

# دورة إدارة جدار الحماية 4: FortiGate Administrator

## Fortinet NSE

7 – 11 يونيو 2027

الدار البيضاء

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

# دورة إدارة جدار الحماية Fortinet NSE 4: FortiGate Administrator

**المرجع:** 264348_2249 **التاريخ:** 7 – 11 يونيو 2027 **المكان:** الدار البيضاء **الرسوم:** 4100 Euro

## نظرة عامة

تطرح دورة إدارة جدار الحماية Fortinet NSE 4: FortiGate Administrator برنامجا تدريبيا يمتد أسبوع لمسؤولي الشبكات وأمن المعلومات لمغادرة القاعة بملف إعدادات أمني متكامل لحماية محيط الشبكات المؤسسية. تعالج الدورة تعقيدات إدارة سياسات جدران الحماية، والتحكم في فحص حركة المرور المشفرة، وتأمين الربط الشبكي عبر تقنيات VPN وحزم المراقبة والتحكم في المحتوى. تقدم أجايل للتدريب دورة إدارة جدار الحماية Fortinet NSE 4: FortiGate Administrator لتطوير مهارات إدارة منظومة FortiOS باحترافية عملية وموثوقة.

## الفئة المستهدفة

- مسؤولو أمن الشبكات المكلفون بإدارة وتحديث سياسات جدران الحماية المؤسسية ومتابعة الامتثال الفني.
- مهندسو الشبكات القائمون على ربط الفروع وتأمين مسارات الاتصال الافتراضي وإدارة حزم تبادل البيانات.
- مسؤولو الجدران النارية المعنيون بفحص حركات البيانات المشفرة وضبط مرشحات تصفح الويب والبرمجيات.
- محللو مراكز العمليات الأمنية SOC المكلفون برصد تنبيهات التهديدات وتتبع السجلات الأمنية عبر المنظومة.
- مهندسو الدعم الفني المسؤولون عن صيانة بيئات الحماية الطرفية واستكشاف أخطاء الاتصال والشبكات.

تفترض الدورة أن المشاركين يمارسون إدارة الشبكات المعتمدة على بروتوكولات TCP/IP وعناوين IP وتقسيم الشبكات، وتترك المبادئ المبدئية في الاتصالات للمستويات التأسيسية.

## الإدارات والقطاعات المستهدفة

تستند الدورة إلى تطبيقات عملية تخدم إدارات هندسية وأمنية متعددة.

- إدارات أمن المعلومات والأمن السيبراني
- أقسام تشغيل وصيانة البنية التحتية والشبكات
- إدارات مراكز العمليات الأمنية والدعم الفني
- قطاع الخدمات المالية والمصرفية
- قطاع الرعاية الصحية والخدمات الطبية الرقمية
- قطاع الاتصالات وتقنية المعلومات

AGILE LEADERS
Training Center

## أهداف التعلم

بنهاية هذه الدورة، سيكون المشاركون قادرين على:

- تطبيق الإعدادات الأساسية لمنظومة FortiOS وإدارة واجهات الشبكة وتقسيمات VLAN.
- بناء سياسات جدار الحماية وقواعد ترجمة عناوين الشبكة NAT وإجراءات توثيق هوية المستخدمين.
- تحليل حركة المرور المشفرة وضبط ملفات فحص المحتوى ومنع الاختراق والبرمجيات الخبيثة.
- تطبيق قنوات الاتصال المشفرة لأنظمة IPsec VPN و SSL-VPN لربط الفروع والمستخدمين الخارجيين.
- تقييم أداء مجموعات التوافر العالي High Availability وإدارة مسارات SD-WAN بكفاءة تشغيلية.

## جدول الدورة

### اليوم 1: إعداد نظام FortiGate والتكامل الشبكي

- الإعداد الأولي لمنظومة FortiGate وضوابط واجهة الوصول الإداري لنظام FortiOS
- هيكلية واجهات الشبكة ومسارات تجميع VLAN وتكوين المحولات البرمجية Software Switch
- تطبيق التوجيه الثابت وتجميع روابط الاتصال ومراقبة مسارات البوابات الافتراضية
- إنشاء سياسات جدار الحماية وكائنات الخدمات وأنماط ترجمة عناوين الشبكة NAT
- تكامل توثيق المستخدمين بالاعتماد على خوادم LDAP و RADIUS وقواعد البيانات المحلية

### اليوم 2: منع التهديدات وفحص المحتوى الرقمي

- إدارة المراجع المصدقة وتطبيق ملفات فحص الحزم المشفرة عبر تقنيات SSL Inspection
- ضبط محرك مكافحة الفيروسات والحماية من شبكات البوت نت ومنع التفشي الأمني
- سياسات تصفية محتوى الويب وتجاوز الفئات وقواعد فرض محركات البحث الآمن
- مطابقة تواقيع التحكم بالتطبيقات وتحديد أولويات حركة البيانات وتطبيق ضوابط البروتوكولات
- تخصيص مستشعرات نظام منع التسلل IPS وتصفية الهجمات المعتمدة على معدل التدفق

### اليوم 3: الاتصال الآمن والشبكات الخاصة الافتراضية

- تصميم طبولوجيا أنفاق IPsec VPN بين المواقع باستخدام إعدادات المرحلتين الأولى والثانية
- تكوين أنفاق IPsec VPN التكرارية مع التوجيه الديناميكي وخاصية كشف النظير المعطل DPD
- إعداد بوابات SSL-VPN وأنماط الوصول عبر المتصفح وتكامل عميل FortiClient للأنفاق
- الاقتران مع شبكة الأمان Fortinet Security Fabric وجمع بيانات القياس ورسم الطبولوجيا
- سياسات الحماية من هجمات حجب الخدمة الموزعة DDoS وتحديد عتبات الحد من المعدلات

## اليوم 4: التوافر العالي وتقنية SD-WAN ومحاذاة الامتثال

- نشر مجموعات التوافر العالي High Availability بأنماط التشغيل الإيجابي-السلبي والإيجابي-الإيجابي
- مزامنة الجلسات ومعالجة انقسام الشبكة Split-Brain وتحديد أولويات واجهات المراقبة
- اتفاقيات مستوى أداء شبكات SD-WAN وتصميم قواعد توجيه مسارات الاتصال
- تصميم سياسات جدار الحماية المتوافقة مع ضوابط الأمن السيبراني المؤسسية
- إجراءات المراجعة الدورية لسياسات الجدار الناري وتصدير أدلة التدقيق والتحقق المؤتمتة

## اليوم 5: التطبيق المؤسسي وحزمة الإعداد الختامية

- نشاط مقترح: إعداد مجموعة توافر عالي بنمط إيجابي-سلبي والتحقق من التبديل الفوري الآمن للجلسات
- نشاط مقترح: تطبيق فحص الحزم العميق لشهادات SSL المدمج مع التحكم بالتطبيقات وتصفية الويب
- نشاط مقترح: استكشاف أخطاء نفق IPsec VPN متعدد الفروع وسياسات توجيه مسارات SD-WAN ومعالجتها
- نشاط مقترح: تنفيذ مراجعة مطابقة لسياسات جدار الحماية وتوليد سجلات التدقيق والامتثال الفني
- تمرين ختامي رئيسي: تجميع وثيقة تصميم وإعدادات الحماية لمحيط الشبكة المؤسسية عبر FortiGate

## التمارين التطبيقية

تعتمد الدورة على مختبرات وحالات عملية تحاكي البيئات المؤسسية وشبكات الأعمال المعقدة.

- نشاط مقترح: تهيئة خيارات توجيه البيانات وتفعيل سياسات ترجمة العناوين NAT والتوثيق المركزي.
- نشاط مقترح: عزل الهجمات السيبرانية من خلال تخصيص مستشعرات IPS وفك تشفير مسارات SSL.
- نشاط مقترح: بناء نفق افتراضي مشفر يربط موقعين مع تفعيل آليات تحويل المسار التلقائي عند الأعطال.

## الأسئلة الشائعة

### من تناسب دورة إدارة جدار الحماية Fortinet NSE 4: FortiGate Administrator وما متطلباتها؟

تناسب مسؤولي أمن الشبكات ومهندسي الأنظمة والدعم الفني المعنيين بتأمين حركة البيانات. تفترض الدورة إلمام المشارك بأساسيات التوجيه الشبكي وبروتوكولات الإنترنت وعناوين IP، وتترك المفاهيم البرمجية المتقدمة لبرامج تخصصية لاحقة.

## كيف تختلف دورة إدارة جدار الحماية Fortinet NSE 4: FortiGate Administrator عن دورات أمن الشبكات العامة؟

تركز هذه الدورة على التنفيذ العملي للإعدادات وإدارة منظومة FortiOS وتقنيات أجهزة FortiGate تحديدا، في حين تغطي الدورات العامة المفاهيم النظرية للأمن المؤسسي دون الخوض في التفاصيل التشغيلية لمنصات محددة.

## ما هي إمكانات فحص حركة المرور التي يوفرها جدار الحماية FortiGate؟

يوفر فحصا دقيقا للمرور عبر فك تشفير SSL وفحص الحزم العميقة، والتحكم في التطبيقات، وتصفية الويب، واستخدام محركات مكافحة الفيروسات، وتكامل نظام منع التسلل IPS لاكتشاف الأنشطة المشبوهة بدقة وكفاءة.

## كيف تعمل مجموعات التوافر العالي High Availability في بيئة FortiOS؟

تعمل بربط جهازين أو أكثر عبر واجهات مراقبة متخصصة لمزامنة إعدادات النظام وجلسات الاتصال المشتركة، مما يضمن استمرارية الخدمة تلقائيا وبلا انقطاع عند حدوث أي خلل في الجهاز الرئيسي.

## الخاتمة

يغادر المشاركون الدورة بحقيبة توثيق وإعدادات هندسية متكاملة لنشر وتأمين منصة FortiGate في البيئات المؤسسية. تسهم هذه المخرجات في رفع جاهزية البنية التحتية وتحقيق أعلى معايير الحماية ومقاومة الاختراقات السيبرانية بكفاءة مستمرة. كما تدعم المهارات المكتسبة تقليل زمن التوقف غير المخطط له وتحسين استجابة الأنظمة للمتطلبات التشغيلية والأمنية المعتمدة.