YNOV CAMPUS

Réponse appel d'offres

Sécurité des SI

Mickael Rigonnaux – Clément Olier
04/04/2019

Table des matières

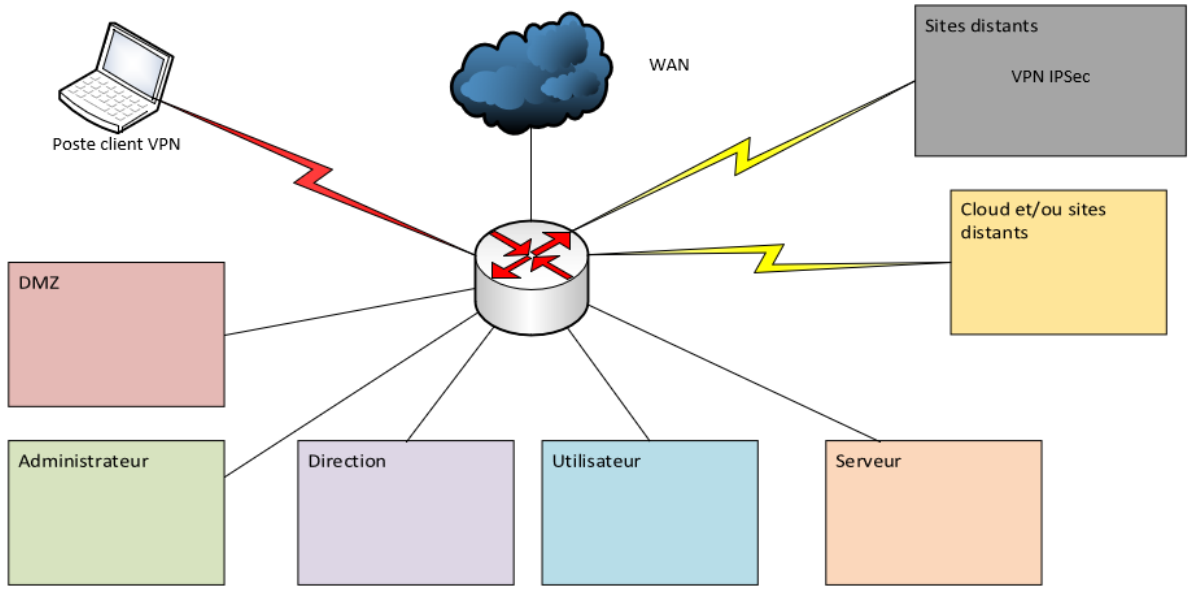
Réponse à Appel d'Offres

Introduction

Ce TD est à rendre dans le cadre du cours de Master 1 Sécurité des SI dans le Campus Ynov d'Aix-en-Provence. Il a pour but de proposer une réponse à un cahier des charges défini spécifiquement pour ce cours.

Présentation de l'infrastructure

Schéma de l'infrastructure



Spécification de l'infrastructure

Dans ce cadre de cet appel d'offres nous avons fait le choix de proposer une architecture virtualisée avec des solutions types VMWare/Hyper-V. L'avantage de ces solutions est qu'elles sont très évolutives et relativement facile à prendre en main pour des initiés.

Pour la partie réseau, nous préconisons l'utilisation d'un matériel homogène pour des raisons de maintenance et de performance évidente. Une marque comme Cisco par exemple permettra d'avoir un parc homogène à tous les niveaux, c'est-à-dire pare-feu, routeur et switch. De plus l'utilisation d'une marque comme celle-ci permet d'avoir un large choix entre différents revendeurs/prestataires externes. Cette homogénéité sur l'ensemble du parc permettra également de réduire le coup de formation de l'entreprise.

Sur la partie réseau afin de mener à bien le projet il est nécessaire d'avoir les équipements suivants (un ou plusieurs) :

- Switch de niveaux 3
- Switch de niveaux 2
- Pare-feu

Ils devront supporter les fonctionnalités suivantes :

- Gestion des réseaux virtuels (VLAN)
- Support SNMPv3
- 802.1x/Radius
- Routage inter-vlan
- GLBP, HSRP, VRRP (haute disponibilité)
- Pare-feu statefull (avec répartition de charge actif/actif)
- Ports miroirs

Segmentation des flux réseaux

Dans le cadre de la réalisation d'une infrastructure réseau la plus adaptées aux besoins du client, il sera nécessaire d'effectuer une matrice de flux qui permettra de rendre une vision claire et précise des flux liée à la fois aux applicatifs utilisés mais aussi à la disposition géographique des différents éléments.

Sécurité de l'intranet

Le plus gros point d'entrée de l'entreprise et sans doute le plus critique est l'intranet/extranet. Il permet à l'ensemble des clients et des collaborateurs de la société de se connecter et de faire des actions. Il faut donc trouver un moyen de gérer l'aspect authentification et l'aspect gestion des droits.

Pour l'aspect authentification vu qu'il s'agit d'une application Web nous préconisons l'usage suivant :

Utilisation d'une solution d'authentification basée sur des fonctions de hachage comme bCrypt. Il faut faire générer côté client un hash avec un salt et l'envoyer au serveur afin de comparer si dans sa base le hash est également présent.

Concernant la gestion des accès nous préconisons également une gestion de type RBAC qui est la plus adaptées aux besoins.

Au niveau du reverse-proxy il faut également mettre en place un système de type « WAF » qui permettra de bloquer automatiquement les attaques applicatives sur l'intranet/extranet.

De plus l'ensemble des flux seront chiffrés avec le protocole TLS et pour finir il faut prévoir une revue du code de l'application avec des tests d'intrusions.

Cela nécessite donc au préalable d'avoir une bonne connaissance du code de l'application et que le reverse-proxy gère correctement l'aspect WAF.

Gestion de l'authentification interne

Au sujet de l'authentification en interne c'est-à-dire au sein des locaux de l'entreprises et les utilisateurs en VPN. Nous conseillons d'utiliser la technologie radius qui utilise elle-même en partie Kerberos.

Elle permet un accès aux différents réseaux en fonction des groupes de l'active directory et permet également de gérer l'aspect autorisation au sein des applications.

Haute disponibilité

Une des demandes principales est d'avoir une infrastructure autonome, il faut donc prévoir la mise en place de plusieurs solutions de secours. L'application la plus importante dans l'entreprise est son intranet/extranet, elle permet à chaque client de gérer ses commandes et aux utilisateurs internes de l'administrer.

Afin d'assurer la pérennité de l'accès à cette application il faut mettre en place les mesures suivantes :

- Mise en place de reverse proxy en haute disponibilité (au moins deux)
    - Le mode utilisé peut-être Round-Robin par exemple avec du 50/50
- Mise en place d'un second serveur intranet pour la haute disponibilité (haut moins deux)
- Avoir deux lignes internet dédiées afin d'assurer en continue l'accès au site (2 FAI si possible)
- Mise en place d'agrégats de lien afin d'assurer la disponibilité et la performance d'accès sur l'intranet
- Mise en œuvre d'une haute disponibilité (actif/actif) au niveau du pare-feu de la société
- Mettre en place le protocole STP (spanning tree) afin de prévoir la panne d'un équipement réseau

En dehors de l'application centrale de l'entreprise il y a d'autres services très impactant pour les utilisateurs comme l'Active Directory et le serveur de mail par exemple. Il est aussi essentiel de mettre en place une haute disponibilité pour ces serveurs-là.

Afin de réaliser les différents points cités au-dessus il est nécessaire d'avoir très bonne vision du fonctionnement de l'intranet et du système actuel. Une phase de découverte et d'apprentissage sera nécessaire afin de trouver les bonnes configurations, notamment au niveau de la base de données de l'application par exemple.

Cependant, même si le client garder vouloir avoir l'ensemble de l'infrastructure sur le site principale de l'entreprise, il faut prévoir une solution de secours. Car en cas d'incident majeur (incendie, etc.) le parc informatique de l'entreprise sera complètement perdu.

Nous préconisons donc l'utilisation d'un second site. Deux choix sont possibles :

- Cloud (Azure, AWS, OVH)
- Utilisation d'un site annexe de la société

Nous préconisons l'utilisation cloud car cela ne nécessite pas de travaux ni d'autres installations. Il existe des solutions sur les hébergeurs cloud qui permettent de répliquer quasiment en temps réelles les modifications faites sur les serveurs.

De plus, il n'est pas nécessaire d'externaliser l'ensemble de l'infrastructure, l'intranet/extranet ainsi que l'active directory devrait permettre à l'entreprise de continuer son activité en cas de problème majeur.

Sécurité des clients de l'entreprise

Pour l'aspect sécurité des clients de l'entreprise nous avons choisis les mécanismes suivants :

- Mise en place d'antivirus sur tous les postes
- Installation d'un filtre SPAM sur le serveur de mail
- Mise en place d'un proxy web pour le filtrage des URLs (si nécessaire)
- Une solution de chiffrement des disques peut également être envisagée
- Mise à jour quotidienne
- Mise en place de TLS sur les applications internes

Afin d'assurer la sécurité des postes client et la pérennité de la société nous avons choisis de proposer un proxy afin de filtrer l'ensemble du trafic. Il ne sera dans un premier temps pas utilisé mais des sondes placées sur le réseau permettront de tracer l'ensemble des flux des utilisateurs en cas de besoin.

De plus ces mêmes sondes permettent de prévenir différentes attaques sur le réseau client (NIDS).

Sécurité des serveurs de l'entreprise

Pour la partie serveur de l'infrastructure les technologies mises en œuvre sont plus importantes :

- Segmentation DMZ et serveurs internes
- Anti-virus sur les serveurs Windows
- Mise en place d'IDS (Intrusion Detected System)
    - HIDS pour la partie serveur basé sur les logs
    - NIDS pour le réseau
- Scan de sécurité mensuel avec Nessus ou Openvas par exemple
- Une solution anti-ddos en coupure de réseau type Arbor
- L'utilisation des protocoles TLS pour l'internet et l'externe
- Hardenning des différentes technologies (OS, services, etc.)
- Mise en place d'un planning de patch management
- Gestion centralisée des configurations
- Mise en place d'un centralisateur de log et d'évènement (SIEM)

L'ensemble de ces solutions permettent d'avoir un parc de serveur sécurisé et d'éviter les attaques les plus communes.

Avec les technologies proposés le client pourra avoir accès à différentes métriques sur l'aspect sécurité de l'infrastructure et pourra être alerté en cas d'attaque et possiblement de la bloquer.

Supervision

Afin de s'assurer du bon fonctionnement des équipements et systèmes de l'infrastructure proposée, et dans l'optique de donner aux équipes un pouvoir de réaction dans les meilleurs délais face aux possibles incidents, des systèmes de supervision seront mis en place.

Une première solution type "centreon" permettra via l'utilisation du protocole SNMP de récupérer les informations essentielles dans le maintien des équipements et services de l'entreprise. Un system NIDS comme "Snort" ou "Suricata" sera aussi installé afin d'effectuer un travail d'analyse des informations récoltés. Il servira par exemple de support pour diminuer les latence et coupure réseau.

Une seconde solution de type HIDS "Elasticsearch Kibana Logstash + Wazuh" se chargera du côté système et permettra une gestion des logs des applications et services (Progiciel, Serveur Mail, AD…) en temps réel. Aussi l'intégralité du trafic de l'infrastructure sera pris en compte et analysé grâce à cette solution.

Les administrateurs de l'entreprise disposeront donc d'interfaces utilisateurs simple et unifié contenant l'intégralité des informations critiques de l'infrastructure. Un système d'alerte sera également mis en place.

Gestion des accès distants

Dans un souci de fournir des accès à distances sécurisés, les connexions distantes seront établies via l'emploi du système VPN. 2 types de connexions chiffrée et authentifié seront alors mise en oeuvre :

- La première connexion VPN sera dite "site to site" et s'emploiera donc lors de la communication vers les sites distants depuis le site interne principal.
- La seconde connexion VPN dite "client to site" s'emploiera lors de la communication des utilisateurs externes (Administrateurs, Commerciaux, Direction) vers le réseau interne de l'entreprise

La connexion "site to site" sera effectué via un tunneling utilisant la suite de protocole IPSec avec certificats. Les communications "client to site" seront réalisé via le protocole SSL.

Gestion des sauvegardes

La mise en place d'une gestion des sauvegardes est indispensable lors de la réalisation d'une infrastructure qui se doit d'être pérenne et hautement disponible. Pour ce faire nous proposons un système de sauvegarde en interne à l'instar de "Veeam", une réplication sur un des sites secondaires, et la mise en place d'un backup en utilisant les services du cloud (AWS, Azure…). Une sauvegarde complète sera effectuée tous les week-ends et des sauvegardes incrémentales le reste de la semaine.

Tests

Dans l'optique de proposer une infrastructure réellement opérationnelle et garantir son bon fonctionnement une batterie de tests sera effectuée, comprenant :

Audits de sécurité interne et externe complet (Applicatif et réseau)

- Pentest
- Tests de charge de l'intégralité des équipements
- Tests de basculements des équipements en haute disponibilité
- Restaurations des sauvegardes et vérification du fonctionnement
- Tests de réplication (Backup cloud)

Conclusion & Prérequis

Avec l'infrastructure proposée il faut également prendre en compte certaines choses qui n'ont pas été abordées jusqu'à maintenant comme l'aspect RGPD. En prérequis il faut donc avoir une très bonne connaissance de l'entreprise et de l'utilisation de ses données.

Il faut également prévoir un PRA mais cela se prévoit en fonction du type d'entreprise et de son cœur de métier.

Pour la partie segmentation du réseau le prérequis est également d'avoir pleinement connaissance des différents accès des employés sur toutes les ressources de l'entreprise. Ce qui n'est pour l'instant pas le cas.

Il faut également prévoir dans les prérequis de former l'ensemble des utilisateurs du SI à la sécurité informatique. Notamment sur le phishing ou la gestion des mots de passe. L'infrastructure peut avoir tous les mécanismes de sécurité si l'utilisateur final n'est pas vigilant ça ne sert à rien.

Nous allons maintenant aborder la partie des fournisseurs/prestataires. Il faut garder une certaine homogénéité dans le choix de ces derniers il faut réaliser le choix en fonction de leurs tailles et leurs disponibilités, que ça soit niveau matériel ou humain. Il ne faut pas que le projet soit abandonné ou retardé à cause d'un prestataire.

Notre choix se tourne donc vers des PME (50 à 100 employés) et non pas des grosses SSII car elles ont l'avantages d'être plus proche des clients et de proposés des solutions plus adaptées. De plus un client comme celui-ci aurait plus de valeur ajoutée pour eux que pour une SSII. Il faut cependant faire attention aux compétences dans ces sociétés-là.

En plus de ce choix-là il faudra également former les administrateurs internes à l'entreprise afin qu'il puisse intervenir en cas de problème sur l'infrastructure au niveau 1 par exemple. Pour les problèmes de plus haut niveau et là maintenant nous vous conseillons de réaliser des contrats de maintenant avec les différents prestataires. Cela permet d'avoir un suivi et une expertise que l'entreprise ne pourrais pas avoir en interne.