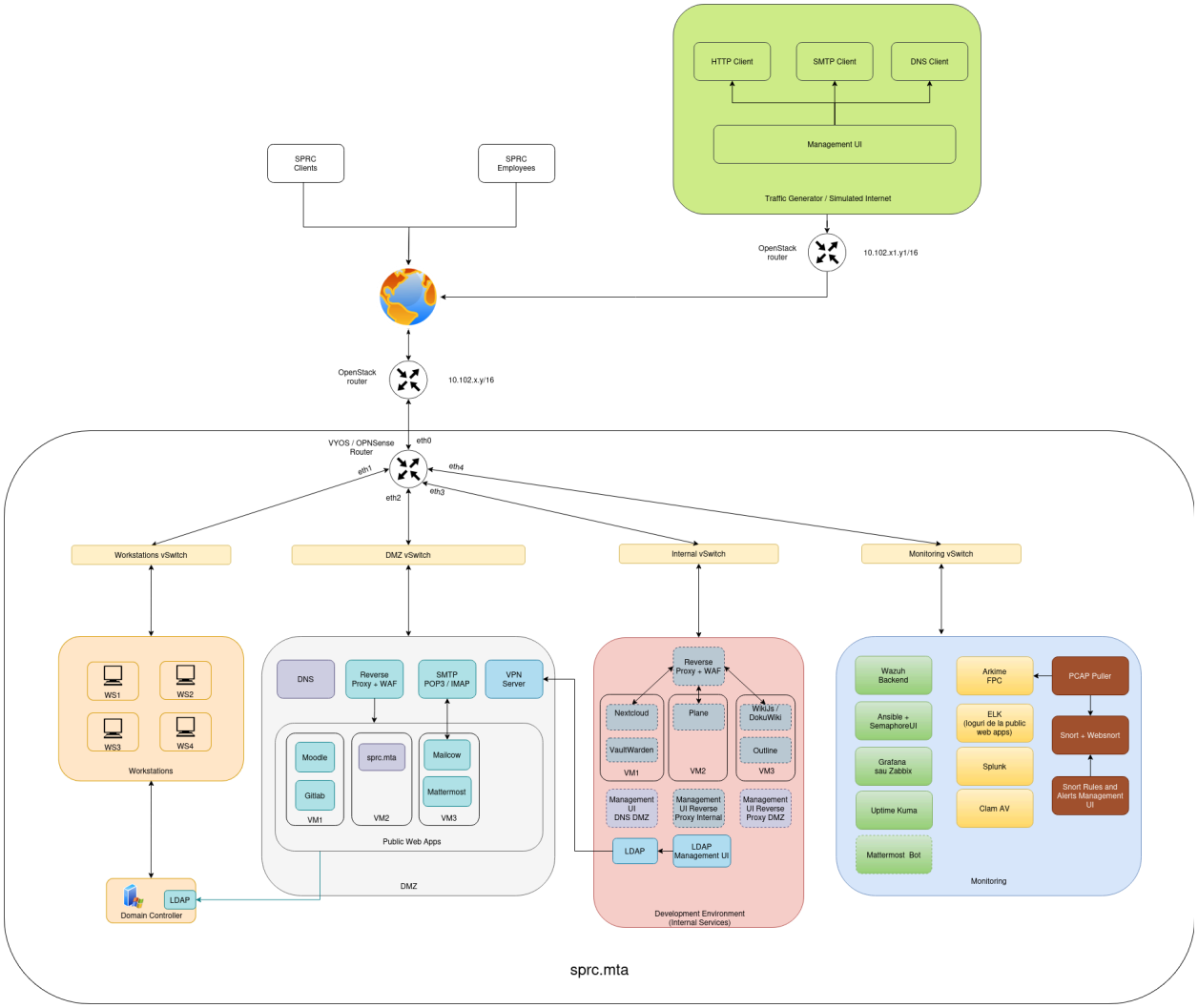
Proiect SPRC 2025 - 2026

Scopul proiectului este de a crea o infrastructura de retea a unei organizatii *sprc.mta*. Aceasta organizatie permite angajatilor sai sa lucreze atat de la birou cat si de acasa.



Infrastructura companiei sprc.mta

Subretelele din cadrul organizației:

1. Workstations – rețeaua în care se afla calculatoarele angajatilor.
2. DMZ – zona în care se regasesc toate serviciile expuse în internet
3. Development Environment – zona unde se testeaza diferite solutii dezvoltate de companie și în care se regasesc serviciile accesibile doar de către angajați.
4. Monitoring – rețea în care se afla serviciile ce monitorizează traficul, mașinile virtuale din DMZ, development environment și stațiile angajaților.

!!Atentie: Fiecare dintre aceste subretele este realizata prin intermediul unui subnet din Openstack.

!!Atentie: Unde sunt specificate mai multe vm-uri (eg. VM1, VM2, VM3 din DMZ) este necesar sa hostati serviciile fie intr-un cluster kubernetes fie docker swarm (la alegere). Puteti folosi orice fel de solutie pentru clusterul kubernetes (Rancher + RKE, minikube etc.).

Notare

In evaluarea proiectelor se va lua in calcul respectarea cerintelor fiecarei componente in parte, raspunsurile la intrebarile adresate si activitatea de la laborator.

!!Atentie: Notarea se va face separat pentru fiecare membru din echipa. De asemenea orice imbunatatire aduceti componentei asignate voua va genera puncte suplimentare.

!!Atentie: Pana la definitivarea notei de la proiect se va lua in calcul si implementarea subechipei cu aceeasi componenta din cea de-a doua infrastructura.

Cerinte

Echipa responsabila de infrastructura

Scopul acestei echipe este de a pregăti toate masinile virtuale necesare realizarii proiectului (crearea in openstack, configurarea retelelor din openstack, configurarea adreselor IP). De asemenea, tot aceasta echipa se va ocupa de masina virtuala de tipul router (OpnSense sau VYOS - la alegere). **!! Atentie: Veti avea la dispozitie doar 2 floating ip in cadrul proiectului (unul pentru router-ul din infrastuctura si unul pentru internetul simulat)**

1. Creati subretele specificate, toate trebuie sa aiba DHCP dezactivat. Serverul de DHCP trebuie configurat la nivelul router-ului. Reteaua de monitorizare trebuie sa foloseasca adresare statica.
2. Creati VM-urile necesare realizarii proiectului (nu exista un numar total de VM-uri corect, singura conditie este sa respectati numarul de vm-uri pentru clusterele de productie, respectiv de dezvoltare (unde apare VM1, VM2…)). Accesul la VM-uri poate fii SSH atat prin intermediul de credentiale cat si de chei SSH.
3. Asignati Floating IP routerului din infrastructura.
4. Asigurati-va ca toate vm-urile din infrastuctura au acces la internet.
5. Configurati port forward pe router catre serviciile din DMZ.
6. Configurati politici de firewall (pe router) astfel incat clientii de VPN sa nu poata accesa decat subreteaua de dezvoltare si cea de monitorizare
7. Configurati politici de firewall (pe router) astfel incat statiile din subreteaua de workstations sa nu poata ajunge in DMZ. In DMZ trebuie sa poata ajunge doar masinile din subreteaua de monitorizare. Setati politici de firewall astfel incat accesul de la monitorizare catre DMZ sa fie permis doar pentru anumite adrese IP (cele ale VM-urilor din acea subretea).
8. Setati o politica de firewall prin care sa fie permis accesul Domain Controller catre serverul de DNS din DMZ.
9. Setati o politica de firewall prin care sa fie permis accesul de la serverul de VPN din DMZ catre serverul de LDAP din subreteaua de development

10. Setati o politica de firewall prin care sa permiteti accesul de la Management UI DNS din subreteaua de development catre serverul de DNS din DMZ.
11. Setati o politica de firewall prin care sa permiteti accesul de la Management UI Proxy din subreteaua de development catre reverse proxy-ul din DMZ.
12. Creati un jumpbox pentru colegi ca sa poata ajunge la VM-uri. Faceti port forward la SSH de pe router catre acest VM (Puteti folosi un alt port pe router, diferit de 22, sa nu va blocati accesul pe router prin floating IP)
13. Redirectati traficul din subretele Workstations, DMZ si internal catre subreteaua de monitorizare. Puteti crea si o subretea separata in care se regaseste Arkime si router-ul si sa redirectati tot traficul catre aceasta.
14. (Bonus) Realizati un script de *terraform* care sa creeze toate VM-urile necesare infrastructurii.

Workstations + Domain Controller

1. Configurati masina virtuala de **Windows Server** sa fie domain controller pentru sprc.mta
2. Inrolati toate statiile angajatilor **(Windows 10)** in domeniu.
3. Creati conturi de utilizator pentru angajatii companiei (n conturi – unde n numarul de workstations)
4. Denumiti fiecare statie dupa urmatorul format: [nume utilizator]_ws (ex. Coratu_ws)
5. Creati un network share care sa se numeasca Transfer_SPRC.
6. Creati un grup care sa se numeasca IT_SPRC si adaugati doi utilizatori existenti in acest grup.
7. Adaugati politici de securitate astfel incat doar utilizatorii din grupul IT_SPRC sa poata accesa Transfer_SPRC.
8. Instalati un exchange server pe domain controller care sa preia conturile de utilizator din Active Directory
9. Instalati outlook pe fiecare statie din domeniu
10. Conectati outlook la server exchange
11. Verificati ca statiile au acces la serviciile interne si la internet
12. Conectati serverul de DNS din cadrul domeniului cu serverul din DMZ.
13. Adaugati un password policy care sa oblige utilizatorii sa isi schimbe parola la un interval de timp, parolele sa fie complexe (minim 1 litera mare, 1 cifra si un caracter special) si care sa blocheze contul dupa 5 incercari gresite.

DMZ (Rev Proxy + Moodle + Gitlab + Mail + Chat)

1. Creati un cluster kubernetes sau docker swarm folosind 3 VM-uri.
2. Instalati si configurati o solutie de tipul reverse proxy (Nginx, Apache, Haproxy - la alegere)
3. Instalati si configurati Mailcow.
4. Instalati si configurati o instanta Gitlab.
5. Instalati si configurati Moodle.
6. Instalati si configurati o instanta Mattermost
    a. Creati un team care sa se numeasca SPRC;
    b. In cadrul acestui team creati mai multe canale printre care unul denumit *monitorizare;*

7. Configurati reverse proxy astfel incat toate serviciile de la 3 - 6 sa poata fi accesate utilizand subdomenii.
8. Autentificarea în cadrul serviciilor de la punctele 3 - 6 trebuie realizata prin intermediul LDAP din Domain Controller.
9. (Bonus) Pe solutia de reverse proxy configurati un WAF.

DMZ + Internal (DNS + site prezentare + management UI DNS + management UI reverse proxy)

1. Creati un site de prezentare al proiectului
    a. Puteti utiliza orice fel de solutie disponibila (Wordpress, Drupal, etc.)
2. Instalati si configurati un server de DNS
    a. Serverul DNS trebuie sa poata furniza raspunsuri pentru toate subdomeniile din cadrul infrastructurii. (eg. moodle.sprc.mta, gitlab.sprc.mta, etc.)
3. Creati o interfata de management pentru serverul DNS
    a. Din cadrul acestei aplicatii trebuie sa puteti adauga noi intrari DNS, sa le modificati pe cele existente si sa stergeti o anumita intrare.
4. UI-ul de management al reverse proxy trebuie sa permita vizualizarea, modificarea si crearea de noi intrari (virtual hosting).

DMZ + Internal (VPN + LDAP + LDAP Management UI)

1. Instalati si configurati un server OpenVPN
    a. Acesta trebuie sa permita autentificarea folosind serverul LDAP din subreteaua de Development
2. Instalati si configurati un server LDAP
3. Realizati o interfata grafica pentru managementul serverului de LDAP.
4. Permiteti clientilor de VPN sa acceseze serviciile interne si serviciile din subreteaua de monitorizare.
5. (Bonus) Monitorizati IP-urile alocate pentru fiecare user in parte.

Internal Services (Rev proxy + next cloud + plane + wikijs/dokuwiki + management UI rev proxy)

1. Creati un cluster kubernetes sau docker swarm folosind 3 VM-uri.
2. Instalati si configurati o instanta nextcloud in cadrul cluster-ului docker swarm/kubernetes
1. Instalati si configurati o instanta plane in cluster
2. Instalati si configurati o instanta wikijs/dokuwiki in cluster
3. Instalati si configurati o instanta de outline
4. Instalati si configurati o instanta de vault warden.
5. Instalati un reverse proxy si configurati instanta sa permita traficul catre nexcloud, plane si wiki
6. Realizati o interfata de management a reverse proxy-ului. Aceasta interfata trebuie sa permita adaugarea/modificarea/stergerea virtual host-urilor.
7. (Bonus) Adaugati o solutie de tipul Web Application Firewall (WAF) pe reverse proxy

Monitorizare (Wazuh + Ansible + Semphore UI + Grafana sau Zabbix + Uptime Kuma + Wazuh Bot)

1. Instalati Wazuh server, indexer si dashboard
    a. Adaugati posibilitatea ca wazuh sa transmita alertele catre mattermost (bot)
2. Instalati ansible si creati urmatoarele playbook-uri:
    a. Creati un playbook ansible care sa faca update la repository-uri pentru toate statiile linux din retea
    b. Creati un playbook care sa instaleze visual studio code pe toate statiile angajatilor
    c. Creati un playbook care sa instaleze docker si sa descarce o serie de imagini default
    d. Creati un playbook care sa instaleze wazuh agent pe toate statiile angajatilor
    e. Creati un playbook care sa instaleze wazuh agent pe toate serverele linux
    f. Creati un playbook care sa instaleze zabbix agent (daca ati ales zabbix ca solutie de monitorizare) sau node exporter daca ati ales prometheus + grafana.
3. Instalati si configurati SemaphoreUI (pentru Ansible)
4. Instalati Prometheus + Grafana sau Zabbix si colectati metrici de pe toate statiile linux din infrastuctura (pentru prometheus puteti folosi node_exporter, pentru zabbix aveti agent).
5. Realizati dashboard-uri in grafana/zabbix in care sa visualizati informatiile colectate de la agent/node exporter.
6. Instalati si configurati Uptime Kuma astfel incat sa monitorizati aplicatiile web din DMZ si din subreteaua de Development.
    a. Verificati ca VM-urile din infrastuctura sunt up folosind ping (optiune din aplicatie) si generati alerte in momentul in care un VM nu mai este disponibil.
    b. Configurati alerte prin intermediul bot-ului de Mattermost in momentul in care una din aplicatiile web nu mai este disponibila.
7. (Bonus) Monitorizati clusterele de kubernetes.

Monitorizare (Arkime + ELK + Splunk + Clam AV)

1. Instalati si configurati Arkime astfel incat sa prinda tot traficul (pentru baza de date din spate puteti folosi fie Elasticsearch, fie Opensearch - la alegere).
2. Instalati si configurati o instanta Elasticsearch (puteti utiliza si opensearch).
3. Instalati si configurati o instanta Logstash (puteti utiliza si fluentd).
    a. Prin intermediul acesteia preluati log-urile de la toate reverse proxy-urile din infrastructura.
    b. Colectati toate log-urile de sistem de pe statiile windows.
4. Instalati si configurati o instanta Kibana care sa permita vizualizarea logurilor din Elasticsearch (puteti folosi si Opensearch Dashboards).
5. Instalati si configurati o instanta Splunk si instalati agentul pe toate statiile din infrastructura
6. Instalati si configurati o instanta ClamAV

Monitorizare (PCAP Puller + Snort + Websnort + Snort Rules and Alerts Management UI)

1. Instalati si configurati snort
    a. Scoateti toate regulile default snort
    b. Adaugati un set de reguli care sa gaseasca payload-uri pentru atacurile ce pot aparea asupra aplicatiilor web. (eg. SQL Injection, NOSQL Injection, Local File Inclusion)
2. Instalati websnort
3. Implementati o aplicatie care sa preia fisiere PCAP din Arkime si sa le incarce in Websnort
4. Implementati o interfata grafica de management a alertelor si a regulilor din snort.
    a. Aceasta interfata trebuie sa permita adaugarea/modificarea/stergerea de reguli
    b. Interfata trebuie sa permita vizualizarea alertelor in urma incarcarii unui fisier PCAP preluat din Arkime.

Internet Simulat

Scopul acestei componente este de a verifica ca toate aplicatiile din cadrul infrastructurii functioneaza corect prin implementarea unor script-uri care testeaza diferite endpoint-uri, DNS-ul, serverul de VPN etc. !!**Atentie: In cadrul acestei componente aveti mana libera, puteti implementa verificarile in orice fel doriti, dar asigurati-va ca testati toate serviciile din infrastructura.**

1. Realizati o suita de scripturi care sa genereze trafic catre toate serviciile expuse
    a. Realizati un script care trimite mail catre toti utilizatorii din AD
    b. Realizati un script care permite realizarea de cereri DNS.
    c. Realizati un script care permite intrarea pe fiecare aplicatie web expusa de voi in parte si realizeaza cateva actiuni (eg. login, navigheaza pe cateva pagini, logout)
    d. Realizati un script care testeaza serverul de VPN si accesul in infrastructura prin intermediul acestuia.
2. Realizati o interfata de management care sa permita:
    a. rularea fiecarui script care simuleaza comportamentul utilizatorilor.
    b. incarcarea unor script-uri suplimentare.
    c. rularea scripturilor la un interval de timp
    d. afisarea unor metrici in urma rularii scripturilor (eg. numarul de cereri transmise, media timpului de raspuns de la server)
3. Transmiteti alerte in momentul in care un serviciu nu raspunde corect prin intermediul mattermost.