

Alerta ID:	112
Fecha del reporte:	17/04/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Recolección de credenciales (credential harvesting)
Herramienta de detección	N/A
Activo involucrado:	• Firewalls FortiGate • Puertas de enlace VPN • Actividad de actores en la dark web
Tipo de alerta:	Alerta
Nivel de riesgo:	Alto

Objetivo:

Informar a las organizaciones del sector salud en Colombia sobre la identificación de una campaña activa de ataques dirigida a dispositivos de seguridad perimetral, específicamente firewalls y puertas de enlace VPN, asociados a fabricantes como Fortinet, en la cual actores de amenaza están realizando actividades masivas de recolección y validación de credenciales comprometidas, explotación de accesos remotos expuestos y ataques automatizados de fuerza bruta.

El propósito de esta alerta es que las entidades del sector salud validen la exposición y configuración de sus dispositivos de seguridad perimetral, tanto en infraestructura local como en entornos híbridos o servicios gestionados por terceros, identificando posibles accesos



expuestos a Internet, credenciales reutilizadas o comprometidas y configuraciones débiles en servicios VPN.

Esta validación debe incluir la revisión de sus inventarios tecnológicos de seguridad de red, sistemas de acceso remoto, portales administrativos, infraestructura de conectividad entre sedes hospitalarias y cualquier componente que actúe como punto de entrada a la red clínica o administrativa, con el fin de reducir el riesgo de acceso no autorizado, compromiso de datos sensibles y afectación de la continuidad operativa de los servicios de salud.

Descripción:



Se ha identificado una campaña activa de amenazas dirigida a dispositivos de seguridad perimetral, especialmente firewalls y concentradores VPN de fabricantes como Fortinet, en la cual actores maliciosos están ejecutando actividades masivas de reconocimiento, validación de credenciales y acceso no autorizado a interfaces de administración expuestas.

La campaña no se asocia a una vulnerabilidad específica de tipo zero-day, sino a la explotación de **credenciales comprometidas previamente**, combinadas con técnicas automatizadas de ataque como **fuerza bruta (brute force)**, **credential stuffing** y **password spraying**, dirigidas a servicios de acceso remoto expuestos a Internet, particularmente interfaces VPN y paneles administrativos de firewalls.

Los atacantes están aprovechando la exposición de dispositivos perimetrales en Internet, así como la reutilización de contraseñas débiles o filtradas, para obtener acceso inicial a infraestructuras de red corporativa. Una vez autenticados, los actores de amenaza pueden acceder a configuraciones críticas del firewall, establecer túneles VPN no autorizados, modificar reglas de filtrado de tráfico y facilitar el movimiento lateral dentro de la red interna.



Fortinet ha indicado que la actividad observada corresponde a la reutilización de credenciales previamente comprometidas y a campañas automatizadas de ataque a gran escala, sin evidencia de explotación de una nueva vulnerabilidad en sus productos. Este comportamiento es consistente con actores de amenaza que operan en la dark web mediante bases de datos de credenciales filtradas y herramientas automatizadas de autenticación masiva.

En el contexto del sector salud, esta amenaza representa un riesgo elevado debido a que los dispositivos afectados suelen actuar como punto de entrada a redes clínicas, sistemas de historia clínica electrónica, plataformas de telemedicina y servicios administrativos, lo que podría derivar en accesos no autorizados, interrupción de servicios críticos o exposición de información sensible de pacientes.

Consecuencias de la explotación



La explotación de esta campaña activa dirigida a dispositivos de seguridad perimetral, como firewalls y puertas de enlace VPN, puede generar impactos severos tanto a nivel técnico como operativo en las organizaciones del sector salud, especialmente cuando estos equipos actúan como punto de entrada a la infraestructura crítica.

1. Acceso no autorizado a la red interna

El compromiso exitoso de credenciales VPN o de administración de firewalls puede permitir a un atacante establecer conexiones legítimas hacia la red interna de la organización, evitando mecanismos tradicionales de detección basados en perímetro.

Esto puede facilitar el acceso a sistemas clínicos, administrativos y de soporte.

2. Movimiento lateral dentro de la infraestructura hospitalaria



Una vez dentro de la red, el atacante puede desplazarse lateralmente hacia sistemas críticos como:

- Historia clínica electrónica (HCE)
- Sistemas de laboratorio
- Servidores de imágenes diagnósticas (PACS)
- Bases de datos administrativas y financieras

3. Compromiso de la disponibilidad de servicios críticos

El acceso a dispositivos de red permite la modificación de reglas de firewall o túneles VPN, lo que puede generar:

- Interrupción de conectividad entre sedes hospitalarias
- Caída de servicios clínicos digitales
- Bloqueo de acceso a plataformas de atención

4. Exposición de información sensible

El acceso no autorizado puede derivar en la extracción de información crítica como:

- Datos personales de pacientes
- Historias clínicas electrónicas
- Credenciales de acceso a sistemas internos
- Información administrativa y financiera

5. Riesgo de despliegue de ransomware

Los dispositivos perimetrales comprometidos pueden ser utilizados como punto de entrada para ataques posteriores de ransomware, afectando tanto servidores como estaciones de trabajo dentro del entorno hospitalario.



6. Compromiso de la infraestructura de seguridad

El atacante, al comprometer firewalls o VPNs, puede modificar políticas de seguridad, desactivar controles de inspección o crear túneles persistentes para mantener acceso prolongado al entorno.

7. Impacto regulatorio y reputacional

La exposición de datos sensibles de pacientes puede derivar en:

- Incumplimiento de la Ley 1581 de 2012 (Colombia)
- Investigaciones por parte de entidades regulatorias
- Pérdida de confianza institucional
- Afectación reputacional del prestador de salud

8. Persistencia del compromiso

Debido al uso de credenciales válidas, el atacante puede mantener acceso durante largos periodos sin ser detectado, incrementando el riesgo de exfiltración continua de información.

Modo de explotación del ataque

La campaña dirigida a dispositivos de seguridad perimetral, como firewalls y puertas de enlace VPN, se basa principalmente en la explotación de credenciales comprometidas y en el abuso de servicios de autenticación expuestos a Internet. La cadena de ataque puede describirse en las siguientes fases:

Fase 1 – Reconocimiento y descubrimiento de servicios expuestos

Los actores de amenaza realizan escaneos masivos en Internet con el objetivo de identificar dispositivos firewall y VPN expuestos públicamente, especialmente interfaces de administración o portales de acceso remoto sin restricciones adecuadas.



Este proceso permite la identificación de superficies de ataque vulnerables o mal configuradas.

Fase 2 – Uso de credenciales filtradas y ataques automatizados

Una vez identificados los objetivos, los atacantes utilizan bases de datos de credenciales previamente filtradas en la dark web, combinadas con técnicas automatizadas de:

- Credential stuffing
- Password spraying
- Fuerza bruta distribuida

El objetivo es validar accesos válidos a servicios VPN o consolas administrativas.

Fase 3 – Acceso inicial a la infraestructura perimetral

Cuando las credenciales son válidas, el atacante obtiene acceso legítimo a:

- VPN corporativa
- Panel de administración del firewall
- Consolas de gestión de red

Este acceso inicial evita muchas detecciones basadas en perímetro, ya que simula comportamiento de usuario autorizado.

Fase 4 – Abuso de la configuración del firewall/VPN

Con acceso autenticado, el atacante puede:

- Modificar reglas de firewall
- Crear o alterar túneles VPN
- Deshabilitar controles de inspección de tráfico
- Expandir permisos de acceso remoto

Esto permite debilitar progresivamente la postura de seguridad de la organización.

Fase 5 – Movimiento lateral dentro de la red interna

Una vez dentro del entorno corporativo, el atacante puede desplazarse hacia sistemas internos críticos del sector salud, incluyendo:



- Sistemas de historia clínica electrónica (HCE)
- Servidores de aplicaciones clínicas
- Bases de datos de pacientes
- Sistemas administrativos y financieros

Fase 6 – Persistencia y mantenimiento del acceso

El atacante puede establecer persistencia mediante:

- Reutilización de credenciales válidas
- Creación de nuevos usuarios administrativos
- Configuración de accesos VPN ocultos o alternos

Esto permite mantener acceso prolongado sin necesidad de explotación adicional.

La campaña no depende de una vulnerabilidad específica, sino de:

- Exposición de servicios VPN/firewall
- Reutilización de credenciales comprometidas
- Automatización de ataques de autenticación
- Falta de MFA o segmentación adecuada

vulnerabilidades asociadas

MITRE ATT&CK + fallos de configuración en firewalls y VPN)

La campaña activa contra dispositivos de seguridad perimetral no se basa en una única vulnerabilidad de software, sino en la combinación de técnicas de ataque documentadas en el marco **MITRE ATT&CK** y en debilidades comunes de configuración en entornos de red empresarial, especialmente en firewalls y servicios VPN utilizados en el sector salud.

✳ 1. Uso de credenciales válidas comprometidas

MITRE ATT&CK: T1078 – Valid Accounts

Descripción:



Los atacantes utilizan credenciales legítimas obtenidas previamente mediante filtraciones, malware infostealer o reutilización de contraseñas.

Impacto:

Permite acceso directo a VPN o paneles de firewall sin necesidad de explotación técnica.

2. Ataques de fuerza bruta y credential stuffing

MITRE ATT&CK: T1110 – Brute Force

Descripción:

Automatización de intentos de autenticación utilizando listas masivas de usuarios y contraseñas filtradas.

Impacto:

Compromiso de cuentas débiles o reutilizadas en sistemas de acceso remoto.

3. Exposición de servicios VPN y paneles de administración**Debilidad de configuración crítica****Descripción:**

Interfaces administrativas y portales VPN expuestos directamente a Internet sin restricciones de acceso (IP allowlist, MFA o segmentación).

Impacto:

Incrementa la superficie de ataque y facilita intentos de autenticación no autorizados.

4. Falta de autenticación multifactor (MFA)**Debilidad de control de acceso****Descripción:**

Muchos entornos de firewall/VPN aún dependen únicamente de usuario y contraseña.

Impacto:

Permite que credenciales filtradas sean suficientes para el acceso inicial.

5. Mala segmentación de red (flat network)

MITRE ATT&CK: T1021 – Remote Services

Descripción:

Ausencia de segmentación entre red perimetral, servidores clínicos y redes administrativas.

Impacto:

Facilita movimiento lateral hacia sistemas críticos del sector salud.

6. Configuraciones débiles de firewall

Debilidad de seguridad perimetral

Descripción:

Reglas de firewall permisivas o mal definidas que permiten tráfico innecesario hacia servicios internos o administrativos.

Impacto:

Exposición de interfaces críticas y aumento del riesgo de intrusión.

7. Falta de monitoreo de autenticaciones sospechosas

MITRE ATT&CK: T1071 – Application Layer Protocol

Descripción:

Ausencia de alertas ante múltiples intentos fallidos, accesos desde ubicaciones inusuales o patrones anómalos de VPN.

Impacto:

Permite que ataques de credential stuffing pasen desapercibidos.

8. Uso de credenciales sin rotación o sin políticas de complejidad

Debilidad organizacional



Descripción:

Contraseñas estáticas, reutilizadas o sin políticas de expiración.

Impacto:

Facilita la explotación de bases de datos filtradas.

Recomendaciones de detección y mitigación

Con el objetivo de fortalecer la capacidad de detección temprana y respuesta ante la campaña activa de compromiso de firewalls y servicios VPN, se recomienda implementar un enfoque de **seguridad por capas**, combinando monitoreo conductual, correlación avanzada en SIEM y endurecimiento de la infraestructura perimetral.

1. DETECCIÓN AVANZADA EN SIEM (CORRELACIÓN DE EVENTOS)**1.1 Detección de ataques de fuerza bruta y credential stuffing**

Configurar reglas que identifiquen:

- ≥ 10 intentos fallidos de login en menos de 5 minutos
- múltiples usuarios autenticados desde la misma IP externa
- intentos de acceso a VPN con listas de usuarios comunes

1.2 Anomalías en autenticación válida (Account Takeover)

Detectar cuando:

- Un usuario exitosamente autenticado cambia de comportamiento
- Se conecta desde país o ASN no habitual
- Realiza acciones administrativas inmediatamente después del login



Indicador crítico:

Login exitoso + cambio de configuración del firewall en < 10 minutos

1.3 Uso sospechoso de credenciales válidas (MITRE T1078)

Alertar sobre:

- Accesos simultáneos con la misma cuenta desde múltiples ubicaciones
- Login de cuentas administrativas fuera de horario institucional
- Acceso a VPN sin patrón histórico previo

1.4 Detección de actividad de administración no autorizada

Monitorear eventos como:

- Creación o modificación de reglas de firewall
- Cambios en políticas de NAT o routing
- Activación/desactivación de VPNs
- Creación de nuevos usuarios administrativos

2. THREAT HUNTING (BÚSQUEDA PROACTIVA)**2.1 Indicadores de compromiso en logs VPN**

Buscar patrones como:

- Reintentos múltiples con variación de contraseña
- Sesiones VPN muy cortas seguidas de reconexión
- Accesos desde IPs asociadas a TOR o VPN públicas

2.2 Búsqueda de actividad lateral temprana

Detectar:



- Escaneo interno después de login VPN
- Conexiones a múltiples subredes en corto tiempo
- Acceso a servicios internos no documentados

2.3 Análisis de comportamiento administrativo

Identificar:

- Uso de comandos de configuración fuera de horario
- Cambios masivos en reglas de firewall
- Exportación de configuraciones del dispositivo

3. HARDENING DE FIREWALL Y VPN

3.1 Control de acceso estricto

- Implementar **IP allowlist obligatoria**
- Restringir acceso a panel de administración solo desde redes internas seguras
- Bloquear acceso administrativo desde Internet público

3.2 MFA obligatorio

- Activar autenticación multifactor en:
 - VPN corporativa
 - Consola de firewall
 - Accesos de administración remota

3.3 Segmentación de red avanzada

Separar claramente:

-  Plano de gestión (firewall / VPN admin)
-  Red de usuarios clínicos



-  Red de servidores críticos
-  Red de invitados

3.4 Reducción de superficie de ataque

- Deshabilitar servicios no utilizados en firewall
- Cerrar puertos de administración expuestos
- Evitar interfaces web administrativas públicas

3.5 Protección de credenciales

- Rotación periódica de credenciales administrativas
- Eliminación de cuentas inactivas
- Uso de gestores de identidad (IAM centralizado)

4. ALERTAS CRÍTICAS EN TIEMPO REAL

Configurar SIEM para alertar sobre:

Nivel ALTO:

- Login administrativo desde país desconocido
- Cambio de reglas firewall + login reciente

Nivel CRÍTICO:

- Desactivación de MFA
- Creación de usuario admin nuevo
- Exportación de configuración del firewall

5. RESPUESTA AUTOMATIZADA (SOAR)

Integrar automatización para:



- Bloquear IP tras múltiples intentos fallidos
- Deshabilitar usuario tras comportamiento anómalo
- Forzar cierre de sesión VPN sospechosa
- Alertar SOC inmediatamente ante cambios críticos

6. VISIÓN DE RIESGO EN SALUD

Este tipo de ataque impacta directamente:

- Historia clínica electrónica (HCE)
- Sistemas de laboratorio (LIS)
- PACS (imágenes diagnósticas)
- Telemedicina
- Sistemas administrativos hospitalarios

El firewall/VPN es el **punto de entrada único crítico (Single Point of Failure)**

Conclusiones



La campaña activa dirigida a dispositivos de seguridad perimetral, como firewalls y servicios VPN, representa un riesgo crítico para las organizaciones del sector salud, debido a que se basa en el abuso de credenciales válidas, la explotación de servicios de acceso remoto expuestos y la falta de controles robustos de autenticación y segmentación de red.

A diferencia de ataques basados en vulnerabilidades técnicas específicas, este escenario se fundamenta en la **debilidad operativa y de configuración de los entornos de red**, lo que incrementa significativamente la superficie de ataque en infraestructuras hospitalarias altamente interconectadas.

El compromiso exitoso de un dispositivo perimetral puede derivar en la exposición completa de la red interna, permitiendo acceso no autorizado a sistemas críticos como historia clínica



electrónica, sistemas de laboratorio, plataformas de telemedicina y servicios administrativos, lo que afecta directamente la continuidad de la atención en salud.

Asimismo, la reutilización de credenciales filtradas y la ausencia de mecanismos de autenticación multifactor facilitan la persistencia de los atacantes dentro del entorno corporativo, dificultando la detección temprana y aumentando el tiempo de permanencia (dwell time) en la infraestructura comprometida.

En este contexto, la implementación de controles de monitoreo avanzado, segmentación de red, fortalecimiento de la gestión de identidades y aplicación de políticas estrictas de acceso se convierten en elementos esenciales para reducir la exposición a este tipo de campañas.

Finalmente, se concluye que la seguridad del sector salud frente a este tipo de amenazas depende en gran medida de la **gestión adecuada de accesos, la visibilidad operativa y la capacidad de detección basada en comportamiento**, más que de la existencia de vulnerabilidades técnicas aisladas.

Fuentes:



- **Fortinet Security Advisories**

<https://www.fortiguard.com/psirt>

Documentación oficial de avisos de seguridad, incidentes activos y recomendaciones de mitigación sobre productos Fortinet (FortiGate, FortiProxy, FortiOS).

- **FortiGuard Threat Intelligence**

<https://www.fortiguard.com>

Plataforma de inteligencia de amenazas utilizada para la detección de campañas activas, reputación de IPs y actividad maliciosa global.



- **MITRE ATT&CK Framework**

<https://attack.mitre.org/>

Marco de referencia utilizado para mapear técnicas de ataque observadas en campañas de:

Credential Access (T1078 – Valid Accounts)

Brute Force (T1110)

External Remote Services (T1133)

- **CISA – Cybersecurity Advisories**

<https://www.cisa.gov/>

Fuente de alertas sobre campañas activas de explotación de VPN, firewalls y accesos remotos en infraestructura crítica.

- **ENISA Threat Landscape**

<https://www.enisa.europa.eu/publications>

Reportes de tendencias de ataques dirigidos a infraestructura perimetral, incluyendo:

Credential stuffing

Exposición de VPN corporativas

Compromiso de firewalls empresariales

- **Shodan (Internet Exposure Monitoring)**

<https://www.shodan.io>

Motor de búsqueda de dispositivos expuestos en Internet, utilizado para identificar:

Firewalls accesibles públicamente

VPN expuestas

Interfaces administrativas sin protección



- **Censys (Attack Surface Intelligence)**

<https://censys.io>

Plataforma de análisis de superficie de ataque global para detección de servicios expuestos en infraestructura crítica.

- **NIST Cybersecurity Framework**

<https://www.nist.gov/cyberframework>

Modelo de referencia para gestión de riesgos en infraestructura crítica, aplicable a redes hospitalarias.

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el **CSIRT Salud** a través de las líneas telefónicas **(+57) 316 893 1490 - 318 155 3570** o mediante el correo electrónico **csirtsalud@minsalud.gov.co**. Nuestro equipo está disponible para brindar el acompañamiento necesario.

