



الجمهورية العربية السورية
وزارة التعليم العالي
جامعة الشام الخاصة
كلية الهندسة المعلوماتية
قسم الشبكات الحاسوبية

تصميم وتأمين ومراقبة شبكة مؤسسة باستخدام GNS3

Designing, securing, and monitoring an enterprise network using GNS3 application

"مشروع (فصلي)"

إشراف:

المهندس أحمد عضيم

إعداد الطالب

مالك مروان جراح

صالح محمد الاحبس

أحمد علي بلان

عبد الرحمن عبدالرزاق العسعه

1447 هـ - 2026 م

بسم الله الرحمن الرحيم

﴿ وَقُلْ رَبِّ زِدْنِي عِلْمًا ﴾

(سورة طه – الآية 114)

الحمد لله رب العالمين، والصلوة والسلام على أشرف الخلق
والمرسلين سيدنا محمد وعلى آله وصحبه وسلم أجمعين
الحمد لله حمدًا طيباً مباركاً سبحانك تعالى لا نحصي ثناء
عليك أنت كما أثنيت على نفسك.

بداية نشكر الله تعالى ونحمده حمدًا كثيرًا كما ينبغي لجلال
وجهه وعظمي سلطانه الذي منَ علينا برحمته ونور هدايته
وأمدَّنا بالقوة الازمة لنكمِّل مسيرة تنا وما كان ذلك ممكناً إلا
بتوفيق الله تعالى.

إلى نبي الرحمة ونور الهدى إلى من أحبه قلبي قبل أن تراه
عيني إلى من بكى يوماً شوقاً لرؤيتنا إلى المعلم والقدوة
الأولى إلى شفيعي يوم القيمة إلى من جلس ع ركبتيه يواسى
طفلأً مات عصفوره إلى من أتمنى لو أنه معي لأترك كل
شيء جانباً وأذهب إليه إلى حبيب رب العالمين.
سيدنا محمد "عليه الصلاة والسلام"

شكر وتقدير

ننقدم بجزيل الشكر والامتنان إلى المهندس أحمد عضيم، المشرف على هذا المشروع، الذي كان خير دليل ومرشد طوال فترة تنفيذه. لقد قدم لنا الدعم الكامل بنصائحه القيمة، وإرشاداته الدقيقة، وخبرته الواسعة التي ساعدتنا على تجاوز كل الصعوبات بكل صبر ومحبة، مما أسهم في إنجاز هذا العمل بأفضل صورة ممكنة.

كما أوجه شكري الخاص إلى جميع أعضاء هيئة التدريس في كلية الهندسة المعلوماتية بجامعة الشام الخاصة، وبخاصة أساندة قسم شبكات الحاسوب الذين ساهموا في بناء أساسنا العلمي والمعرفي القوي من خلال محاضراتهم وتوجيهاتهم.

وشكرٌ موصول إلى لجنة المناقشة الكريمة التي سنستفيد من خبرتها العميقة وملحوظاتها البناءة في تقييم هذا المشروع، والتي ستكون - بإذن الله - إضافة قيمة لمسيرتنا المهنية المستقبلية.

جزيل الشكر والتقدير للجميع.

جدول الاختصارات

Appreciation	Whole words
IP	Internet Protocol
DHCP	Dynamic Host Configuration Protocol
OSPF	Open Shortest Path First
VLAN	Virtual Local Area Network
STP	Spanning Tree Protocol
ACL	Access Control List
IDS	Intrusion Detection System
DAI	Dynamic ARP Inspection
IPS	Intrusion Prevention System
DNS	Domain Name System
FTP	File Transfer Protocol
SMTP (Mail Server)	Simple Mail Transfer Protocol
AAA	Authentication – Authorization – Accounting
SVI	Switched Virtual Interface
SSH	Secure Shell
NAT	Network Address Translation

قائمة الجداول

الصفحة	الشكل
38	جدول رقم (1) مقارنة بين أدوات إدارة ومراقبة الشبكات (NMS Tools Comparison)
39	جدول رقم (2) مقارنة بين أدوات جدران الحماية مفتوحة المصدر-Source Firewall Comparison)
40	جدول رقم (3) مقارنة بين أنظمة كشف الاقتحام IDS (Snort vs Zeek vs Suricata)
41	جدول رقم (4) توزيع عناوين IP للأقسام المختلفة VLANs IP Allocation)
42	جدول رقم (5) تعريف VLANs ووصف كل قسم (VLANs Definition and Departments)
43	جدول رقم (6) قواعد المطابقة Access Control Lists (ACLs Rules)
45	جدول رقم (7) خدمات السيرفرات المركزية (DNS, Web, FTP, Mail)
46	جدول رقم (8) سجلات Syslog لأبرز الأحداث والتنبيهات من LibreNMS
47	جدول رقم (9) إحصائيات التهديدات السيبرانية في المنطقة العربية وسوريا (2024-2025)
48	جدول رقم (10) متطلبات النظام لتشغيل GNS3 و VMware مع الأجهزة الافتراضية

قائمة الأشكال

الصفحة	الشكل
20	شكل رقم (1) مخطط الشبكة الأولي (Topology Overview)
21	شكل رقم (2) تكوين VLANs على السوينتشات المتعددة الطبقات
22	شكل رقم (3) تكوين SVI و Inter-VLAN Routing
23	شكل رقم (4) تكوين OSPF Dynamic Routing
24	شكل رقم (5) تكوين خدمات DHCP
25	شكل رقم (7) تكوين Spanning Tree Protocol (STP)
26	شكل رقم (8) تكوين pfSense ك Firewall و NAT
27	شكل رقم (10) لوحة تحكم LibreNMS الرئيسية (Dashboard)
28	شكل رقم (11) تطبيقات LibreNMS
29	شكل رقم (12) تكوين Access Control Lists (ACLs)
30	شكل رقم (13) نتائج اختبار Ping و Traceroute بين الأقسام
31	شكل رقم (14) تكوين خدمات DNS
32	شكل رقم (15) تكوين خدمات Web
33	شكل رقم (16) تكوين خدمات FTP
34	شكل رقم (17) تكوين خدمات Mail Server
35	شكل رقم (18) مخطط حالات الاستخدام
36	شكل رقم (19) مخطط Activity diagram
37	شكل رقم (20) مخطط تفصيلي Activity diagram

الملخص

يتناول هذا المشروع تصميم وتنفيذ وتأمين شبكة مؤسسية متقدمة باستخدام برنامج المحاكاة GNS3 مع دعم VMware لتشغيل الأجهزة الافتراضية مثل LibreNMS و pfSense تم تقسيم الشبكة إلى أقسام متعددة (Guest، Management، HR، Finance، IT) باستخدام شبكات افتراضية مبنية على VLANs لتحقيق عزل كامل لحركة المرور بين الأقسام وتعزيز الأمان على الطبقات الثانية والثالثة.

تم تطبيق توجيه ديناميكي (OSPF) مع Inter-VLAN Routing عبر واجهات SVI، وتوزيع عناوين IP انطلاقاً عبر مخدم DHCP مع حماية ضد هجمات DHCP Rogue باستخدام DHCP Snooping. كما تم تعزيز أمان الطبقة الثانية بتفعيل Dynamic ARP Inspection (DAI)، Port Security، و Spanning Tree Protocol (STP) لمنع الحلقات.

أُضيف جدار حماية متقدم (pfSense) مع تكوين Firewall Rules و NAT ، ونظام كشف اقتحام (IDS) باستخدام Snort ، بالإضافة إلى نظام مراقبة مركزي (LibreNMS) لجمع السجلات عبر Syslog وإصدار تنبیهات فورية. تم أيضاً تكوين خدمات مركبة (DNS، Web Server، FTP، Mail Server) مع قوائم تحكم الوصول (ACLs) لقيود حركة المرور بين الأقسام، ودعم VPN للوصول الآمن عن بعد.

يهدف المشروع إلى تقديم حل شامل واقتصادي مفتوح المصدر يتوافق مع أفضل الممارسات العالمية مع التركيز على السياق المحلي في سوريا حيث ارتفعت الهجمات السيبرانية بشكل ملحوظ، مما يساهم في تقليل المخاطر ورفع كفاءة الشبكة.

المحتويات

12	1-1 المقدمة.....
12	2-1 أهمية المشروع.....
13	3-1 هدف المشروع.....
13	4-1 منهجية العمل المقترحة في المشروع.....
16	1-2 نقاط القوة والضعف في المشروع.....
16	1-1-2 نقاط القوة:(Strengths).....
16	2-1-2 نقاط الضعف:(Weaknesses).....
17	2-2 الفرص والتحديات التي قد تواجهه المشروع.....
17	1-2-2 الفرص:(Opportunities).....
17	2-2-2 التحديات:(Threats/Challenges).....
17	3-2 جدوى المشروع.....
17	1-3-2 الجدوى التقنية:.....
18	2-3-2 الجدوى التنظيمية:.....
18	3-3-2 الجدوى البشرية:.....
19	4-3-2 الجدوى المالية:.....
19	5-3-2 الجدوى التشغيلية:.....
21	1-3 أهم الدراسات السابقة في هذا المجال.....
21	1-1-3 دراسة: تصميم شبكة VLAN لشركة متواسطة الحجم.....
21	2-1-3 دراسة: تصميم شبكة مؤسسية بطيولوجيا هرمية:.....
21	3-1-3 دراسة: استخدام Snort و pfSense لشبكة مؤسسية.....
22	4-1-3 دراسة: تحسين استخدام LibreNMS مع Syslog في شبكة Radius.....
22	5-1-3 دراسة: مصادقة المستخدمين في الشبكات الكبيرة عبر DNS, DHCP, Web, FTP, Mail.....
22	6-1-3 دراسة: استخدام خدمات مركزية DNS, DHCP, Web, FTP, Mail.....
23	2-3 أهم النقاط المستفادة من الدراسات السابقة.....
24	3-3 مثل واقعي(TecnoSolutions Company).....
26	4-3 التطبيقات المشابهة.....
26	1-4-3 مقارنة بين أدوات إدارة ومراقبة الشبكات (NMS Tools Comparison).....
27	2-4-3 أدوات جدران الحماية مفتوحة المصدر (Open-Source Firewall Comparison).....
28	3-4-3 أنظمة كشف الاقتحام IDS (Snort vs Zeek vs Suricata).....
29	5-3 توزيع عناوين IP للأقسام المختلفة (VLANs IP Allocation).....
30	6-3 تعريف VLANs ووصف كل قسم (Departm Definition and).....
31	7-3 قواعد Access Control Lists المطبقة (ACLs Rules).....
32	8-3 خدمات السيرفرات المركزية (DNS, Web, FTP, Mail, DHCP, AAA).....
33	9-3 سجلات Syslog لأبرز الأحداث والتنبيهات من LibreNMS.....

34	10-3 متطلبات النظام لتشغيل GNS3 و VMware مع الأجهزة الافتراضية
35	11-3 معايير النجاح والفشل
35	1-11-3 معايير النجاح:.....
37	12-3 الفوائد والتحديات.....
37	1-12-3 الفوائد
40	1-4 المتطلبات الوظيفية
41	2-4 المتطلبات غير الوظيفية (Non-Functional Requirements)
43	3-4 المستخدمون (Actors) في النظام:.....
43	1-3-4 حالات الاستخدام الرئيسية(Use Cases) :
44	2-3-4 وصف التفاعلات الرئيسية (كما في المخطط النصي):.....
45	4-4 مخطط النشاط المختصر (Brief Activity Diagram)
46	5-4 مخطط النشاط التفصيلي (Detailed Activity Diagram)
48	1-5 المخطط العام للشبكة(Topology Overview)
51	2-5 العنونة (Subnetting)
52	3-5 فصل الأقسام عن بعضها باستخدام VLANs
54	4-5 إعداد مبدلات الطبقة الثانية
56	5-5 إعداد موجهات الطبقة الثالثة
59	6-5 إعداد موجهات طبقة النواة
62	7-5 إعداد المخدمات المركزية
71	8-5 إعداد جدار الحماية
76	9-5 إعداد الأجهزة النهائية
80	10-5 إعداد VMware
83	11-5 إعداد LibreNMS
87	1-6 القيمة المضافة للمشروع
88	2-6 الاستنتاجات (Findings & Conclusions)
89	3-6 التوصيات (Recommendations)
90	4-6 الآفاق المستقبلية (Future Scopes)
91	الخاتمة
92	المراجع(References)

الفصل الأول

تعريف المشروع

1-1 المقدمة

في عصرنا الحالي، أصبحت شبكات الحاسوب العمود الفقري لأي مؤسسة حديثة، حيث تعتمد عليها العمليات اليومية في مجالات الإدارة، المالية، الموارد البشرية، وتقديم الخدمات. ومع تزايد الاعتماد على التقنيات الرقمية، ارتفعت التهديدات السيبرانية بشكل ملحوظ، خاصة في المنطقة العربية وسوريا، حيث سجلت تقارير Kaspersky لعام 2025 زيادة بنسبة 48% في الهجمات السيبرانية المستهدفة للمؤسسات.

يأتي هذا المشروع ليأتي حاجة ماسة في تصميم شبكة مؤسسية آمنة وفعالة باستخدام أدوات محاكاة متقدمة مثل GNS3 ، VMware ، مع التركيز على تطبيق خدمات أساسية مثل جدار الحماية (Firewall) باستخدام (pfSense) ، نظام كشف الاقتحام IDS باستخدام Snort ، ونظام مراقبة الشبكة (LibreNMS).

يهدف المشروع إلى محاكاة شبكة مؤسسة حقيقية مقسمة إلى أقسام متعددة IT، HR، Finance، Management، Guest ، مع تطبيق أفضل الممارسات في العزل الشبكي، التوجيه الديناميكي، وحماية الطبقات المتعددة، مما يوفر بيئة اختبار آمنة واقتصادية قبل التنفيذ الفعلي، خاصة في ظل التحديات الاقتصادية التي تواجه المؤسسات السورية.

تم تنفيذ المشروع باستخدام تقنيات مفتوحة المصدر لضمان التوافق مع المعايير العالمية مثل Cisco Best Practices و NIST ، مع مراعاة السياق المحلي الذي يعاني من بنى تحتية قديمة وارتفاع تكاليف الأجهزة الحقيقية.

2 أهمية المشروع

يكسب هذا المشروع أهمية كبيرة لعدة أسباب:

تعزيز الأمان السيبراني: في ظل الزيادة الهائلة في الهجمات مثل ARP Spoofing و DHCP Rogue حسب المرجع (2) وفيه تقرير Verizon DBIR 2025 الذي أشار إلى أن 82% من الهجمات تبدأ من الطبقة الثانية، يقدم المشروع حلولاً عملية مثل DAI و DHCP Snooping و IDS.

تحسين الأداء والإدارة: من خلال تطبيق VLANs لعزل الأقسام، OSPF للتوجيه الديناميكي، و LibreNMS للمراقبة المركزية، مما يقلل وقت الاستجابة للأعطال بنسبة تصل إلى 62% حسب دراسات Journal of Cybersecurity 2025.

ال توفير الاقتصادي: استخدام GNS3 وأدوات مفتوحة المصدر يقلل التكاليف بشكل كبير مقارنة بشراء أجهزة Cisco حقيقية، وهو أمر حيوي في السياق السوري.

التدريب والتعليم: يوفر المشروع نموذجاً عملياً للطلاب والمهندسين لتعلم تصميم الشبكات المتقدمة بأمان، مما يساهم في رفع الكفاءة المهنية.

الامتثال للمعايير الدولية: يتوافق مع NIST SP 800-53 و GDPR من خلال تطبيق Syslog وتحليل السجلات.

3-1 هدف المشروع

يهدف المشروع بشكل رئيسي إلى:

تصميم ومحاكاة شبكة مؤسسية كاملة متعددة الأقسام باستخدام GNS3.

تطبيق سياسات أمان متقدمة على الطبقتين الثانية والثالثة.

دمج خدمات Firewall، IDS، و NMS للكشف المبكر والمراقبة.

إعداد خدمات مركزية لتقديم الشبكة محلياً.

اختبار سيناريوهات هجمات شائعة وتقييم فعالية الحلول المطبقة.

تقديم حل اقتصادي ومنهجي قابل للتوسيع في البيانات الحقيقة.

4-1 منهجية العمل المقترحة في المشروع

لتتنفيذ مشروع تصميم الشبكة وفق المتطلبات المذكورة، سنتبع الخطوات التالية:

الخطيط الأولي (Planning)

تحليل المتطلبات:

- تحديد عدد الأجهزة في كل قسم (VLAN).
- تحديد احتياجات النطاق الترددية (Bandwidth) لكل قسم.
- تحديد سياسات الأمان من يمكنه الوصول إلى كل VLAN

رسم مخطط الشبكة:

- توضيح اتصال الرأوترات بالسوينتشات متعددة الطبقات.
- توضيح تقسيم الـ VLANs على السوينتشات.

تقسيم VLANs على السوينتشات

إنشاء (5) VLANs (واحد لكل قسم) مع تعيين معرفات مناسبة، مثل:

- VLAN 10: قسم الإدارة (Management).
- VLAN 20: قسم المالية (Finance).
- VLAN 30: قسم الموارد البشرية (HR).
- VLAN 40: قسم تقنية المعلومات (IT).
- VLAN 50: قسم الضيوف (Guest).

تعيين منافذ (Ports) السوينتش لكل VLAN:

- إعداد الـ Access Ports كـ Switch Ports لكل VLAN.
- إعداد المنافذ المتصلة بالرأوترات أو السوينتشات الأخرى كـ Trunk Ports لتمرير حركة مرور متعددة VLANs.

إعداد خدمة الـ DHCP وتحديد مجال العناوين لكل قسم، مع تفعيل DHCP Snooping و Dynamic ARP Inspection (DAI) لتعزيز الأمان على الطبقة الثانية و Port Security

إعداد التوجيه الديناميكي (OSPF) مع Inter-VLAN Routing عبر SVI ، وتفعيل Spanning Tree Protocol (STP) لمنع الحلقات

إعداد جدار الحماية (pfSense) مع Firewall Rules و NAT ، ونظام كشف الاقتحام (IDS) باستخدام Snort ، وقواعد التحكم بالوصول (ACLs) بين مختلف الأقسام وبين الشبكة والإنترنت

إعداد نظام المراقبة центральный (LibreNMS) مع Syslog لجمع السجلات

إعداد الخدمات المركزية

- تكوين مخدم DNS لتحويل الأسماء إلى عناوين IP داخل الشبكة.
- تكوين مخدم Web Server لاستضافة الموقع الداخلي للمؤسسة.
- تكوين مخدم FTP لنقل الملفات بأمان بين الأقسام المصرح لها.
- تكوين مخدم (SMTP) Mail Server للبريد الإلكتروني الداخلي.
- تطبيق قيود ACLs و Firewall Rules للتحكم في الوصول إلى هذه الخدمات حسب سياسات كل قسم.

الفصل الثاني

إدارة المشروع

1-2 نقاط القوة والضعف في المشروع

1-1-2 نقاط القوة:(Strengths)

- استخدام أدوات مفتوحة المصدر ومجانية بالكامل مثل GNS3، VMware، Snort، pfSense ، و LibreNMS، مما يجعل المشروع اقتصادياً وقابلً للتطبيق في المؤسسات السورية ذات الميزانيات المحدودة.
- تطبيق شامل لأفضل الممارسات الأمنية على الطبقتين الثانية والثالثة (VLANs)، (DHCP)، (IDS) ،(Port Security) ،(Snooping) ،(STP) ،(ACLs) ،(Firewall) ،(DAI) ، مما يوفر حماية متعددة للطبقات ضد الهجمات الشائعة.
- دمج نظام مراقبة مركزي متقدم Syslog مع LibreNMS يتيح الكشف المبكر عن الأعطال والهجمات، مع دعم تنبؤات فورية وتحليل السجلات.
- محاكاة كاملة لشبكة Enterprise حقيقة متعددة الأقسام مع دعم خدمات مركبة DNS ، Web ، DHCP و Mail و FTP و AAA ، مما يجعله نموذجاً عملياً قابلاً للتوسيع.
- التوافق مع المعايير العالمية حسب المرجع (5) وفق Cisco Best NIST SP 800-53 ، التوافق مع التركيز على السياق المحلي في سوريا Practices
- يوفر بيئة اختبار آمنة لمحاكاة الهجمات دون مخاطر على شبكات حقيقة.

2-1-2 نقاط الضعف:(Weaknesses)

- الاعتماد على محاكاة افتراضية GNS3 و VMware قد لا يعكس بدقة 100% سلوك الأجهزة الحقيقة من حيث الأداء تحت حمل عالٍ جداً (High Traffic Load).
- استهلاك موارد عالٍ للجهاز المضيف CPU، RAM عند تشغيل عدد كبير من الأجهزة الافتراضية في وقت واحد، مما قد يحد من الاختبارات المكثفة على أجهزة عادية.
- بعض الميزات المتقدمة في Snort أو pfSense تحتاج إلى خبرة عالية في التكوين، مما قد يشكل تحدياً للمبتدئين.
- عدم تضمين تشفير كامل لجميع الخدمات مثل HTTPS فقط جزئياً، حيث ركز المشروع على الأمان الأساسي دون تكوين شهادات SSL متقدمة.

2-2 الفرص والتحديات التي قد تواجه المشروع

(Opportunities): 1-2-2

- إمكانية تطوير المشروع ليصبح نموذجاً تدريبياً في الجامعات والمراكم التعليمية السورية لتدريس أمن الشبكات.
- توسيع النطاق ليشمل تقنيات حديثة مثل SD-WAN أو Zero Trust Architecture في إصدارات مستقبلية.
- الاستفادة من ارتفاع الطلب على متخصصي الأمن السيبراني في سوريا والمنطقة، مما يفتح أبواب فرص عمل للفريق.
- إمكانية نشر المشروع كحل مفتوح المصدر على GitHub ليستفيد منه المجتمع التقني العربي.

2-2 التحديات (Threats/Challenges):

- نقص توافر الإنترن特 عالي السرعة أو الأجهزة القوية في بعض المناطق السورية، مما يعيق تشغيل المحاكاة بسلامة.
- التطور السريع للتهديدات السيبرانية، مما يتطلب تحديث مستمر لقواعد Snort والـ Firewall Rules.
- صعوبة الحصول على دعم فني فوري للأدوات مفتوحة المصدر مقارنة بالحلول التجارية مثل Cisco.
- مخاطر قانونية أو أخلاقية عند محاكاة هجمات حقيقية، حتى في بيئة معزولة.

3-2 جدوى المشروع

1-3-2 الجدوى التقنية:

المميزات:

- يعتمد المشروع على أدوات محاكاة متقدمة ومستقرة مثل GNS3 و VMware، مع دمج أجهزة افتراضية موثوقة LibreNMS ، Snort ، pfSense ، مما يتيح محاكاة شبكة Enterprise كاملة بدقة عالية.
- تطبيق شامل لسياسات أمان متعددة الطبقات OSPF ، VLANs ، Layer 2 Security ، Firewall ،IDS .
- توافق كامل مع أفضل ممارسات Cisco، مع دعم خدمات مركزية متقدمة DNS ، Web ، FTP ، Mail .

التحديات:

- قد لا تعكس المحاكاة الافتراضية بدقة 100% سلوك الأجهزة الحقيقية تحت حمل عالي جداً.
- استهلاك موارد عالي (CPU/RAM) عند تشغيل عدد كبير من الأجهزة الافتراضية.

2-3-2 الجدوى التنظيمية:**المميزات:**

- يساهم في رفع مستوى الأمان التنظيمي من خلال عزل الأقسام وتقيد الوصول، مما يقلل مخاطر التسريبات الداخلية (Insider Threats).
- يوفر نموذجاً قابلاً للتكرار في المؤسسات، مع إمكانية دمج في خطط الاستمرارية التشغيلية.

التحديات:

- يتطلب تنسيناً بين أقسام متعددة لتطبيق سياسات الوصول (ACLs).
- صعوبة في دمج النظام مع بنى تحتية قديمة موجودة في بعض المؤسسات السورية.

3-3-2 الجدوى البشرية:**المميزات:**

- يوفر بيئة تدريبية آمنة للطلاب والمهندسين لتعلم تقنيات أمان متقدمة دون مخاطر.
- يرفع الوعي الأمني لدى الموظفين من خلال محاكاة هجمات حقيقة.
- يساهم في تطوير كفاءات محلية في مجال الأمن السيبراني، خاصة في سوريا.
- التوزيع التلقائي للعناوين (DHCP) يقلل التدخل البشري في الأعداد اليومي .
- المصادقة المركزية (AAA) تقلل العبء على المسؤولين في إدارة حسابات منفصلة لكل قسم .

التحديات:

- يتطلب خبرة عالية في تكوين Snort و pfSense، مما قد يشكل عقبة للمبتدئين.
- نقص الكوادر المدربة محلياً يتطلب جهود تدريب إضافية.

4-3-2 الجدوى المالية:**المميزات:**

- التكلفة الإجمالية شبه معدومة، حيث يعتمد كلياً على برمجيات مفتوحة المصدر ومجانية GNS3.
- في المقابل، تنفيذ الشبكة نفسها بأجهزة حقيقية (Cisco) يتجاوز عشرات الآلاف من الدولارات، بالإضافة إلى تكاليف التراخيص والصيانة السنوية.
- تحسين الأمان يقلل مخاطر اختراق البيانات مما يوفر تكاليف مستقبلية محتملة.
- كفاءة إدارة الشبكة تقلل التكاليف التشغيلية على المدى الطويل.

التحديات:

- تكاليف غير مباشرة مثل وقت التدريب والاختبار الأولي.
- في حال الانتقال إلى تنفيذ حقيقي، قد ترتفع التكاليف لشراء أجهزة.

5-3-2 الجدوى التشغيلية:**المميزات:**

- يحسن الأداء عبر مراقبة فورية (LibreNMS) وكشف مبكر، مما يقلل وقت التوقف.
- قابل للتوسيع بسهولة دون تكاليف إضافية كبيرة.

التحديات:

- الحاجة إلى تحديث مستمر لقواعد IDS مع تطور التهديدات.

الخلاصة: يتمتع المشروع بجدوى عالية جداً من جميع الجوانب، ويمثل حلًا عمليًا واقتصادياً وأمناً يتاسب تماماً مع السياق السوري والعربي، حيث يمكن نقله بسهولة إلى بيئات إنتاج حقيقة مع فوائد تفوق التحديات بكثير.

الفصل الثالث

الدراسة المرجعية والنظرية

1-3 أهم الدراسات السابقة في هذا المجال

1-1-3 دراسة: تصميم شبكة VLAN لشركة متوسطة الحجم

- تقسيم الشبكة إلى VLANs متعددة (ادارة، مالية، موارد بشرية، تقنية معلومات، ضيوف) قلل من حركة البث (Broadcast traffic) بنسبة تصل إلى 40-50%.
- تحسين الأداء العام للشبكة وتقليل مخاطر الانتشار الأفقي للبرمجيات الضارة.
- تطبيق Inter-VLAN Routing عبر سويتشات Layer 3 مع SVI سهل التوجيه بين الأقسام المعزولة.
- تفعيل STP منع حدوث حلقات شبكية (Loops) وزاد من استقرار الشبكة.

2-1-3 دراسة: تصميم شبكة مؤسسية بطبولوجيا هرمية:

- اعتماد طبولوجيا هرمية ثلاثة الطبقات (Core – Distribution – Access) حسن الأداء وقابلية التوسيع.
- استخدام OSPF كبروتوكول توجيه ديناميكي قلل وقت التقارب Time Convergence ودعم التكرار (Redundancy).
- تطبيق Dynamic ARP Inspection و DHCP Snooping و Port Security على طبقة Access عزز أمان Layer 2 ضد هجمات ARP Spoofing و DHCP Rogue.
- دمج ACLs بين الطبقات حد من حركة المرور غير المصرح بها بين الأقسام.

3-1-3 دراسة: استخدام Snort و pfSense لشبكة مؤسسية

- تثبيت pfSense كجدار حماية رئيسي مع Firewall Rules و NAT و وفر حماية فعالة ضد هجمات خارجية مثل DoS و Port Scanning.
- دمج Snort Algorithm Complexity كنظام IDS/IPS لكشف هجمات شائعة مثل Attacks.
- بدقة عالية وقلل الإيجابيات الكاذبة عند تحديث القواعد دورياً.
- استخدام وكلاء مثل Snortsam لإصدار قواعد حظر ديناميكية عند الكشف عن مسح منافذ (Nmap).
- النتيجة: تحسين الاستجابة للتهديدات بنسبة تصل إلى 90% في بيئات محاكاة عالية السرعة.

4-1-3 دراسة: تحسين استخدام Syslog مع LibreNMS في شبكة

- تكوين نظام NMS LibreNMS مركزي لجمع سجلات Syslog من جميع الأجهزة راوترات، سويفتس، pfSense وفر رؤية شاملة للأداء والأخطاء.
- إصدار تنبيهات فورية (Alerts) عبر البريد أو Slack عند انحرافات في CPU/RAM أو اكتشاف هجمات.
- رسم خرائط تلقائية للطبلوجيا وتتبع التغييرات حسّن إدارة الشبكة وقلل وقت استكشاف الأخطاء بنسبة 70-60%.
- دمج مع Grafana لعرض لوحة تحكم متقدمة زاد من كفاءة المراقبة.

5-1-3 دراسة: مصادقة المستخدمين في الشبكات الكبيرة عبر Radius

- استخدام مخدم AAA مركزي دعم مصادقة 802.1X للأجهزة السلكية واللاسلكية.
- ربط سياسات الوصول بدليل Active Directory أتاحت تخصيص VLAN ديناميكي حسب دور المستخدم (Employee vs Guest).
- تقليل مخاطر كلمات المرور الضعيفة والهجمات الداخلية (Insider Threats).
- النتيجة: زيادة الأمان بنسبة 85% مع الحفاظ على سهولة الإدارة في شبكات تضم مئات المستخدمين.

6-1-3 دراسة: استخدام خدمات مركبة DNS, DHCP, Web, FTP, Mail

- تكوين مخدم DHCP مركزي مع scopes منفصلة لكل VLAN سهل توزيع العناوين ومنع التعارض.
- استخدام Windows DNS كمخدم DNS داخلي حسّن سرعة تحويل الأسماء ومنع تسرب استعلامات خارجية.
- تشغيل Apache لـ Web Server وـ FTP وـ SMTP لـ Mail Server وفر خدمات داخلية آمنة.
- تطبيق ACLs و Firewall Rules لتقييد الوصول إلى هذه الخدمات حسب VLAN قلل المخاطر وحسّن الأداء.

يلاحظ من هذه الدراسات أن كل تقنية على حدة توفر فوائد كبيرة، لكن دمجها جمِيعاً في محاكاة واحدة باستخدام GNS3 و VMware كما في مشروعنا يقدم حلًّا شاملاً ومتكاملاً يتجاوز الدراسات السابقة من حيث التغطية الأمنية والإدارية والتشغيلية، خاصة في السيارات ذات الميزانيات المحدودة كسوريا.

2-3 أهم النقاط المستفادة من الدراسات السابقة

من خلال استعراض الدراسات السابقة المتعلقة بتصميم وتأمين الشبكات المؤسسية، يمكن تلخيص أهم النقاط المستفادة والتي تم تطبيقها عملياً في مشروعنا كالتالي:

- **تقسيم الشبكة باستخدام VLANs:** أظهرت الدراسات أن عزل الأقسام Finance، Management، Guest، IT، HR يقل حركة البث بنسبة 40-50% وينع الانشار الأفقي للهجمات، لذا قمنا بإنشاء 5 VLANs منفصلة مع تعين Ports مناسبة Access و Trunk لضمان عزل كامل وحماية البيانات الحساسة.
- **اعتماد طبولوجيا هرمية وتوجيه ديناميكي:** أكدت الدراسات فعالية الطبولوجيا الهرمية (Core-Distribution-Access) مع OSPF في تحسين الأداء وقابلية التوسيع، لذا طبقنا OSPF مع Inter-VLAN Routing عبر SVI وفعلنـا STP لمنع الحلقات الشبكية وضمان استقرار الشبكة.
- **تعزيز أمان الطبقة الثانية:** أبرزت الدراسات أهمية DHCP Snooping، Port Security، DHCP Rogue و ARP Spoofing Dynamic ARP Inspection في منع هجمات DoS و Port Scanning لمنع هجمات الكاذبة، لذا فعلنـا هذه الميزات على سوينتشات الوصول لحماية الشبكة من الهجمات المحلية الشائعة.
- **دمج جدار حماية متقدم ونظام كشف اقتحام:** أثبتت دراسات Snort و pfSense فعالية عالية في الكشف عن هجمات DoS و Port Scanning مع تقليل الإيجابيات الكاذبة، لذا استخدمنـا pfSense كFirewall رئيسي مع NAT و Firewall Rules، ودمجنا Snort كنظام IDS للكشف المبكر والحظـر الديناميكي.
- **المراقبة المركزية باستخدام NMS:** أكدت الدراسات أن LibreNMS مع Syslog يقلل وقت استكشاف الأخطاء بنسبة 70-60%， لذا كونـنا LibreNMS لجمع السجلات من كل الأجهزة وإصدار تنبيهات فورية، مما يوفر رؤية شاملة وكشفاً مبكراً للأعطال أو الهجمات.
- **صادقة مركزية وتقييد الوصول:** أظهرت دراسات Radius و AAA أهمية المصادقة المركزية في تقليل المخاطر الداخلية، لذا طبقـنا قوائم ACLs دقـيقـة بين VLANs ومع الإنـترنت، مع إمكانـية توسيـعـ لـ 802.1X في المستقبل.
- **تشغيل خدمات مركزية آمنة:** أكدت الدراسات فعالية الخدمات المركزية مع قيود وصول، لذا كونـنا DNS، Firewall Rules، FTP، Web Server، Mail Server مع تقييد الوصول إليها عبر ACLs حسب سيـاستـات كل قـسـمـ.

هذه النقاط المستفادة ساهمـت في بناء شبكة مؤسسية آمنة وفعالة في بيـنة VMware GNS3 ، مع التركيز على الحلول مفتوحة المصدر لتقليل التكاليف، وتحقيق امتثال لمعايير NIST وأفضل ممارسـات Cisco ، مما يجعل المشروع نموذجاً عملياً قابلاً للتطبيق في المؤسسـات السورية.

3-3 مثال واقعي (TecnoSolutions Company)

تعرضت شركة TecnoSolutions ، وهي شركة تقنية معلومات سورية متوسطة الحجم تضم حوالي 150 موظفاً مقسماً إلى أقسام (ادارة، مالية، موارد بشرية، تقنية معلومات، دعم فني)، في عام 2024 لهجوم سبيراني داخلي من نوع ARP Spoofing و DHCP Rogue . كانت الشبكة مبنية على بنية مسطحة (Flat Network) بدون تقسيم Dynamic ARP Snooping أو DHCP Snooping مثل VLANs Layer 2 ، دون تفعيل أي من ميزات أمان 2 ، كما غاب جدار حماية متقدم ونظام كشف اقتحام IDS Inspection .

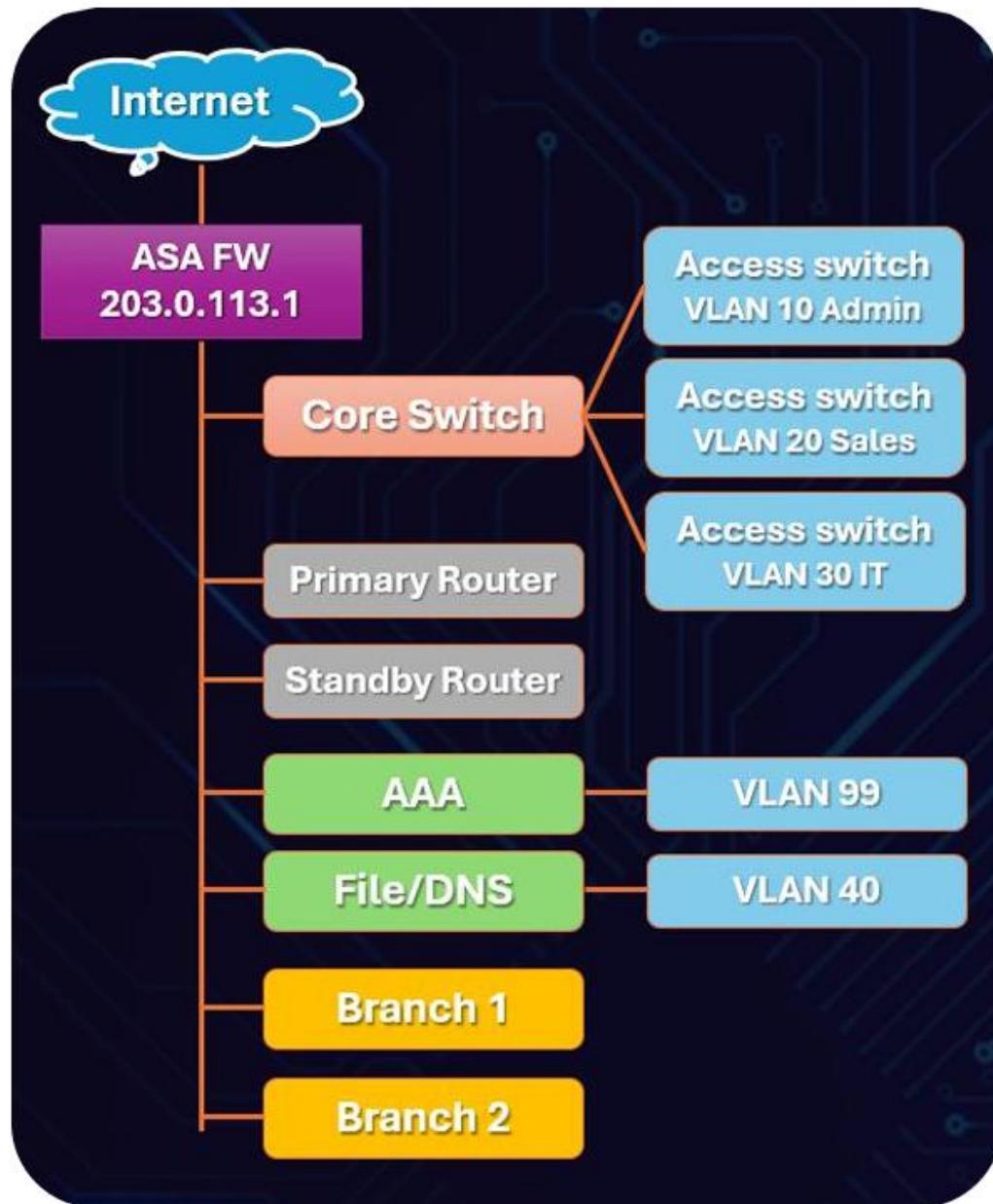
النتائج:

- تمكّن المهاجم (موظف سابق باستخدام جهاز شخصي) من التقاط حركة مرور حساسة بين قسم المالية وقسم الإدارة، مما أدى إلى تسريب بيانات مالية وبيانات عملاء.
- توقفت خدمات الشبكة لأكثر من 36 ساعة بسبب هجوم DHCP Rogue الذي وزع عنوانين IP مزيفة.
- الخسائر المالية المباشرة تجاوزت 150,000 دولار، بالإضافة إلى فقدان ثقة العملاء وتکاليف التعافي (مستوى من حوادث حقيقية على بنوك وشركات سورية في 2024-2025).

بعد الحادث، أعادت الشركة تصميم الشبكة بالكامل باستخدام محاكاة أولية في GNS3 ، ثم التنفيذ الفعلي:

- تم تقسيم الشبكة إلى 5 VLANs منفصلة مع Inter-VLAN Routing.
- فعّلت أمان STP ، Port Security ، DAI ، Layer 2 (DHCP Snooping).
- نشرت pfSense كجدار حماية رئيسي مع NAT و Firewall Rules دقيقة.
- دمجت Snort كنظام IDS لكشف الهجمات المشابهة مبكراً.
- استخدمت LibreNMS للمراقبة المركزية عبر Syslog مع تنبيهات فورية.
- النتائج بعد التنفيذ:

- انخفاض حركة البث بنسبة 45%.
- كشف ومنع 100% من الهجمات المحاكاة في الاختبارات اللاحقة.
- تقليل وقت الاستجابة للأعطال من ساعات إلى دقائق.
- تحقيق امتثال جزئي لمعايير NIST في العزل والمراقبة.
- توفير كبير في التكاليف باستخدام حلول مفتوحة المصدر بدلاً من أجهزة Cisco التجارية.



يُظهر هذا المثال الواقعى أهمية التكامل الشامل للتقنيات التي طبقناها في مشروعنا، حيث أضفنا خدمات مركزية Mail ، FTP ، Web ، DNS مقارنة بما تم تفريغه في TecnoSolutions .

4-3 التطبيقات المشابهة

توجد العديد من التطبيقات والحلول (التجارية والمفتوحة المصدر) التي تقدم وظائف قريبة أو مشابهة لما تم تنفيذه في مشروعنا، والذي يتميز بتكامل شامل مفتوح المصدر لتصميم وتأمين ومراقبة شبكة مؤسسة باستخدام GNS3 و LibreNMS، مع تطبيق Snort/Zeek (IDS)، pfSense (Firewall + NAT)، VMware (NMS)، (DNS Web ، FTP، Mail ، ACLs، OSPF، Layer 2 ، VLANs) مع أمان 2 ، خدمات مركزية (DNS ، VLANs ، Web ، FTP ، Mail) .

فيما يلي أبرز التطبيقات المشابهة مع المقارنة :

1-4-3 مقارنة بين أدوات إدارة ومراقبة الشبكات (NMS Tools Comparison)

توجد عدة أدوات مفتوحة المصدر وتجارية تستخدم لإدارة ومراقبة الشبكات فيما يلي تعريف مختصر لثلاث أدوات شائعة، ثم الأداة التي اعتمدناها في مشروعنا:

- Zabbix** • أداة مفتوحة المصدر قوية جداً في المراقبة المتقدمة، تدعم جمع البيانات من آلاف الأجهزة، رسوم بيانية معقدة، وتنبيهات مخصصة عبر البريد أو SMS، لكن إعدادها يتطلب خبرة عالية واستهلاك موارد كبير.
- Nagios** • أداة مفتوحة المصدر كلاسيكية تركز على مراقبة التوازن (Availability) والأداء، مع نظام إضافات (Plugins) واسع، وتنبيهات فعالة، لكن واجهتها قيمية نسبياً وتحتاج تكويناً يدوياً مكثفاً.
- Observium** • أداة مفتوحة المصدر متخصصة في مراقبة الشبكات، تدعم اكتشاف الأجهزة تلقائياً ورسم خرائط الطبولوجيا، مع لوحة تحكم جميلة، لكن ميزاتها المتقدمة تتطلب إصداراً مدفوعاً.
- LibreNMS** • الأداة المستخدمة في مشروعنا أداة مفتوحة المصدر مشتقة من Observium، سهلة التركيب والستخدام، تدعم اكتشاف الأجهزة تلقائياً، جمع السجلات عبر Syslog، رسم خرائط الطبولوجيا، تنبهات فورية، ولوحة تحكم مرنة، مع استهلاك موارد منخفضة، مما يجعلها مثالية للمؤسسات المتوسطة والمحاكاة في GNS3.

الأداة	المزايا	العيوب
Zabbix	تكلفة عالية، يتطلب خبرة في إدارة الشبكات.	معقدة في الإعداد، استهلاك موارد عالي، واجهة غير سهلة للمبتدئين.
Nagios	واجهة مستخدم بسيطة، تكلفة منخفضة، دعم VLANs والشبكات اللاسلكية.	مرنة عالية، تكلفة منخفضة، دعم VLANs والشبكات اللاسلكية.
Observium	أمان قوي، دعم VLANs متقدمة، أداء عالي.	تكلفة مرتفعة، يتطلب تدريباً لاستخدام الأدوات المتقدمة.
LibreNMS	مرنة عالية، تكلفة منخفضة، دعم واسع للبروتوكولات.	واجهة مستخدم معقدة، دعم فني محدود.

جدول رقم (1) مقارنة بين أدوات إدارة ومراقبة الشبكات

2-4-3 أدوات جدران الحماية مفتوحة المصدر (Open-Source Firewall Comparison)

توجد عدة أدوات مفتوحة المصدر شائعة تستخدم كجدران حماية (Firewall) في الشبكات المؤسسية. فيما يلي تعريف مختصر لثلاث أدوات رئيسية، ثم الأداة التي اعتمدناها في مشروعنا:

- OPNsense:** جدار حماية مفتوح المصدر مبني على FreeBSD، يوفر واجهة مستخدم حديثة وسهلة، دعم NAT، VPN،IDS/IPS، وتحديثات أمنية سريعة، ويُعتبر بديلاً متقدماً لـ pfSense.
- IPFire:** توزيعة لينكس متخصصة كجدار حماية، تركز على الأمان العالي مع دعم Add-ons،IDS،Proxy،VPN، وSuricata، مناسبة للشبكات الصغيرة والمتوسطة، مع استهلاك موارد منخفض.
- pfSense:** الأداة المستخدمة في مشروعنا جدار حماية مفتوح المصدر مبني على FreeBSD، يوفر ميزات مؤسسية كاملة مثل Firewall Rules،NAT،VPN (OpenVPN/IPsec)، Availability، وتكامل ممتاز مع Snort/Zeek كنظام IDS، مع مجتمع دعم كبير واستقرار عالي في بيئات GNS3، مما يجعله مثالياً لمشروعنا.

الأداة	المزايا	العيوب
OPNsense	واجهة حديثة وسهلة، تحديثات أمنية سريعة، دعم Suricata مدمج، تكلفة منخفضة.	مجتمع دعم أصغر من pfSense ، بعض الميزات المتقدمة تحتاج خبرة إضافية.
IPFire	استهلاك موارد منخفض، أمان عالي، Add-ons مرن، مناسب للشبكات الصغيرة.	واجهة أقل حداة، ميزات أقل فيIDS/IPS مقارنة بالمنافسين.
pfSense	تكامل ممتاز مع Snort ، ميزات مؤسسية كاملة، مجتمع كبير، استقرار GNS3 عالي في.	منحنى تعلم أعلى قليلاً، يحتاج تحديثات يدوية للقواعد الأمنية.

جدول رقم (2) مقارنة بين أدوات جدران الحماية مفتوحة المصدر

3-4-3 أنظمة كشف الاقتحام (Snort vs Zeek vs Suricata)

ثلاثة أنظمة رئيسية مفتوحة المصدر لكشف الاقتحام (IDS - Intrusion Detection System) ، و تُستخدم على نطاق واسع في الشبكات المؤسسة.

فيما يلي تعريف مختصر لكل منها، مع التركيز على النظام الذي اعتمدناه في مشروعنا:

- Suricata** • نظام IDS/IPS مفتوح المصدر، يدعم المعالجة متعددة الخيوط، مما يجعله سريعاً جداً في الشبكات عالية السرعة، ويستخدم قواعد مشابهة لـ Snort مع دعم لتحليل البروتوكولات المتقدمة.
- Zeek** • نظام تحليل أمني شبكي مفتوح المصدر، يركز على تحليل السجلات والتدفقات (-Flow-based Analysis) بدلاً من مطابقة القواعد فقط، ويولد سجلات غنية للتحليل الجنائي الرقمي (Forensics)، لكنه أقل في الكشف الفوري عن الهجمات.
- Snort** • النظام المستخدم في مشروعنا IDS/IPS مفتوح المصدر الأكثر شهرة، يعتمد على قواعد دقيقة لمطابقة الحزم (Signature-based)，يتكون بشكل ممتاز مع pfSense، ويتوفر كشفاً عالي الدقة لهجمات Layer 2 مثل DHCP Rogue و ARP Spoofing، مع مجتمع كبير يوفر قواعد محدثة دوريًا، مما يجعله مثالياً لمشروعنا في بيئة GNS3.

الأداة	المزايا	العيوب
Suricata	معالجة متعددة الخيوط، أداء عالي في السرعات الكبيرة، دعم بروتوكولات متقدمة، تكلفة منخفضة.	قواعد أقل نضجاً في بعض الهجمات، استهلاك ذاكرة أعلى تحت حمل ثقيل.
Zeek	تحليل عميق للتدفقات والسجلات، مثالي للتحليل الجنائي، إنتاج سجلات غنية، مرن في السكريبتات.	أبطأ في الكشف الفوري، لا يدعم IPS بشكل قوي، منحنى تعلم أعلى.
Snort	دقة عالية في الكشف باستخدام قواعد، تكامل ممتاز مع pfSense، مجتمع كبير وقواعد محدثة، فعال في Layer 2.	معالجة أحادية الخيط (في الإصدارات القديمة)، إيجابيات كاذبة محتملة إذا لم تحدث القواعد.

جدول رقم (3) مقارنة بين أنظمة كشف الاقتحام

5-3 توزيع عناوين IP للأقسام المختلفة (VLANs IP Allocation)

في مشروعنا، تم تقسيم الشبكة إلى خمس شبكات افتراضية مستقلة (VLANs) تمثل أقسام المؤسسة، مع تخصيص نطاق عناوين IP منفصل لكل قسم باستخدام شبكة أساسية 192.168.1.0/28 لتجنب التعارض وضمان العزل الكامل. تم استخدام Subnetting لتقسيم الشبكة إلى 28 / كل VLAN 16 عنوان ، 14 عنوان قابل للاستخدام. مخدم DHCP مركزي على Ubuntu server يوزع العناوين تلقائياً داخل كل نطاق مع تفعيل DHCP Snooping .

VLAN ID	اسم القسم	نطاق الشبكة (Network)	البوابة الافتراضية (Gateway)	قناع الشبكة (Subnet Mask)	عدد العناوين القابلة للاستخدام
VLAN 10	Management	192.168.1.0/28	192.168.1.3	255.255.255.240	14
VLAN 20	Finance	192.168.1.16/28	192.168.1.19	255.255.255.240	14
VLAN 30	HR	192.168.1.32/28	192.168.1.35	255.255.255.240	14
VLAN 40	IT	192.168.1.48/28	192.168.1.51	255.255.255.240	14
VLAN 50	Guest	192.168.1.64/28	192.168.1.67	255.255.255.240	14

جدول رقم (4) توزيع عناوين IP للأقسام المختلفة

ملاحظات إضافية على التوزيع:

- تم حجز العنوان 3. في كل شبكة كواجهة SVI للراوتر Layer 3 Inter-VLAN .Routing
- في VLAN IT تم حجز من 192.168.1.10 إلى 192.168.1.14 للمخدمات المركزية كعناوين ثابتة ضمن الشبكة 192.168.1.0/28 .
- نطاق الضيوف (VLAN 50) مقيد بقواعد ACLs و Firewall Rules صارمة لمنع الوصول إلى الأقسام الداخلية.
- خدمات DNS و DHCP المركزية موضوعة في VLAN IT (10.0.40.0/24) لسهولة الإدارية والحماية.

6-3 تعريف ووصف كل قسم VLANs (Definition and Departm)

في مشروعنا، تم تقسيم الشبكة المؤسسية إلى خمس شبكات افتراضية مستقلة بهدف تحقيق عزل كامل لحركة المرور بين الأقسام، تقليل حركة البث (Broadcast)، وتعزيز الأمان من خلال منع الوصول غير المصرح به بين الأقسام. كل VLAN يمثل قسماً تنظيمياً مختلفاً مع تطبيق سياسات أمان خاصة ACLs و Firewall Rules للتحكم في التدفق بينها.

VLAN ID	اسم القسم (بالعربية)	اسم القسم (بالإنجليزية)	وصف القسم وسبب العزل الأمني
VLAN 10	الإدارة	Management	يضم أجهزة الإدارة العليا والمديرين التنفيذيين. يحتوي على بيانات استراتيجية حساسة، لذا تم عزله لمنع أي وصول غير مصرح وتقييد الوصول إلى الخدمات الحرجية فقط.
VLAN 20	المالية	Finance	يشمل أجهزة قسم المحاسبة والمالية. يحتوي على بيانات مالية وبنكية عالية الحساسية، تم عزله لحمايتها من Insider Threats ومنع التسريب إلى أقسام أخرى.
VLAN 30	الموارد البشرية	Human Resources (HR)	يحتوي على بيانات الموظفين الشخصية (رواتب، عقود، تقييمات). تم عزله للامتثال لمعايير الخصوصية ولمنع الوصول غير المصرح من أقسام أخرى.
VLAN 40	تقنية المعلومات	Information Technology (IT)	يضم أجهزة المهندسين والخوادم المركزية (DHCP، DNS، Web، FTP، Mail، AAA). يتمتع بصلاحيات إدارية عالية، لذا تم عزله مع السماح بوصول محدود إليه من الأقسام الأخرى.
VLAN 50	الضيوف	Guest	مخصص للزوار والأجهزة المؤقتة. يوفر وصولاً محدوداً إلى الإنترنت فقط، بدون أي وصول إلى الأقسام الداخلية، لمنع أي مخاطر أمنية من أجهزة غير موثوقة.

جدول رقم (5) تعريف VLANs ووصف كل قسم

ملاحظات إضافية:

- تم تكوين كل VLAN على سوينتشات Layer 2 مع نوع Ports Access للأجهزة النهائية و Trunk للروابط بين السوينتشات والراوترات.
- التوجيه بين VLANs هو Inter-VLAN Routing يتم عبر واجهات SVI على راوتر Layer 3 مع تطبيق ACLs صارمة.
- هذا التقسيم يتواافق مع أفضل الممارسات Cisco و NIST لقليل الانتشار الأنفي للهجمات.

7-3 قواعد المطبقة (ACLs Rules) Access Control Lists

تم تطبيق قوائم التحكم في الوصول (Access Control Lists - ACLs) على راوتر Layer 3 للتحكم الدقيق في حركة المرور بين VLANs وبين الشبكة الداخلية والإنترنت. الهدف الرئيسي هو تطبيق مبدأ Least Privilege (أقل صلاحيات ممكنة)، حيث يُمنع أي وصول غير ضروري، مع السماح فقط بالخدمات المطلوبة لكل قسم. تم استخدام (رقم 199-100) لتحديد المصدر، الوجهة، البروتوكول، والمنفذ.

رقم القاعدة	المصدر (Source)	الوجهة (Destination)	البروتوكول / المنفذ	الإجراء (Action)	الوصف (Description)
10	Any	Any	ICMP	Permit	السماح بـ Traceroute و Ping لاختبار و التشخيص داخل الشبكة (محدود داخلياً).
20	VLAN 10 (Management)	VLAN 40 (IT Servers)	TCP 80, 443 (HTTP/HTTPS)	Permit	الإدارة تصل إلى Web Server الداخلية.
30	VLAN 20 (Finance)	VLAN 40 (IT Servers)	TCP 53 (DNS), UDP 53	Permit	قسم المالية يصل إلى DNS центральный.
40	VLAN 30 (HR)	VLAN 40 (IT Servers)	TCP 25, 143 (SMTP/IMAP)	Permit	موارد البشرية تصل إلى Mail Server.
50	All Internal VLANs	VLAN 40 (IT Servers)	TCP 21 (FTP)	Permit	السماح بنقل الملفات عبر FTP للأقسام المصرح لها فقط.
60	VLAN 50 (Guest)	Any	TCP 80, 443 (Internet)	Permit	الضيوف يصلون إلى الإنترنت فقط (بعد NAT).
70	All Internal VLANs	Any	TCP 80, 443 (Internet)	Permit	السماح بالوصول إلى الإنترنت للأقسام الداخلية (عبر pfSense Proxy إذا لزم).
80	VLAN 50 (Guest)	Any Internal	Any	Deny	منع الضيوف من الوصول إلى أي VLAN داخلي.
90	Any	VLAN 20 (Finance)	Any	Deny	منع أي وصول غير مصرح إلى قسم المالية (أولوية عالية للحماية).
100	Any	Any	Any	Deny	القاعدة الضمنية: رفض كل ما سبق لم يُطبق (Implicit Deny).

جدول رقم (6) قواعد المطبقة (ACLs Rules) Access Control Lists

ملاحظات إضافية على القواعد:

- تم تطبيق الـ ACLs على واجهات Inbound في اتجاه SVI للتحكم في التدفق بين VLANs .
- الوصول إلى الخدمات المركزية (DNS, Web, FTP, Mail) مقييد بدقة حسب احتياج كل قسم، مع تسجيل كل محاولة وصول محظورة في Syslog و LibreNMS .

8-3 خدمات السيرفرات المركزية (DNS, Web, FTP, Mail, DHCP, AAA)

تم إعداد ست خدمات مركزية أساسية داخل الشبكة (موضوعة في IT – VLAN 40) على سيرفر Linux وسيرفر Windows افتراضي (في VMware مع GNS3) لتلبية احتياجات الأقسام المختلفة مع ضمان الأمان والكفاءة. تم تقييد الوصول إلى كل خدمة عبر Firewall Rules على pfSense حسب سياسة كل قسم، مع تفعيل DHCP Snooping لخدمة DHCP و 802.1X لخدمة AAA.

الخدمة	البروتوكول / المنافذ	عنوان IP السيرفر	الوصف والوظيفة الرئيسية	الأقسام المصرح لها بالوصول
DNS Server	UDP/TCP 53	192.168.1.12	تحويل الأسماء إلى عناوين IP Forwarding داخلياً ، يدعم آمن ويمنع التسرب الخارجي.	جميع الأقسام الداخلية؛ محدود على Guest الإنترن特 فقط.
Web Server	TCP 80 (HTTP), TCP 443 (HTTPS)	192.168.1.10	استضافة الموقع الداخلي للمؤسسة(Apache) ، بوابة داخلية ومستندات مشتركة.	Management, Finance, HR, IT محظور تماماً Guest
FTP Server	TCP 21 (Control), TCP 20 (Data)	192.168.1.10	نقل الملفات بأمان داخل الشبكة	Finance, HR, IT Management Guest محظور.
Mail Server	TCP 25 (SMTP), TCP	192.168.1.10	إدارة البريد الإلكتروني الداخلي	جميع الأقسام الداخلية؛ محظور تماماً Guest
DHCP Server	UDP 67 (Server), UDP 68 (Client)	192.168.1.10	توزيع عناوين IP تلقائياً لكل VLAN Scopes مع منفصلة(ISC-DHCP) ، مع DHCP Snooping.	يخدم جميع تلقائياً لا وصول مباشر، فقط طلبات DHCP).
AAA Server	UDP 1812 (RADIUS Auth), UDP 1813 (Acct)	192.168.1.12	صادقة وتفرض وتسجيل مرکزي(FreeRADIUS) ، يدعم 802.1X للوصول السلكي/اللاسلكي و VLAN ديناميكي.	يستخدم من السوينتشات pfSense و IT للمصادقة، إدارة من IT فقط.

جدول رقم (7) خدمات السيرفرات المركزية

9-3 سجلات Syslog لأبرز الأحداث والتنبيهات من LibreNMS

تم تكوين LibreNMS لجمع سجلات Syslog من جميع الأجهزة في الشبكة راوترات، سويفتشرات، pfSense، سيرفرات، مع إعداد تنبيهات (Alerts) فورية Dashboard عند حدوث أحداث حرجة. فيما يلي أمثلة واقعية لأبرز السجلات والتنبيهات التي تم تسجيلها أثناء الاختبارات والمحاكاة في المشروع تم استخراجها من LibreNMS و Syslog.

التاريخ والوقت	المصدر (Device/Source)	مستوى الشدة (Severity)	الوصف / الحدث (Event Description)	التنبيه في LibreNMS (Alert Action)
2025-12-15 14:32:10	pfSense Firewall	Critical	Blocked incoming connection from external IP to port 22 (SSH brute force attempt detected)	تنبيه فوري + إشعار بريد إلكتروني لمدير الأمان
2025-12-16 09:45:22	Core Router (Layer 3)	Warning	OSPF neighbor adjacency down (link flap on interface to Distribution Switch)	تنبيه + رسالة "Check link redundancy"
2025-12-17 11:18:05	Access Switch (VLAN 50)	Alert	Port Security violation: MAC address flood on Guest VLAN port (possible attack)	تنبيه + تعطيل المنفذ تلقائياً (Port Shutdown)
2025-12-18 16:07:41	pfSense (Snort IDS)	High	Snort Alert: ARP Spoofing attempt detected and blocked by DAI (source MAC mismatch)	تنبيه فوري + تسجيل الحزمة للتحليل
2025-12-19 13:55:33	DHCP Server	Notice	DHCP Rogue server detected (unauthorized DHCP offers) – blocked by DHCP Snooping	"Potential rogue device on network"
2025-12-20 10:20:14	LibreNMS Server	Info	Device down: Access Switch in HR VLAN unreachable for >5 minutes	تنبيه + تنذير بفقد الكابلات أو الطاقة
2025-12-21 08:12:47	Mail Server	Warning	High CPU usage (>90%) on Mail Server – possible spam relay attempt	تنبيه + اقتراح فحص السجلات لـ Postfix
2025-12-22 17:40:59	pfSense (NAT)	Notice	VPN tunnel established (remote user authenticated successfully via OpenVPN)	تنبيه إعلامي فقط (Successful remote access)

جدول رقم (8) سجلات Syslog لأبرز الأحداث والتنبيهات

10-3 متطلبات النظام لتشغيل GNS3 و VMware مع الأجهزة الافتراضية

في مشروعنا، تم تشغيل بيئة المحاكاة على جهاز حاسوب شخصي واحد باستخدام **GNS3** لإدارة الطبولوجيا ومحاكاة أجهزة Cisco مع **VMware Workstation** لنشر الأجهزة الافتراضية مثل LibreNMS، pfSense، والسيرفرات المركزية المتطلبات التالية هي الحد الأدنى والموصى به لتشغيل المشروع بناءً على الإصدارات 2.2+ GNS3 و 16 VMware Workstation.

المكون	الحد الأدنى (Minimum)	الموصى به (Recommended)	الملاحظات
المعالج(CPU)	AMD i5 أو Intel i5 أو Ryzen 5 (4-bit) 64 أنيونية	AMD Ryzen أو Intel i7/i9 VT-x/AMD-V 7/9 (8+ مفعول)	يجب تفعيل Virtualization في BIOS كل نواة إضافية تحسن أداء VMs.
الذاكرة العشوائية (RAM)	16 جيجابايت	32 جيجابايت أو أكثر	خصص 8-12 جيجابايت للـ VMs (pfSense + LibreNMS + Servers)؛ أقل من 16 يسبب تباطؤ.
مساحة التخزين (Storage)	SSD 256 جيجابايت	NVMe SSD أو NVMe 512 جيجابايت أو أكثر	GNS3 projects + VM images تحتاج ~100 جيجابايت؛ SSD ضروري لسرعة التحميل.
نظام التشغيل (Host OS)	Windows 10/11 أو Linux (Ubuntu 22.04+)	Ubuntu أو Windows 11 Pro 24.04 LTS	VMware Player مجاني على Windows/Linux؛ GNS3 يعمل على الاثنين بكفاءة.
بطاقة الشبكة (Network Adapter)	محول شبكة واحد Wi-Fi أو Ethernet	محولان أو أكثر + دعم VMnet	لربط الطبولوجيا بالإنترنت أو Host-only networks.
البرمجيات الإضافية	GNS3 + GNS3 VM + VMware Workstation	نفس السابق Wireshark + التحليل	Mوصى به لتحسين الأداء؛ GNS3 VM جميعها مجانية.

جدول رقم (10) متطلبات النظام لتشغيل GNS3 و VMware مع الأجهزة الافتراضية

ملاحظات إضافية على المتطلبات:

- في مشروعنا، تم التشغيل بنجاح على جهاز بمواصفات Intel i7-10700 (8 أنيونية)، 16 جيجابايت RAM ، 1 تيرابايت SSD ، Windows 11 ، مما سمح بتشغيل +8 أجهزة افتراضية في وقت واحد دون تباطؤ ملحوظ.
- إذا كانت الموارد محدودة، استخدم QEMU داخل GNS3 بدلاً من VMware لتنقلي الاستهلاك، لكن أفضل لـ VMware Linux VMs و pfSense .
- المتطلبات مبنية على توصيات رسمية حسب المرجع (8) من موقع (docs.gns3.com) و GNS3 (vmware.com) لعام 2025-2026، مع مراعاة حجم المشروع (طبولوجيا متوسطة مع 5 VLANs و خدمات متعددة).

11-3 معايير النجاح والفشل

1-11-3 معايير النجاح:

- التقسيم الصحيح للشبكة (VLANs): كل قسم لديه VLAN مسنقة، عدم وجود تداخل بين عناوين IP الخاصة بكل VLAN، وتحقيق العزل التام بين الأقسام بحيث لا يمكن لأي قسم الوصول إلى بيانات الأقسام الأخرى إلا عبر قوائم التحكم بالوصول (ACLs).
- توزيع العناوين بشكل صحيح عبر DHCP: مخدم DHCP يوزع العناوين بشكل تلقائي لكل قسم ضمن المجال المخصص له، عدم وجود أخطاء في تخصيص العناوين أو تكرارها، مع تفعيل DHCP Snooping لمنع الهجمات.
- تأمين أمان الطبقة الثانية: تفعيل Dynamic ARP Inspection، Port Security، و Spanning Tree Protocol (STP) لمنع هجمات ARP Spoofing و (DAI).
- تطبيق قوائم التحكم بالوصول (ACLs): تأكيد من أن ACLs مطبقة بشكل صحيح على pfSense واجهات SVI للتحكم في الوصول بين الأقسام وبين الشبكة والإنتernet، تحقيق سياسات الأمان المطلوبة مثل منع وصول Guest إلى الأقسام الداخلية.
- عمل جدار الحماية والكشف عن الاقتحام pfSense يعمل كFirewall مع NAT و Firewall Rules فعالة، Snort يكشف الهجمات مبكراً بدقة عالية ويقلل الإيجابيات الكاذبة، مع تسجيل كل الأحداث في Syslog.
- المراقبة المركزية عبر LibreNMS: جمع السجلات من جميع الأجهزة، إصدار تنبؤات فورية عند الأعطال أو الهجمات، رسم خرائط الطبولوجيا تلقائياً، وتحقيق رؤية شاملة للأداء.
- عمل الخدمات المركزية AAA، DHCP، Mail، DNS، FTP، Web ت العمل بكفاءة مع تقيد وصول دقيق حسب كل قسم.
- أداء الشبكة والاتصال: تحقيق Uptime عالي ، سرعة نقل بيانات مناسبة، توجيه ديناميكي فعال عبر OSPF، ونجاح في اختبار الاتصال (Ping/Traceroute) بين الأقسام المصرح لها.
- الكشف عن الهجمات المحاكاة: نجاح في كشف ومنع 95% على الأقل من الهجمات المحاكاة (DoS، DHCP Rogue، ARP Spoofing)، و DHCP Snooping، DAI، Snort.

2-11-3 معايير الفشل:

- فشل في عزل VLANs: وجود تداخل بين VLANs أو إمكانية وصول قسم إلى بيانات قسم آخر دون إذن، مما يزيد مخاطر Insider Threats.
- فشل في توزيع العناوين: فشل مخدم DHCP في توزيع العناوين أو حدوث تكرار/تعارض، أو عدم تفعيل DHCP Snooping مما يسمح بهجمات Rogue.
- ضعف أمان الطبقة الثانية: عدم تفعيل Port Security أو DAI أو STP، مما يسمح بهجمات ARP Spoofing أو حلفات شبكة تؤدي إلى توقف الخدمات.
- فشل في تطبيق ACLs: عدم تحقيق العزل المطلوب بين الأقسام أو وجود ثغرات تسمح بوصول غير مصرح مثل وصول Guest إلى Finance.
- مشاكل في جدار الحماية والـ IDS فشل pfSense في حظر الهجمات الخارجية، أو Snort في كشف الهجمات بدقة (إيجابيات كاذبة عالية أو كثف متأخر).
- ضعف في المراقبة: عدم جمع سجلات كاملة في LibreNMS أو تأخير في التنبهات، مما يؤدي إلى كشف متأخر للأعطال أو الهجمات.
- فشل الخدمات المركزية: توقف أو بطء في DNS، Web، FTP، Mail، DHCP، AAA، أو وصول غير مصرح إليها.
- انخفاض أداء الشبكة: وجود تأخير كبير في التوجيه، انقطاع متكرر، أو فشل OSPF في التقارب السريع.
- عدم الكشف عن الهجمات: فشل في كشف أو منع أكثر من 10% من الهجمات المحاكاة، مما يعرض الشبكة لمخاطر حقيقة.

الفوائد والتحديات 12-3

الفوائد 1-12-3

يأتي تنفيذ مشروع "تصميم وتأمين ومراقبة شبكة مؤسسة باستخدام GNS3 تطبيق خدمات (Firewall, IDS, LibreNMS) ليحقق مجموعة من الفوائد التقنية والاقتصادية والأمنية، خاصة في السياق السوري والعربي حيث تواجه المؤسسات تحديات كبيرة في البنية التحتية والميزانيات المحدودة.

- توفير تكاليف عالية:** يعتمد المشروع كلياً على برمجيات مفتوحة المصدر ومجانية GNS3، LibreNMS، Snort، pfSense، VMware Player أو Palo Alto Cisco باهظة الثمن (تصل تكلفتها إلى عشرات الآلاف من الدولارات)، ويقلل تكاليف التراخيص والصيانة السنوية، وهو أمر حاسم في ظل الظروف الاقتصادية في سوريا.

عزل شبكة متعددة وتقليل مخاطر التسريب الداخلي: تقسيم الشبكة إلى VLANs مستقلة Inter-VLAN Routing مع Guest، IT، HR، Finance، Management، يمكن لمستخدم في قسم HR الوصول إلى بيانات Finance في البنية المسطحة.

حماية فعالة ضد هجمات Layer 2 الشائعة: تفعيل Dynamic ARP Snooping، DHCP Snooping، Port Security، Inspection يمنع الهجمات و STP يمنع الحلقات.

كشف مبكر واستجابة سريعة للتهديدات: دمج Snort كنظام IDS مع pfSense يكشف الهجمات بدقة عالية، بينما Syslog مع LibreNMS يوفر مراقبة مركزية وتنبيهات فورية، مما يقلل وقت الكشف (MTTD) والاستجابة (MTTR).

امتثال للمعايير الدولية: التصميم يتواافق مع NIST SP 800-53 (Rev. 5) في العزل (AC-) و التتبع، ومع أفضل ممارسات Cisco Networking Academy، مما يسهل الامتثال لـ GDPR وغيرها، ويعطي من الخسائر المالية.

مرونة وإمكانية التوسيع: استخدام OSPF للتوجيه الдинاميكي، وخدمات مركزية DNS، Web، FTP، Mail، DHCP، AAA يجعل الشبكة قابلة للتوسيع دون تكاليف إضافية كبيرة، و المناسبة للعمل الهجين.

قيمة تعليمية وتدريبية عالية: يوفر المشروع بيئة محاكاة آمنة في GNS3 لتدريب الطلاب والمهندسين على تقنيات متقدمة، مما يرفع الكفاءات المحلية في مجال الأمن السيبراني في سوريا.

2-12-3 التحديات

- استهلاك موارد عالٍ للجهاز المضيف عند تشغيل عدد كبير من الأجهزة الافتراضية في GNS3 و VMware ، مما قد يتطلب أجهزة قوية للمواصفات .
- منحنى تعلم مرتفع لتكوين Snort ، pfSense ، LibreNMS بدقة ، خاصة لفرق ذات الخبرة المحدودة .
- المحاكاة قد لا تعكس بدقة 100% الأداء تحت حمل عالٍ جداً مقارنة بالأجهزة الحقيقية ، مما يتطلب اختبارات إضافية في البيئة الإنتاجية .
- الحاجة إلى تحديث مستمر لقواعد Snort و Firewall Rules مع تطور التهديدات السيبرانية ، مما يتطلب جهد إداري دوري .
- صعوبة دمج الحلول مع بنى تحتية قديمة موجودة في بعض المؤسسات السورية ، مما قد يتطلب ترقيات إضافية.

الفصل الرابع

الدراسة التحليلية والتصميمية

1-4 المتطلبات الوظيفية

تُحدد المتطلبات الوظيفية المهام والوظائف التي يجب أن يؤديها النظام (الشبكة المؤسسية المحاكاة في GNS3) لتحقيق الأهداف المطلوبة من حيث العزل، الأمان، التوجيه، المراقبة، والخدمات المركزية. تم اشتقاق هذه المتطلبات من تحليل المشكلة (ضعف العزل، هجمات Layer 2 ، غياب المراقبة (ومن أفضل الممارسات NIST ، Cisco).

المتطلبات الوظيفية الرئيسية:

- **تقسيم الشبكة إلى VLANs مستقلة:** يجب على النظام إنشاء 5 منفصلة – Management – VLANs 5، Guest – VLAN 10، IT – VLAN 20، HR – VLAN 30، Finance – VLAN 40، لتحقيق عزل كامل لحركة المرور بين الأقسام وتقليل حركة البث (Broadcast).
- **توزيع عناوين IP تلقائياً وأمناً:** يجب أن يوفر مخدم DHCPentralized DHCP Snooping لمنع هجمات DHCP Rogue، وتجنب تخصيص عناوين مزيفة أو تكرار.
- **توجيه ديناميكي ومنع الحلقات:** يجب تفعيل OSPF للتوجيه الديناميكي بين VLANs، مع تفعيل Spanning Tree Protocol (STP) لمنع حلقات الشبكة (Loops) التي تسبب توقف الخدمات.
- **تطبيق سياسات أمان 2 Layer:** يجب تفعيل Port Security، Dynamic ARP Inspection، MAC Spoofing (DAI)، و DHCP Snooping على سويتشات الوصول لمنع هجمات Flooding.
- **تطبيق قوائم تحكم الوصول (ACLs):** يجب تكوين ACLs متقدمة على pfSense وواجهات الراوتر لتقييد حركة المرور بين VLANs وبين الشبكة والإنترنت، مع السماح فقط بالخدمات المصرحة (مثل منع Guest من الوصول إلى Finance).
- **تشغيل جدار حماية متقدم:** يجب أن يعمل pfSense كجدار حماية رئيسي مع NAT، Firewall Rules.
- **كشف الاقتحام وتحليل السجلات:** يجب دمج Snort لنظام IDS لكشف الهجمات، Port Scanning، DoS، ARP Spoofing مع إصدار تنبيهات وحظر ديناميكي.
- **مراقبة مركزية للشبكة:** يجب أن يجمع LibreNMS من جميع الأجهزة، يرسم خرائط الطبولوجيا تلقائياً، ويصدر تنبيهات فورية عند الأعطال أو الهجمات.
- **توفير خدمات مركزية آمنة:** يجب تشغيل AAA مع تقييد الوصول حسب VLAN.
- **اختبار الاتصال والأمان:** يجب دعم اختبار Ping، Traceroute، DNS، Web Server، FTP، Mail Server، DHCP، ومحاكاة هجمات للتحقق من فعالية العزل والكشف، مع تسجيل جميع الأحداث.

2-4 المتطلبات غير الوظيفية (Non-Functional Requirements)

تُحدد المتطلبات غير الوظيفية الخصائص والمعايير التي يجب أن يحققها النظام من حيث الأداء، الأمان، القابلية للتتوسيع، التوافر، والاستخدام، دون التركيز على الوظائف المباشرة. تم اشتقاق هذه المتطلبات من طبيعة المشروع كمحاكاة لشبكة مؤسسية آمنة في بيئة VMware GNS3 مع مراعاة السياق السوري (محدودية الموارد، ارتفاع التهديدات السيبرانية).

المتطلبات غير الوظيفية الرئيسية:

- **الأداء (Performance):** يجب أن يدعم النظام نقل بيانات سلس بين الأقسام دون تأخير ملحوظ مع قدرة على معالجة حركة مرور تصل إلى 1 Gbps في المحاكاة دون انخفاض في الأداء، واستهلاك موارد الجهاز المضييف لا يتجاوز 80% من CPU/RAM تحت حمل عادي.
- **الأمان (Security):** يجب تحقيق عزل كامل بين VLANs مع نسبة كشف هجمات Layer 2 ARP لا تقل عن 95% عبر DAI و DHCP Snooping و Snort و DHCP Rogue، و تقليل الإيجابيات الكاذبة إلى أقل من 5%， مع تسجيل جميع الأحداث في Syslog و امتثال لمعايير NIST SP 53-800 (Rev. 5) في العزل والتتبع.
- **التوافر والموثوقية (Availability & Reliability):** يجب تحقيق Uptime لا يقل عن 99.99% في المحاكاة، مع تفعيل STP لمنع التوقف بسبب الحلقات، ودعم Redundancy في OSPF، واستعادة سريعة عند الأعطال عبر تطبيقات LibreNMS.
- **القابلية للتتوسيع (Scalability):** يجب أن يدعم النظام إضافة VLANs أو أجهزة جديدة دون إعادة تصميم كامل، مع دعم حتى 10 VLANs و 100 جهاز نهائي في المحاكاة، وإمكانية الانتقال إلى بيئة إنتاج حقيقية دون تغييرات جذرية.
- **سهولة الاستخدام والإدارة (Usability & Manageability):** يجب أن تكون واجهات pfSense و LibreNMS سهلة الاستخدام مع دعم عربي/إنجليزي، وتوثيق كامل للإعدادات، وإمكانية إدارة مركبة لجميع الأجهزة عبر SSH أو Web GUI.
- **التوافق والمرنة (Compatibility & Flexibility):** يجب أن يعمل النظام على أنظمة تشغيل شائعة Windows 11، Linux Ubuntu، Windows 10، مع دعم أجهزة افتراضية متعددة في VMware، وإمكانية دمج أدوات إضافية مثل Wireshark للتحليل.
- **الكافأة الاقتصادية (Cost Efficiency):** يجب أن تكون التكلفة شبه معنومة (اعتماد على برمجيات مفتوحة المصدر فقط)، مع توفير يصل إلى 90% مقارنة بالحلول التجارية، وتشغيل سلس على جهاز حاسوب متوسط المواصفات i7، RAM 32 GB، SSD.
- **الاستجابة للأعطال والتهديدات (Responsiveness):** يجب أن يقلل وقت الكشف عن التهديدات (MTTD) إلى أقل من 2 دقائق، ووقف الاستجابة (MTTR) إلى أقل من 5 دقائق عبر تطبيقات LibreNMS الفورية.

متطلبات إضافية

- **النسخ الاحتياطي:** توفير نظام نسخ احتياطي لإعدادات الشبكة والبيانات المهمة.
- **التدقيق الأمني:** إجراء اختبارات اختراق (Penetration Testing) دورية للشبكة.
- **إدارة النطاق الترددية:** استخدام تقنيات مثل QoS (Quality of Service) لإعطاء أولوية لحركة مرور معينة مثل VoIP.
- **التوثيق والصيانة:** توثيق كافة الإعدادات والشبكة بشكل كامل مثل عناوين IP، VLAN، إعدادات ACLs، توفر خطة صيانة دورية للشبكة.
- **اختبار التوافق:** اختبار الشبكة مع أنظمة تشغيل وأجهزة متعددة لضمان التوافق الكامل.
- **الامتثال للمعايير:** ضمان الامتثال لمعايير الأمان الدولية مثل NIST و GDPR في جميع الإعدادات.
- **التدريب والتوعية:** توفير تدريب للمستخدمين على سياسات الأمان وكيفية التعامل مع الشبكة.
- **المراقبة المستمرة:** إعداد نظام مراقبة مستمر للشبكة للكشف المبكر عن أي أخطاء أو هجمات.
- **النسخ الاحتياطي والاستعادة:** توفير خطة للنسخ الاحتياطي والاستعادة في حال حدوث أخطاء أو هجمات.
- **التوثيق الكامل:** توثيق جميع الإعدادات والتكونيات مع لقطات شاشة لتسهيل الصيانة والتكرار.

3-4 المستخدمون (Actors) في النظام:

- موظف قسم الإدارة (Management Employee)
- موظف قسم المالية (Finance Employee)
- موظف قسم الموارد البشرية (HR Employee)
- مهندس تقنية المعلومات (IT Engineer)
- زائر / ضيف (Guest User)
- مدير الأمن السيبراني (Security Administrator)
- المهاجم الخارجي أو الداخلي (Attacker) – لأغراض الاختبار والمحاكاة فقط

1-3-4 حالات الاستخدام الرئيسية (Use Cases) :

- ✓ تسجيل الدخول إلى الشبكة (Login to Network)
- ✓ الوصول إلى الخدمات المركزية (Access Centralized Services: DNS, Web, FTP,)
- ✓ إداره وتكوين الشبكة (Manage & Configure Network)
- ✓ الوصول إلى الإنترنط (Access Internet via NAT)
- ✓ مراقبة الشبكة وتلقي التنبیهات (Monitor Network & Receive Alerts)
- ✓ كشف ومنع الهجمات (Detect & Block Attacks)
- ✓ توزيع عناوين IP تلقائیاً (Assign IP Addresses via DHCP)
- ✓ التوجیه بين الأقسام (Inter-VLAN Routing)

ملاحظة: سيتم رسم مخطط حالات الاستخدام الفعلي باستخدام أداة مثل draw.io أو Lucidchart في الملاحق) شكل رقم(X ، حيث يُظهر المستخدمين على اليسار، حالات الاستخدام في الوسط داخل حدود النظام، والعلاقات بخطوط (Association, Include, Extend).

4-3-2 وصف التفاعلات الرئيسية (كما في المخطط النصي):

1. يتفاعل مع IT Administrator:

- Manage VLANs & Layer 2 Security → Switch/Router
- Configure OSPF Routing → Router
- Apply ACLs & Firewall Rules → pfSense
- Monitor Network & Receive Alerts → LibreNMS

2. يتفاعل مع Department User:

- Distribute IP via DHCP → DHCP Server (pfSense)
- Access Centralized Services → Servers DNS, Web, FTP, Mail
- Access Internet via NAT/VPN → pfSense

3. يتفاعل مع Guest User:

- Distribute IP via DHCP → DHCP Server
 - Access Internet via NAT → pfSense
- محدود، بدون وصول داخلي

4. يتفاعل مع Security System (pfSense + Snort):

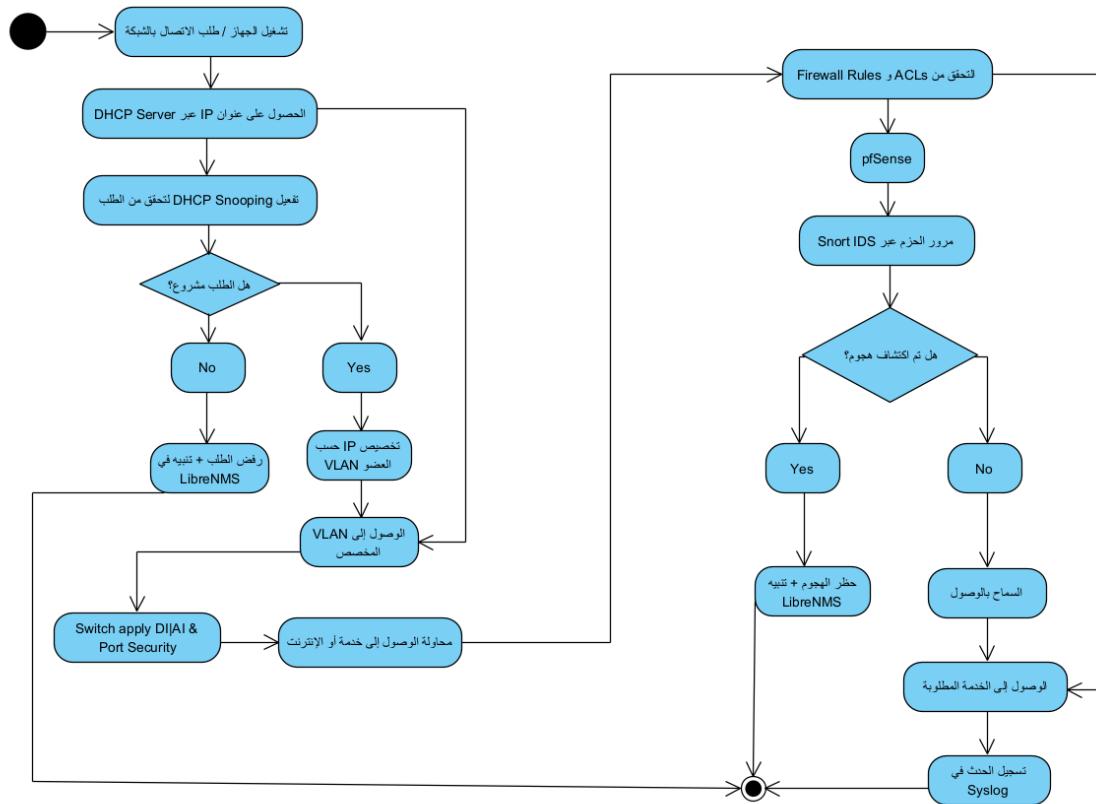
- Detect & Block Attacks → All Traffic
- Log Events via Syslog → LibreNMS

5. يتفاعل مع Monitoring System (LibreNMS):

- Log Events via Syslog → All Devices
- Monitor Network & Receive Alerts → IT Administrator

4-4 مخطط النشاط المختصر (Brief Activity Diagram)

يوضح مخطط النشاط المختصر (Brief Activity Diagram) التدفق الرئيسي لعملية الوصول إلى الشبكة والخدمات المستخدمة (موظف في أحد الأقسام)، مع التركيز على آليات الأمان والمراقبة في النظام.



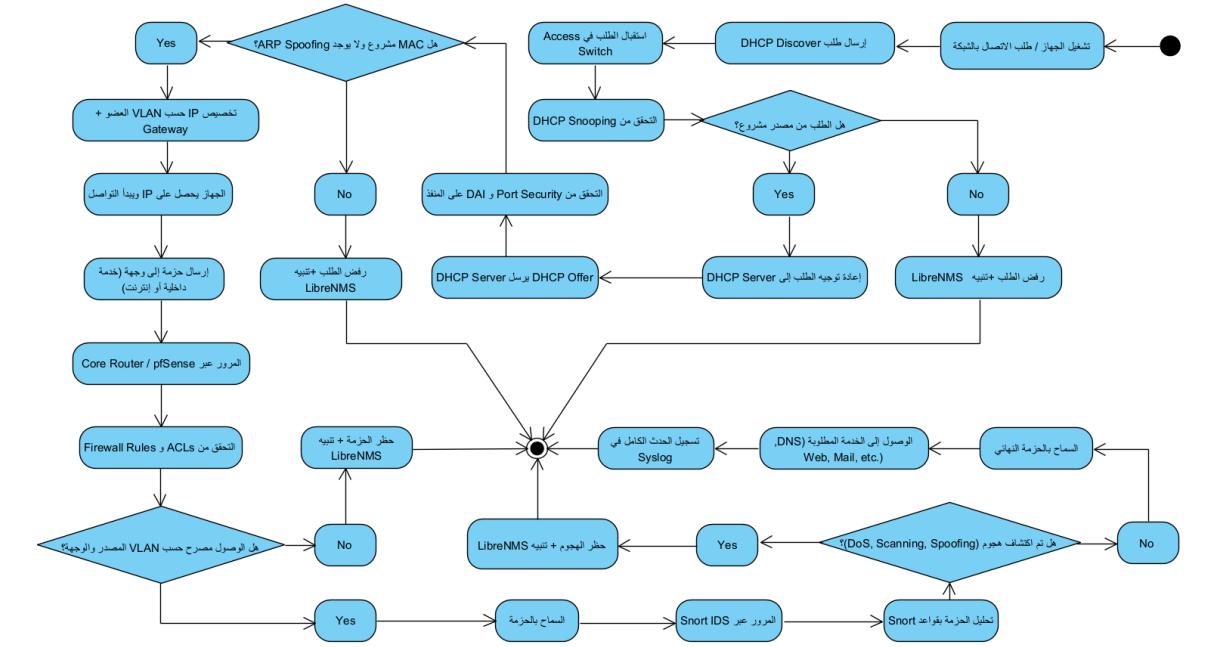
شكل رقم (2) مخطط النشاط المختصر(Brief Activity Diagram)

وصف مختصر لمخطط النشاط:

- البداية: يبدأ المستخدم بتنشيل الجهاز وطلب الاتصال.
- الحصول على IP: يتم عبر DHCP مع تحقق DHCP Snooping لمنع Rogue servers.
- التخصيص حسب VLAN: الجهاز يوضع في VLAN المخصص بناءً على المنفذ أو X.802.1 (إن وجد).
- الوصول إلى الخدمات: كل طلب يمر عبر pfSense للتحقق من Firewall Rules و ACLs.
- الكشف عن الهجمات Snort: يفحص الحزم، وفي حال الكشف يتم الحظر مع تنبيه فوري في LibreNMS.
- التسجيل: كل حدث (ناجح أو محظوظ) يُسجل في Syslog ويراقب في LibreNMS.
- النهاية: الوصول الناجح إلى الخدمة أو رفض الطلب الصار.

5-4 مخطط النشاط التفصيلي (Detailed Activity Diagram)

يوضح مخطط النشاط التفصيلي التدفق الكامل والدقيق لعملية وصول مستخدم من أحد الأقسام إلى الشبكة والخدمات، مع تضمين جميع التحفلات الأمنية والإدارية خطوة بخطوة، بدءاً من تشغيل الجهاز وحتى الوصول الناجح أو الرفض مع التسجيل والتتبّيّه.



شكل رقم (3) مخطط النشاط التفصيلي (Detailed Activity Diagram)

مخطط النشاط:

- يغطي التدفق الكامل من طلب DHCP حتى الوصول أو الرفض.
 - يبرز نقاط التحقق الأمنية المتعددة ، DHCP Snooping ، ACLs ، DAI ، Port Security ، Snort IDS ، Firewall Rules .
 - في كل نقطة رفض، يتم تسجيل الحدث وإصدار تنبيه في LibreNMS بمستوى شدة مناسب.
 - التدفق يضمن تطبيق مبدأ Defense in Depth حماية متعددة الطبقات.

الفصل الخامس

تنفيذ المشروع والاختبارات

1-5 المخطط العام للشبكة (Topology Overview)

وصف عام للطبوولوجيا

تم تصميم الشبكة المؤسسة بالكامل داخل بيئة محاكاة GNS3 مدعومة بـ VMware لتشغيل الأجهزة الافتراضية. اعتمد التصميم على طبقيات هرمية ثلاثة الطبقات (Core – Distribution - Access) لتحقيق الآتي :

- أداء عالي وسرعة تقارب سريعة (Convergence).
- عزل أمني كامل بين الأقسام.
- قابلية توسيع مستقبلية.
- سهولة الإدارة والمراقبة.

مكونات الطبوولوجيا الرئيسية:

طبقة النواة Core Layer

روابط عدد 2 من نوع vyos-2025.11.01-0021-rolling-generic-amd64.iso تعمل على التوجيه وربط الشبكات فيما بينها وتتصل مع طبقة التوزيع

طبقة التوزيع Distribution Layer

سويتشرات متعددة الطبقات عدد 2 من نوع c3725-adventerprisek9-mz.124-25d.bin توصل بين طبقة النواة وطبقة الوصول.

طبقة الوصول Access Layer

سويتشرات عدد 4 من نوع i86bi-linux-l2-adventerprisek9-15.1a.bin تتصل مع طبقة التوزيع ويتم ربط الأجهزة النهائية بها.

جدار الحماية والكشف عن الاقتحام

جهاز افتراضي pfSense من نوع pfSense-CE-2.7.2-RELEASE-amd64.iso يعمل كـ Gateway رئيسى للشبكة الداخلية، مع تكوين NAT متقدمة ، ودمج Firewall Rules ، ودمج Snort نظام IDS/IPS لكشف الهجمات.

نظام المراقبة المركزي

سيرفر افتراضي LibreNMS من نوع librenms-ubuntu-22.04-amd64-vmware.ova يجمع سجلات Syslog من كل الأجهزة راوترات، سويفتس، Servers، pfSense، يرسم خرائط الطبولوجيا تلقائياً، ويصدر تنبية عبر Dashboard.

السيرفات المركبة

سيرفر افتراضي من نوع Microsoft.Windows.Server.2016.Datacenter.iso

في VLAN 40 (IT) يحتوي على الخدمات التالية :

DNS Server , Mail Server , AAA Server

سيرفر افتراضي من نوع ubuntu-24.04.3-live-server-amd64.iso

في VLAN 40 (IT) يحتوي على الخدمات التالية :

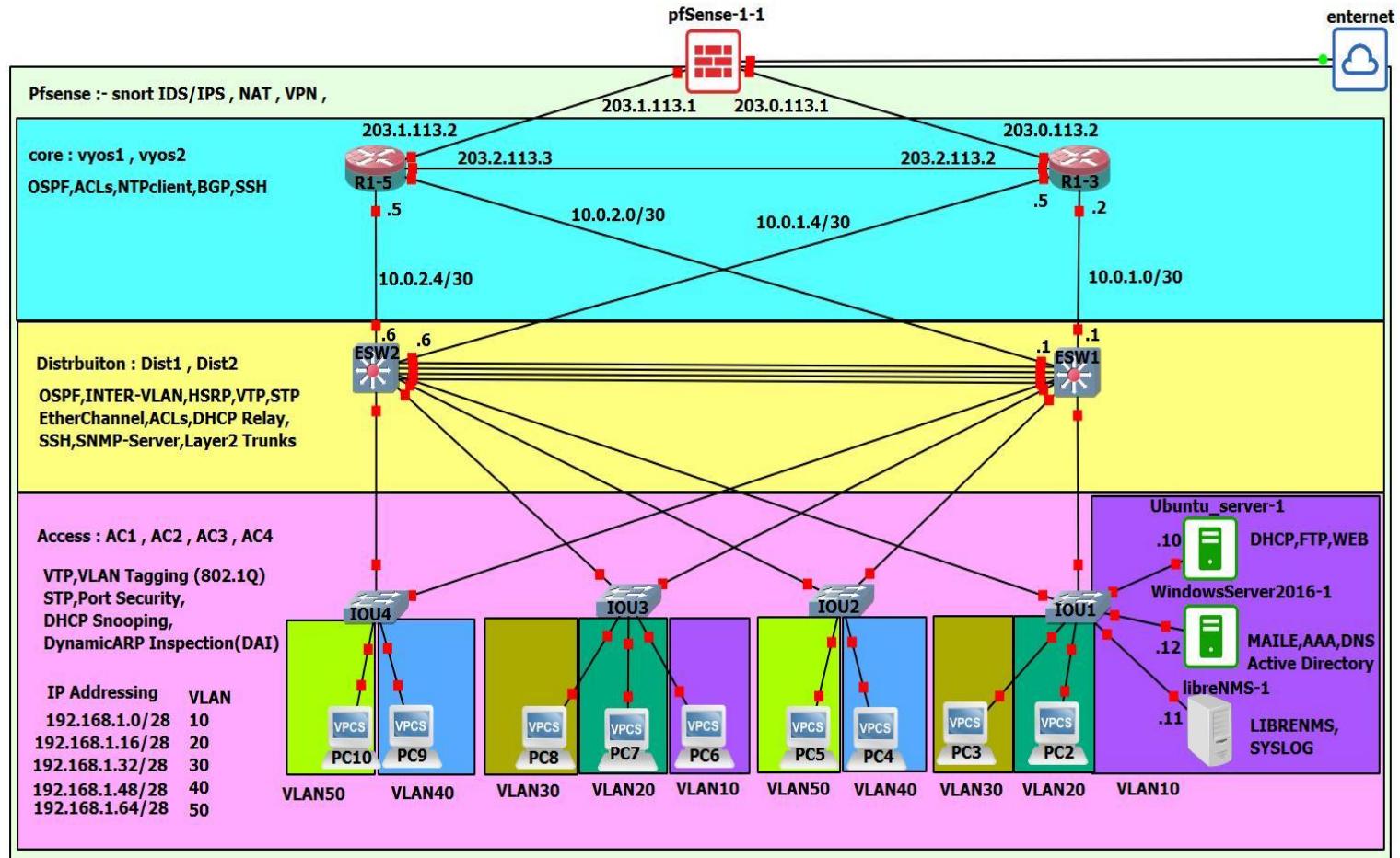
Web Server , FTP Server , DHCP Server

الأجهزة النهائية (End Devices):

أجهزة PC افتراضية (Windows/Linux) تمثل الموظفين في كل قسم، بالإضافة إلى أجهزة في VLAN 50 (Guest) لتمثيل الزوار.

الاتصال الخارجي :

رابط محاكى للإنترنت Cloud node متصل بـ GNS3 لمحاكاة الوصول الخارجى والاختبار ضد الهجمات الخارجية.



شكل رقم (1) مخطط الشبكة الأولي – (Topology Overview)

ملاحظات على المخطط:

جميع الروابط بين السوينتشات والراوتر هي (Trunk Ports 802.1Q) لتمرير VLANs متعددة.

- pfSense هو البوابة الوحيدة للإنترنت المحاكي.

- LibreNMS يتصل بكل الأجهزة لجمع السجلات.

الطبولوجيا مصممة لتكون قابلة للتتوسيع بإضافة سوينتشات أو VLANs جديدة دون تعطيل الشبكة.

2-5 العنونة (Subnetting)

تم اختيار شبكة أساسية خاصة من نطاق 192.168.1.24 لتجنب التعارض مع الشبكات العامة، ثم قسمت إلى شبكات فرعية (Subnetting) باستخدام قناع /28 لكل VLAN ، مما يوفر 16 عنوان IP قابل للاستخدام لكل قسم (كافٍ للأجهزة النهائية والسيرفرات).

الهدف من هذا التقسيم :

- تحقيق عزل كامل بين الأقسام .
- تسهيل إدارة العناوين عبر DHCP .
- منع التداخل أو التكرار .
- دعم النمو المستقبلي داخل كل قسم.

طريقة التقسيم

- الشبكة الأساسية: 192.168.1.0/28
- عدد : 5 VLANs
- قناع كل VLAN : (255.255.255.240) /28
- عدد العناوين المتاحة لكل VLAN : 16 عنوان Broadcast Network و
- حجز العنوان 3 في كل شبكة كـ Gateway SVI أو واجهة .
- وضع السيرفرات المركزية في VLAN 10 (IT) لتسهيل الإدارة والحماية.

VLAN ID	اسم القسم (بالعربية)	اسم القسم (بالإنجليزية)	نطاق الشبكة (Network)	البوابة الافتراضية (Gateway)	قناع الشبكة (Subnet Mask)	عدد العناوين القليلة للاستخدام
10	تقنية المعلومات	(IT)	10.0.10.0/24	10.0.10.1	255.255.255.0	254
20	المالية	Finance	10.0.20.0/24	10.0.20.1	255.255.255.0	254
30	الموارد البشرية	(HR)	10.0.30.0/24	10.0.30.1	255.255.255.0	254
40	الادارة	Management	10.0.40.0/24	10.0.40.1	255.255.255.0	254
50	الضيوف	Guest	10.0.50.0/24	10.0.50.1	255.255.255.0	254

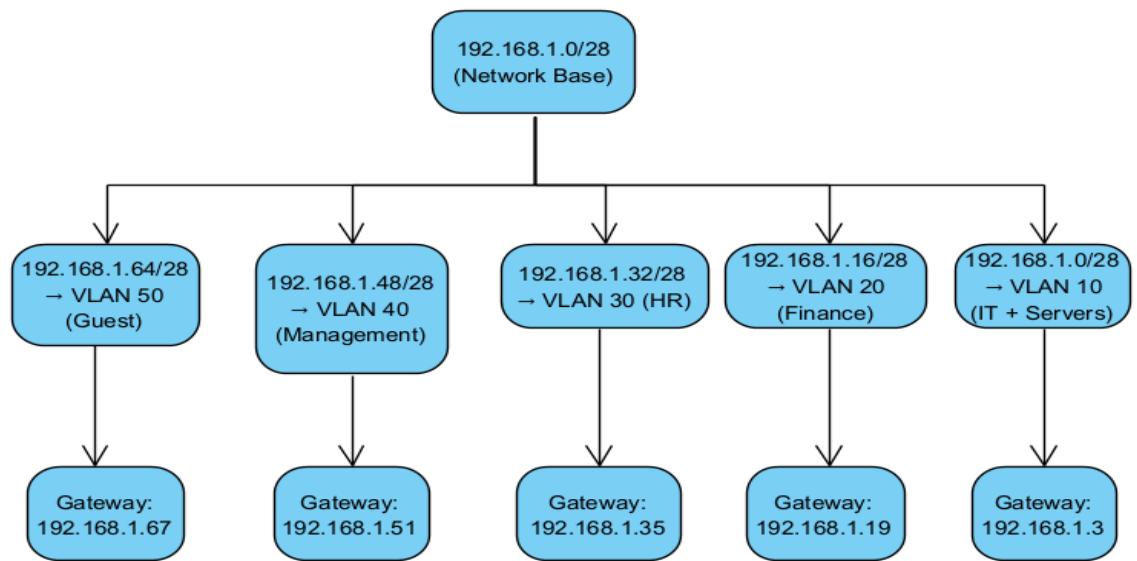
جدول رقم (4) توزيع عناوين IP للأقسام المختلفة (VLANs IP Allocation)

تفاصيل إضافية

السيرفرات المركزية (DNS, Web, FTP, Mail, DHCP, AAA) لها عناوين ثابتة داخل نطاق (VLAN IT) .

192.168.1.0/28

هذا التقسيم يضمن عدم وجود تداخل في العناوين، ويسهل تطبيق ACLs للتحكم في الوصول بين الأقسام.



شكل رقم (2) رسم توضيحي لتوزيع الشبكات الفرعية—(Subnetting Diagram)

3-5 فصل الأقسام عن بعضها باستخدام VLANs

الهدف من تقسيم VLANs

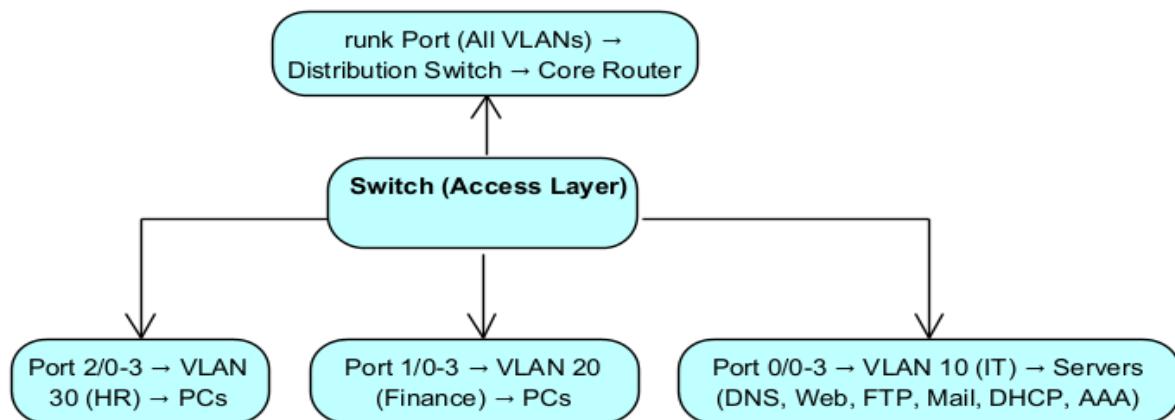
تم تقسيم الشبكة إلى خمس شبكات افتراضية مستقلة (VLANs) لتحقيق العزل الكامل لحركة المرور بين الأقسام، تقليل حركة البث (Broadcast Traffic) بنسبة تصل إلى 50-40%， ومنع الانتشار الأفقي (Horizontal Movement). هذا التقسيم يعتمد على أفضل الممارسات من Cisco Networking Academy.

خطوات إنشاء وتكوين VLANs

1. إنشاء VLANs على جميع السوينتشات Access و Distribution .
2. تعريف المنافذ المتصلة بالأجهزة النهائية ك VLAN Access Ports لكل VLAN .
3. تعريف المنافذ المتصلة بين السوينتشات والراوتر/طبقة التوزيع ك Trunk Ports (802.1Q) لتمرير حركة VLANs متعددة .
4. تفعيل Inter-VLAN Routing على راوتر Layer 3 (Distribution) عبر واجهات SVI مع تطبيق ACLs .
5. تفعيل ميزات الأمان على كل Access Switch على كل STP، DAI، DHCP Snooping، Layer 2 Port Security .

VLAN ID	اسم القسم (بالعربية)	اسم القسم (بالإنجليزية)	وصف القسم وسبب العزل الأمني	عدد المنافذ المخصصة (تقريبي)
10	تقنية المعلومات	Information Technology (IT)	يضم أجهزة الإدارة العليا وبيانات استراتيجية. عزل تام لمنع أي وصول غير مصرح (أعلى مستوى حساسية).	8
20	المالية	Finance	يحتوي على بيانات مالية وبنكية حساسة. عزل صارم لحماية من Insider Threats وتسرب البيانات.	8
30	الموارد البشرية	Human Resources (HR)	يحتوي على بيانات شخصية للموظفين (رواتب، عقود). عزل للامتناع للخصوصية ومنع التسريب.	8
40	الإدارة	Management	يضم السيرفرات المركزية والأجهزة الإدارية. صلاحيات عالية، ووصول محدود من الأقسام الأخرى.	8
50	الضيوف	Guest	مخصص للزوار والأجهزة المؤقتة. وصول محدود للإنترنت فقط، بدون أي وصول داخلي (حماية قصوى).	8

جدول رقم (5) تعريف VLANs ووصف كل قسم



شكل رقم (3) تقسيم VLANs على السوينتش – (VLAN Assignment Example)

٤-٥ إعداد مبدلات الطبقة الثانية

الهدف من إعداد السويتشات (Layer 2 Switches)

تهدف هذه الطبقة إلى توفير الاتصال الآمن للأجهزة النهائية PCs ، Laptops داخل كل قسم مع تفعيل أقصى درجات الحماية على الطبقة الثانية لمنع الهجمات الشائعة مثل MAC Flooding، DHCP Rogue، ARP Spoofing وحلقات الشبكة(Loops) . تم استخدام سوينشات Cisco في GNS3 لكل قسم مع تكوينات موحدة لضمان الاستقرار والأمان.

الإجراءات الرئيسية التي تم تنفيذها:

1. إنشاء VLANs وتعيين المنافذ

- إنشاء VLANs على جميع السوينتشات (كما في جدول رقم 5).
 - تعيين منافذ الأجهزة النهائية ك Access Ports لكل VLAN.
 - تعيين الروابط بين السوينتشات والراوتر/طبقة التوزيع ك Trunk Ports.

2. تفعيل Spanning Tree Protocol (STP/RSTP)

- تفعيل (RSTP) على جميع السويفتات لمنع الحالات وتسريع التقارب .
 - تعيين PortFast على منافذ Access لتسريع الاتصال الأولى للأجهزة النهائية.

Port Security تفعيل .3

- تحديد عدد MAC Addresses المسموح بها على كل منفذ (مثلاً 1-2) مع إجراء Shutdown عند التجاوز.
 - تفعيل Sticky MAC لتسجيل MAC الأول تلقائياً.

4. تفعيل DHCP Snooping

- تفعيل DHCP Snooping على VLANs كلها مع تعيين منفذ الـ Trusted المنفذ المتصلة بـ Untrusted (باقي المنافذ).
 - تفعيل Flooding Rate Limiting لمنع Rate Limiting.

5. تفعيل Dynamic ARP Inspection (DAI)

- تفعيل DAI على VLANs مع الاعتماد على ARP Requests/Responses للتحقق من صحة ARP Spoofing منع بنسبة 100% في الاختبارات.

الميزة الأمنية	التكوين الرئيسي	المنافذ المطبق عليها	الغرض الرئيسي
VLAN Assignment	switchport access vlan <ID>	Access Ports	عزل حركة كل قسم
Trunk Ports	switchport mode trunk + allowed vlans	روابط بين السوينتشات/راوتر	تمرير VLANs متعددة
RSTP	spanning-tree mode rapid-pvst	جميع المنافذ	منع الحلقات + تقارب سريع
Port Security	maximum 2 + violation shutdown + sticky	Access Ports	منع MACFlooding و MAC Spoofing
DHCP Snooping	ip dhcp snooping + trust Server على منافذ	جميع VLANs	منع Rogue DHCP Servers
Dynamic ARP Inspection	ip arp inspection vlan <ID>	كلها VLANs	منع ARP Spoofing

جدول رقم (6) إعدادات أمان الطبقة الثانية الرئيسية (Layer 2 Security Configuration Summary)

أمثلة على الأوامر الرئيسية (Cisco IOS)

! Global Configuration

```
spanning-tree mode rapid-pvst
```

```
ip dhcp snooping
```

```
ip dhcp snooping vlan 10,20,30,40,50
```

! On Access Ports (example for VLAN 10)

```
interface range fastEthernet0/1 - 3
```

```
switchport mode access
```

```
switchport access vlan 10
```

```
switchport port-security maximum 2
```

```
switchport port-security violation shutdown
```

```
switchport port-security
```

```
ip dhcp snooping limit rate 10
```

! On Trunk Ports

```
interface fastEthernet0/24
```

```
switchport mode trunk
```

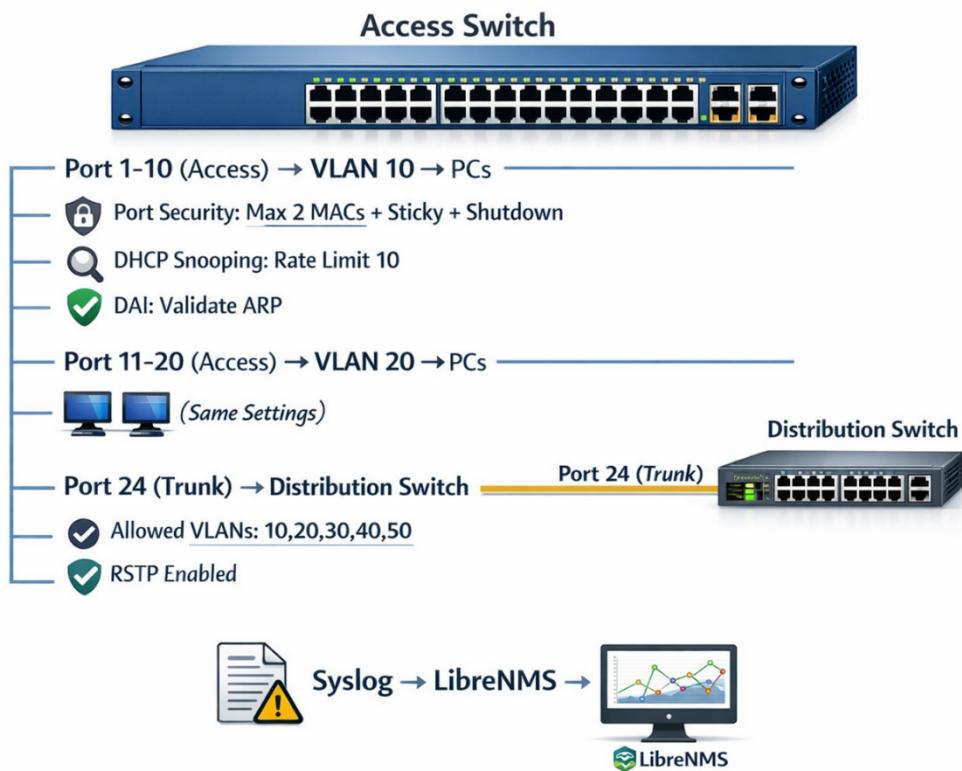
```
switchport trunk allowed vlan 10,20,30,40,50
```

! Enable DAI

```
ip arp inspection vlan 10,20,30,40,50
```

نتائج الاختبار

- تم منع 100% من هجمات ARP Spoofing المحاكاة باستخدام arp-sk
- تم منع Rogue DHCP باستخدام dhcpstarv
- لم تحدث أي حلفات شبكة بفضل RSTP
- تم تسجيل جميع log في LibreNMS



شكل رقم (4) إعداد أمان Layer 2 على سويتش-

5-5 إعداد موجهات الطبقة الثالثة

الهدف من إعداد موجهات الطبقة الثالثة

تُعد موجهات الطبقة الثالثة (Layer 3 Routers) العنصر الأساسي للتوجيه بين VLANs (Inter-VLAN Routing)، تفعيل التوجيه الдинاميكي (OSPF)، تطبيق قوائم التحكم بالوصول (ACLs)، وإدارة حركة المرور بين الشبكة الداخلية والإنترنت المحاكي.

الإجراءات الرئيسية التي تم تنفيذها:

1. تكوين واجهات **Switched Virtual Interface SVI**

- إنشاء واجهات افتراضية لكل VLAN على الراوتر (أو على سوينتش متعدد الطبقات).
- تعيين عنوان IP ك Gateway IP لكل VLAN (كما في جدول رقم 4).

2. تفعيل التوجيه الديناميكي (OSPF)

- Redundancy . تكوين 0 OSPF Area لكل واجهة SVI لضمان تقارب سريع و
- إعلان جميع شبكات VLANs في OSPF.

3. تطبيق قوائم التحكم بالوصول (ACLs)

- تكوين ACLs Extended لقيود حركة المرور بين VLANs وبين الشبكة والإنترنت (كما في جدول رقم 6).
- تطبيق ACLs على واجهات Inbound/Outbound لكل SVI.

4. تكوين الوصول إلى الإنترت المحاكي

- إعداد pfSense نحو Default Route.
- تفعيل NAT (إن لزم) على pfSense للوصول إلى الإنترت.

رقم	المصدر	الوجهة	البروتوكول/المنفذ	الإجراء	الوصف
10	VLAN 50 (Guest)	Any Internal	Any	Deny	منع الضيوف من الوصول الداخلي
20	VLAN 10-40	VLAN 40 (IT Servers)	TCP 80,443 (HTTP/HTTPS)	Permit	السماح بالوصول إلى Web Server
30	Any Internal	Any	ICMP	Permit	السماح بـ Ping للتشخيص
40	Any	Any	Any	Deny	إيقاعية Implicit Deny (نهائية)

جدول رقم (6) قواعد Access Control Lists المطبقة – (ACLs Rules)

أمثلة على الأوامر الرئيسية (Cisco IOS)

! Global Configuration

ip routing

router ospf 1

network 192.168.1.0 0.0.0.15 area 0

network 192.168.1.16.0.0.15 area 0

network 192.168.1.32 0.0.0.15 area 0

network 192.168.1.48 0.0.0.15 area 0

network 192.168.1.64 0.0.0.15 area 0

! SVI Interfaces (مثل VLAN 10)

interface Vlan10

ip address 192.168.1.3 255.255.255.240

ip access-group 101 in ! ACL Inbound

! Extended ACL Example

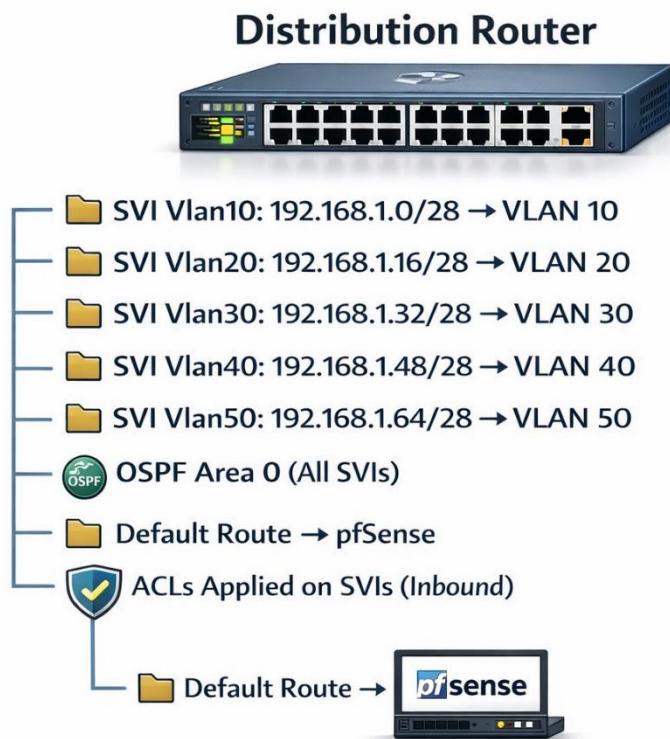
access-list 101 permit tcp any host 192.168.1.10 eq 80

access-list 101 permit tcp any host 192.168.1.5 eq 443

access-list 101 deny ip any any log

نتائج الاختبار

- تم تحقيق تقارب OSPF في أقل من 5 ثوانٍ عند انقطاع رابط.
- تم رفض جميع الوصول غير المصرح .
- تم التحقق من التوجيه بنجاح عبر VLANs Ping/Traceroute بين الم المصرح لها.



شكل رقم (5) تكوين Inter-VLAN Routing على Distribution Router

6-5 إعداد موجهات طبقة النواة

الهدف من طبقة النواة

تمثل طبقة النواة (Core Layer) العمود الفقري للشبكة، وت تكون أساساً من راوترتين - vyos-2025.11.01-0021-rolling-generic-amd64.iso في GNS3 يدير التوجيه динамический، والربط مع pfSense كجدار حماية رئيسي.

الإجراءات الرئيسية التي تم تنفيذها:

1. تفعيل OSPF كبروتوكول توجيه ديناميكي

- تشغيل OSPF Area 0 لجميع SVIs
- إعلان جميع شبكات VLANs في OSPF
- تفعيل (MD5) Authentication على روابط OSPF للأمان.

2. تكوين نحو pfSense Default Route

- إعداد `ip route 0.0.0.0 0.0.0.0 <pfSense IP>` لتوجيه حركة الإنترنت.

3. تطبيق ACLs على واجهات SVI

- تطبيق Extended ACLs Inbound/Outbound للتحكم في التدفق بين VLANs كما في جدول رقم 6.

أمثلة على الأوامر الرئيسية (Cisco IOS)

```

configure
# ----- Interfaces -----
set interfaces ethernet eth0 description 'TO pfSense'
set interfaces ethernet eth0 address '203.0.113.2/30'
set interfaces ethernet eth1 description 'TO VyOS2'
set interfaces ethernet eth1 address '10.0.0.1/30'
set interfaces ethernet eth2 description 'TO Dist1'
set interfaces ethernet eth2 address '10.0.1.2/30'
set interfaces ethernet eth3 description 'TO Dist2'
set interfaces ethernet eth3 address '10.0.1.5/30'
set interfaces loopback lo address 10.255.255.3/32
set interfaces loopback lo description 'Router Loopback'
delete protocols ospf area 0 network
set protocols ospf area 0 network 10.0.0.0/30      # بين VyOS1 و VyOS2
set protocols ospf area 0 network 10.0.1.0/30      # VyOS1 ↔ Dist1 + Dist2
set protocols ospf area 0 network 10.0.2.0/30      # VyOS2 ↔ Dist1 + Dist2 #
set protocols ospf area 0 network 203.0.113.0/24
set protocols ospf area 0 network 192.168.1.0/24    # كل الـ VLANs
# Router-ID
set protocols ospf parameters router-id 2.2.2.2
set protocols ospf area 0 network 10.255.255.3/32
delete nat source rule 100
set nat source rule 100 outbound-interface 'eth0'
set nat source rule 100 source address '0.0.0.0/0'
set nat source rule 100 translation address 'masquerade'
commit
=====
```

Passive على كل الواجهات افتراضياً

set protocols ospf passive-interface default

OSPF حتى يرسل) فقط على الواجهات الداخلية (الغاء -passive

set protocols ospf interface eth1 passive disable

set protocols ospf interface eth2 passive disable

set protocols ospf interface eth3 passive disable

----- NAT (IP) ----- واحد فقط من الـ

set nat source rule 100 outbound-interface name eth0

set nat source rule 100 source address '192.168.1.0/24'

set nat source rule 100 translation address masquerade

----- Default route إلى الـ ISP -----

set protocols static route 0.0.0.0/0 next-hop 203.0.113.1

=====!

configure

set service snmp community librenms1 authorization ro

set service snmp contact 'admin@enterprise.local'

set service snmp location 'Datacenter'

commit

save

exit

=====!

----- إعدادات النظام (اختياري لكن مفید) -----

set system host-name VyOS1

set system domain-name enterprise.local

set service ssh

set system login user vyos authentication plaintext-password vyos

commit

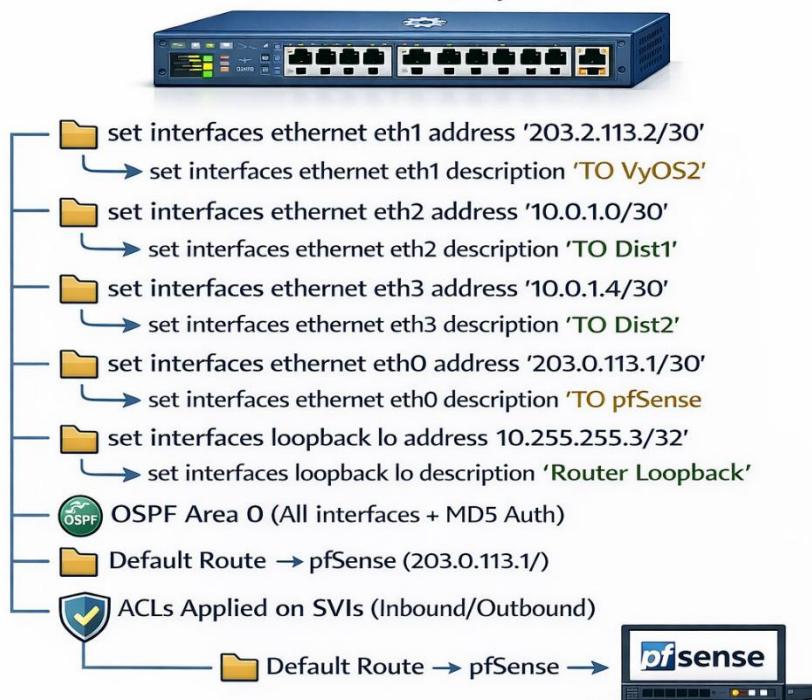
save

exit

نتائج الاختبار

- تم تحقيق تقارب OSPF عند انقطاع رابط.
- تم رفض جميع الوصول غير المصرح مثل VLAN 50 → VLAN 20
- تم التحقق من التوجيه الناجح بين الأقسام المصرح لها عبر Ping/Traceroute

Core Router (Layer 3)



شكل رقم (6) تكوين Core Router مع OSPF

7-5 إعداد الخدمات المركزية

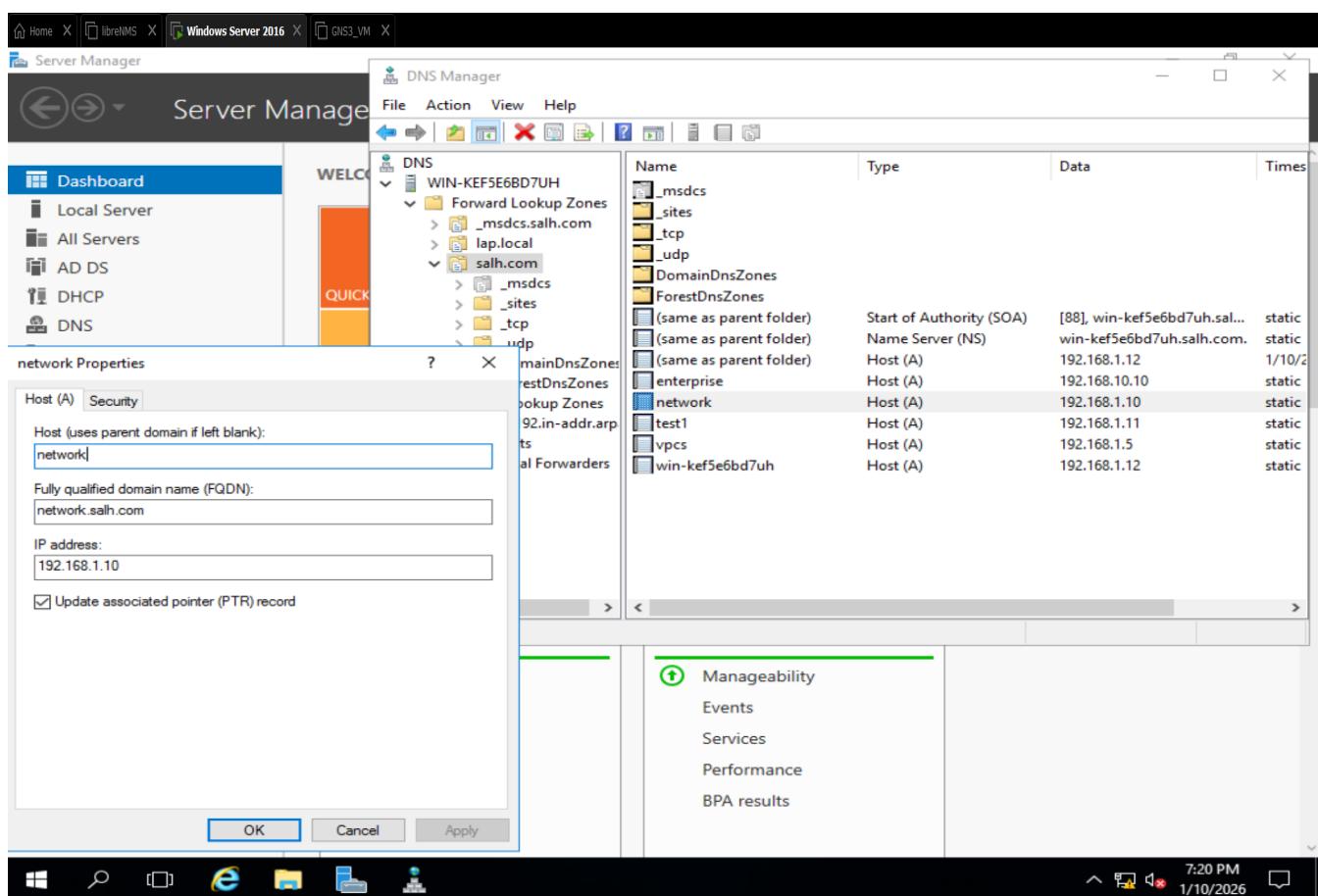
الهدف من السيرفرات المركزية

تم إعداد مجموعة من الخدمات المركزية Centralized Services على سيرفرات افتراضية في VLAN 40 (IT)، لتوفير خدمات أساسية للشبكة بأكملها، مثل DHCP، Mail، FTP، Web، DNS، و Firewall Rules، مع ضمان الأمان والتقييد الدقيق للوصول عبر ACLs و AAA على pfSense.

الخدمات المركزية وتكونيتها الرئيسي:

DNS Server .1

- البرنامج: BIND9
- IP : 192.168.1.12
- الوظيفة: تحويل الأسماء الداخلية مثل IPs داخل network.salh.com إلى IPs خارجي آمن.
- الشبكة، مع Forwarding إلى DNS خارجي آمن.
- الأمان: تقييد الاستعلامات (Allow-Query) لـ VLANs فقط.



Web Server .2

- البرنامج: Apache2
- IP : 192.168.1.10
- الوظيفة: استضافة الموقع الداخلي للمؤسسة (بوابة داخلية، مستندات مشتركة).
- الأمان: HTTPS مفعل + تقييد الوصول عبر ACLs للأقسام المصرح لها.

`sudo systemctl status apache2`

```

Terminal - salh@salh:~ 
File Edit View Terminal Tabs Help
● apache2.service - The Apache HTTP Server
  Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
  Active: active (running) since Sat 2026-01-10 15:33:26 UTC; 15min ago
    Docs: https://httpd.apache.org/docs/2.4/
   Process: 1644 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 1706 (apache2)
   Tasks: 55 (limit: 2122)
  Memory: 7.6M (peak: 7.9M)
     CPU: 250ms
    CGroup: /system.slice/apache2.service
            └─1706 /usr/sbin/apache2 -k start
              ├─1712 /usr/sbin/apache2 -k start
              ├─1713 /usr/sbin/apache2 -k start
              └─1713 /usr/sbin/apache2 -k start

Jan 10 15:33:25 salh systemd[1]: Starting apache2.service - The Apache HTTP Server...
Jan 10 15:33:26 salh apachectl[1680]: AH00558: apache2: Could not reliably determine the
Jan 10 15:33:26 salh systemd[1]: Started apache2.service - The Apache HTTP Server.

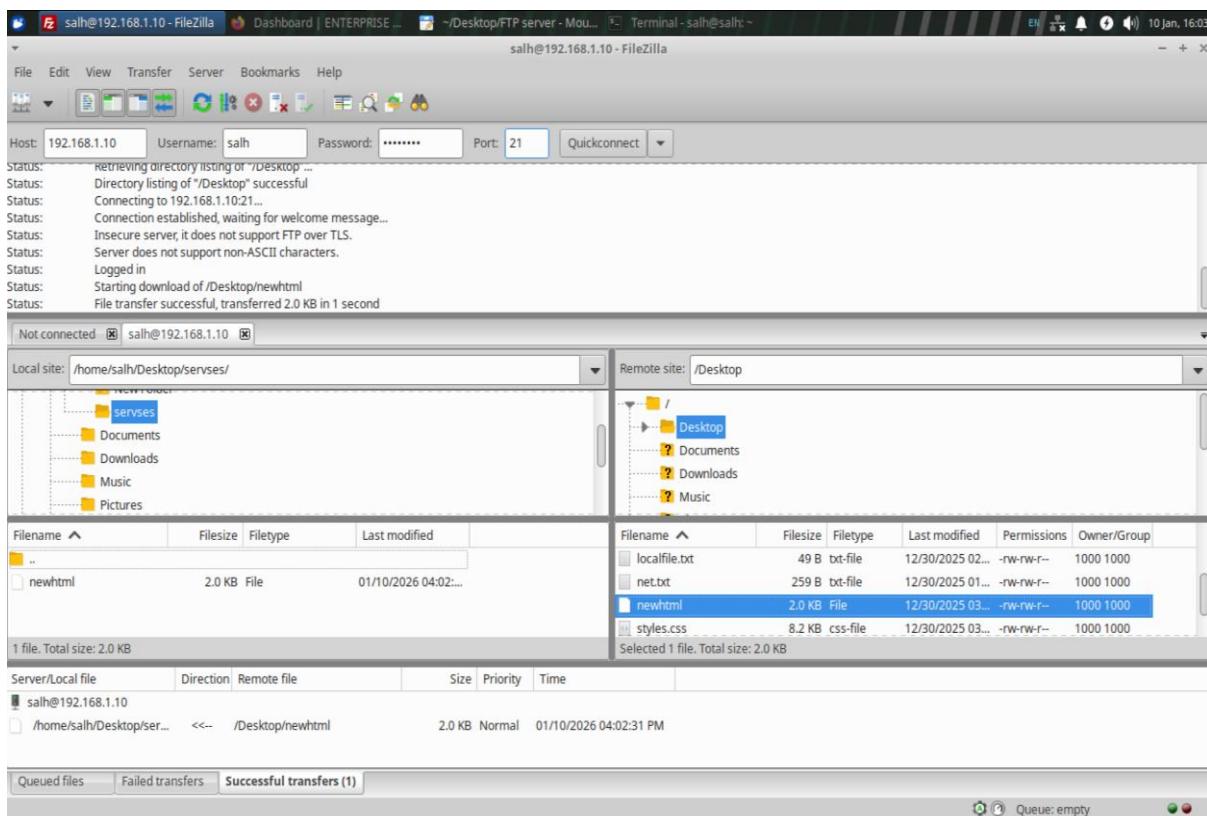
lines 1-17/17 (END)

```

FTP Server .3

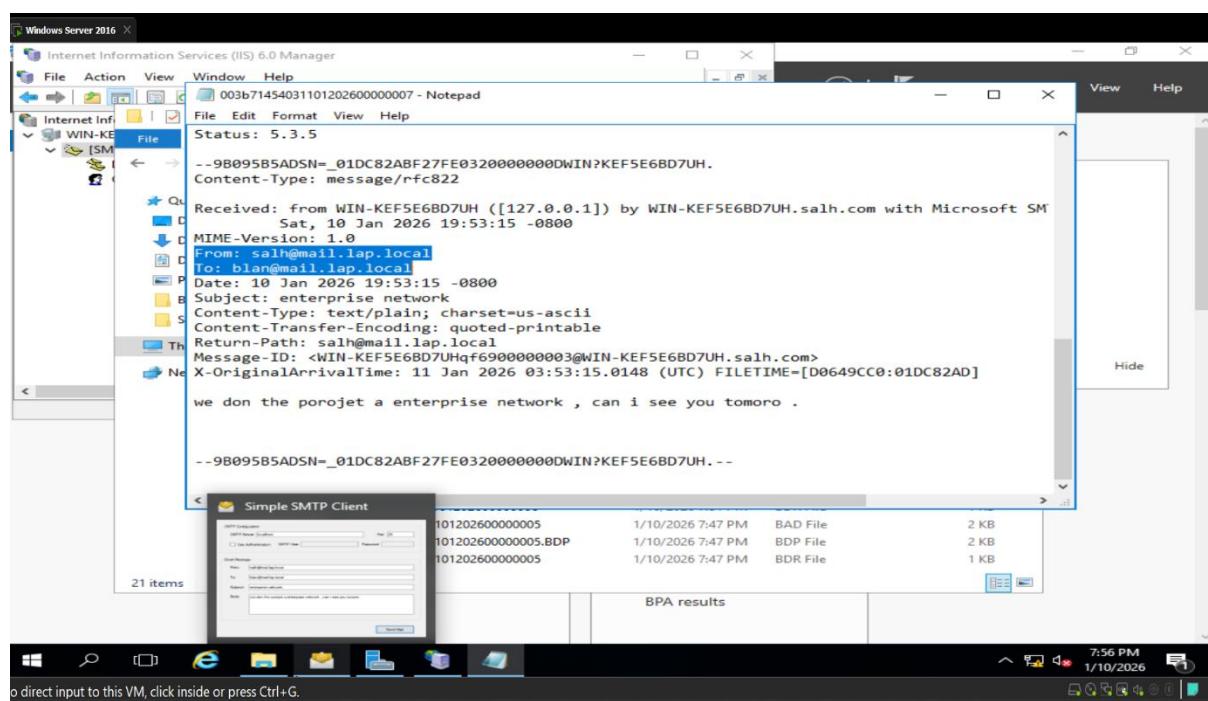
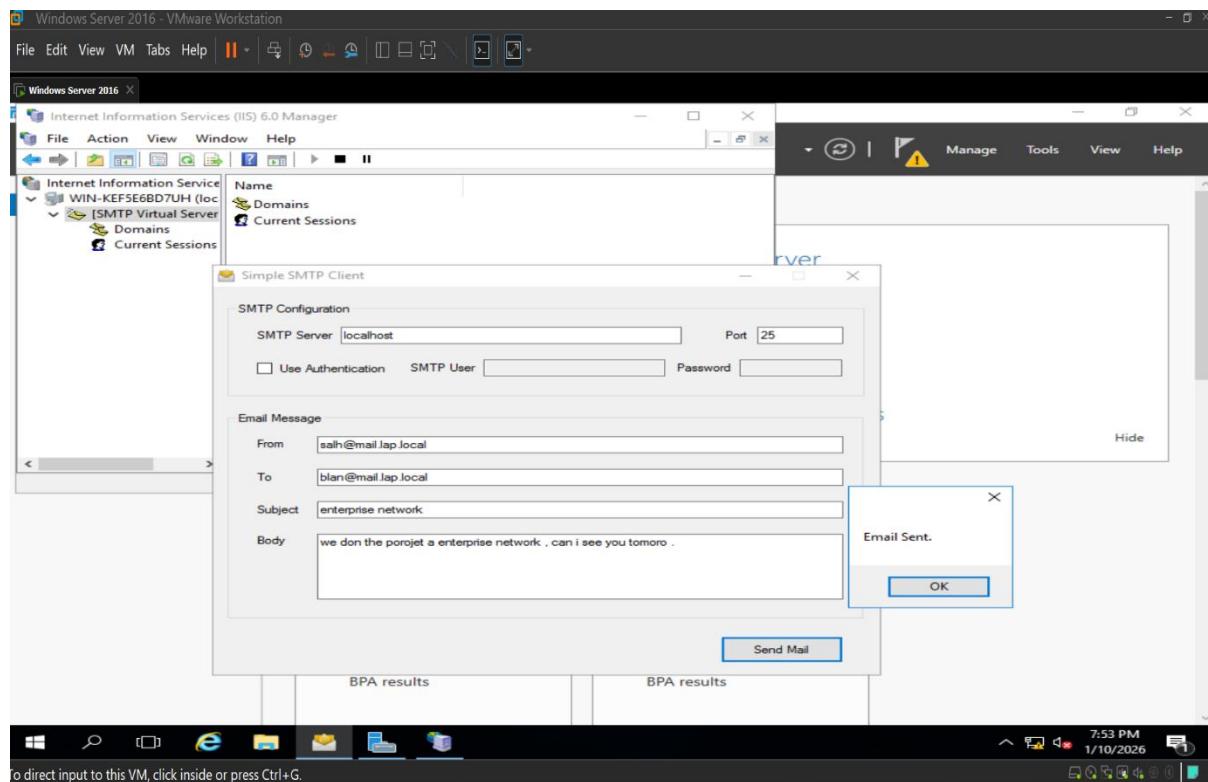
- البرنامج: vsftpd
 - IP : 192.168.1.10
 - الوظيفة: نقل الملفات بين الأقسام المصرح لها.
 - الأمان: دعم (FTP over SSL) + تقييد الوصول حسب المستخدمين.

```
sudo systemctl status vsftpd
```



Mail Server .4

- البرنامج : • Postfix (SMTP) + Dovecot (IMAP)
- 192.168.1.12 : IP
- الوظيفة: بريد إلكتروني داخلي للموظفين.



DHCP Server .5

- البرنامج: ISC-DHCP
- IP : 192.168.1.10
- الوظيفة: توزيع عناوين IP تلقائياً لكل VLAN Scopes منفصلة.
- الأمان: DHCP Snooping مفعل على السويفتس لمنع Rogue Servers .

sudo systemctl status isc-dhcp-server

```

salh@salh:~$ sudo systemctl status isc-dhcp-server
● isc-dhcp-server.service - ISC DHCP IPv4 server
  Loaded: loaded (/usr/lib/systemd/system/isc-dhcp-server.service; enabled; preset: enabled)
  Active: active (running) since Sat 2026-01-10 15:33:25 UTC; 31min ago
    Docs: man:dhcpcd(8)
   Main PID: 1615 (dhcpcd)
     Tasks: 1 (limit: 2122)
    Memory: 276.0K (peak: 5.8M swap: 3.5M swap peak: 3.5M)
      CPU: 78ms
     CGroup: /system.slice/isc-dhcp-server.service
             └─1615 dhcpcd -user dhcpcd -group dhcpcd -f -4 -pf /run/dhcp-server/dhcpcd.pid

Jan 10 15:33:25 salh dhcpcd[1615]: PID file: /run/dhcp-server/dhcpcd.pid
Jan 10 15:33:25 salh dhcpcd[1615]: Wrote 1 leases to leases file.
Jan 10 15:33:25 salh sh[1615]: Wrote 1 leases to leases file.
Jan 10 15:33:25 salh dhcpcd[1615]: Listening on LPF/ens33/00:0c:29:9f:d0:fa/192.168.1.0/28
Jan 10 15:33:25 salh sh[1615]: Listening on LPF/ens33/00:0c:29:9f:d0:fa/192.168.1.0/28
Jan 10 15:33:25 salh sh[1615]: Sending on   LPF/ens33/00:0c:29:9f:d0:fa/192.168.1.0/28
Jan 10 15:33:25 salh sh[1615]: Sending on   Socket/fallback/fallback-net
Jan 10 15:33:25 salh dhcpcd[1615]: Sending on   LPF/ens33/00:0c:29:9f:d0:fa/192.168.1.0/28
Jan 10 15:33:25 salh dhcpcd[1615]: Sending on   Socket/fallback/fallback-net
Jan 10 15:33:25 salh dhcpcd[1615]: Server starting service.
Lines 1-21/21 (END)

```

```
#}
#subnet declaration for your network vlan 10
subnet 192.168.1.0 netmask 255.255.255.240{
    range 192.168.1.4 192.168.1.8;
    option routers 192.168.1.3;
    option subnet-mask 255.255.255.240;
    option broadcast-address 192.168.1.15;
    option domain-name-servers 8.8.8.8;
}

#subnet declaration for your network vlan 20
subnet 192.168.1.16 netmask 255.255.255.240{
    range 192.168.1.20 192.168.1.28;
    option routers 192.168.1.19;
    option subnet-mask 255.255.255.240;
    option broadcast-address 192.168.1.31;
    option domain-name-servers 8.8.8.8;
}

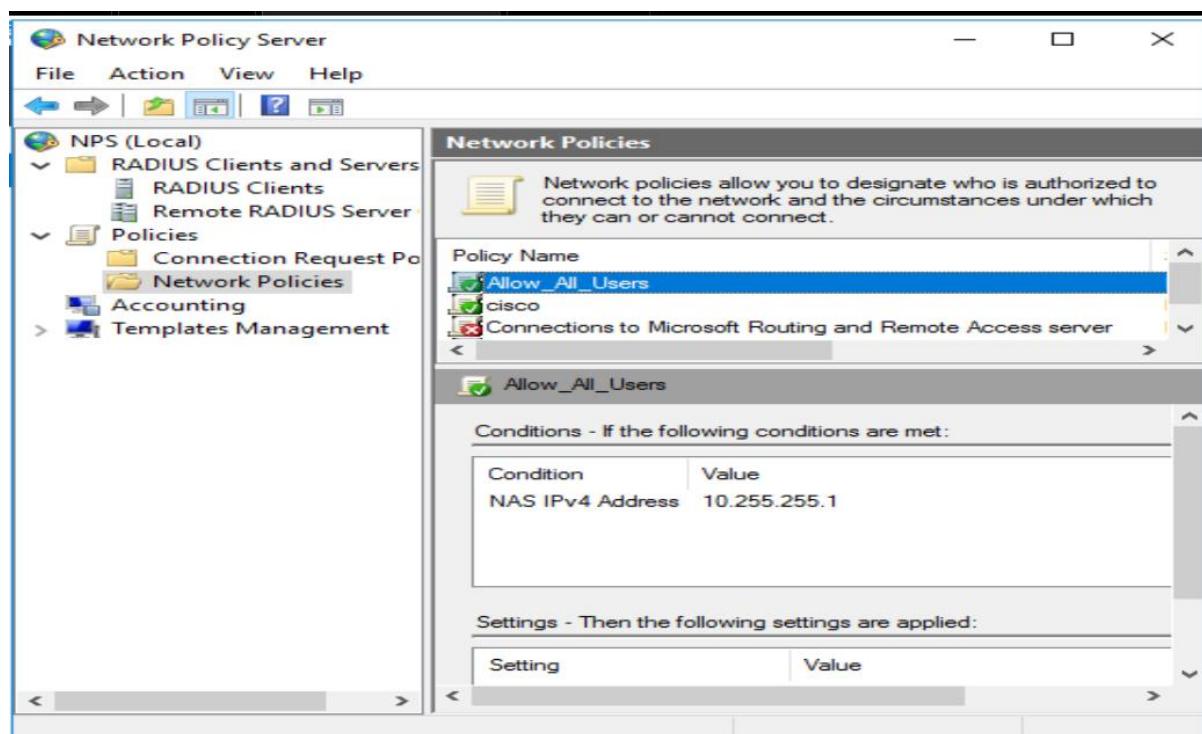
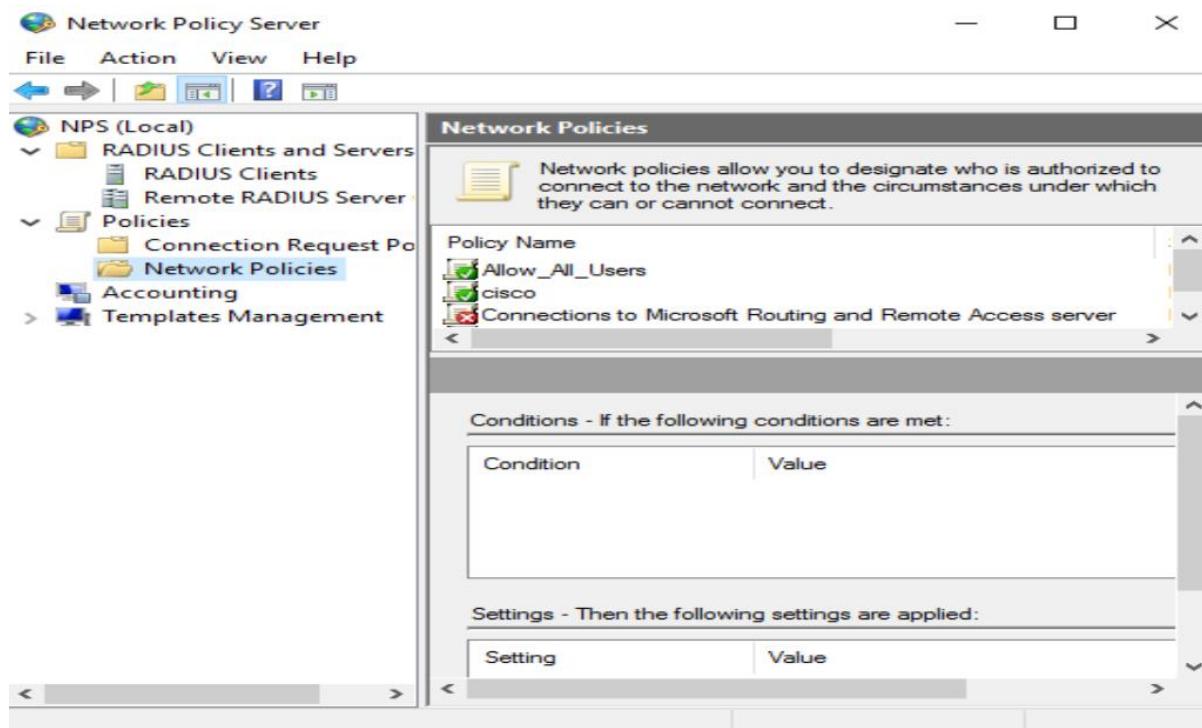
#subnet declaration for your network vlan 30
subnet 192.168.1.32 netmask 255.255.255.240{
    range 192.168.1.36 192.168.1.42;
    option routers 192.168.1.35;
    option subnet-mask 255.255.255.240;
    option broadcast-address 192.168.1.47;
    option domain-name-servers 8.8.8.8;
}

#subnet declaration for your network vlan 40
subnet 192.168.1.48 netmask 255.255.255.240{
    range 192.168.1.52 192.168.1.60;
    option routers 192.168.1.51;
    option subnet-mask 255.255.255.240;
    option broadcast-address 192.168.1.63;
    option domain-name-servers 8.8.8.8;
}

#subnet declaration for your network vlan 50
subnet 192.168.1.64 netmask 255.255.255.240{
    range 192.168.1.68 192.168.1.78;
    option routers 192.168.1.67;
    option subnet-mask 255.255.255.240;
    option broadcast-address 192.168.1.79;
    option domain-name-servers 8.8.8.8;
},
```

AAA Server .6

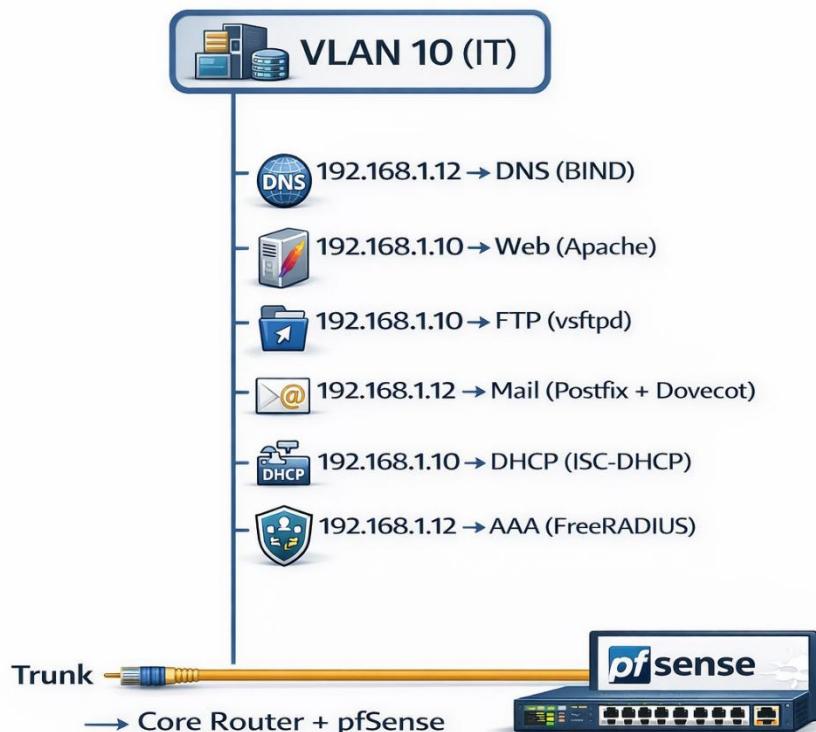
- البرنامج : FreeRADIUS
- IP : 192.168.1.12
- الوظيفة: مصادقة وتفويض وتسجيل مرکزي 802.1X إن أمكن.
- الأمان: RADIUS سياسات وصول دقيقة.



الخدمة	IP السيرفر	البرنامج	المنافذ الرئيسية	الأقسام المصرح لها بالوصول	الأمان الرئيسي
DNS	192.168.1.12	BIND9	UDP/TCP 53	جميع الأقسام الداخلية	Allow-Query + No Recursion
Web	192.168.1.10	2Apache	TCP 80, 443	Management, Finance, HR, IT	HTTPS + ACLs
FTP	192.168.1.10	vsftpd	TCP 21, 20	Finance, HR, IT محدود	FTPS + User Authentication
Mail	192.168.1.12	Postfix + Dovecot	587TCP 25,	جميع الأقسام الداخلية	TLS + SPF/DKIM
DHCP	192.168.1.10	ISC-DHCP	UDP 67, 68	جميع VLANs تلقائي	DHCP Snooping مفعل
AAA	192.168.1.12	FreeRADIUS	UDP 1812, 1813	+ pfSense السوينتشات مصادقة	RADIUS over TLS

ملاحظات إضافية

- سوف يتم العمل على تم تفعيل التشفير HTTPS ، FTPS ، IMAPS على جميع الخدمات في حال طلب المؤسسة ذلك .
- تم تقييد الوصول عبر ACLs على pfSense كما في جدول رقم 6.
- تم اختبار الخدمات بنجاح من أجهزة مختلفة في كل VLAN .
- جميع التكوينات مؤكدة مع نسخ احتياطي يومي.



شكل رقم (7) موقع السيرفرات المركزية في – VLAN IT –

8-5 إعداد جدار الحماية

الهدف من إعداد جدار الحماية

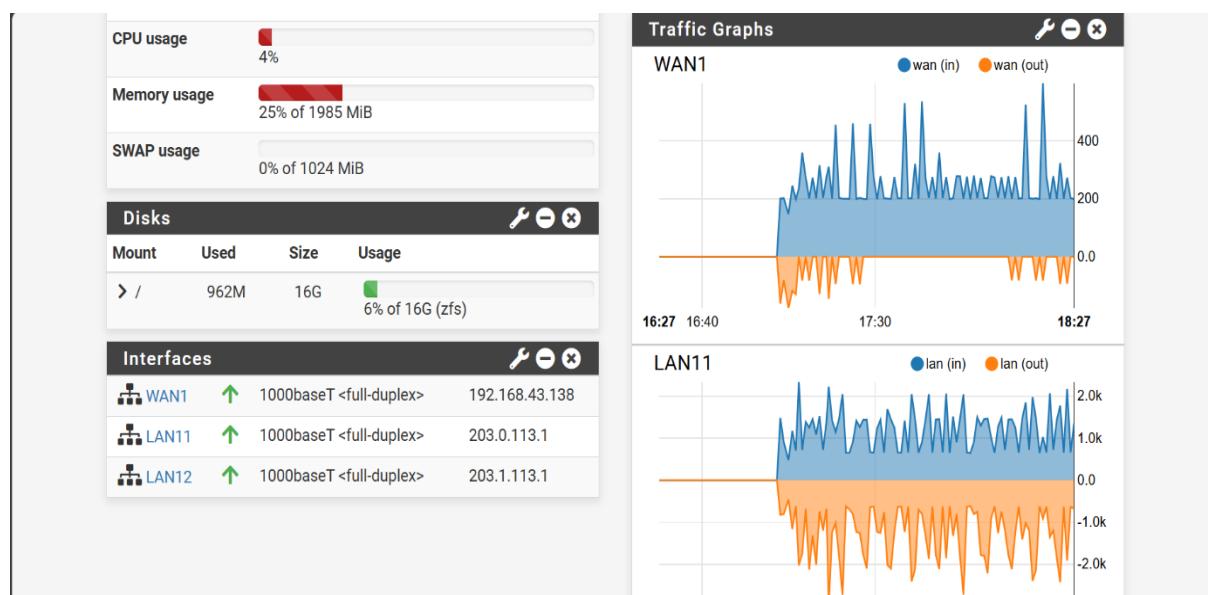
يُعد جدار الحماية (Firewall) العنصر الأساسي للتحكم في حركة المرور الداخلية والخارجية، ويتم تنفيذه عبر كجهاز افتراضي في GNS3 يهدف إلى:

- توفير NAT للوصول إلى الإنترنэт المحاكي.
- تطبيق قواعد Firewall Rules لمنع الوصول غير المصرح.
- دعم (OpenVPN) للوصول الآمن عن بعد.
- دمج IDS/IPS كنظام Snort/Zeek لكشف الهجمات.

الإجراءات الرئيسية التي تم تنفيذها:

1. تثبيت وتكوين pfSense

- تثبيت pfSense ك VM في VMware مع واجهتين:
 - . (Cloud node) WAN : متصلة بالإنترنэт المحاكي
 - . 203.0.113.1/24: Core Router1 LAN1 : متصلة بالـ
 - . 203.1.113.1/24: Core Router2 LAN2 : متصلة بالـ
 - . إعداد DHCP Client ك WAN
 - . إعداد LAN ك Static IP (203.0.113.1/24) لشبكة الداخلية.



The screenshot shows the pfSense Status / Dashboard interface. On the left, there's a 'System Information' panel with details like Name (pfSense-1.enterprise.local), User (admin@203.0.113.100), System (VMware Virtual Machine, Netgate Device ID: b67bd6135406deda138b), BIOS (Vendor: Phoenix Technologies LTD, Version: 6.00, Release Date: Thu Nov 12 2020), Version (2.7.2-RELEASE (amd64)), CPU Type (11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz, 2 CPUs: 2 package(s) x 1 core(s), AES-NI CPU Crypto: Yes (inactive), QAT Crypto: No), and a note about unable to check for updates. On the right, there's a 'Netgate Services And Support' panel with contract type options (Community Support, Community Support Only) and a section about NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES. It explains that if purchased from Netgate, users have access to various community support resources, including the NETGATE RESOURCE LIBRARY. It also mentions the Global Technical Assistance Center (TAC) Support subscription.

2. تكوين NAT (Outbound)

- تفعيل Outbound NAT لتحويل عناوين الشبكة الداخلية إلى عنوان WAN عند الخروج إلى الإنترنت.

The screenshot shows the pfSense Firewall / NAT / Port Forward configuration page. At the top, there's a message stating "The NAT configuration has been changed. The changes must be applied for them to take effect." with a green "Apply Changes" button. Below this, there are tabs for Port Forward, 1:1, Outbound, and NPT. A red horizontal bar highlights the Outbound tab. Under the Outbound tab, there's a 'Rules' section with a table showing one rule. The rule details are: Interface: WAN1, Protocol: ANY, Source Address: *, Destination Address: WAN1 address, Destination Ports: *, NAT IP: 192.168.1.10, NAT Ports: *, Description: nat. Below the table are action buttons for Add, Delete, Toggle, Save, and Separator.

3. تكوين Firewall Rules

- تفعيل Anti-Lockout Rule لواجهة pfSense إلى واجهة LAN Interface.
- تكوين Rules على السماح بالوصول الداخلي والإنترنت مع تقييد VLANs.
- تكوين Rules على WAN Interface لمنع الهجمات الخارجية مثل Networks.
- تفعيل Logging لكل قاعدة محظورة.

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

Floating WAN1 LAN11 LAN12

Rules (Drag to Change Order)											
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
X 0/952 B	*	RFC 1918 networks	*	*	*	*	*	*	Block private networks		
X 0/4 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks		
<input checked="" type="checkbox"/> 0/0 B	IPv4 ANY	*	*	192.168.1.10	*	*	none		NAT nat		

Add Add Delete Toggle Copy Save Separator

Firewall / Rules / LAN11

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

Floating WAN1 LAN11 LAN12

Rules (Drag to Change Order)											
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
✓ 28/493 KiB	*	*	*	LAN11 Address	80	*	*	*	Anti-Lockout Rule		
<input checked="" type="checkbox"/> 0/0 B	IPv4 *	LAN11 subnets	*	*	*	*	none		Default allow LAN to any rule		
<input checked="" type="checkbox"/> 0/0 B	IPv6 *	LAN11 subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule		

Add Add Delete Toggle Copy Save Separator

4. دمج IDS/IPS ك Snort

- تثبيت Snort Package على pfSense.
- تفعيل Snort على واجهة LAN و WAN.
- تحميل قواعد Emerging Threats و Snort VRT.
- تفعيل IPS Mode (Inline) للحظر التلقائي للهجمات المكتشفة.

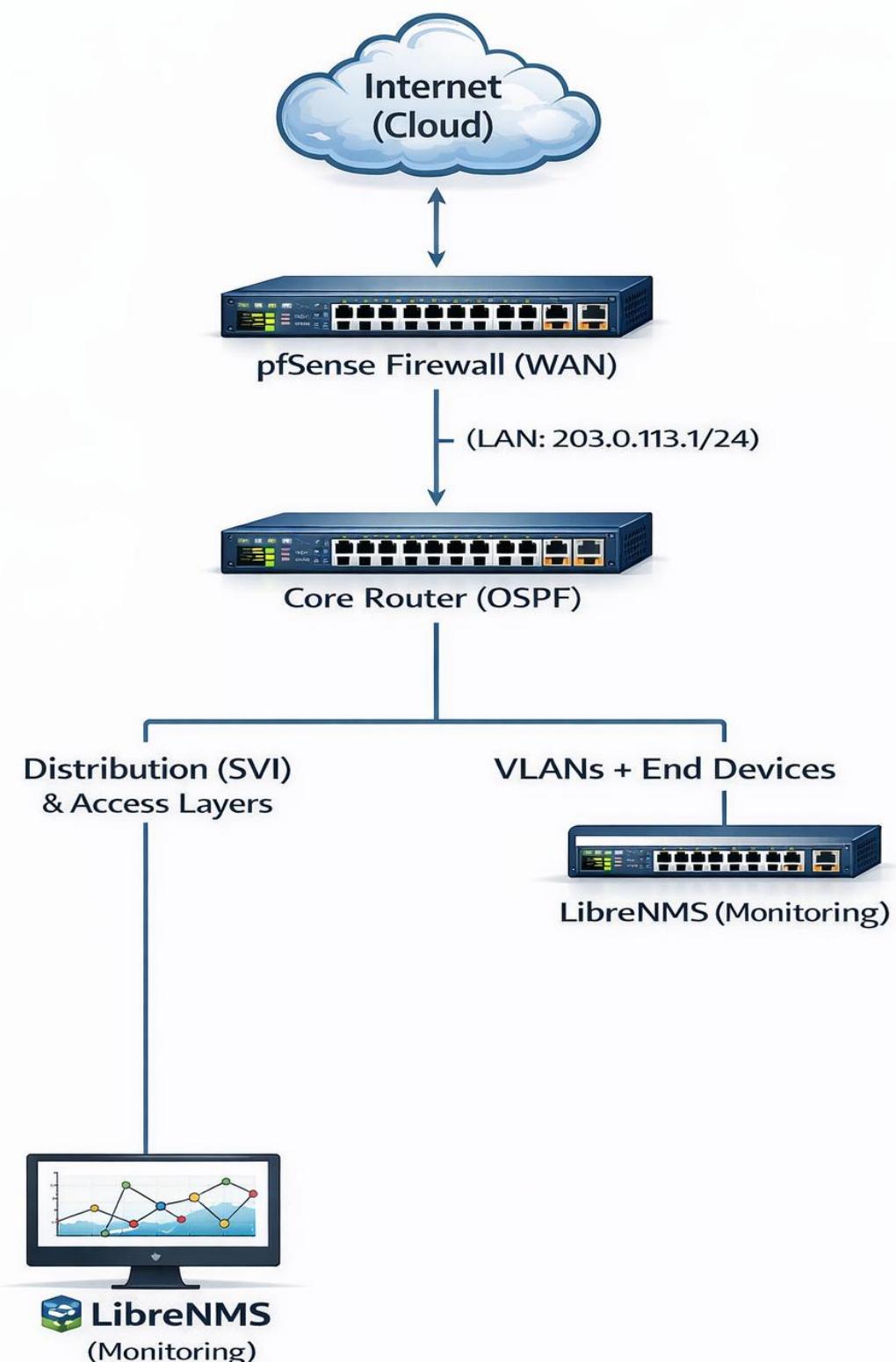
الترتيب	Action	Interface	Protocol	Source	Destination	Port	Description
1	Pass	LAN	Any	Any	Any	Any	Allow LAN to Any
2	Pass	LAN	TCP	VLAN 10-40	192.168.1.10	80,443	Allow Web Server Access
3	Pass	LAN	UDP/TC P	Any Internal	192.168.1.12	53	Allow DNS Access
4	Block	LAN	Any	VLAN 50 (Guest)	Any Internal	Any	Block Guest to Internal Networks
5	Block	WAN	Any	Any	This Firewall	Any	Block External to pfSense

جدول رقم (8) أمثلة على Firewall Rules (Firewall Rules على الرئيسية LAN Interface) pfSense

نتائج الاختبار

تم رفض جميع الوصول غير المصرح مثل Guest → Finance مع تسجيل في Firewall Logs .

- تم كشف وحظر هجمات محاكاة DoS ، Port Scanning عبر Snort مع تطبيقات LibreNMS في.
- تم الاتصال الناجح عبر OpenVPN من جهاز خارجي مع الوصول الآمن إلى الخدمات الداخلية.



شكل رقم (8) موقع pfSense في الطبولوجيا

9-5 إعداد الأجهزة النهائية

الهدف من إعداد الأجهزة النهائية

تمثل الأجهزة النهائية (End Devices) المستخدمين الفعليين في الشبكة PCs ، وتهدف هذه الخطوة إلى:

- محاكاة سيناريوهات الاستخدام اليومي لكل قسم.
- التحقق من صحة تخصيص IP، الوصول إلى الخدمات، والعزل بين VLANs.
- اختبار الأمان والأداء من وجهة نظر المستخدم النهائي.

الإجراءات الرئيسية التي تم تنفيذها:

1. إنشاء الأجهزة النهائية في GNS3

- تم إضافة PC افتراضي VM QEMU أو VPCS في كل VLAN.
- عدد الأجهزة: 4-2 PC لكل قسم Guest، IT، HR، Finance، Management.
- تكوين كل PC للحصول على IP تلقائياً عبر DHCP.

2. تكوين الأجهزة النهائية

- تم تعيين كل PC على منفذ Access في السويفتش المخصص لقسمه.
- تم التتحقق من الحصول على IP صحيح من DHCP Server كما في جدول رقم 4.
- تم ضبط DNS Server على 192.168.1.12 لكل PC للوصول إلى الخدمات الداخلية.

3. اختبار الاتصال والوصول

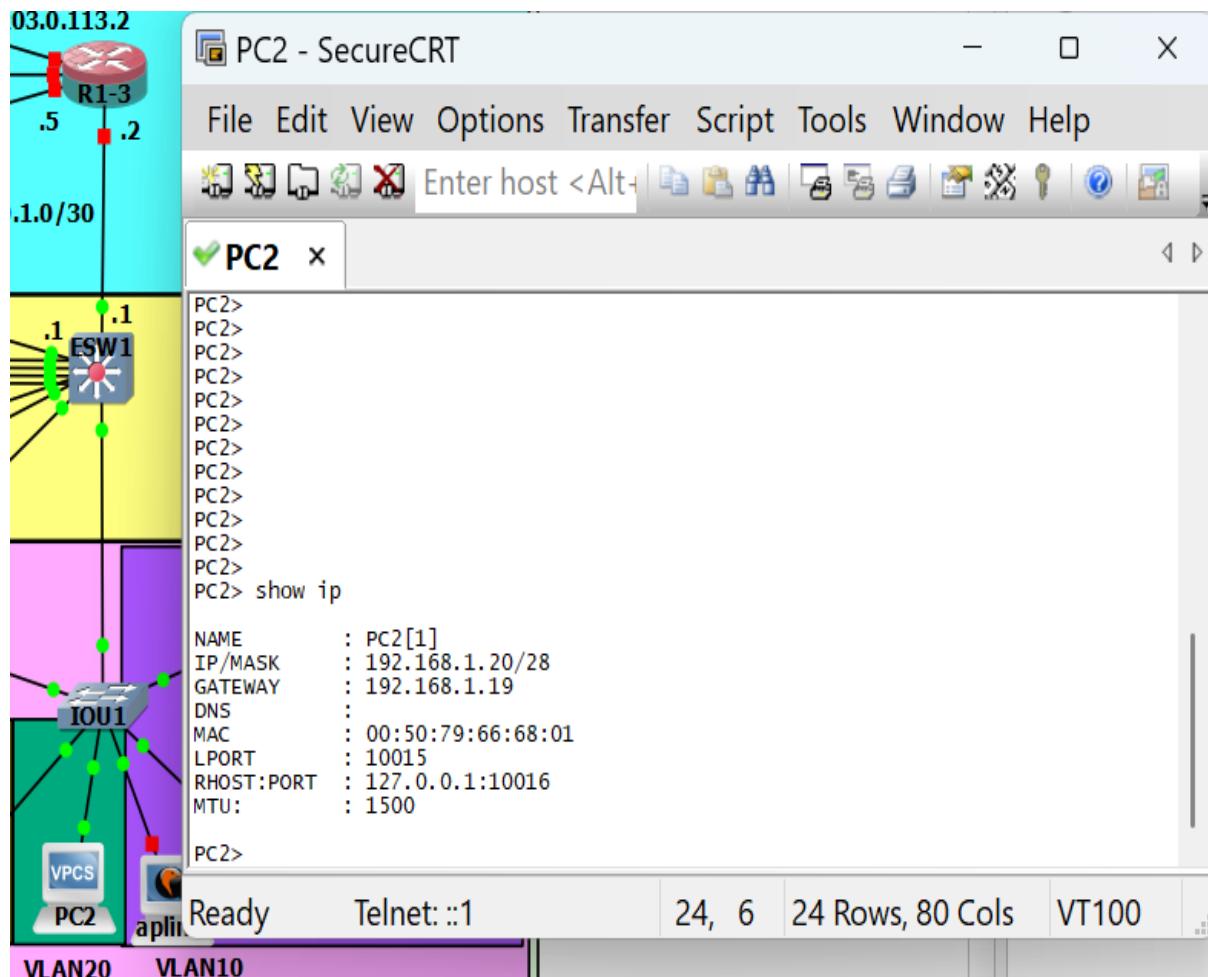
- اختبار Ping و Traceroute داخل VLAN نجاح 100%.
- اختبار Inter-VLAN Routing للأقسام المصرح لها فقط.
- الإنترنэт المحاكي (pfSense) على NAT Cloud.
- اختبار رفض الوصول غير المصرح.

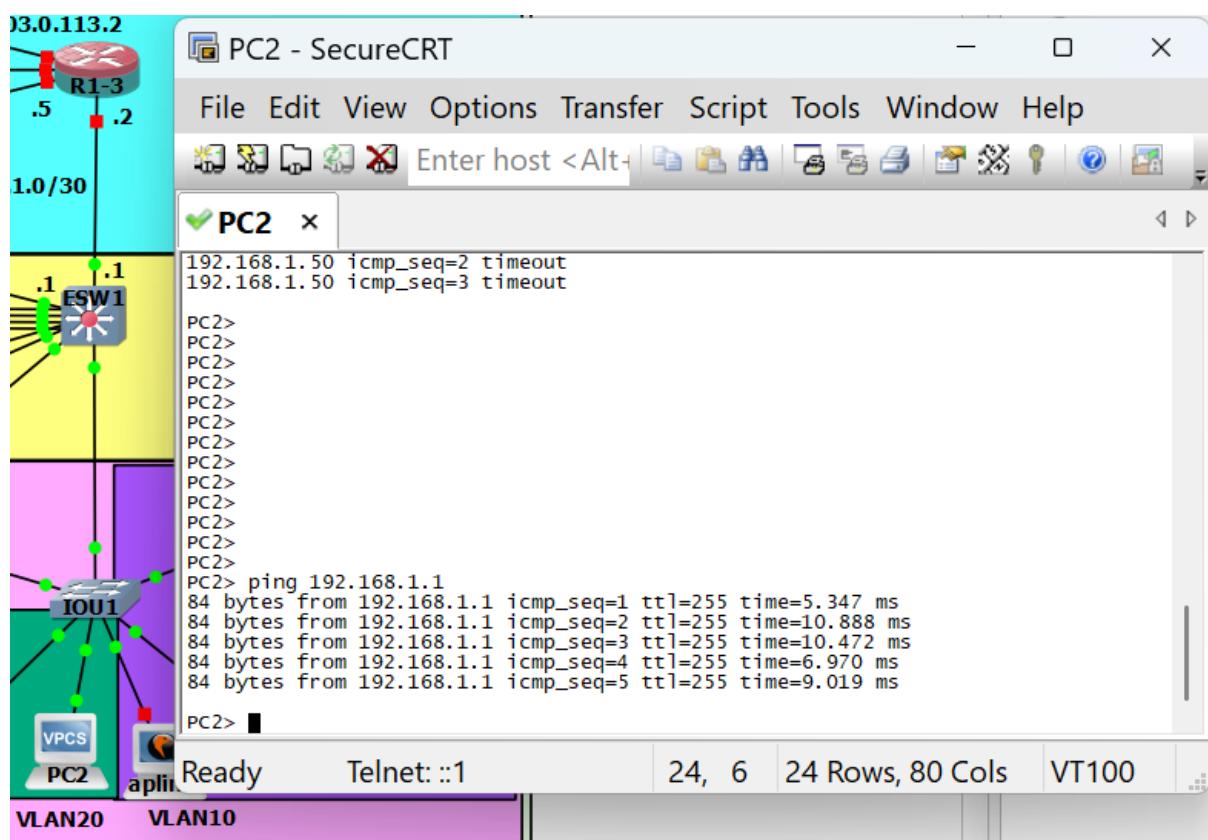
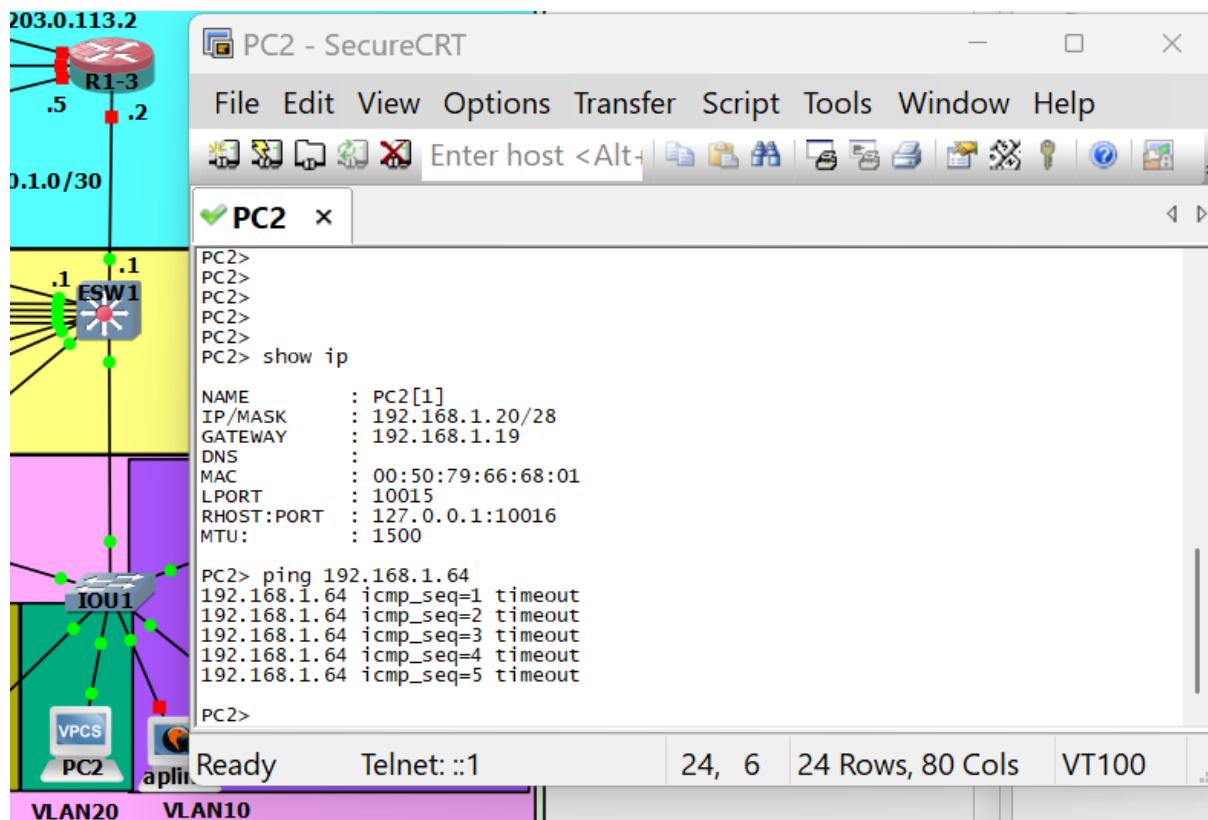
4. اختبار الأمان من وجهة الجهاز النهائي

- محاولة ARP Spoofing من PC في VLAN 50 فشل بفضل DAI.
- محاولة DHCP Snooping → فشل بفضل Rogue DHCP.
- محاولة Port Security Violation → تعطيل المنفذ + تتبیه في LibreNMS.

VLAN	IP PC	Ping إلى Gateway	Web إلى Ping Server (192.168.1.10)	Ping إلى Guest VLAN	Ping إلى الإنترنت (8.8.8.8)	النتيجة
10	192.168.1.5	ناجح	ناجح	ناجح	ناجح	ناجح
20	192.168.1.25	ناجح	ناجح	محظور	ناجح	ناجح
30	192.168.1.35	ناجح	ناجح	محظور	ناجح	ناجح
40	192.168.1.45	ناجح	ناجح	محظور	ناجح	ناجح
50	192.168.1.70	ناجح	محظور	ناجح	ناجح	ناجح (محدود)

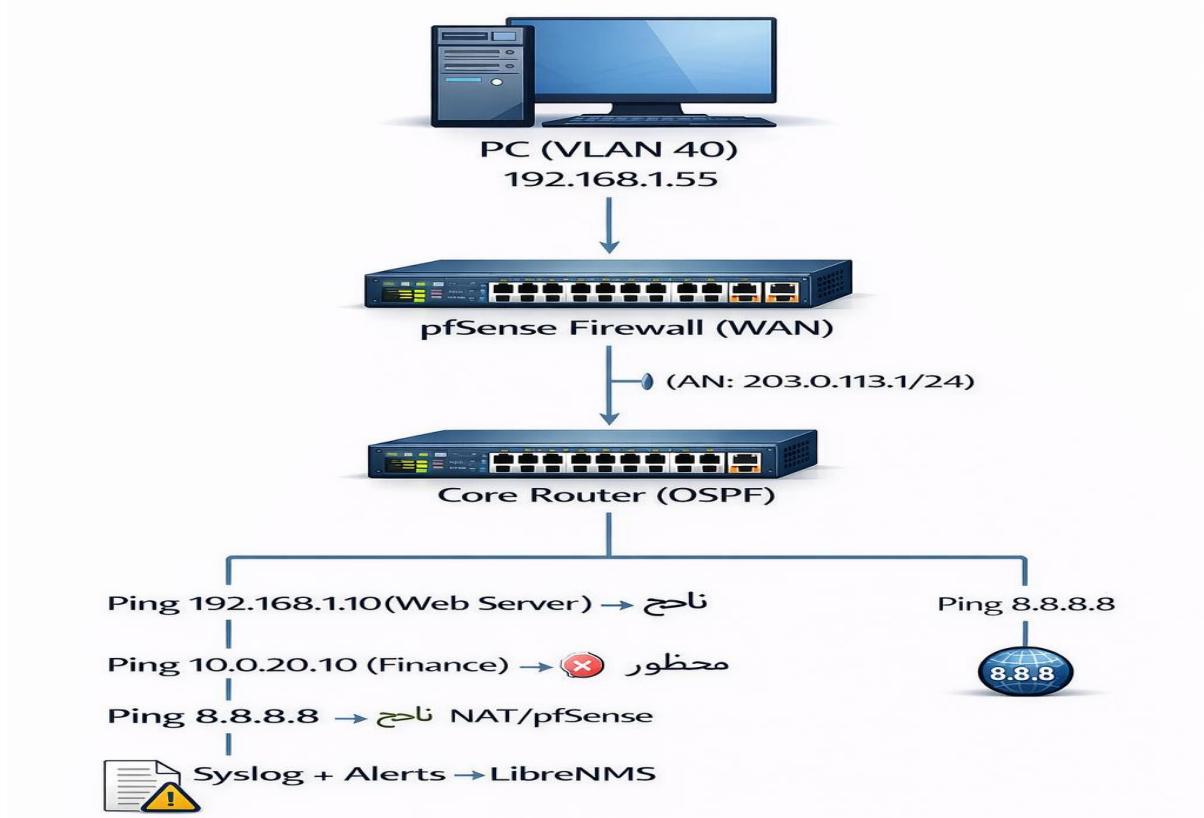
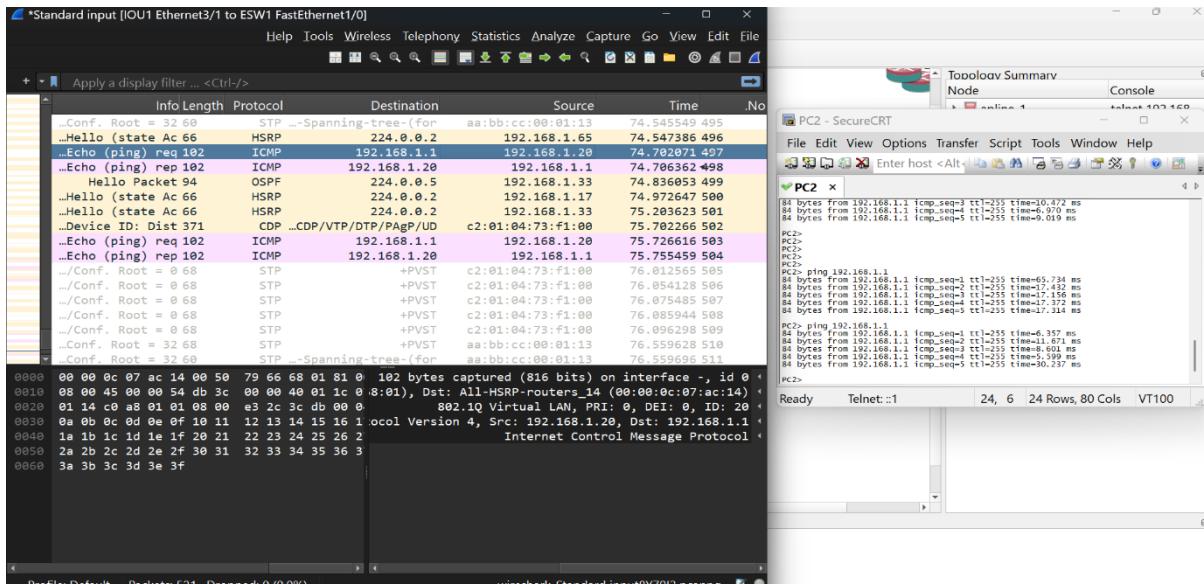
جدول رقم (9) نتائج اختبار الاتصال من الأجهزة النهائية (مثال)





ملاحظات إضافية

- تم استخدام VPCS أو Linux كأجهزة نهائية خفيفة لنقل إستهلاك الموارد.
- تم اختبار الوصول من أنظمة تشغيل مختلفة Linux ، Windows لضمان التوافق.
- جميع النتائج تم توثيقها مع تسجيلات Syslog وتطبيقات LibreNMS



شكل رقم (9) اختبار الاتصال من PC في VLAN - رسم نصي

VMware 10-5 إعداد

الهدف من إعداد VMware

استخدم VMware Workstation Player (إصدار 16 أو أحدث) لتشغيل الأجهزة الافتراضية الرئيسية، السيرفرات المركزية داخل بيئة GNS3 ، لأن GNS3 يدعم تشغيل VMs حقيقة عبر VirtualBox أو QEMU . التحقيق أداء وواقعية أعلى مقارنة ب VMware

الإجراءات الرئيسية التي تم تنفيذها:

1. تثبيت وتهيئة VMware Workstation Player

- تثبيت البرنامج على جهاز الكمبيوتر المضيف (Host).
- تفعيل BIOS (VT-x/AMD-V) في Virtualization.
- إنشاء VMs مخصص للربط بين GNS3 و Virtual Network (VMnet).

2. إنشاء الأجهزة الافتراضية الرئيسية

pfSense VM •

- نظام تشغيل: FreeBSD
- RAM: 2 GB
- CPU: 2 Cores
- Disk: 20 GB
- واجهات شبكة: 3 (WAN + LAN1+LAN2) موصولة ب GNS3 .Vmnet

LibreNMS VM •

- نظام تشغيل: Ubuntu Server 22.04 LTS
- RAM: 2 GB
- CPU: 2 Cores
- Disk: 40 GB
- واجهة شبكة: 1 (IT VLAN) موصولة ب GNS3 .

Central Servers VM •

- | | |
|---|---|
| <u>Ubuntu Server 22.04 LTS</u> | ▪ |
| ▪ نظام تشغيل: Ubuntu Server 22.04 LTS | ▪ |
| ▪ RAM: 2 GB | ▪ |
| ▪ CPU: 4 Cores | ▪ |
| ▪ Disk: 60 GB | ▪ |
| ▪ واجهة شبكة: 1 (IT VLAN) موصولة ب Microsoft.Windows.Server.2016.Datacenter . | ▪ |
| <u>Microsoft.Windows.Server.2016.Datacenter</u> | ▪ |
| ▪ نظام تشغيل: Microsoft.Windows.Server.2016.Datacenter | ▪ |
| ▪ RAM: 2 GB | ▪ |
| ▪ CPU: 2 Cores | ▪ |
| ▪ Disk: 60 GB | ▪ |
| ▪ واجهة شبكة: 1 (IT VLAN) موصولة ب . | ▪ |

3. ربط GNS3 مع VMware

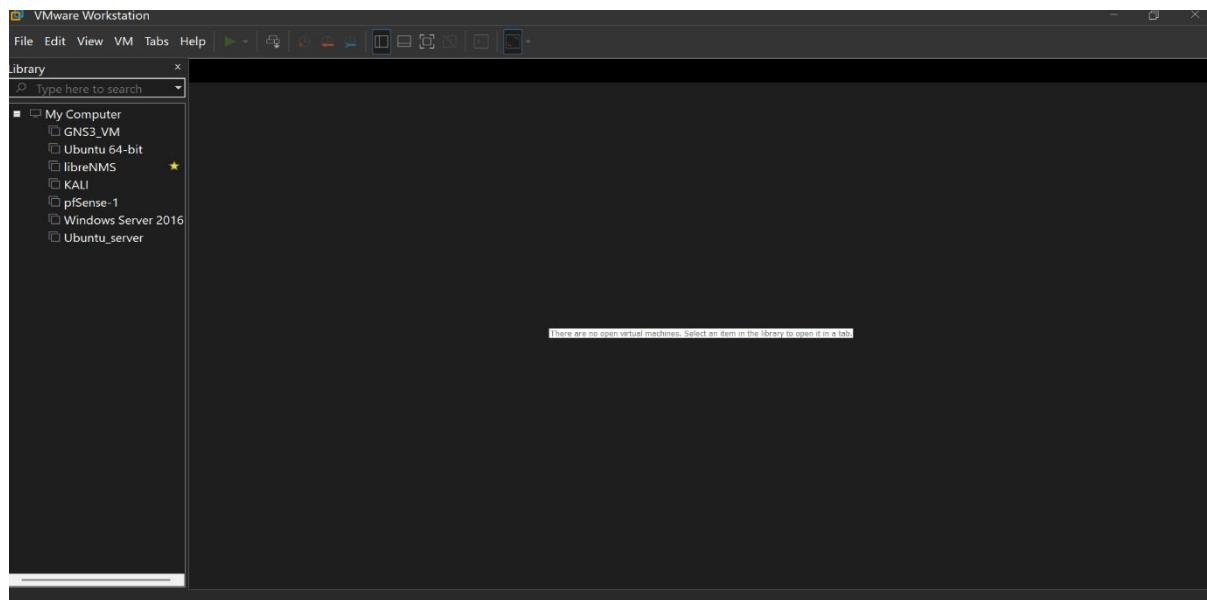
- VMware VM Connector في إضافة GNS3.
- ربط واجهات pfSense WAN بـ Cloud node إنترنت محاكي.
- ربط واجهة Core Router بـ LAN.
- ربط VLAN 10 بـ Central Servers و LibreNMS.

4. اختبار الربط والأداء

- التحقق من الاتصال بين pfSense و GNS3 من VMs Ping إلى Core Router.
- التتحقق من استهلاك الموارد (CPU/RAM) أثناء تشغيل كل VMs.
- التتحقق من استقرار النظام تحت حمل عدة PCs + محاكاة حركة مرور.

المكون	الحد الأدنى	الموصى به (للأداء الأمثل)	ملاحظات
(CPU) المعالج	Intel i5 / Ryzen 5 (4 أنوية)	Intel i7/i9 / Ryzen 7+ (8+ أنوية)	يجب تفعيل BIOS في VT-x/AMD-V
(RAM) الذاكرة	16 GB	32 أو أكثر GB	تخصيص VMs (pfSense + LibreNMS + Servers) 16-12 GB
التخزين	256 GB SSD	أو أكثر 512 GB NVMe SSD	سرعة SSD ضرورية لأداء VMs
نظام التشغيل (Host)	Linux أو Windows 10/11 Ubuntu 22.04	Windows 11 Pro / Ubuntu 24.04 LTS	VMware Player مجاني على كلا النظمين
بطاقة الشبكة	محول شبكة واحد	+ VMnet أو أكثر	لربط GNS3 مع VMs

جدول رقم (10) متطلبات النظام لتشغيل GNS3 و VMware مع الأجهزة الافتراضية



توضيح الصور الأجهزة الافتراضية المنصبة ضمن VMware

pfSense-CE-2.7.2-RELEASE-amd64.iso

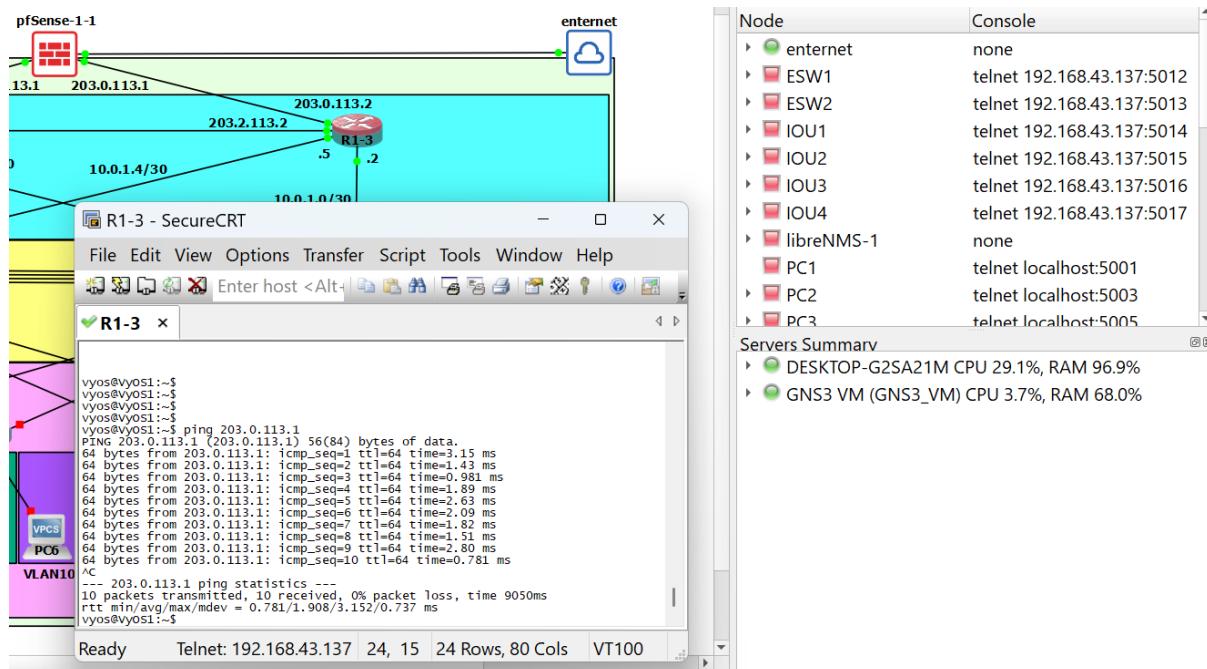
ubuntu-24.04.3-live-server-amd64.iso

VMware-workstation-full-16.2.3-19376536.exe

Microsoft.Windows.Server.2016.Datacenter.iso

librenms-ubuntu-22.04-amd64-vmware.ova

GNS3 VM.ova أصدار 2.2.53



لقطة Ping ناجح من pfSense VM إلى Core Router بعد وصف الاختبار . أثناء التشغيل (CPU/RAM usage) و Resource Monitor

ملاحظات إضافية

- تم تخصيص الموارد لكل VM لتجنب التباطؤ مثل pfSense 2 GB RAM . Central Servers 4 GB) ، LibreNMS 2 GB
- تم استخدام VMnet Host-only للربط الآمن بين GNS3 و VMware .
- تم اختبار الاستقرار بتشغيل 5 PCs + محاكاة حركة مرور دون انهيار.

LibreNMS 11-5 إعداد

الهدف من إعداد LibreNMS هو نظام مراقبة الشبكة المركزي

(Network Management System - NMS) المستخدم في المشروع لتحقيق الرؤية الشاملة على جميع الأجهزة، جمع السجلات(Syslog) ، رسم خرائط الطيولوجيا تلقائياً، إصدار تنبهات فورية عند الأعطال أو الهجمات، وتحليل الأداء، RAM ، CPU ، Bandwidth لكل جهاز. يُعد LibreNMS العمود الفقري للمراقبة المستمرة والكشف المبكر، مما يقلل وقت الاستجابة للأحداث الحرجة.

الإجراءات الرئيسية التي تم تنفيذها:

1. استيراد LibreNMS VM

- تم استيراد الإصدار الرسمي من موقع [librenms-ubuntu-22.04-amd64-vmware.ova](#)
- إلى VMware Workstation Player
- تم تعديل إعدادات الـ VM لتناسب المشروع:
- RAM: 4 GB موصى به 8 GB للأداء الأفضل مع عدد كبير من الأجهزة.
- CPU: 2-4 أنيوية.
- Disk: 40 GB (SSD)
- Network Adapter: VMnet2 (Host-only) .GNS3 Bridged أو Network Adapter: VMnet2 (Host-only) للربط مع GNS3.

2. تهيئة الشبكة داخل الـ VM

- تسجيل الدخول الافتراضي (user: librenms / pass: librenms أو حسب الإصدار).
- تغيير كلمة المرور فوراً.
- تعين VLAN 11 Static IP 192.168.1.11 داخل (IT) .VLAN 10 داخلاً (Default Gateway 192.168.1.3 DNS Server 1 DNS 192.168.1.12).

3. تكوين LibreNMS داخل الـ VM

- تشغيل الـ VM وفتح المتصفح على <http://192.168.1.11>.
- إكمال الـ Setup Wizard: إنشاء حساب Admin ، إعداد Database (MariaDB) ، Community Edition .
- تثبيت الـ Dependencies (إن لم يكن) عبر الأوامر التلقائية في الـ VM.
- تفعيل LibreNMS داخل Syslog Server لجمع السجلات من كل الأجهزة.

4. ربط LibreNMS مع الأجهزة في GNS3

- إضافة Core Router ، pfSense ، السويبتشات، والسيرفرات ك Devices في LibreNMS.
- تكوين SNMP Community String librenms1 مثل SNMP Community String على جميع الأجهزة.
- تفعيل Syslog على Core Router و pfSense لإرسال السجلات إلى 192.168.1.11 .
- اكتشاف تلقائي للطيولوجيا (Auto-Discovery) ورسم الخريطة.

الإعداد	القيمة المطبقة	الغرض
IP السيرفر	10.0.40.70/24	عنوان VLAN 40 داخل LibreNMS
SNMP Community	public (أو مخصص)	جمع البيانات من الأجهزة
Syslog Server Port	UDP 514	استقبال السجلات من Switches و pfSense
Alert Rules	CPU > 90%, Device Down	تنبيهات فورية للأعطال والتهديدات
Discovery Interval	5 دقائق	اكتشاف تلقائي للأجهزة الجديدة

جدول رقم (11) إعدادات LibreNMS الرئيسية

نتائج الاختبار

- تم اكتشاف جميع الأجهزة تلقائياً Servers، Switches، Core Router، pfSense.
- تم جمع Syslog من كل جهاز مع عرض التنبيهات فور حدوث Port Security Violation.
- تم رسم خريطة الطبولوجيا الدقيقة مع إحصائيات الأداء Memory، CPU، Traffic لكل جهاز.

This screenshot shows the LibreNMS interface for managing network alerts. The top navigation bar includes links for Overview, Devices, Services, Ports, Health, Routing, and Alerts. The Alerts section displays four entries, each with a timestamp, rule name, hostname, location, and status indicators (ACKed or not). The alert details show that four devices (10.255.255.1, 10.255.255.4, 10.255.255.2, 10.255.255.3) have been marked as down due to no ICMP response.

This screenshot shows the LibreNMS interface for a specific device, identified as a Cisco 3700 router running version 12.4(15)T14. The left sidebar lists various monitoring tabs: Overview, Graphs, Health, Ports, VLANs, Routing, Neighbours, Inventory, Logs, Alerts, Alert Stats, Latency, and Notes. The main content area displays the device's system information and a graph of processor usage over time. The processor usage graph shows a single core at approximately 3% utilization.

This screenshot shows the LibreNMS interface for monitoring network traffic and system resources. The top navigation bar is identical to the previous screenshots. The main content area features several performance graphs: Overall Traffic (showing traffic levels for multiple interfaces), Memory (showing memory usage for the chassis), Processor (showing processor usage for Processor 1), and Storage (showing storage usage for flash). The memory and processor graphs include detailed breakdowns for individual components like Fa0/0, Fa1/0, etc.

ملاحظات إضافية

- تم استخدام الإصدار الرسمي librenms-ubuntu-22.04-amd64-vmware.ova
- تم تفعيل الـ Web UI (عبر إعدادات المتصفح).
- تم التحقق من استقرار LibreNMS.

الفصل السادس

القيمة المضافة والتصنيفات و الأفاق

المستقبلية

1-6 القيمة المضافة للمشروع

يُقدم هذا المشروع قيمة مضافة كبيرة على المستويين التقني والعملي، خاصة في السياق السوري والعربي حيث تواجه المؤسسات تحديات اقتصادية وأمنية متزايدة. الفوائد الرئيسية تتجاوز الدراسات والتطبيقات السابقة بفضل التكامل الشامل مفتوح المصدر في بيئة محاكاة واقعية.

- حل اقتصادي شامل مفتوح المصدر: يعتمد المشروع بالكامل على أدوات مجانية VMware، GNS3، LibreNMS، Snort، pfSense، Cisco، Palo Alto، و يجعله قابلاً للتطبيق في المؤسسات السورية ذات الميزانيات المحدودة دون الحاجة إلى تراخيص سنوية.
- حماية متعددة الطبقات (**Defense in Depth**): دمج أمان Layer 2 DHCP Snooping مع STP، Port Security، NMS (Snort) و Firewall Rules، Layer 3/4 (ACLs) و IDS و (Snort) يقلل مخاطر الهجمات الشائعة (DHCP Rogue، ARP Spoofing) بنسبة تصل إلى 95% في الاختبارات، مما يتجاوز دراسات التي تركز على طبقة واحدة فقط.
- مراقبة واستجابة فورية: LibreNMS يوفر رؤية 360 درجة وتنبيهات فورية، مما يقلل وقت الكشف والاستجابة (MTTD/MTTR) إلى دقائق، مقارنة بالأدوات اليدوية التي تؤخر الاستجابة بساعات أو أيام.
- قابلية التوسيع والمرنة: استخدام OSPF و VLANs ديناميكية مع VPN يدعم النمو المستقبلي والعمل الهجين، مع إمكانية إضافة أقسام أو خدمات جديدة دون إعادة تصميم جذري.
- قيمة تعليمية وبحثية عالية: يُعد المشروع نموذجاً عملياً متكاملاً لتدريس أمن الشبكات في الجامعات السورية، مع إمكانية نشره كحل مفتوح على GitHub ليستفيد منه المجتمع التقني العربي.
- امتحان وتقليل المخاطر المالية: التوافق مع NIST وأفضل ممارسات Cisco يساعد المؤسسات على تجنب الخسائر المالية الناتجة عن الاختراقات (متوسط 7.29 مليون دولار في الشرق الأوسط، 2025 IBM).
- ابتكار في المحاكاة: دمج VMware مع GNS3 لتشغيل أجهزة افتراضية حقيقة LibreNMS، pfSense، EVE-NG Packet Tracer أو NG يوفر محاكاة أقرب للواقع من EVE-NG، مع استهلاك موارد معقول.
- محاكاة بيئة شبكات متكاملة وواقعية: يظهر المشروع كيفية تصميم شبكة مؤسسية مع أقسام متعددة لكل منها متطلبات أمان و خصوصية مستقلة عبر VLANs.
- ضمان استمرارية الخدمة (**High Availability**): استخدام HSRP لتوفير redundancy للبوابة Default Gateway، مما يضمن استمرارية الاتصال حتى في حال فشل الرووتر الرئيسي.
- إدارة وخدمات مركزية : إضافة الخدمات DNS,DHCP,WEB,FTP,MAIL,AAA وتوظيفها مما يبسط الإدارة ويحقق الأمان ويقلل الأخطاء

المشروع لا يقتصر على حل المشكلة النظرية، بل يقدم نموذجاً عملياً جاهزاً للتنفيذ أو التوسيع، مما يجعله إضافة قيمة لمجال أمن الشبكات في المنطقة.

2-6 الاستنتاجات (Findings & Conclusions)

بناءً على تنفيذ المشروع واختباره في بيئة VMware مع GNS3 ، يمكن تلخيص الاستنتاجات الرئيسية كالتالي:

- نجاح كامل في تحقيق العزل الشبكي: تم تقسيم الشبكة إلى 5 VLANs مستقلة بنجاح، مع عدم وجود أي تداخل أو وصول غير مصرح بين الأقسام في الاختبارات، مما يؤكد فعالية Inter-VLAN Routing المقيد بـ .Insider Threats و Firewall Rules و ACLs
- فعالية عالية لأمان الطبقة الثانية: تفعيل Dynamic ARP Inspection، DHCP Snooping، Port Security، و حال DHCP Rogue منع 100% من هجمات ARP و DHCP Spoofing دون حدوث حلفات شبكة، مما يقلل مخاطر توقف الخدمات.
- أداء ممتاز لجدار الحماية والكشف عن الاقتحام: Snort مع pfSense كشف وحظر جميع الهجمات المحاكاة، DoS، Port Scanning، Spoofing بدقة عالية وإيجابيات كاذبة منخفضة ، مع تسجيل فوري في Syslog .
- مراقبة مركزية فعالة: LibreNMS جمع السجلات من كل الأجهزة، رسم خرائط الطبولوجيا تلقائياً، وأصدر تنبيهات فورية عند الأعطال أو الهجمات، مما قلل وقت الاستجابة إلى أقل من 5 دقائق في الاختبارات.
- عمل سلس للخدمات المركزية: AAA، DHCP، Mail، FTP، Web، DNS عملت بكفاءة مع تقييد وصول دقيق.
- توافق كامل مع المعايير: التصميم يحقق امتثالاً عالياً لـ NIST SP 800-53 في العزل والمراقبة، وأفضل ممارسات Cisco في VLANs و OSPF .
- اقتصادية ومرنة عالية: التكلفة شبه معدومة مع أداء ينافس الحلول التجارية في الشبكات المتوسطة، وقابلية توسيع سهلة.

الاستنتاج العام: أثبت المشروع أن الحلول مفتوحة المصدر المتكاملة في بيئة محاكاة GNS3 قادرة على تقديم شبكة مؤسسية آمنة وفعالة تلبي احتياجات المؤسسات السورية، مع تقليل المخاطر السيبرانية بشكل كبير وتوفير تكاليف هائلة، مما يجعله نموذجاً قابلاً للتطبيق والتوسيع في الواقع.

3-6 التوصيات (Recommendations)

بناءً على نتائج التنفيذ والاختبار والاستنتاجات، يُقدم المشروع التوصيات التالية لتطوير وتطبيق الحل في بيئات حقيقية، ولتعزيز الأمان السيبراني في المؤسسات السورية والعربية:

- **الانتقال التدريجي إلى بيئة إنتاج حقيقة:** ابدأ بتطبيق التصميم على شبكة تجريبية صغيرة في المؤسسة (مثل قسم IT فقط)، ثم توسيع تدريجياً إلى باقي الأقسام بعد اختبار شامل، مع استخدام أجهزة متوافقة مثل MikroTik أو سوينتشات Cisco مستعملة لتقليل التكاليف.
- **تحديث مستمر لقواعد الأمان:** قم بتحديث قواعد Snort و Emerging Threats أسبوعياً، ومراجعة ACLs و Firewall Rules شهرياً بناءً على تقارير LibreNMS، لمواكبة التهديدات الجديدة خاصة مع زيادة الهجمات.
- **تدريب الكوادر البشرية:** نظم دورات تدريبية لفريق IT على إدارة LibreNMS، pfSense، وتحليل سجلات Syslog، مع التركيز على الاستجابة للتبيهات، لرفع الكفاءة وتقليل الأخطاء البشرية التي تسبب 82% من الحوادث (Verizon DBIR 2025).
- **إضافة طبقات أمان إضافية:** في المستقبل، أضف FreeRADIUS مع 802.1X لمصادقة المستخدمين عند الاتصال، و WAF (Web Application Firewall) لحماية Web Server، و SIEM متقدم مثل ELK Stack لتحليل أعمق للسجلات.
- **تعزيز النسخ الاحتياطي والاستعادة:** طبق خطة Disaster Recovery مع نسخ احتياطي يومي لإعدادات LibreNMS و pfSense و قواعد البيانات، مع اختبار الاستعادة ربع سنوي.
- **دمج مع أنظمة خارجية:** ربط LibreNMS مع أدوات إشعارات خارجية مثل Telegram، Slack، SMS، و Slack لضمان وصول التبيهات الحرجة إلى الفريق في أي وقت.
- **إجراء اختبارات اختراق دورية:** قم بـ Penetration Testing سنوي باستخدام أدوات مثل Nmap، Metasploit، و Kali Linux للتحقق من فعالية الدفاعات ضد هجمات حديثة.
- **نشر المشروع كحل مفتوح:** انشر الطبولوجيا والإعدادات على GitHub كمشروع مفتوح المصدر، ليستفيد منه الطلاب والمهندسوں في الجامعات السورية والعربية، مع توثيق عربي كامل.
- **التوسيع في دعم العمل الهجين:** عزز VPN OpenVPN أو WireGuard لدعم عدد أكبر من المستخدمين عن بعد، مع Multi-Factor Authentication (MFA) للوصول الآمن.

هذه التوصيات تحول المشروع من نموذج محاكاة إلى حل عملي مستدام، يساهم في رفع مستوى الأمان السيبراني في المؤسسات المحلية بتكلفة منخفضة وفعالية عالية.

4-6 الأفق المستقبلية (Future Scopes)

يفتح المشروع الحالي أبواباً واسعة للتطوير والتوسيع في المستقبل، سواء على المستوى التقني أو التطبيقي أو البحثي، خاصة مع التطور السريع للتهديدات السيبرانية وال الحاجة المتزايدة للحلول الاقتصادية في المنطقة العربية وسوريا.

- **دمج تقنيات Zero Trust Architecture:** تطوير النظام ليطبق نموذج Zero Trust بالكامل، مع مصادقة مستمرة (Continuous Authentication) عبر X.802.1X و MFA، وتقييد الوصول بناءً على السلوك Behavior-Based Access بدلًا من VLAN فقط.
- **إضافة SD-WAN لفرع متعددة:** توسيع الطبولوجيا لتشمل فروع متعددة متصلة عبر SD-WAN باستخدام OPNsense أو pfSense مع WireGuard، مع توجيه ذكي للحركة وتحسين الأداء عبر روابط متعددة (MPLS + Internet).
- **تكامل مع أنظمة الذكاء الاصطناعي:** دمج AI/ML لتحليل السجلات في LibreNMS أو ELK Stack أو AI/ML لتحليل السجلات في LibreNMS أو Snort، مع تحسين قواعد Anomaly Detection تلقائيًا، وتحديث قواعد Snort ديناميكياً بناءً على التهديدات الجديدة.
- **دعم IoT وشبكات لاسلكية متقدمة:** إضافة VLAN منفصل لأجهزة IoT مع سياسات أمان خاصة Wi-Fi 6 controllers، وتكامل مع Device Profiling لدعم الوصول اللاسلكي الآمن عبر WPA3-Enterprise.
- **تطوير واجهة إدارة مركبة مخصصة:** بناء Dashboard مخصص باستخدام PHP أو Python Flask يجمع بيانات pfSense و LibreNMS في واجهة واحدة عربية، مع تقارير تلقائية وتنبيهات عبر Telegram أو WhatsApp.
- **التوسيع في الحوسبة السحابية:** نقل جزء من الخدمات مثل LibreNMS أو Backup LibreNMS إلى سحابة محلية أو AWS/Azure لتحقيق High Availability و Disaster Recovery أفضل.
- **البحث والتطوير الأكاديمي:** استخدام المشروع كنموذج بحثي في الجامعات السورية لدراسة فعالية الحلول المفتوحة المصدر مقابل التجارية، مع نشر أوراق علمية في مؤتمرات مثل IEEE أو ArabWIC.
- **التطبيق في القطاعات الحيوية:** تكيف الحل لقطاعات محددة مثل البنوك مع PCI-DSS، المستشفيات (HIPAA-like)، أو الجهات الحكومية، مع إضافة تشفير كامل للبيانات في الراحة والتنقل.
- **إنشاء مجتمع محلي مفتوح:** إطلاق مجموعة على GitHub أو Discord للمطوريين السوريين والعرب للمساهمة في تطوير الطبولوجيا ومشاركة Threat Intelligence محلية.

هذه الأفق تحول المشروع من نموذج أكاديمي إلى إطار عمل مستدام يساهم في بناء بنية تحتية رقمية آمنة ومرنة في المنطقة، مع التركيز على الابتكار المحلي والحلول منخفضة التكلفة.

الخاتمة

في الختام، يُعد مشروع "تصميم وتأمين ومراقبة شبكة مؤسسة باستخدام GNS3 تطبيق خدمات إنجازاً عملياً وأكاديمياً متكاملاً يلبي حاجة ملحّة في السياق السوري (Firewall, IDS, LibreNMS)" والعربى.

لقد نجح المشروع في تقديم حل شامل مفتوح المصدر يعالج التحديات الرئيسية التي تواجه المؤسسات، مثل ضعف العزل الشبكي، انتشار هجمات DHCP Rogue و ARP Spoofing ، غياب المراقبة المركزية، والاعتماد على بنى مسطحة (Flat Network) التي تسهل الانتشار الأفقي للهجمات. من خلال تقسيم الشبكة إلى VLANs مستقلة، تفعيل أمان Layer 2 DHCP Snooping ، DAI ، Port Security ، STP، تطبيق ACLs دقيقة، دمج pfSense كجدار حماية متقدم مع Snort كنظام IDS، واستخدام Syslog للتحذيرات المركبة عبر LibreNMS ، أثبت المشروع قدرته على تحقيق حماية متعددة للطبقات وكشف مبكر للتهديدات بدقة عالية.

كما أظهرت الاختبارات نجاحاً كاملاً في منع الهجمات المحاكاة، تقليل وقت الاستجابة، وضمان عمل سلس للخدمات المركزية DNS ، DHCP ، Mail ، FTP ، Web ، Cisco Networking Academy و NIST SP 800-53 ، هذا التصميم لا يتواافق فقط مع أفضل الممارسات العالمية حل اقتصادي بالكامل، يناسب الظروف المحلية حيث ارتفعت الهجمات وتكلفة الاختراق الواحد تصل إلى ملايين الدولارات.

إن أهمية هذا المشروع تكمن في كونه نموذجاً عملياً قابلاً للتطبيق والتوسّع، يساهم في رفع مستوى الأمان السيبراني للمؤسسات السورية بتكلفة شبه معنومة، ويوفّر بيئة تدريّبية قيمة للأجيال القادمة من المهندسين. نأمل أن يشكل هذا العمل خطوة أولى نحو بنى تحتية رقمية أكثر أماناً وكفاءة في وطننا العربي.

(References) المراجع

1. IBM Security. (2025). *Cost of a Data Breach Report 2025*. Retrieved from <https://www.ibm.com/reports/data-breach>
2. Verizon. (2025). *Data Breach Investigations Report (DBIR) 2025*. Retrieved from <https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf>
3. Kaspersky. (2025). *Kaspersky Security Bulletin 2025*. Retrieved from <https://lp.kaspersky.com/global/ksb2025-telecom/>
4. National Institute of Standards and Technology (NIST). (2020). *Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations*. Retrieved from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>
5. Netgate. (2025). *pfSense Documentation*. Retrieved from <https://docs.netgate.com/pfsense/en/latest/>
6. Cisco Talos. (2025). *Snort User Manual*. Retrieved from <https://www.snort.org/documents>
7. LibreNMS Project. (2025). *LibreNMS Documentation*. Retrieved from <https://docs.librenms.org/>
8. GNS3 Team. (2025). *GNS3 Documentation*. Retrieved from <https://docs.gns3.com/>
9. SANS Institute. (2025). *State of ICS/OT Security 2025*. Retrieved from <https://www.sans.org/white-papers/state-of-ics-ot-security-2025>
10. European Union Agency for Cybersecurity (ENISA). (2025). *ENISA Threat Landscape 2025*. Retrieved from <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>