گزارش پروژه تخصصی پیاده‌سازی فایروال متمرکز دانشگاه

نصب و پیکربندی OPNsense در محیط مجازی‌سازی VMware ESXi

استاد ارجمند:

جناب آقای مهندس امین حجت

اجرا و تنظیم:

هومان میریان

اسفند ۱۴۰۴

۱. مشخصات فنی زیرساخت سخت‌افزاری و نرم‌افزاری

جهت اجرای این پروژه، از یک دستگاه سرور فیزیکی با پیکربندی زیر استفاده شده است:

- **سازنده و مدل:** HP ProLiant DL380 Gen9
- **پردازنده مرکزی:** 28 CPUs x Intel(R) Xeon(R) CPU E5-2695 v3 @ 2.30GHz
- **حافظه موقت (RAM):** 127.88 GB
- **پلتفرم مجازی‌سازی:** VMware ESXi 7 Update 2
- **سیستم‌عامل فایروال:** OPNsense 25.7.11_9-amd64
- **وضعیت ذخیره‌سازی:** بدون استفاده از RAID عملیاتی گردید.

۲. مهندسی اینترفیس‌ها و تخصیص شبکه‌های مجازی (VLANs)

پیکربندی اینترفیس‌های فایروال به چهار بخش اصلی تقسیم شده است:

۱. **اینترفیس LAN:** جهت انتقال ترافیک لایه ۲ (بدون آدرس IP مستقیم، صرفاً فعال).

۲. **اینترفیس Management:** جهت مدیریت سیستم با آدرس IP: 192.168.195.133.

۳. **اینترفیس WAN:** جهت اتصال به شبکه خارجی و اینترنت.

۴. **اینترفیس سرورها:** جهت جداسازی ترافیک بخش سرویس‌دهنده‌ها.

۱.۲. پیکربندی ساب‌اینترفیس‌های VLAN

تمامی VLANهای ذیل به صورت Trunk از طریق اینترفیس LAN به سوییچ متصل شده‌اند. لازم به ذکر است سرویس DHCP بر روی هیچ‌کدام فعال نبوده و صرفاً عملیات مسیریابی (Forwarding) انجام می‌پذیرد:

Address IP	ID VLAN
192.168.60.3	vlan60
Assigned IP No	vlan86
192.168.88.4	vlan88
192.168.94.2	vlan94
192.168.122.2	vlan122
192.168.168.4	vlan168
192.168.196.3	vlan196
192.168.230.3	vlan230
192.168.0.115	vlan252

۳. شرح فرآیند نصب و آماده‌سازی زیرساخت

در مرحله نخست، رسانه نصب (Flash Drive) توسط ابزار Ventoy به‌صورت Bootable آماده شده و سیستم‌عامل ESXi نسخه 7.2 بر روی سرور نصب گردید. پس از انجام تنظیمات اولیه شبکه، دسترسی به محیط مدیریت GUI از طریق پنل وب برقرار شد. در ادامه، فایل ISO سیستم‌عامل OPNsense در فضای Datastore بارگذاری گردید.

جهت برقراری ارتباط با شبکه داخلی، Uplinkهای مربوطه در بخش Networking به یک vSwitch تخصیص داده شده و از طریق Portgroup به ماشین مجازی متصل شدند. نکته حائز اهمیت در این بخش، انجام عملیات Passthrough برای کارت شبکه متصل به LAN در مسیر Host > Manage > PCI Devices است.

> **تحلیل فنی:** به دلیل اتصال این کارت شبکه به پورت Trunk سوییچ، استفاده از لایه مجازی‌سازی مانع از رویت پکت‌های تگ‌گذاری شده (802.1Q) توسط ماشین مجازی می‌گردد. با عبور مستقیم (Passthrough)، فایروال مستقیماً با پکت‌های تگ‌گذاری شده در تعامل خواهد بود. این رویکرد جهت شناسایی VLANهای مختلف دانشگاه، اعمال محدودیت‌های دسترسی و مانیتورینگ دقیق پهنای باند هر بخش اتخاذ شده است.

۴. پیکربندی عملیاتی فایروال OPNsense

پس از اتمام مراحل نصب سیستم‌عامل، تخصیص کارت‌های شبکه به اینترفیس‌های LAN، WAN و سایر بخش‌ها انجام گرفت. سپس از طریق آدرس IP اختصاص یافته به اینترفیس مدیریت، دسترسی به پنل وب جهت انجام تنظیمات تکمیلی ایجاد شد.

۱.۴. تعریف VLANها و انتساب اینترفیس‌ها

فرآیند ایجاد VLANها در مسیر Interfaces > Devices > VLAN با تعریف شماره تگ اختصاصی انجام یافت. پس از ذخیره‌سازی و اعمال تغییرات (Apply)، هر VLAN به اینترفیس LAN انتساب (Assign) داده شد. در این سناریو، دسترسی به پنل مدیریت صرفاً از طریق اینترفیس مجزای Management امکان‌پذیر است؛ زیرا اینترفیس LAN فاقد آدرس IP بوده و صرفاً در وضعیت Active قرار دارد.

۲.۴. سیاست‌های امنیتی و قوانین فیلترینگ (Firewall Rules)

- **قوانین شناور (Float Rules):** یک قانون شناور جهت تامین دسترسی به شبکه اینترنت برای تمامی اینترفیس‌های VLAN تدوین گردید.
- **قوانین ورودی (Inbound):** برای هر VLAN، قانونی از نوع IN جهت اجازه ورود ترافیک به فایروال تعریف شد. جهت رعایت پروتکل‌های امنیتی، از نگارش قوانین خروجی (Outbound) اجتناب شده است.
- **قانون مدیریت:** دسترسی به اینترفیس Management به‌صورت Any/Any پیکربندی شده، اما دسترسی به فایروال منوط به برقراری اتصال VPN از رنج 195 می‌باشد.
- **امنیت پیشرفته:** سرویس IDS (سیستم تشخیص نفوذ) جهت پایش تهدیدات بر روی سرور فعال‌سازی شد.

۳.۴. سرویس‌های شبکه و مانیتورینگ

جهت مدیریت بهینه اسامی دامنه، از سرویس DNSmasq استفاده شده است. برخلاف سرویس پیش‌فرض (Unbound) که مستقیماً از Root DNS استعلام می‌کند، DNSmasq درخواست‌ها را به Upstream DNSهای تنظیم شده (217.218.127.127 و 217.218.155.155) ارجاع می‌دهد. این امر پایداری دسترسی به سرویس‌های داخلی و خارجی را تضمین می‌کند.

همچنین جهت تحلیل ترافیک و مانیتورینگ، سرویس‌های زیر پیاده‌سازی شدند:

- **ntopng:** جهت تحلیل عمیق ترافیک شبکه (قابل دسترسی بر روی پورت 3000).
- **vnstat:** جهت گزارش‌گیری از میزان مصرف پهنای باند هر اینترفیس.
- **SSH:** جهت مدیریت سیستم از طریق خط فرمان.

۵. ارزیابی و تست نهایی

در پایان پروژه، صحت عملکرد سیستم از طریق تست‌های پینگ (ICMP) از تمامی VLANها به سمت فایروال و همچنین بررسی ارتباطات متقابل میان اینترفیس‌های موجود با موفقیت مورد تایید قرار گرفت.