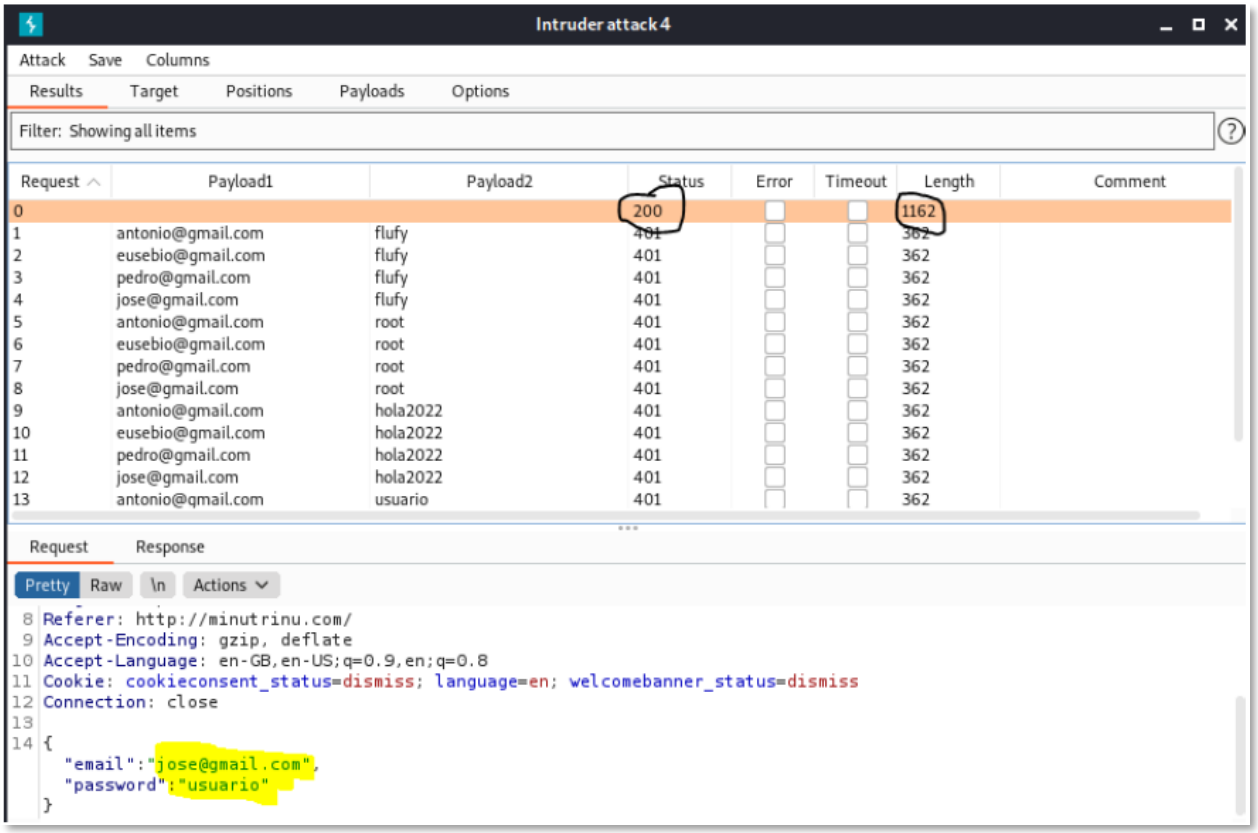
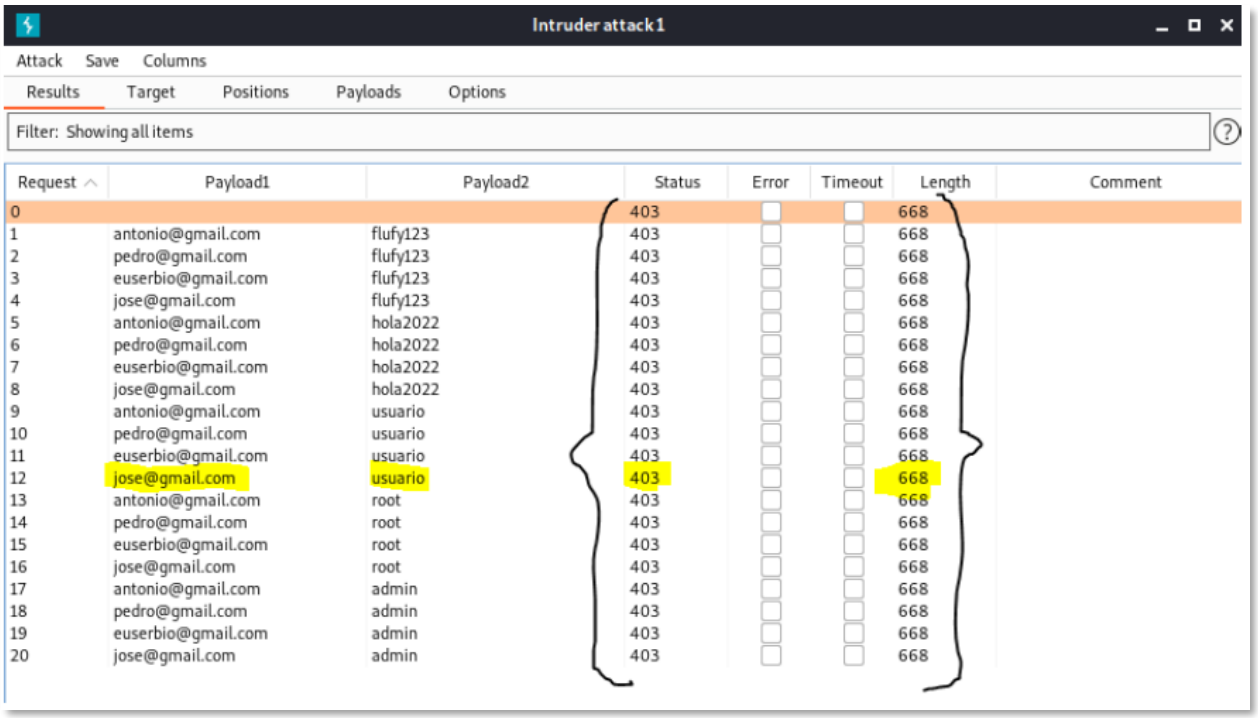


Figura 80 Credenciales detectadas

Lanzamos ahora el mismo ataque con la regla activada y comprobamos los resultados. De los resultados devueltos por BurpSuite, ninguno se diferencia del resto, nada indica que de todos los pares de credenciales usados alguno de ellos sea el correcto. Todos las respuestas a las peticiones lanzadas son un 403 (forbidden) y todas tienen la misma longitud de bytes. En definitiva, se ha evitado el ataque por fuerza bruta mediante la regla implementada.



Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
0			403			668	
1	antonio@gmail.com	flufy123	403			668	
2	pedro@gmail.com	flufy123	403			668	
3	euserbio@gmail.com	flufy123	403			668	
4	jose@gmail.com	flufy123	403			668	
5	antonio@gmail.com	hola2022	403			668	
6	pedro@gmail.com	hola2022	403			668	
7	euserbio@gmail.com	hola2022	403			668	
8	jose@gmail.com	hola2022	403			668	
9	antonio@gmail.com	usuario	403			668	
10	pedro@gmail.com	usuario	403			668	
11	euserbio@gmail.com	usuario	403			668	
12	jose@gmail.com	usuario	403			668	
13	antonio@gmail.com	root	403			668	
14	pedro@gmail.com	root	403			668	
15	euserbio@gmail.com	root	403			668	
16	jose@gmail.com	root	403			668	
17	antonio@gmail.com	admin	403			668	
18	pedro@gmail.com	admin	403			668	
19	euserbio@gmail.com	admin	403			668	
20	jose@gmail.com	admin	403			668	

Figura 81 Credenciales no detectadas

ANEXO V: IMPLEMENTACIÓN DE VPN CON 2FA USANDO KEYCLOAK Y GOOGLE AUTHENTICATOR

En este apartado se describe la implementación de una VPN con un firewall del vendedor Palo Alto. Para conectar con la VPN, se usará la aplicación cliente Global Protect, del mismo vendedor.

Para conectar con la VPN se usará 2FA. Este 2FA se implementará mediante:

a) Keycloak: Un software open source que proporciona diferentes capacidades de autenticación. En este caso se usará el protocolo SAML, y dentro del entorno de este protocolo, Keycloak será el Proveedor de Identidad y el firewall Palo Alto será el Proveedor de Servicios.

b) Google Authenticator: aplicación de Google que se sincronizará con Keycloak para proporcionar un código de autenticación que se solicitará a la hora de conectar con la VPN.

Configuración de Keycloak como Proveedor de Identidad (IDP)

Creación de un Realm

Los Realms en Keycloak permiten gestionar usuarios, credenciales, roles y grupos. Los usuarios pertenecen y se identifican en un Realm determinado. Los Realm están aislados unos de otros y sólo pueden gestionar los usuarios que controlan.

Para crear un Realm en Keycloak, nos dirigimos a *Realms* < *Add Realm*.

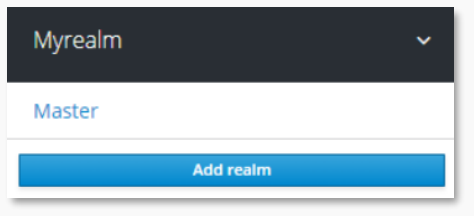


Figura 82 Creación de un Realm

Damos nombre al Realm y lo creamos.

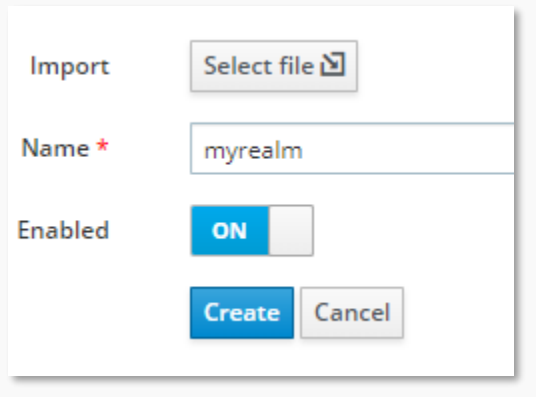


Figura 83 Creando el realm

Creación de usuarios

Los usuarios pertenecen a un sólo Realm. Para crear un usuario, dentro del Realm correspondiente, dirigirse a *Manage* < *Users* < *Add User*.

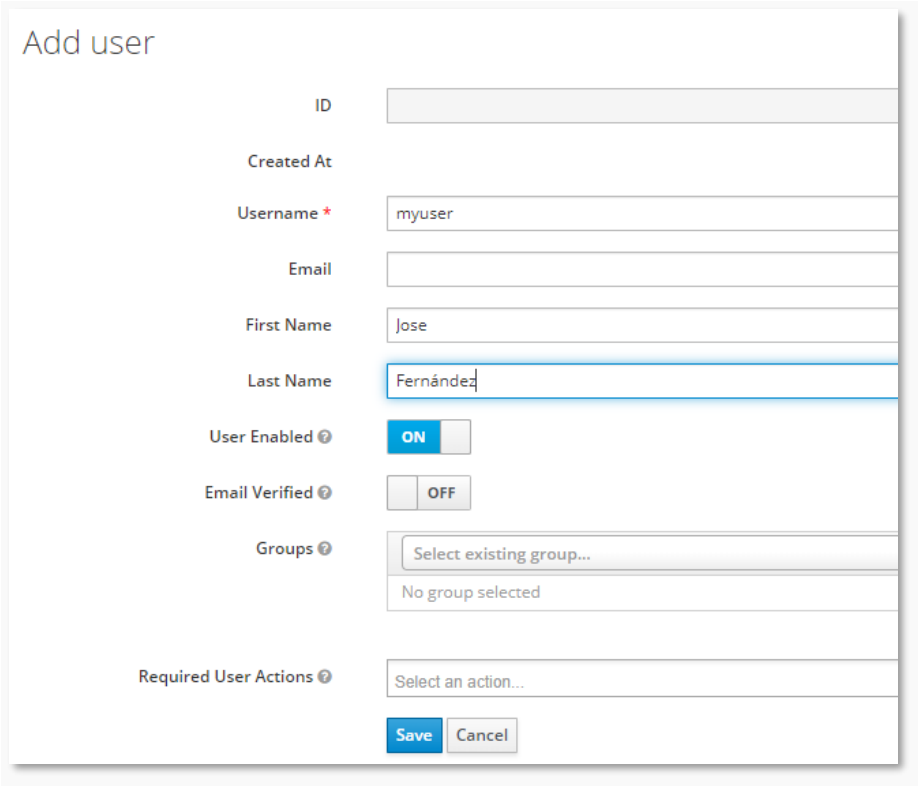


Figura 84 Creación de usuario en un Realm

Configuramos las credenciales de acceso para el usuario creado en la pestaña *Credentials*. Si queremos que el usuario modifique sus credenciales la primera vez que se loguea, marcar *Temporary* < *ON*.

Creación de un cliente. Keycloak como proveedor de identidad

Para configurar Keycloak como Proveedor de Identidad, nos dirigimos a *Manage < Client < Add Client*.

- Client ID: Aquí debemos indicar la IP de nuestra Gateway en el firewall Palo Alto. Esta será la IP a la que conectaremos usando el cliente Global Protect. Indicamos el puerto 443 (HTTPS) seguido de /SAML20/SP. Para nuestro ejemplo nos queda:

  https://52.71.143.237:443/SAML20/SP

- Client Protocol: saml.

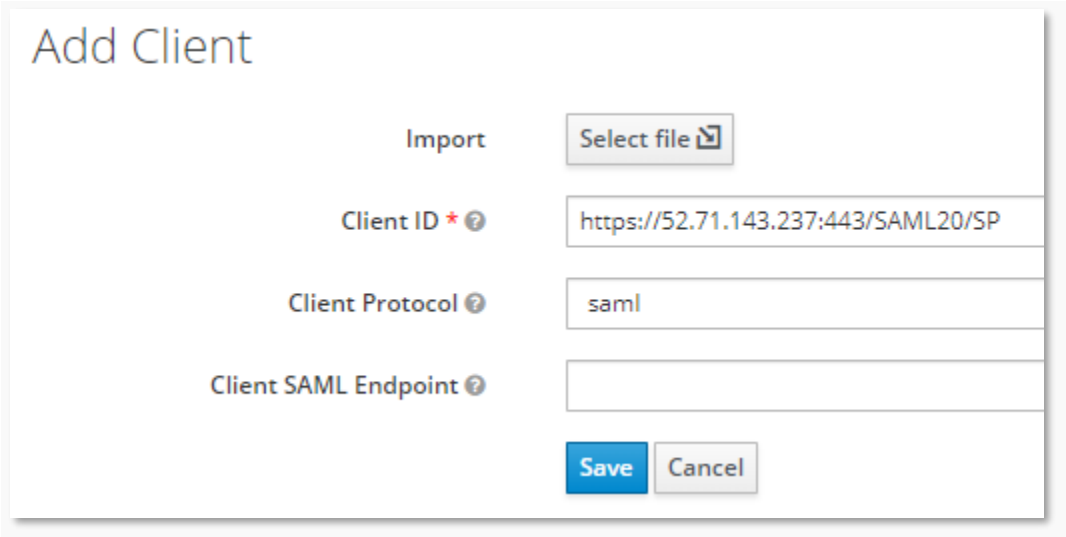


Figura 85 Creación cliente SAML

En la configuración del cliente, para empezar a funcionar nos interesan los parámetros:

- Enabled: ON.
- Force Post Binding: ON.
- Front Channel Logout: ON.
- Name ID Format: username.
- Signature Algorith: RSA_SHA_256.
- SAML Signature Key Name: CERT_SUBJECT.
- Canonicalization Method: EXCLUSIVE.

- Root URL: https://52.71.143.237:443/SAML20/SP
- Valid Redirect URIs: https://52.71.143.237:443/*
- Base URL: https://52.71.143.237:443/

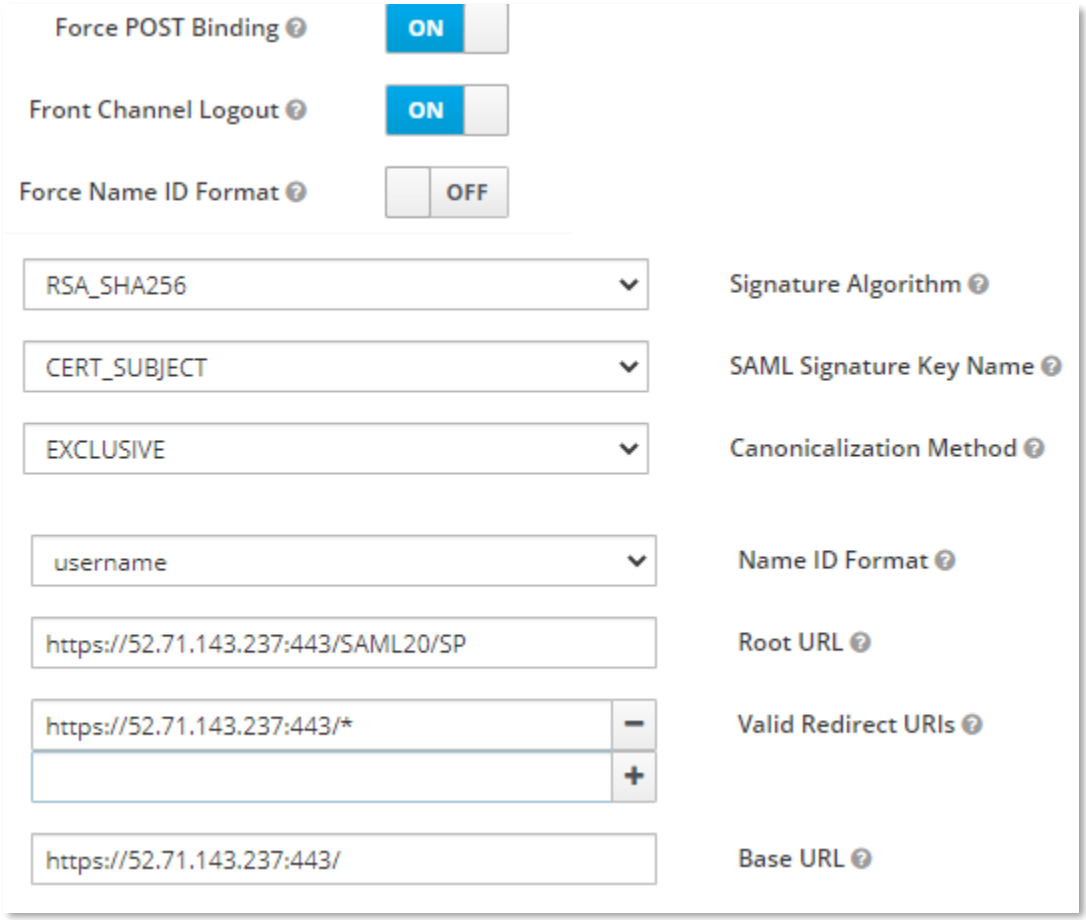


Figura 86 Configuración cliente SAML

Una vez configurado el cliente. En la pestaña *Installation*, descargamos el fichero como *Mod Auth Mellon files*. Se nos descargará un fichero .zip conteniendo dos archivos .xml, de los cuales vamos a necesitar el archivo '*idp-metadata.xml*'. Este archivo contiene la configuración de cliente necesaria para el proveedor de servicios (firewall Palo Alto).

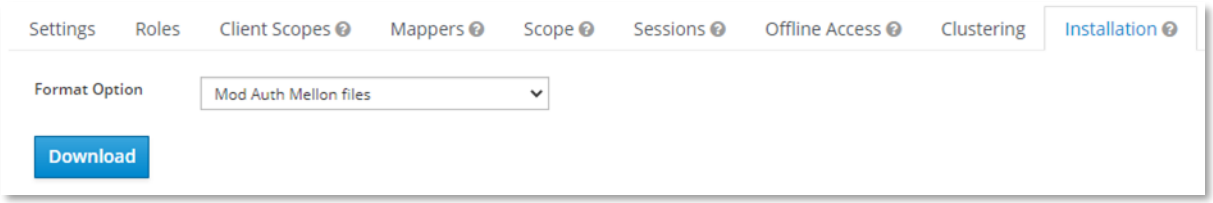


Figura 87 Descargar fichero de configuración SAML

Configuración del flujo de autenticación

El flujo de autenticación es el curso de acciones que se realizarán para la autenticación. El flujo de autenticación se configura en *Configure* < *Authentication*.

En primera instancia podemos dejarlo por defecto. Vamos a modificarlo en el punto siguiente.

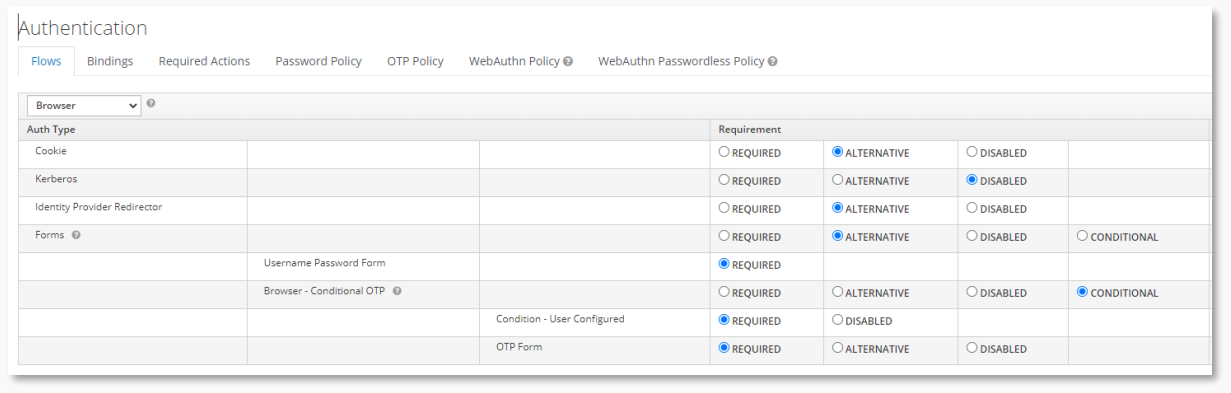


Figura 88 Flujo de autenticación

Añadir 2FA Google OTP al flujo de autenticación

Nos dirigimos a *Authentication* < *Required Action* y habilitamos *Configure OTP* < *Default Action*.

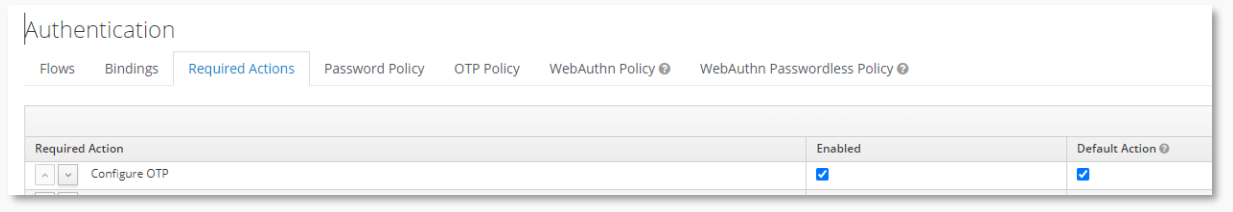


Figura 89 Añadir Google OTP

En Configure < *Authentication* < *Flows* habilitamos el requerimiento de usar el OTP. Para ello marcamos como *REQUIRED* el campo *Browser – Conditional OTP*.

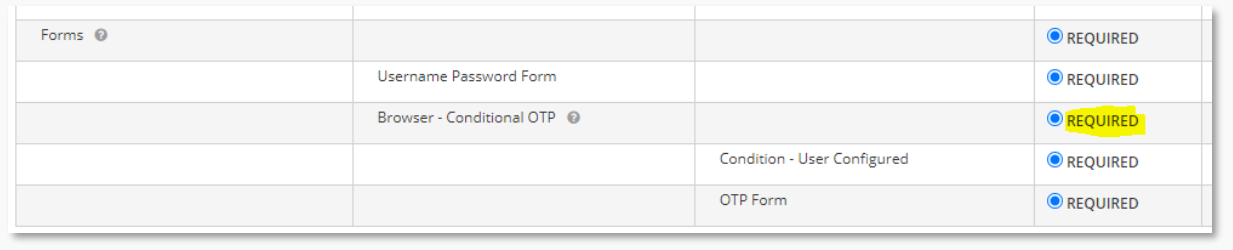


Figura 90 Elementos flujo de autenticación

El apartado *Authentication* < *OTP Policy* podemos dejarlo por defecto, pero conviene echarle un vistazo ya que contiene configuraciones interesantes.

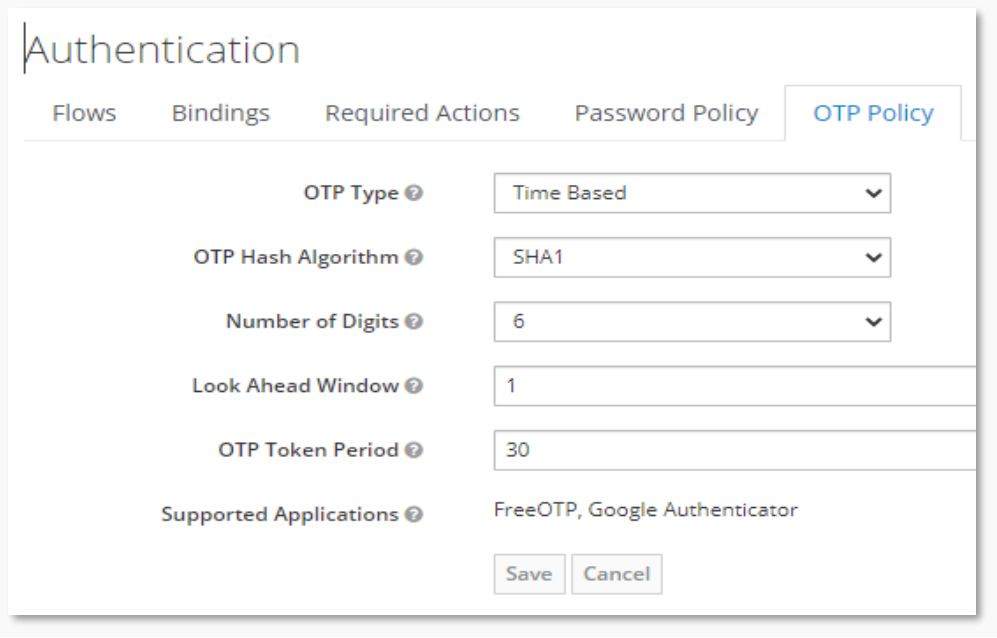


Figura 91 Otros parámetros configurables

Una vez habilitada la configuración de OTP, en *Manage* < *Users* seleccionamos a nuestro usuario y en *Required User Actions* seleccionamos *Configure OTP*.

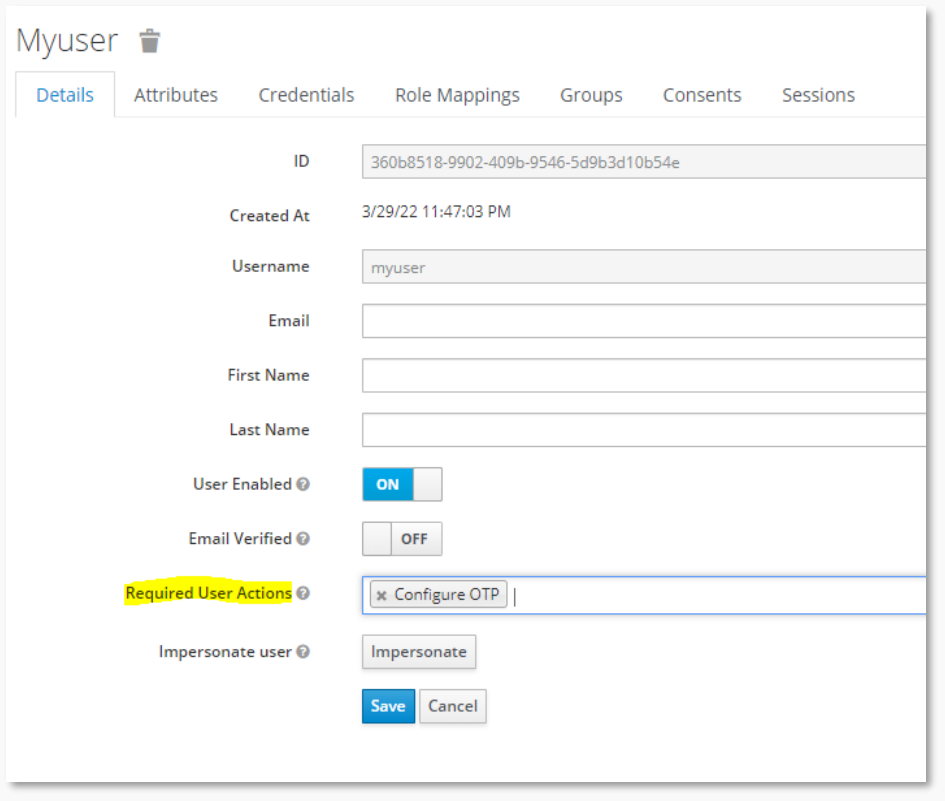


Figura 92 Requerir OTP para el usuario

Con todo esto, cuando el usuario se conecte por primera vez a la VPN usando el cliente GP, tras introducir sus credenciales en el navegador (que se ejecutará automáticamente), se le presentará un código QR que el usuario deberá escanear para realizar el emparejamiento con el dispositivo mediante la aplicación Google Authenticator.

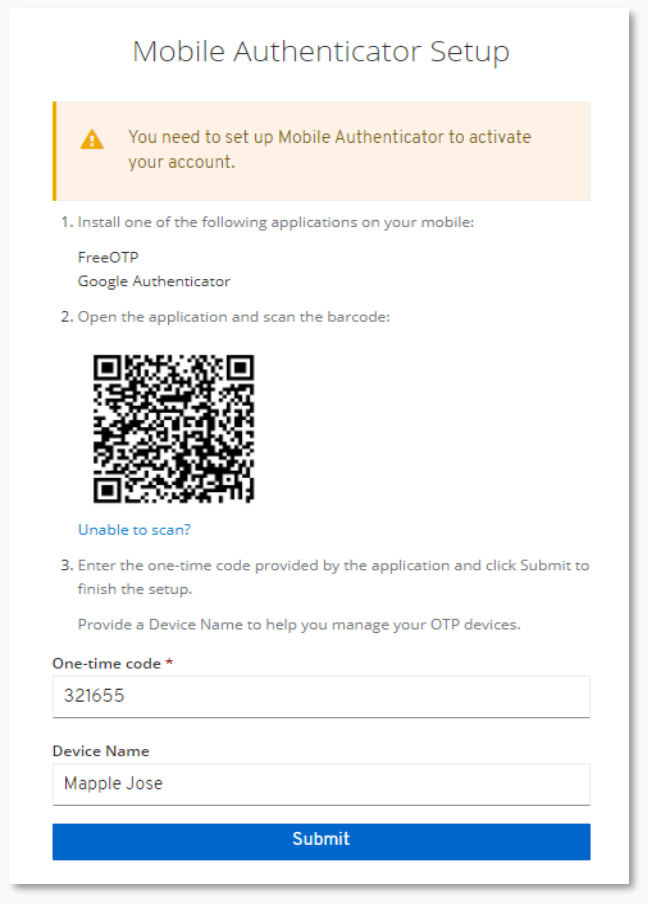


Figura 93 Sincronización dispositivo móvil

Configuración para conexión a VPN mediante cliente Global Protect (GP)

Los pasos descritos en este apartado se realizan en el firewall Palo Alto.

Creación de Certificados

Creación de un certificado actuando como CA

Para crear el certificado vamos a la pestaña *Device* < *Certificate Management* < *Certificates*. En este caso vamos a generar un certificado autofirmado por nosotros actuando como CA. Pulsamos sobre *Generate* y configuramos el certificado.

Para este caso en el que actuamos como CA es imprescindible marcar *Certificate Authority.*

En *Certificate Attributes* podemos configurar los campos Country, State, Locality, Department, Email, Host Name, IP, Alt Email.

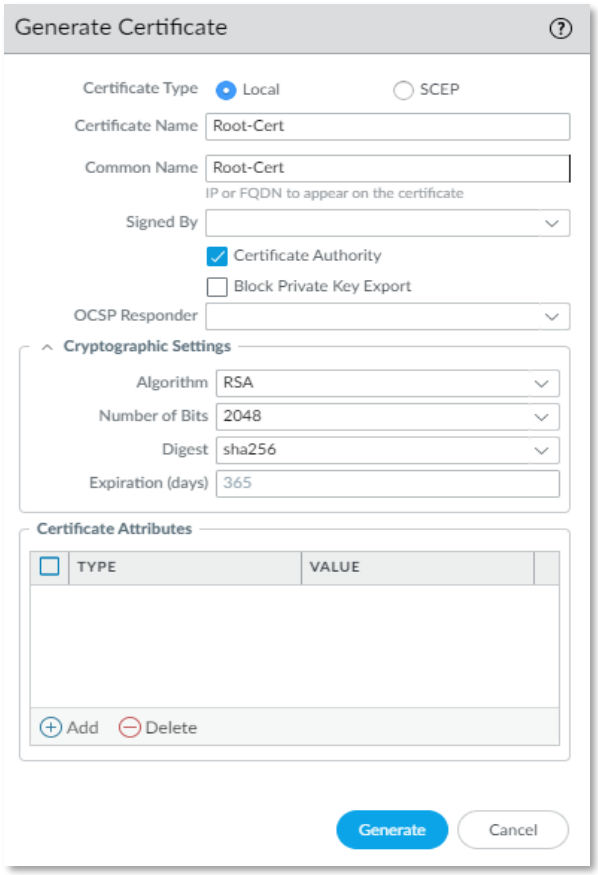


Figura 94 Creación certificado como CA

Crear otro certificado firmado por nuestra CA

Nuevamente en *Device* < *Certificate Management* < *Certificates* < *Generate* generamos un nuevo certificado.

En *Common Name* debemos indicar el nombre de dominio que apunta a la IP de nuestra Gateway.

NOTA: Recordar aquí la equivalencia del parámetro *Common Name* con la que configuramos en el apartado ’Creación del cliente. Keycloak como Proveedor de Identidad (IDP)’ y los parámetros en los que usamos la IP de nuestra Gateway.

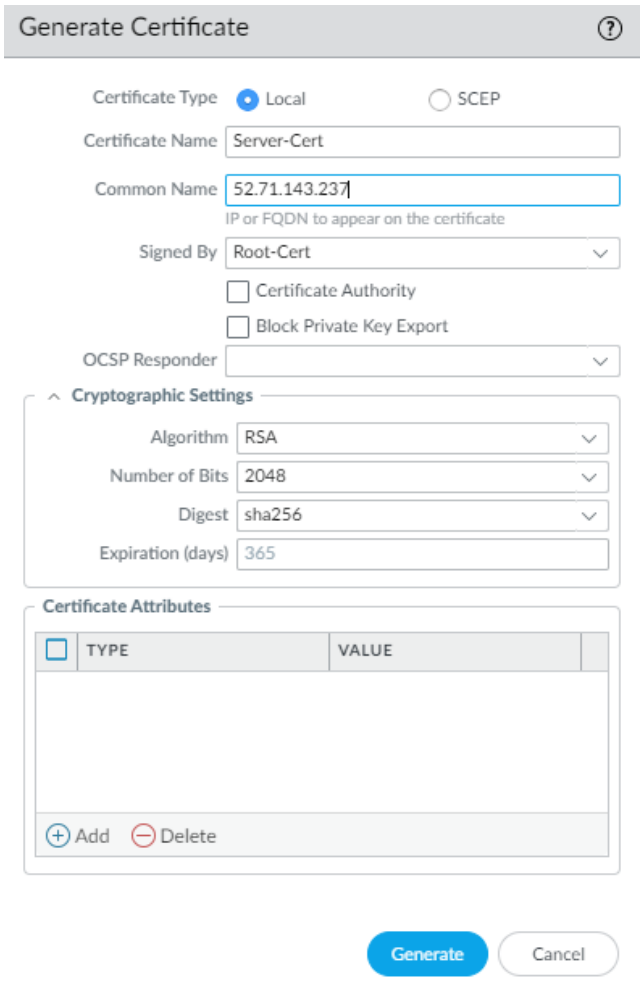


Figura 95 Creación de Certificado firmado por nuestra CA

Configurar el perfil SSL

Para configurar el perfil SSL nos dirigimos a *Device* < *Certificate Management* < *SSL/TLS Profile*.

Estamos configurando el Certificado que se le presentará a los clientes de Global Protect para la autenticación.

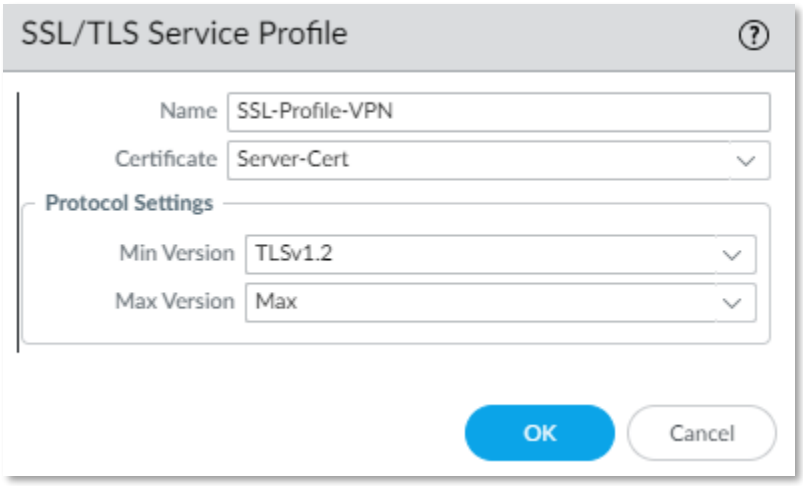


Figura 96 SSL/TLS profile

Configurar un proveedor de identidad SAML

Nos dirigimos a *Device* < *Server Profiles* < *SAML Identity Provider* < *Import*. Le damos el nombre deseado e importamos el archivo *idp-metadata.xml* generado previamente en Keycloak en el punto 'Creación del cliente. Keycloak como Proveedor de Identidad (IDP)'.

El archivo *idp-metadata.xml* contiene toda la configuración necesaria, por lo que basta únicamente con importarlo para generar la configuración.

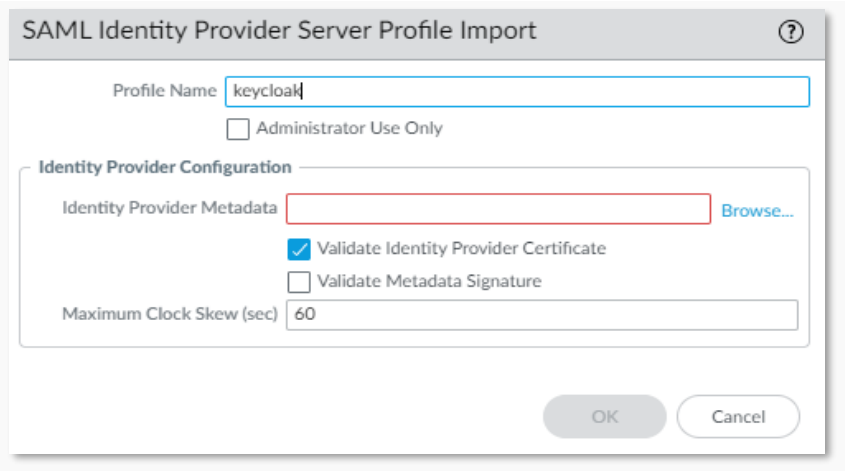


Figura 97 Carga de configuración SAML

Una vez importado, podemos comprobar la configuración clicando sobre el nombre de nuestro Proveedor de Identidad generado. En este caso el proveedor de identidad es nuestro servidor Keycloak, con IP 52.44.40.221.

Dentro de la configuración del Proveedor de Identidad, desmarcar *Validate Identity Provider Certificate* y *Sign SAML Message to IDP*.

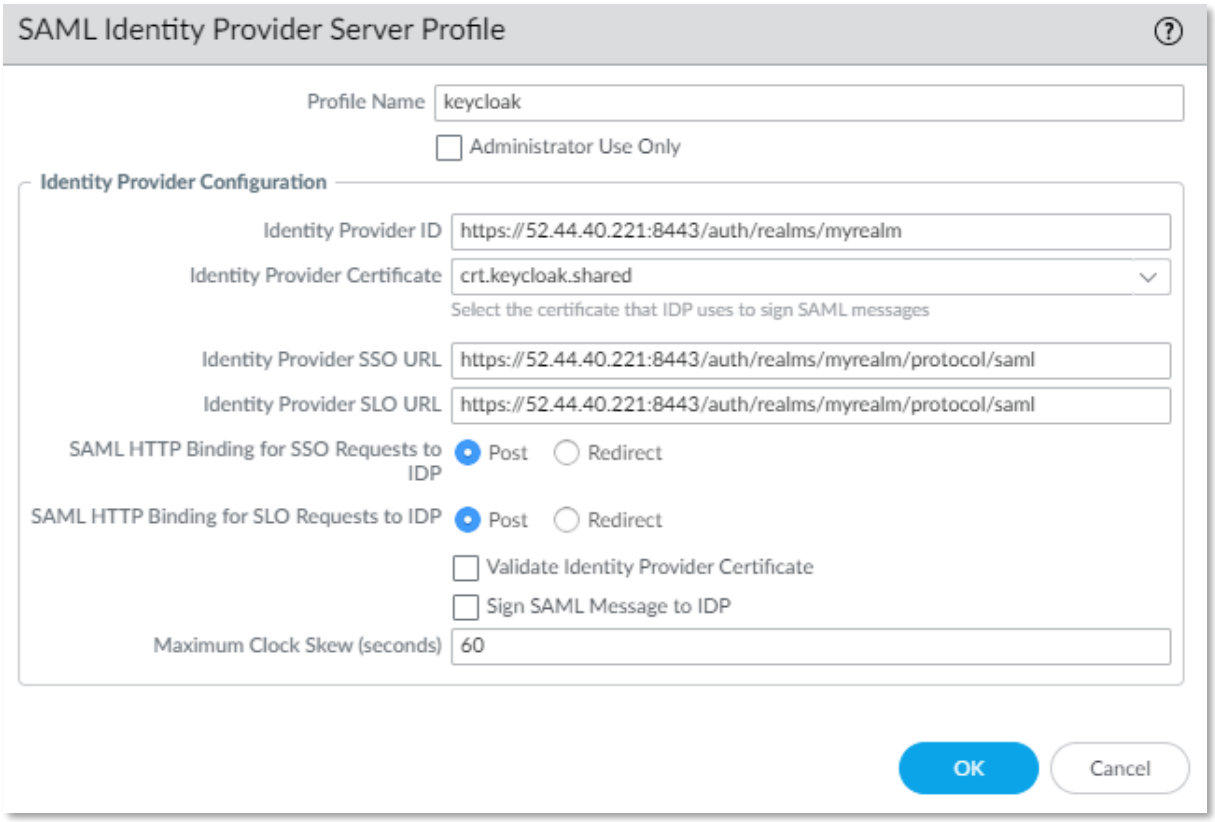


Figura 98 Configuración SAML

Configurar el Authentication Profile

Nos dirigimos a *Device* < *Authentication Profile*.

En la pestaña *Advanced* indicamos los usuarios que están autorizados para conectar a la VPN. Hemos seleccionado *All* a efectos de simplicidad, pero lo recomendable es indicar los usuarios locales o un grupo de usuarios que incluya a todos los usuarios que queremos autorizar para conectar.

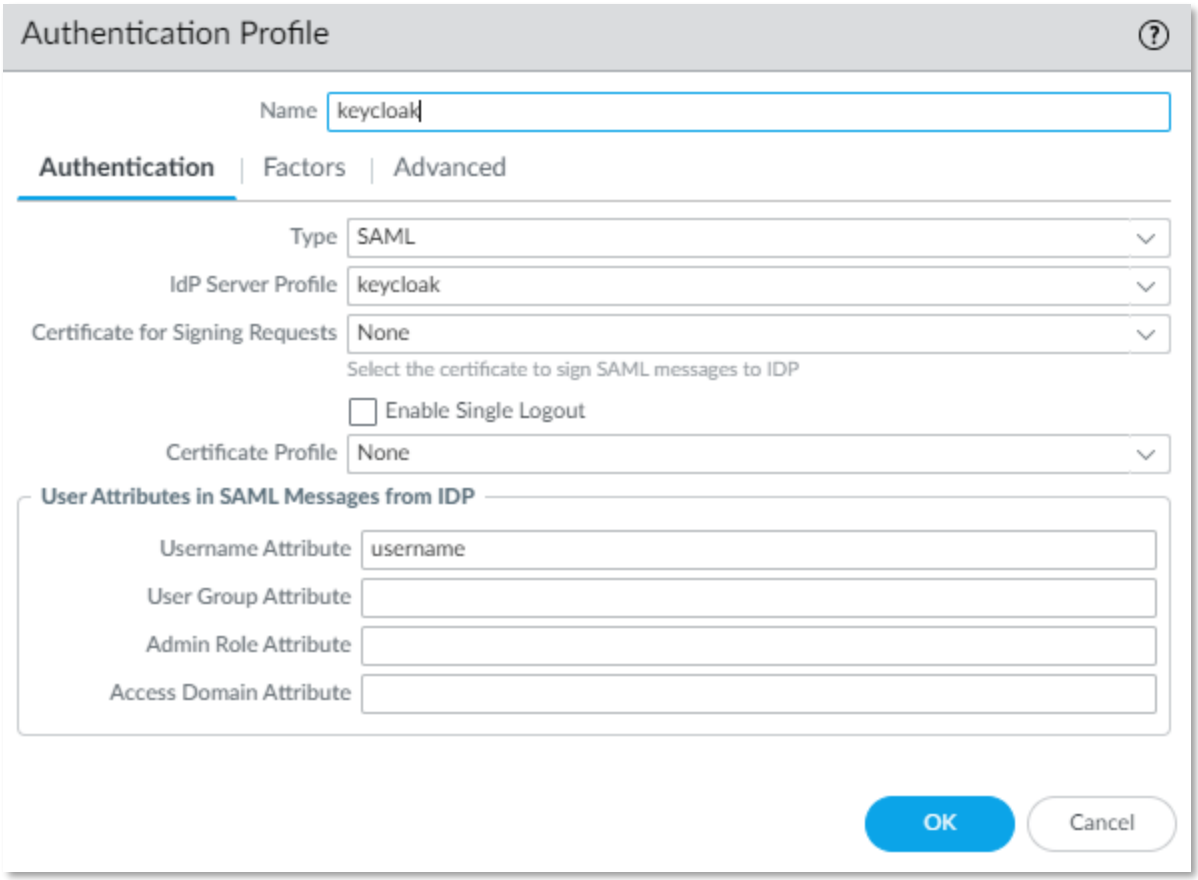


Figura 99 Authentication Profile

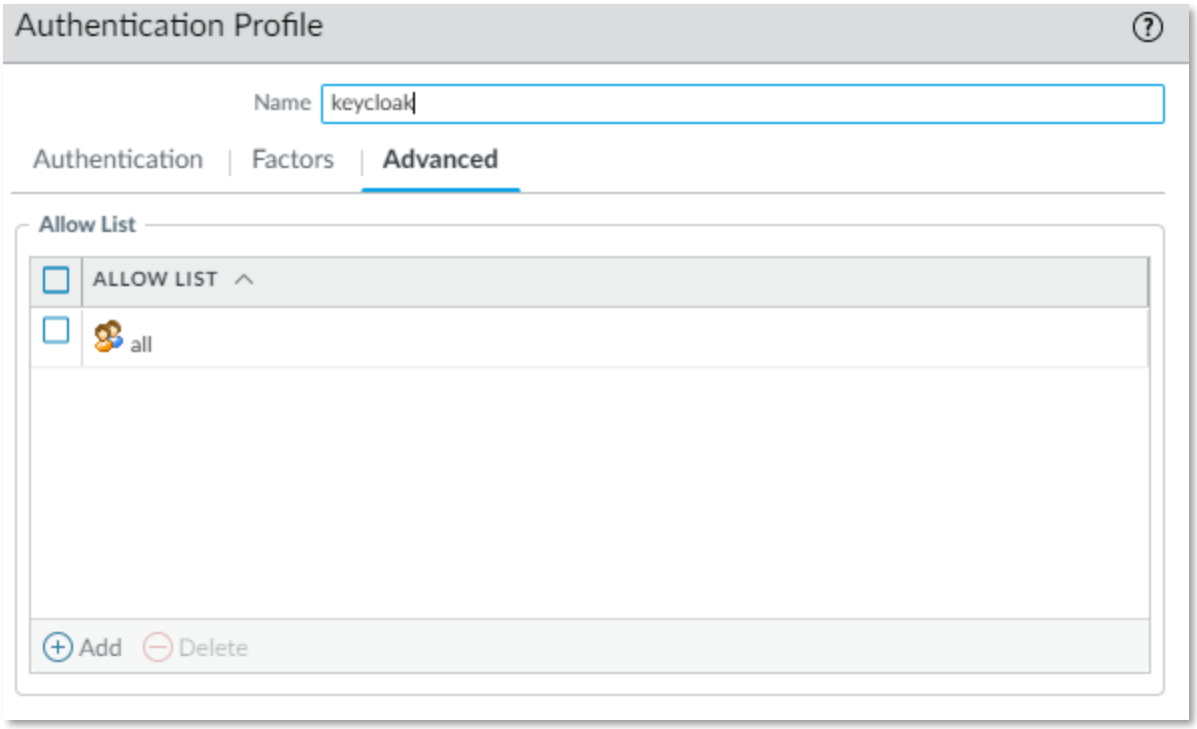


Figura 100 Usuarios Authentication Profile

Configurar la interfaz Túnel

Nos vamos a *Network* < *Interfaces* < *Tunnel.*

Es la interfaz para la terminación de la conexión del cliente GP, que dará acceso a la red local. Debemos de indicar el Virtual Router y la zona correspondiente. Por norma general, la zona será aquella zona en la que se encuentran los recursos a los que se pretende acceder mediante la VPN.

Importante también el Virtual Router que se elige, para aquellos casos en los que se hayan creado otros Virtual Routers aparte del *default* que viene por defecto.

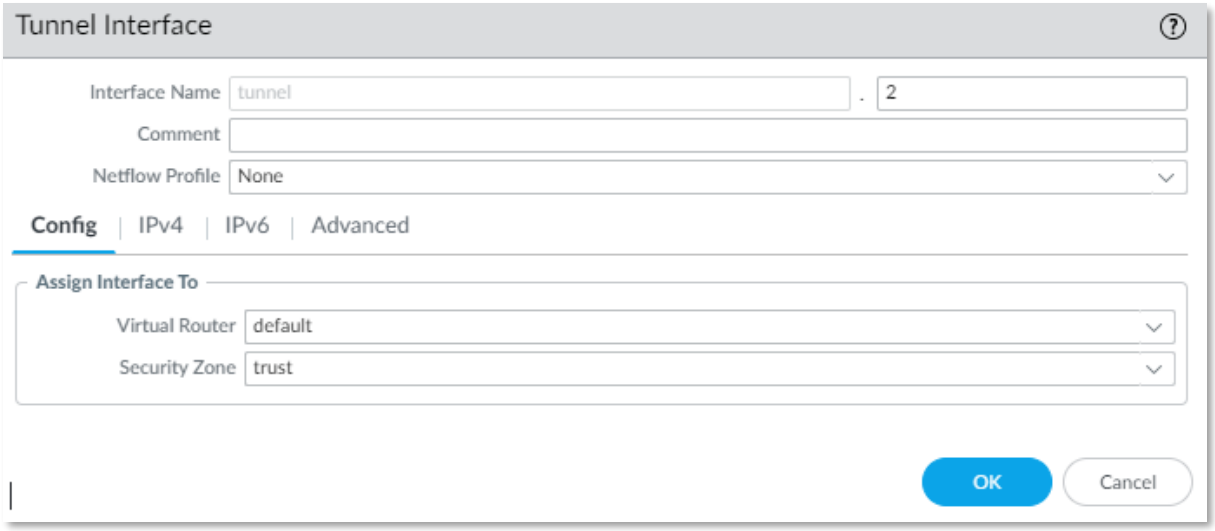


Figura 101 Interface Túnel

Configuración del Portal

El Portal contiene la configuración sobre la Gateway/s. En nuestro ejemplo el Portal y la Gateway se encuentran en la misma interfaz.

Para configurarlo nos vamos a *Network* < *Portals* y seguimos los pasos siguientes.

General

Seleccionar la interfaz en la que queremos configurar el Portal (en nuestro caso es la misma interfaz en la que se encuentra la Gateway).

NOTA: En el apartado de IPv4 address, al ser una instancia de Firewall virtualizada, no nos permite seleccionar una IP, por lo que lo dejamos en *None*. Esto es así ya que las interfaces de la instancia virtualizada se configuran como clientes DHCP, y toman la dirección IP que se configura en las subredes previamente configuradas en AWS.

El resto de parámetros pueden dejarse los que vienen por defecto, a menos que se quiera personalizar.

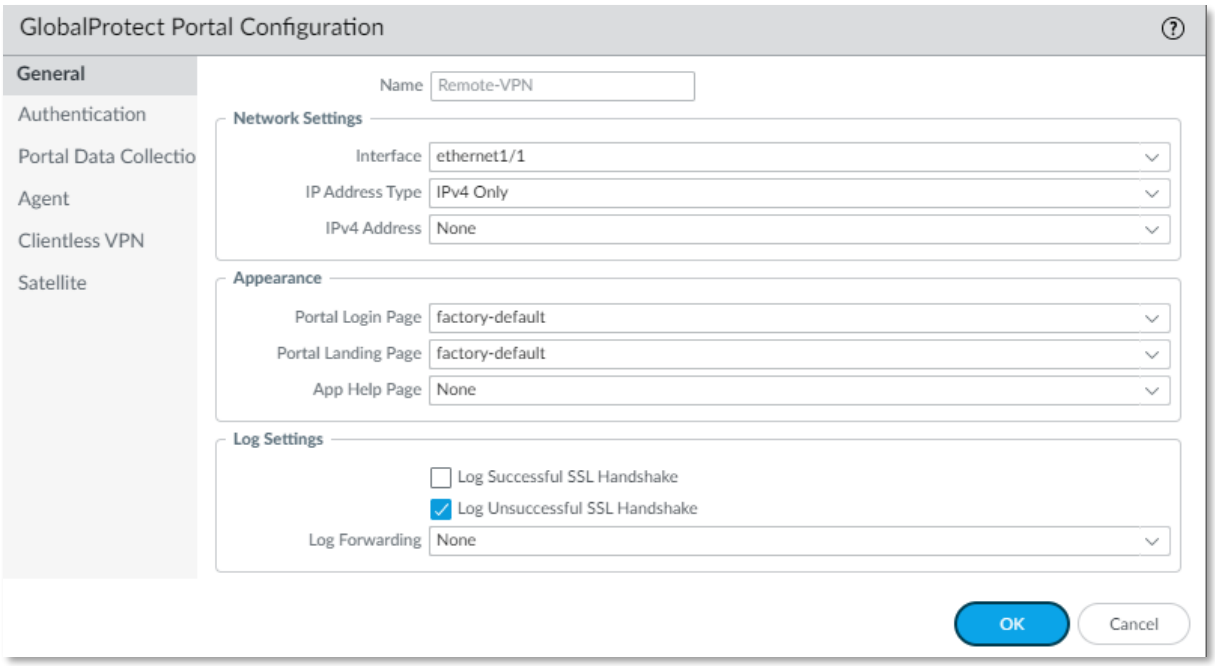


Figura 102 Configuración General Portal

Authentication

Seleccionamos el perfil SSL/TLS creado previamente.

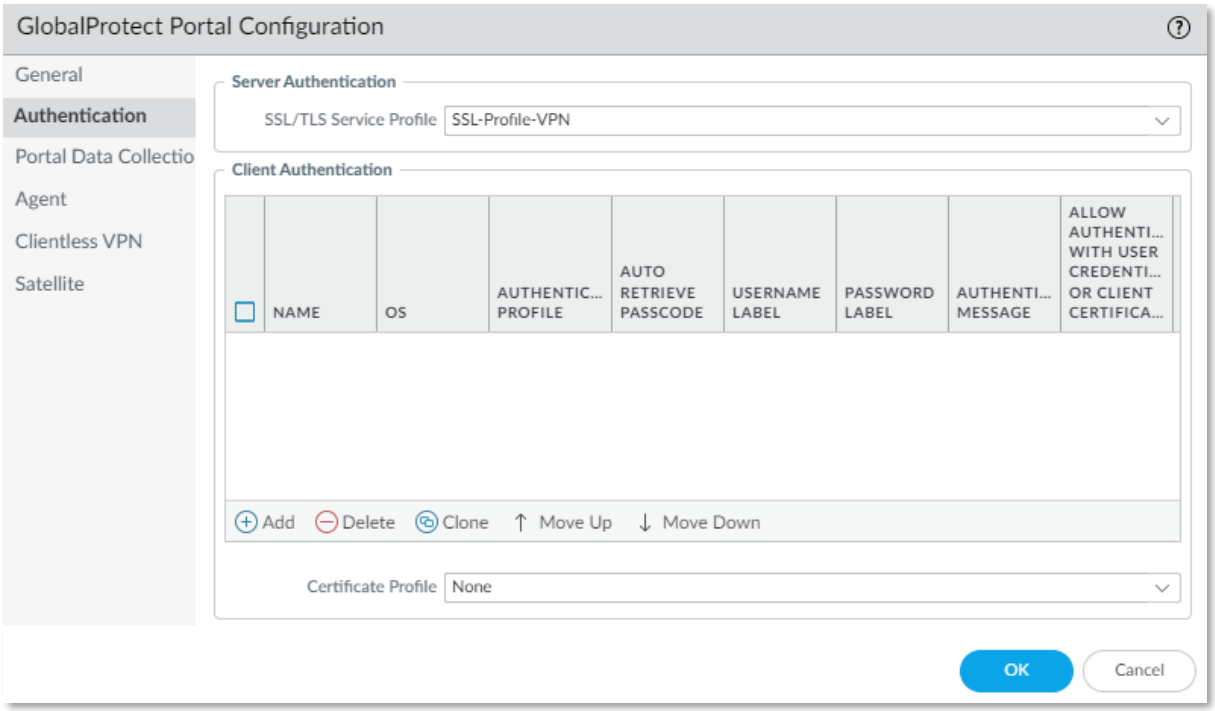


Figura 103 Configuración Autenticación

Dentro de Authentication, creamos un perfil '*Client Authentication*' en *Authentication < Client Authentication < Add*. El *Authentication Profile* es nuestro perfil creado previamente, el cual incluye los datos del Proveedor de Identidad. Elegir '*Yes (User Credentials OR Client Certificate Required)*'.

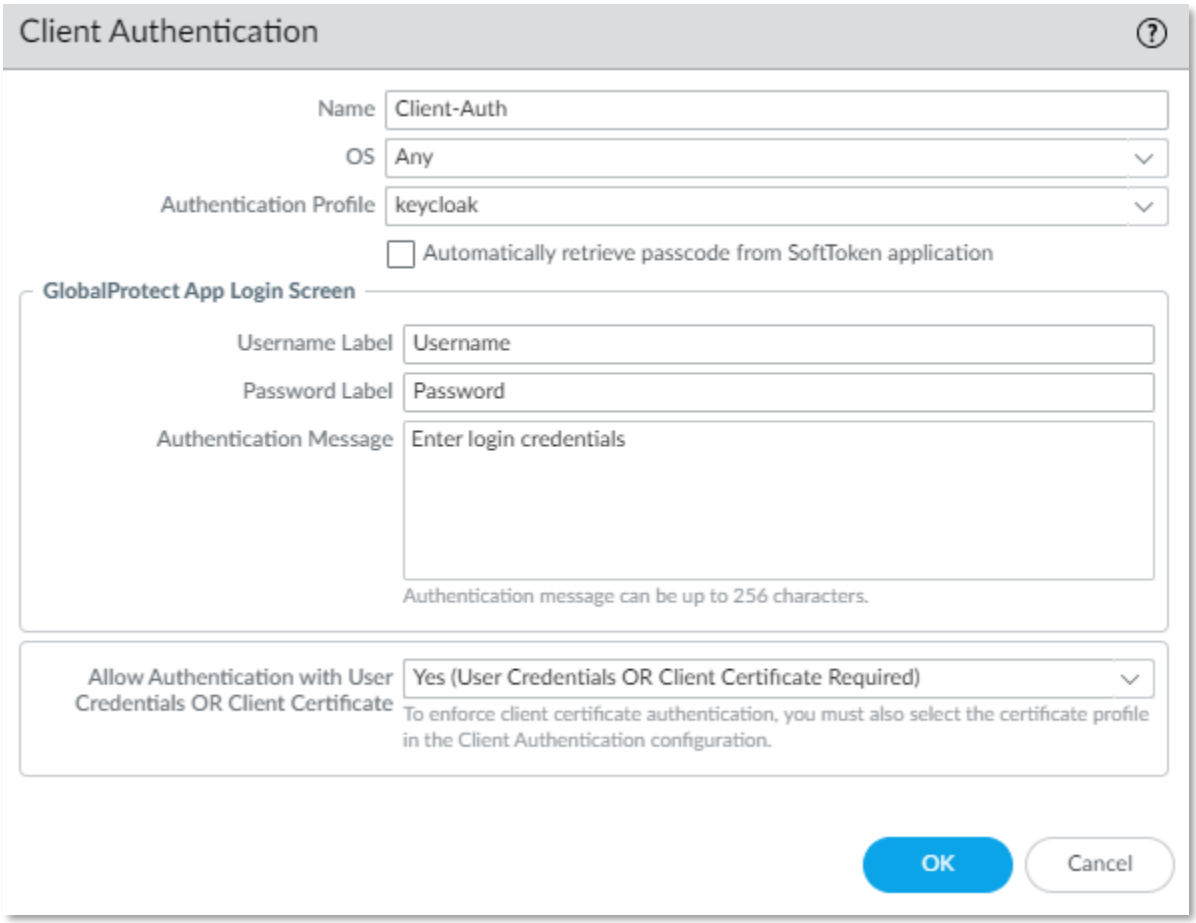


Figura 104 Client Authentication

Nos quedará:

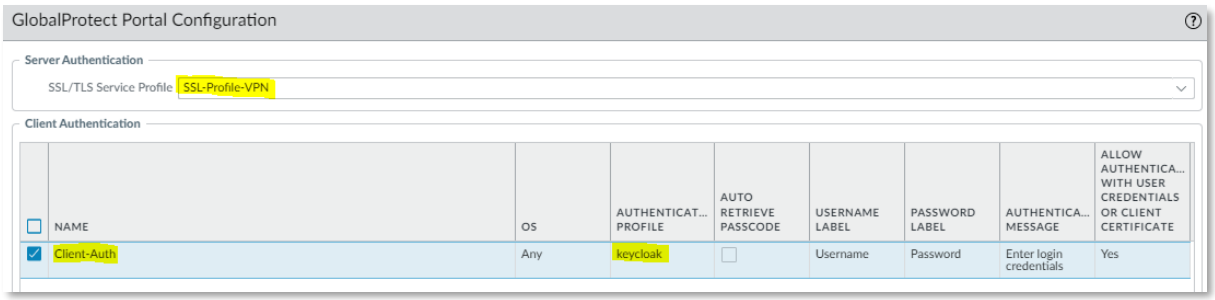


Figura 105 Resumen configuración

Agent

Añadimos el Agente en Agent < *Add.* Para la configuración de nuestro agente nos interesan los apartados *Authentication*, *External* y *App*.

En el apartado Authentication, vamos a marcar *'Generate cookie for authentication override'* y *'Accept cookie for authentication override'*. Esto nos permitirá posteriormente evitar tener que loguearnos tanto en el Portal como en la Gateway.

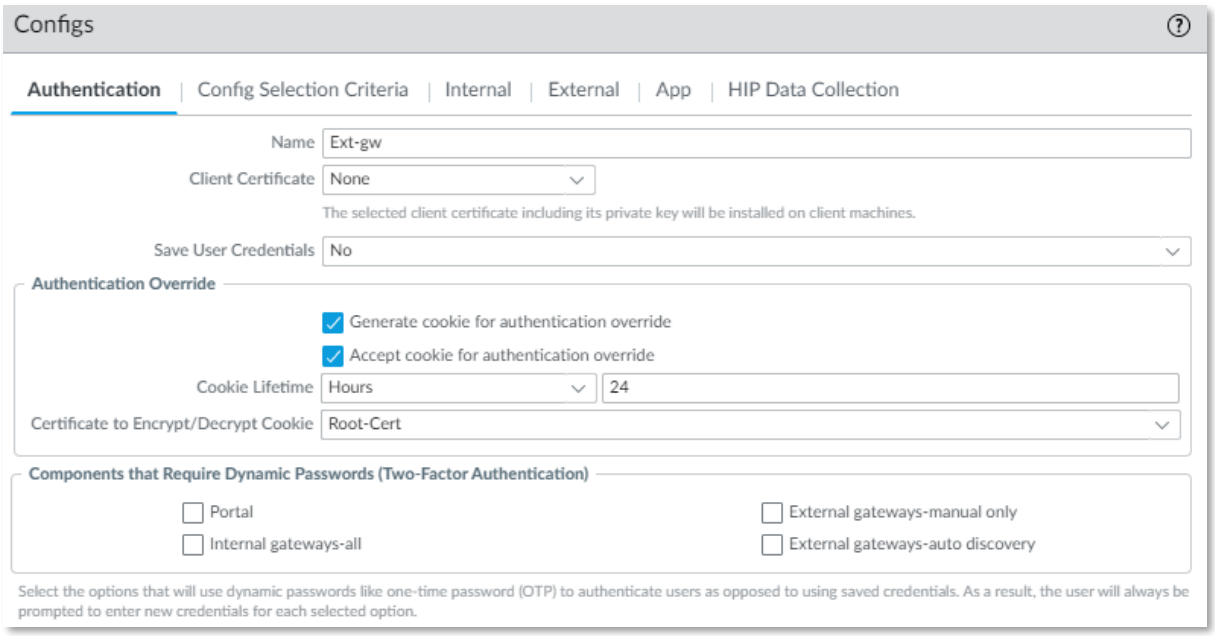


Figura 106 Configuración Agente Portal

En el apartado *External* añadimos una gateway configurándole los parámetros de nuestra Gateway.

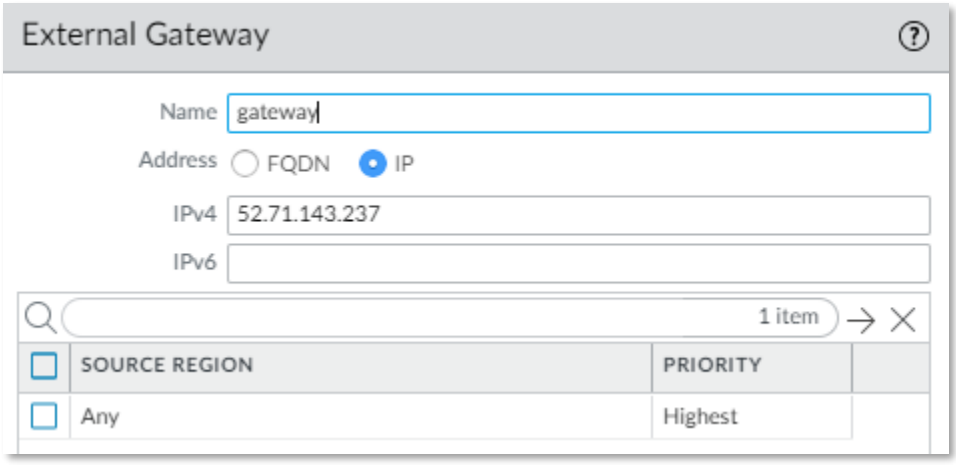


Figura 107 External Gateway

Nos quedará:

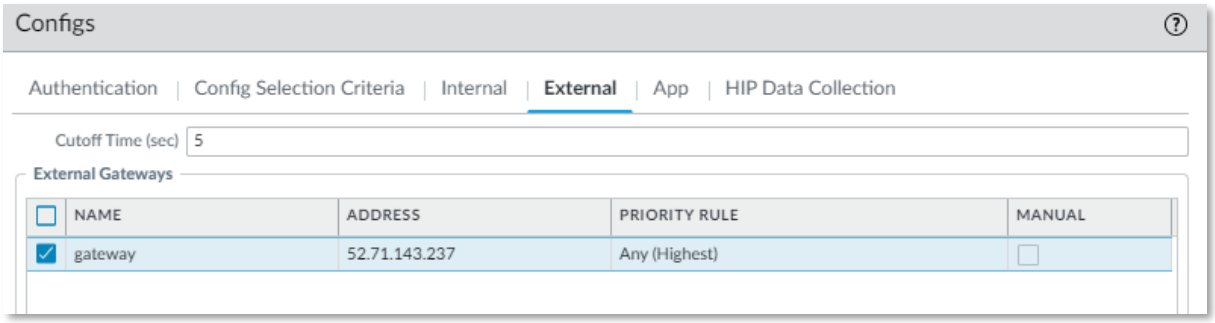


Figura 108 Resumen Configuración

En el apartado *App* < *App Configuration* configurar '*Connect Method - On-demand (Manual user initiated connection)*' y *'Use Default Browser for SAML Authentication - Yes'*.

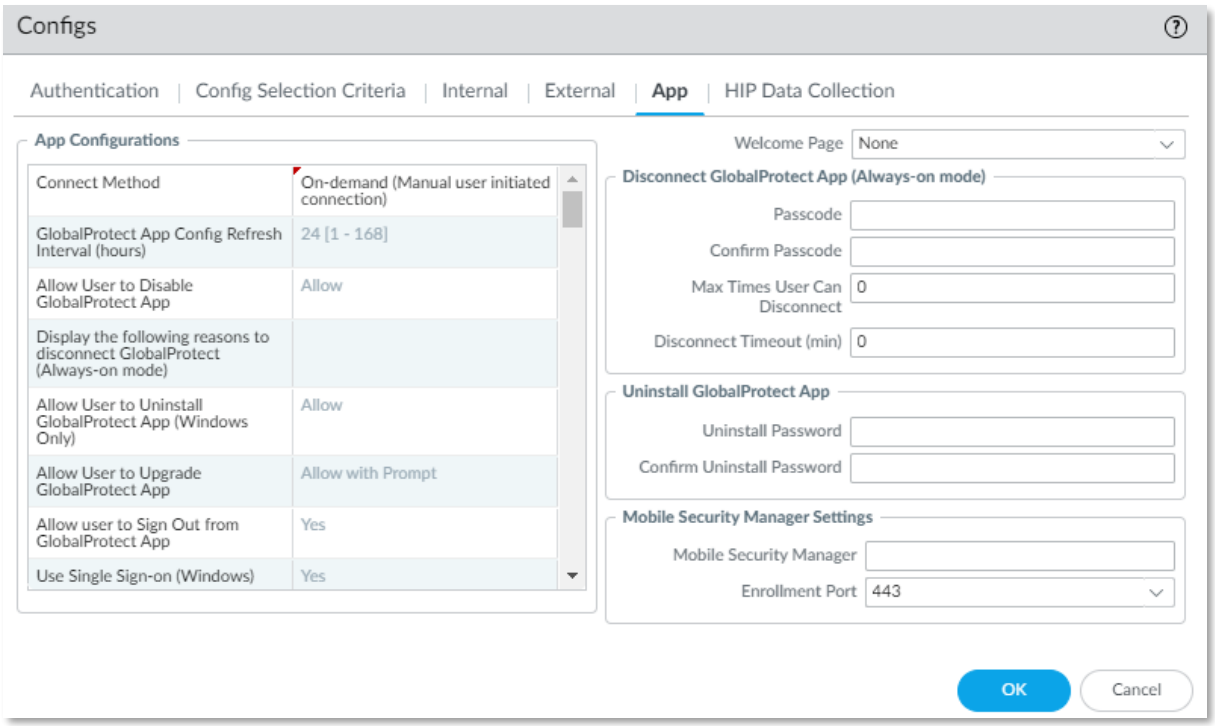


Figura 109 Configuración APP

Configurar la Gateway

En este caso vamos a configurar la Gateway en la misma interfaz que el portal. Nos dirigimos a Network < *Gateways* < *Add*.

General

En el apartado General configuramos el nombre y la Interfaz.

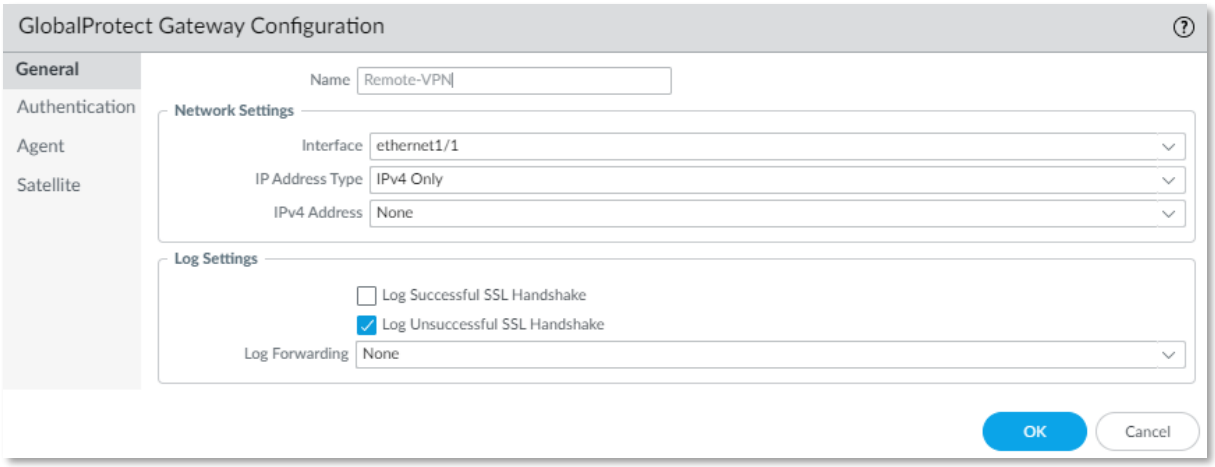


Figura 110 Configuración General Gateway

Authentication

En el apartado *Authentication* configuramos el perfil SSL/TLS creado previamente (que es el mismo que configuramos en el Portal) y añadimos un *Client Authentication*, al cual le daremos el *Authentication Profile* que creamos previamente y que nuevamente será el mismo que configuramos para el Portal.

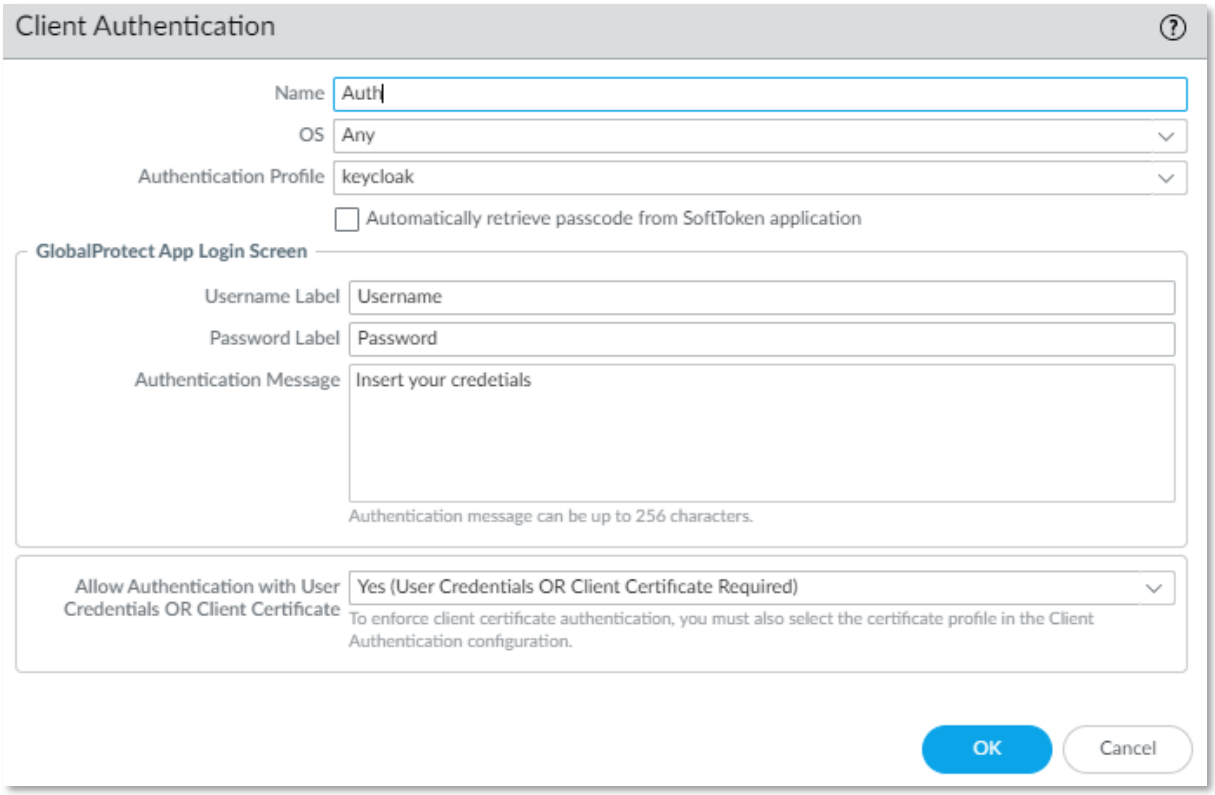


Figura 111 Client Authentication Gateway

Agent

En *Agent* < *Tunnel Settings* indicamos la interfaz túnel creada previamente.

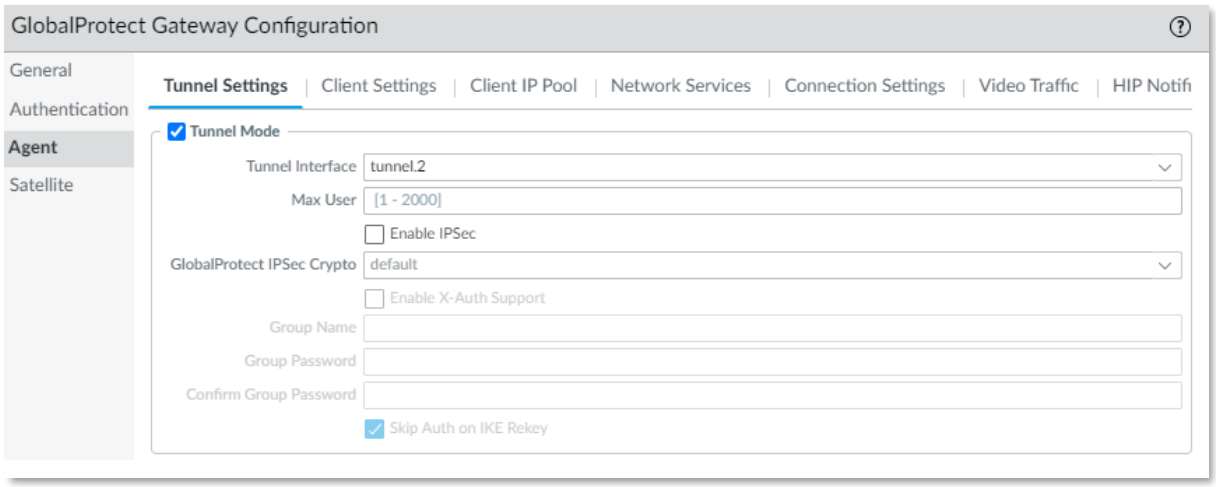


Figura 112 Configuración Agente Gateway

En *Agent < Client Settings < Add < Authentication Override* marcamos *Generate cookie for authentication override* y *Accept cookie for authentication override*. Esto es, tal y como hicimos previamente, para que la Gateway y el Portal se autentiquen entre ellos y el usuario no tenga que autenticarse en ambas.

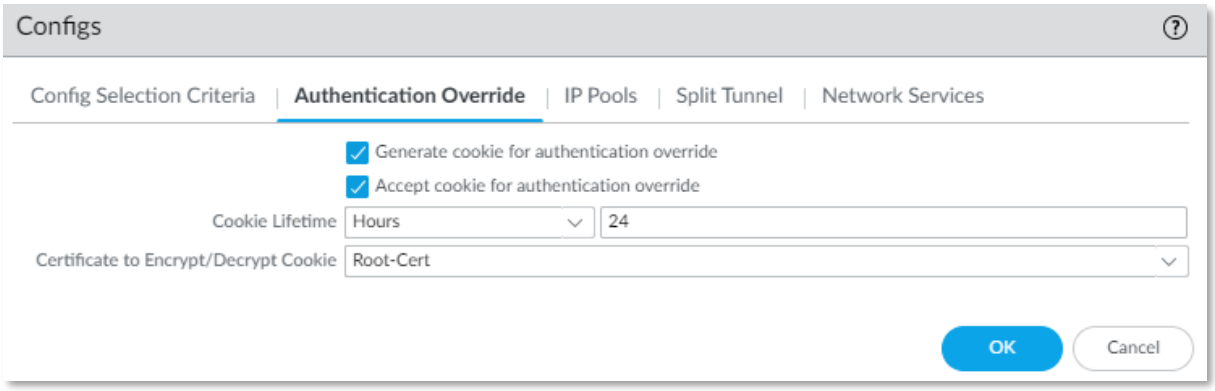


Figura 113 Autenticación Portal

En *Agent < Client Settings < Add < IP* Pools configuramos una pool de IPs. Estas será la IP que tomará el usuario una vez conectado en la VPN, en la interfaz lógica que se genera con la conexión.

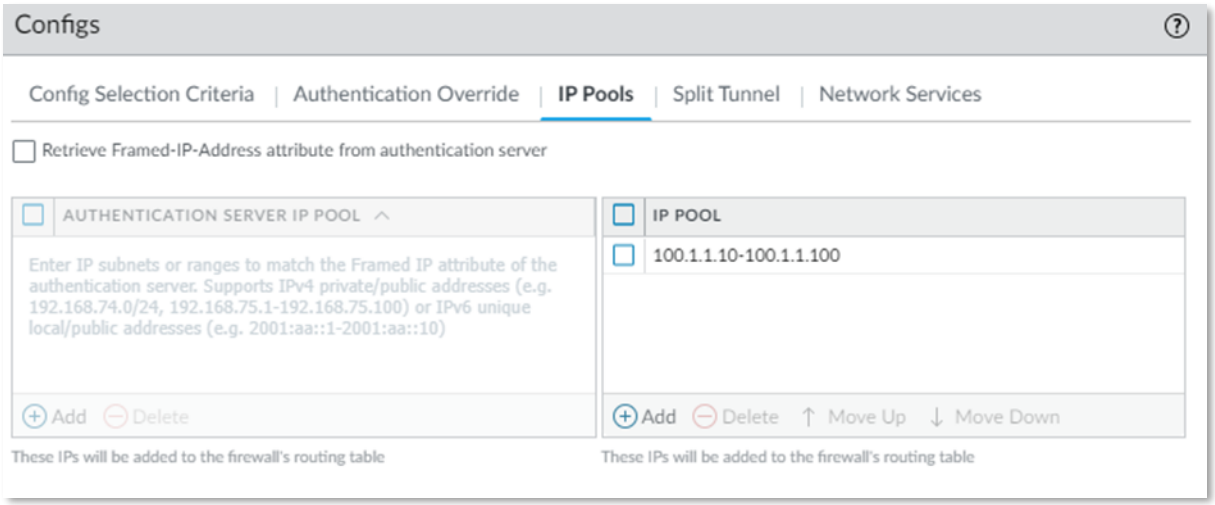


Figura 114 Pool de IPs para clietes de la VPN

Llegado este punto de la configuración, tanto el servidor Keycloak como el Firewall Palo Alto están listos para actuar como IDP y Prestador de Servicios respectivamente. Usando el cliente Global Protect y configurando en el mismo la IP o URL de la Gateway, podremos iniciar la conexión. Se muestra a continuación una serie de figuras en las que

se captura el proceso de inicio de conexión usando el cliente Global Protect, redirección automática a Keycloak, solicitud de credenciales (user y pass y posterior OTP) y consecución de la conexión.

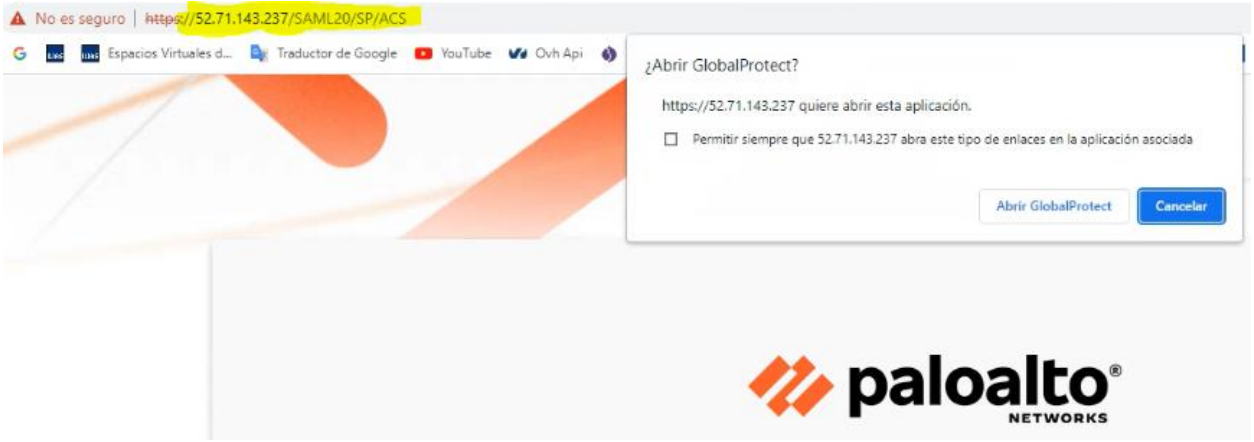


Figura 115 Inicio de conexión con cliente VPN (Global Protect)

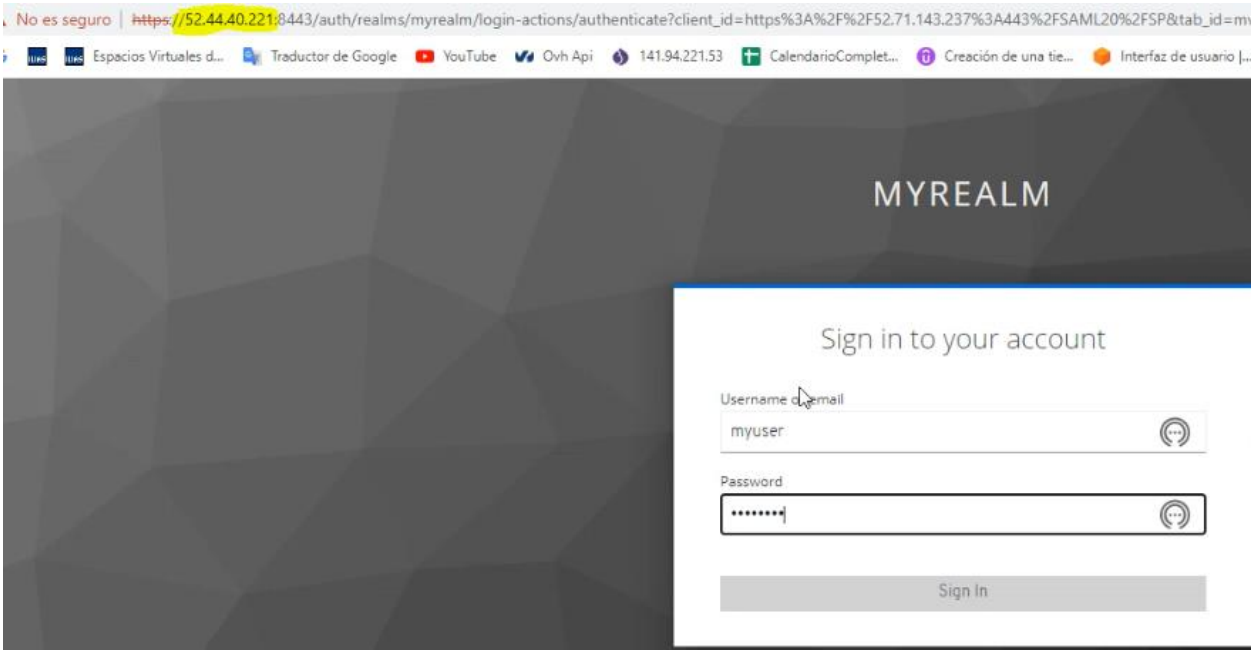


Figura 116 Redirección hacia Keycloak

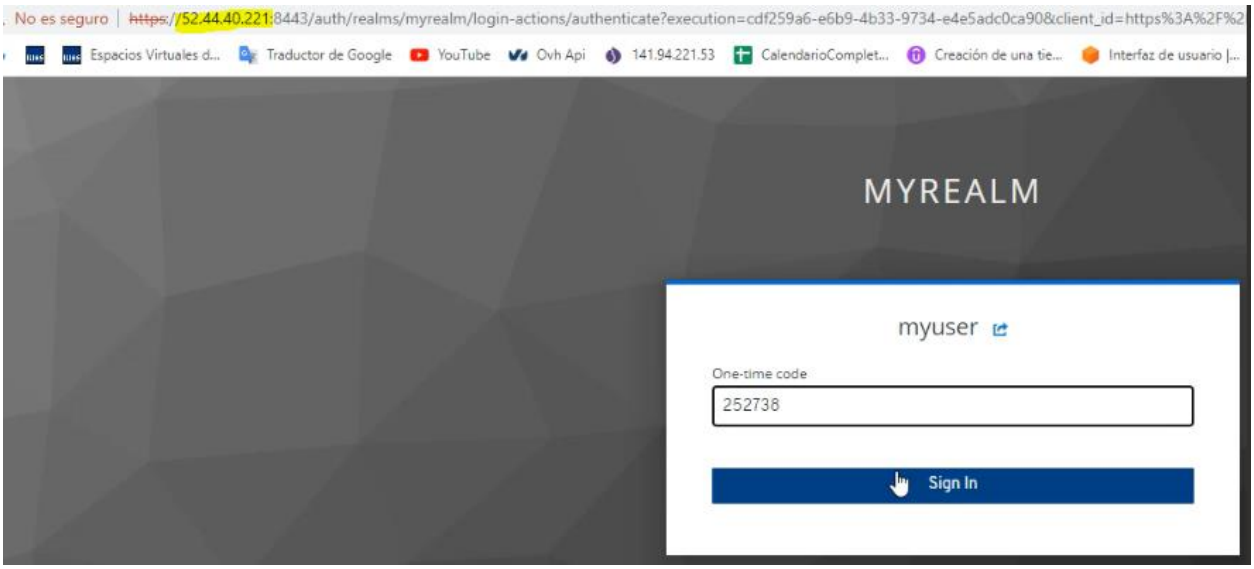


Figura 117 2FA con Google OTP en Keycloak

Figura 118 Cliente VPN Conectado

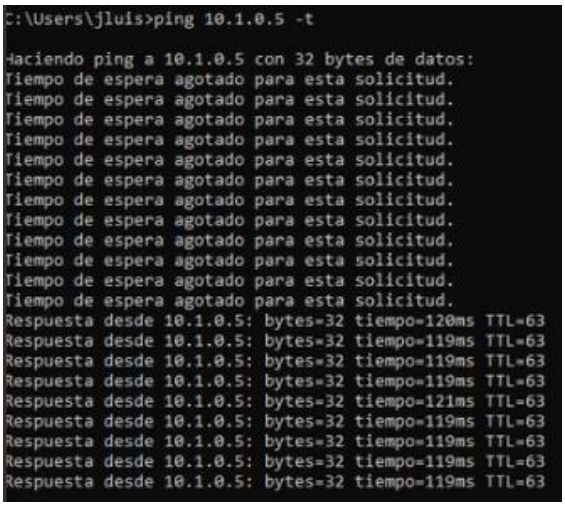


Figura 119 Ping a red Interna tras conexión con VPN

Posible Troubleshooting

Cliente Global Protect no reconoce el certificado y no permite importarlo

Si se ha seguido la configuración indicada en este anexo puede ocurrir que cuando tratamos de loguearnos, el cliente GP descargue automáticamente el certificado que le ofrece el Firewall. Si es un certificado autofirmado (como es nuestro caso), el cliente GP solicitará ambos, el firmado y el de la CA, pero no nos dejará importar el segundo (botón *Continuar* no es clicable).

Solución: Exportar manualmente desde el Firewall el certificado y añadirlo como confiable en nuestro sistema operativo. En este caso para Windows 10, ir a *Manage User Certificates* e importar el certificado/s exportados del firewall (Clic derecho sobre la carpeta *Certificates* < *All Task* < *Import*).

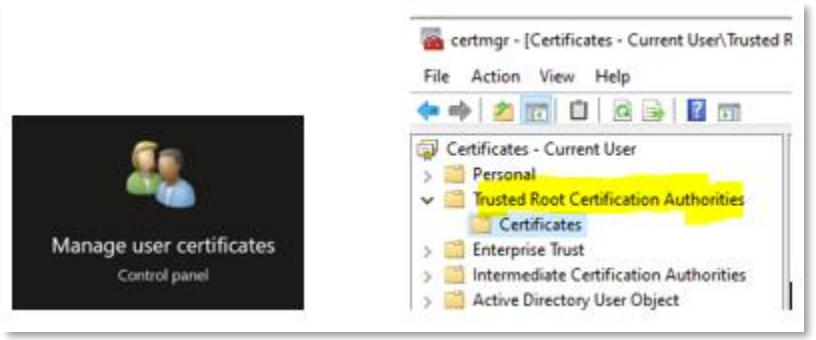


Figura 120 Añadir certificado de confianza en Windows

Keycloak devuelve error 'Invalid requester' al conectar a la VPN con el cliente GP

El navegador muestra el siguiente error:

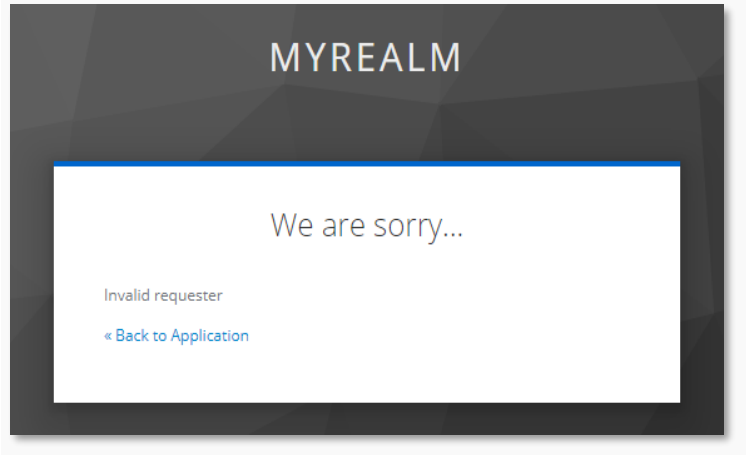


Figura 121 Error de autenticación en Keycloak

Solución: Asegurar que en el servidor Keycloak, en la configuración de nuestro Cliente (Punto ‘Creación del cliente. Keycloak como Proveedor de Identidad (IDP)’) tenemos deshabilitada la opción *Client Signature Required*.

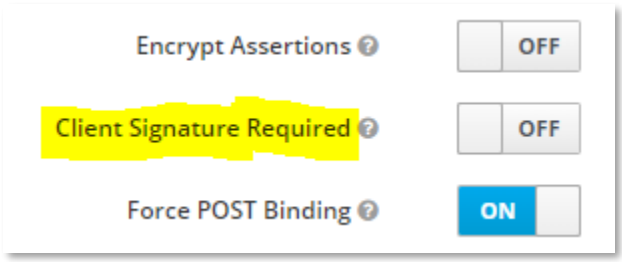


Figura 122 Deshabilitar requerimiento firma

NOTA: Cabe mencionar que esto aplica para la configuración seguida en este anexo. Si se desea que el cliente se autentique mediante firma, este parámetro deberá habilitarse y podría ser posible tener que realizar otras configuraciones adicionales no descritas en este anexo.

El cliente GP se conecta directamente a la VPN y no se solicitan credenciales

Esto puede ocurrir siempre que se haya realizado una autenticación y conexión a la VPN previas y posterior desconexión de la misma.

Solución: Controlar el Flow de autenticación en el cliente creado en Keycloak (punto ‘Configuración del flujo de autenticación’) y asegurarse de que se requiere *Username Password Form* y *Browser – Conditional OTP*.

Figura 123 Requerimientos flujo de autenticación

Posible solución: En la configuración de las zonas del firewall, controlar si se ha habilitado o no la Identificación de usuario.

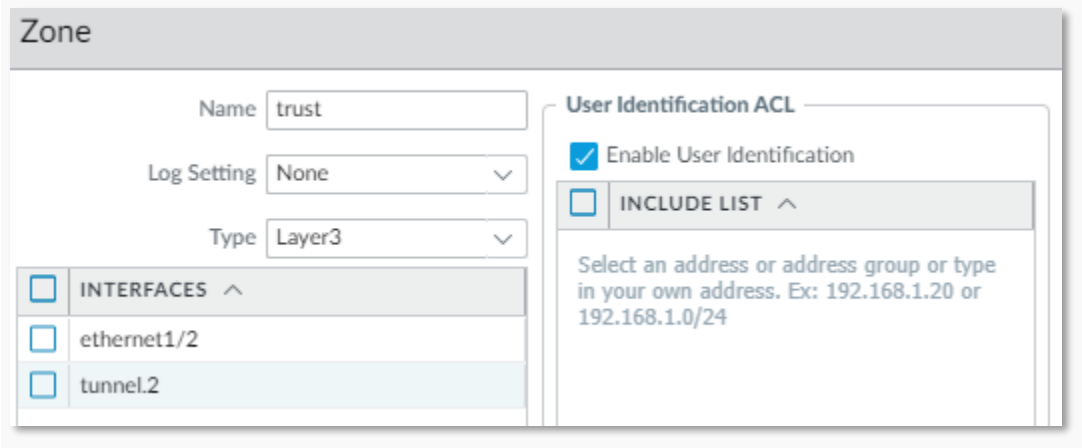


Figura 124 Habilitar autenticación en Zona del firewall

Se solicitan credenciales y OTP por duplicado

Al conectar con la VPN mediante el cliente GP, el navegador nos pide nuestras credenciales y el OTP, una vez proporcionados, el navegador vuelve a solicitar ambos nuevamente.

Solución: Permitir que el Portal y la Gateway se autentiquen entre ellos mediante cookies. En la configuración del Portal, marcar estas opciones.

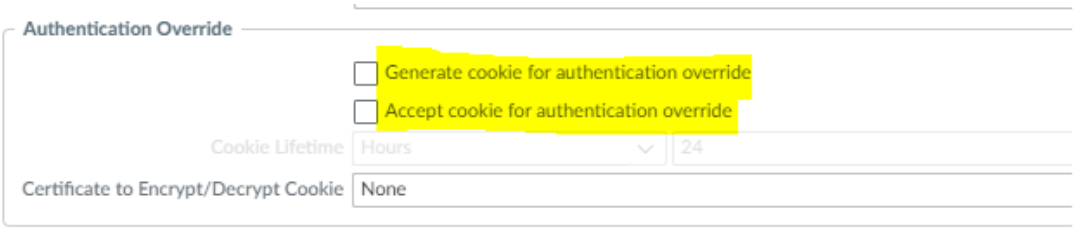


Figura 125 Generar y aceptar cookies entre Gateway y Portal