

Nicolas BOUGET
✉ nicolas.bouget@esial.net
3A TRS1

Marc PINHÈDE
✉ marc.pinhede@esial.net
3A LE

Julien GUÉPIN
✉ julien.guepin@esial.net
3A IL

Julien VAUBOURG
✉ julien@vaubourg.com
3A TRS2

Authentifications RADIUS

Note de cadrage

Projet industriel
encadré par Guillaume ROCHE
pour la société B.H. Consulting

Le 17 octobre 2012



Table des matières

1	Présentation	3
1.1	L'entreprise	3
1.2	L'équipe de projet	3
1.3	Problématique et bénéfices pour l'entreprise	3
1.4	Contexte	4
2	Spécifications	4
2.1	Objectifs précis	4
2.2	Délai	4
2.3	Budget	4
2.4	Niveau de qualité attendu	5
2.5	Priorités des objectifs	5
2.6	Risques	5

1 Présentation

1.1 L'entreprise

Ce projet est réalisé pour l'entreprise B.H. Consulting¹. Située à Nancy, elle est chargée de la mise en place de solutions techniques pour des réseaux d'entreprise ou d'institutions.

Cette PME compte cinq employés :

- Bertrand PÉTAT, directeur de l'entreprise
- Guillaume ROCHE, ingénieur réseau
- Jérémie KRAEMER, ingénieur réseau
- Simon KOSMERL, ingénieur réseau
- Christine MARCILLAT, Secrétaire de direction

1.2 L'équipe de projet

L'équipe chargée du projet est composée de quatre étudiants de l'École TELECOM Nancy, qui représentent trois des quatre spécialités proposées par l'École :

- Nicolas BOUGET, 3e année, Télécommunications, Réseaux et Services
- Julien GUÉPIN, 3e année, Ingénierie du Logiciel
- Marc PINHÈDE, 3e année, Logiciels Embarqués
- Julien VAUBOURG, 3e année, Télécommunications, Réseaux et Services

Le chef de projet est Nicolas BOUGET.

1.3 Problématique et bénéfices pour l'entreprise

L'objectif de ce projet est la mise en place d'une solution d'authentification forte grâce au standard 802.1X et la gestion des configurations de plusieurs éléments actifs au sein d'un réseau (commutateurs et routeurs). Un système de sauvegardes automatiques des configurations de ces équipements est également demandé.

Le standard 802.1X permet à un utilisateur de se connecter physiquement à un réseau, en se voyant attribuer automatiquement une vue de celui-ci (VLAN) correspondant au groupe auquel il appartient dans l'entreprise cliente. Le standard permet de gérer son authentification de différentes manières (adresse MAC de son ordinateur, couple utilisateur/mot de passe, certificat préinstallé, etc.). Cette authentification devra également permettre de gérer les droits d'accès des utilisateurs aux équipements actifs du réseau, le tout via Radius, un protocole d'authentification couramment utilisé en réseau.

La réalisation de ce projet permettra de faciliter le travail du personnel de B.H. Consulting lors de l'installation et la maintenance des équipements actifs que l'entreprise propose à ces clients. Une interface web leur permettra de gagner du temps pour configurer les accès au réseau, et permettre aux administrateurs locaux d'être plus indépendants. La partie gestion et sauvegardes des configurations permettra aux employés de B.H. Consulting, comme aux administrateurs, de gagner du temps pour la configuration des équipements, tout en leur éliminant le stress des sauvegardes à effectuer. Ces dernières permettront d'assurer que le remplacement d'un équipement défectueux se fera rapidement, et permettront de revenir rapidement en arrière en cas d'erreur.

L'objectif est donc la gestion de réseaux plus sécurisés, un gain de temps pour B.H. Consulting et ses clients, et moins de risques de coupures pour les utilisateurs finaux. Cet outil sera stratégique dans le développement de l'entreprise.

1. <http://bh-consulting.net>

1.4 Contexte

Ce projet a été proposé dans le cadre des projets industriels de l'École TELECOM Nancy. L'entreprise B.H. Consulting a besoin de cette solution technique sans pour autant avoir le crédit de temps nécessaire à sa mise en place.

Cela permet aux étudiants d'avoir un aperçu sur un véritable projet professionnel et également de montrer leurs compétences.

Le responsable du projet au sein de B.H. Consulting sera Guillaume ROCHE. De plus, Bertrand PÉTAT sera également tenu au courant de l'avancée des différentes tâches.

2 Spécifications

2.1 Objectifs précis

Dans un premier temps, le groupe devra mettre en place une authentification forte et des autorisations d'accès sur les équipements actifs (commutateurs et routeurs) grâce à un serveur d'authentification Radius. L'autorisation permet à la fois d'accéder au réseau mais aussi de configurer les éléments de réseau.

Dans un deuxième temps, il s'agira de mettre en place le standard 802.1X (décrit dans la problématique) au sein d'un réseau et d'utiliser le même serveur Radius pour l'authentification et l'autorisation. Les différentes méthodes d'authentification à considérer sont : MAC (identifiant unique du poste utilisateur, permettant une authentification transparente pour l'utilisateur final), EAP-TLS et EAP-TTLS (mots de passe ou certificats).

Enfin, l'entreprise souhaite gérer, contrôler, sauvegarder et versionner les configurations de chacun des éléments du réseau installés de manière automatique et sécurisée.

Le tout sera géré au moyen d'une interface web ergonomique et sécurisée.

2.2 Délai

La date de rendu du projet est fixée au 21 mars 2013. À cette date aura lieu la présentation du projet dans sa globalité devant un jury. De plus, une présentation intermédiaire aura lieu le 20 décembre 2012 (en anglais) afin de présenter l'avancement du projet.

Il est rappelé que le groupe a une obligation de moyens et qu'il est prévu 250 heures de travail par élève, soit un total de 1000 heures sur le projet.

2.3 Budget

Ce projet est développé dans le cadre d'un projet industriel effectué au sein de l'École TELECOM Nancy. Ainsi, aucune rémunération ne sera versée aux élèves.

Cependant, B.H. Consulting propose de fournir un environnement de tests constitué d'un routeur et d'un commutateur Cisco.

De plus, l'École fournit deux machines de travail qui pourront faire office de client/serveur Radius, avec un accès vers l'extérieur.

2.4 Niveau de qualité attendu

Le groupe doit s'assurer que le niveau de sécurité mis en place correspond bien à celui du protocole 802.1X couplé à un serveur Radius. Il s'agit de vérifier la bonne configuration des serveurs et NAS (équipements actifs servant de passerelle pour l'authentification dans le cadre du protocole 802.1X), et également de s'assurer que l'interface web n'introduise pas de problèmes de sécurité.

L'entreprise souhaite que, dans la mesure du possible, l'interface web soit ergonomique. Elles seront conçues en accord avec le responsable du projet, Guillaume ROCHE.

2.5 Priorités des objectifs

Il est indispensable que l'authentification forte soit mise en place avec trois méthodes d'authentification : adresse MAC (automatique pour l'utilisateur), login/password (simple pour l'utilisateur) et certificats (nécessite une installation en amont, mais plus sécurisé).

Une fois cette étape terminée, il est important de mettre en place une architecture qui permette la gestion et la sauvegarde des configurations du matériel réseau installé.

De plus, si les conditions le permettent, une automatisation complète du système de sauvegarde sera la bienvenue.

Il est également important que le tout puisse être géré au sein d'une interface web sécurisée.

S'il reste du temps, le groupe devra mettre en œuvre une supervision des sessions (qui s'est connecté, et quand) et des actions pour chaque utilisateur, un système de gestion des certificats, l'importation de nouveaux utilisateurs avec un fichier CSV (fichier texte plat de données, par ligne et dont les valeurs sont séparées à l'aide de virgules) la gestion d'une hiérarchie des droits, un terminal émulé (configuration via l'interface des équipements actifs) et l'envoi de courriels en cas de problème sur l'infrastructure.

2.6 Risques

Le projet n'impliquant pas d'intervenir directement sur des infrastructures en production, les risques pour l'équipe sont limités.

La notion de sécurité sera prépondérante, et pourrait induire des effets de bord non-désirés sur l'étanchéité du réseau de l'entreprise, si l'équipe ne voit pas les possibilités d'attaques qui pourraient être offertes par la nouvelle installation. L'entreprise B.H. Consulting pourrait ensuite être tenue responsable d'une intrusion par l'un de ses clients à cause de notre produit. L'équipe garantit de surveiller cet aspect avec vigilance, à la mesure de notre expérience et de nos compétences. Des tests d'écoute du réseau seront effectués et reportés.

L'ergonomie de l'interface pouvant sembler une notion subjective, il faudra également veiller régulièrement à ce que l'expérience utilisateur corresponde bien aux attentes de Guillaume ROCHE, qui lui-même représentera les clients qui auront aussi à l'utiliser.