Certaines parties de ce laboratoire doivent être faites en équipe

Certaines parties de ce laboratoire doivent être faites individuellement

Objectifs

- Comprendre les possibilités offertes par une solution VPN
- Paramétrer un serveur VPN sous Active Directory
- Paramétrer les autorisations des utilisateurs, par UOAD et par GPO
- Paramétrer les postes clients, par le «Centre de réseautage»

Étape 1 (En équipe) - Mise en place du serveur VPN

Pour tester ce laboratoire vous devez utiliser des postes qui seront vos «clients externes» ou «clients VPN».

Votre «serveur virtuel» installé sur votre routeur, ou encore les postes d'une autre équipe sont les ordinateurs qui peuvent tenir le rôle de postes externes. À partir de ces postes vous allez faire des accès à votre réseau via une configuration VPN.

Sur votre routeur

Désactiver le routage et l'accès à distance

Configurer et activer le routage à distance

- Choisir l'option 3 - «Accès VPN (Virtual Private Network) et NAT
- Choisir la carte «OnBoardConfig»
- Choisir l'attribution d'adresses IP «Automatiquement»
- Répondre «Non» pour l'interaction avec un serveur radius
- Lire le message d'avertissement et faire «OK»

Dans la feuille des propriétés du serveur

- Onglet «IPv6» les deux crochets doivent être retirés

Sous le serveur, section «Ports», Écran «Propriétés»

> *Accepter les messages d'avertissement*

- Configurer «WAN Miniport (IKEv2)» à 2 ports
- Configurer «WAN Miniport (SSTP)» à 3 ports
- Configurer «WAN Miniport (PPTP)» à 5 ports
  - Décocher l'option «Connexions de routage à la demande (entrantes et sortantes)»
- Configurer «WAN Miniport (L2TP)» à 4 ports
  - Décocher l'option «Connexions de routage à la demande (entrantes et sortantes)»

N.B.

Après une configuration du routeur il est préférable de faire une actualisation.

Il est quelques fois obligatoire de faire un redémarrage des services.

Que vous dit le message d'avertissement lors de la configuration du routeur?

Étape 2 (En équipe) – Répartition des adresses

Vous aurez besoin de plusieurs adresses supplémentaires pour nos clients VPN. Si jamais les adresses mentionnées sont déjà utilisées sur votre réseau, prévoir en équipe des intervalles d'adresses différents. Voici ce qui est prévu comme adresses clients :

Pour la section de test : Adressage IP via une réservation

Équipier 1 : 172.61.G.231

Équipier 2 : 172.61.G.232

Équipier 3 : 172.61.G.233

G correspond au numéro propre à votre équipe

Aucune configuration n'est nécessaire sur le routeur

Pour la section de test : Adressage IP via le routeur

172.61.G.200 à 172.61.G.220

G correspond au numéro propre à votre équipe

Sur votre routeur

Dans la feuille des propriétés du serveur, onglet «IPv4»

- Choisir «Pool d'adresses statique»
- Bouton «Ajouter»,
- Donner la plage d'adresses 172.61.G.200 à 172.61.G.220

Étape 3 (Individuellement)- Mise en place d'un client VPN

Choisissez un poste d'une autre équipe ou encore utiliser votre serveur virtuel sur votre routeur.

> *Ce sera votre poste externe.*
>
> *Si vous utilisez le poste d'une autre équipe, assurez-vous que la session est ouverte avec un utilisateur de type administrateur de leur domaine.*

Dans le «Centre Réseau et partage»

- Choisir «Configurer une nouvelle connexion ou un nouveau réseau»
- Choisir «Connexion à votre espace de travail»
- Choisir «Utiliser ma connexion Internet (VPN)»
- Dans «Adresse Internet»
  - Donner l'adresse principale **publique** de votre routeur (serveur VPN)
- Dans «Nom de la destination»
  - Donner un nom significatif à la connexion
  - Exemple : VPN vers prénom_domaine
- Enlever le crochet à «Mémoriser mes informations d'identification»
- Mettre un crochet à «Autoriser d'autres personnes à utiliser cette connexion»

Ne faire aucune tentative de connexion,

le paramétrage du service VPN n'est pas terminé.

Ouvrir la console «ncpa.cpl»

- Votre connexion VPN devrait être présente comme une autre carte réseau
  - Porter attention à l'icône
- Vérifier les options du menu contextuel
- Vérifier la feuille des propriétés de votre connexion

Vous pouvez avoir accès à votre connexion en cliquant sur l'icône «Réseau» dans votre barre de tâche à droite. Cette action affichera une bande à droite de votre écran où vous retrouverez chacun des éléments présents dans «ncpa.cpl». En cliquant sur la connexion VPN vous aurez accès à l'option «Connecter/Déconnecter» selon votre état.

Étape 4 (Individuellement)

Configuration utilisateur – Mode : Adresse IP via le routeur

Sur votre serveur personnel

À partir d'une console «UOAD» modifier les propriétés de votre utilisateur personnel.

Dans l'onglet «Appel entrant»,

- Autoriser les accès

Sur votre poste externe

Connecter en VPN à l'aide de votre utilisateur personnel

- Icône «Réseau» dans la barre de tâches
- Cliquer sur votre connexion VPN
- Faire «Connecter»
- Identifiez-vous

Une fois connecté, faire un ipconfig/all dans une invite de commande

Qu'avez-vous comme adresse et expliquer sa provenance ?

Comment se nomme votre carte ayant l'adresse 172 de votre réseau ?

Selon vous, est-ce que les sites web de votre réseau privé devraient être accessibles par adresse ou par nom, même si le pare-feu n'est pas ouvert ? Tester l'accès.

Sur votre routeur où peut-on voir qui est connecté et quelles informations voyez-vous ?

Sur votre routeur dans la section Ports comment sont signalés les ports utilisés ?

Déconnectez-vous de l'accès VPN et faire un ipconfig/all.

Qu'avez-vous comme adresses IP ?

Étape 5 (Individuellement)
Configuration utilisateur – Mode : Adresse IP via une réservation

Sur votre serveur personnel

À partir d'une console «UOAD» modifier les propriétés de votre utilisateur personnel.

Dans l'onglet «Appel entrant»,

- Autoriser les accès
- Cocher «Attribuer des adresses IP statiques»
  - Via le bouton, attribuer une adresse IPv4
  - Choisir l'adresse selon l'étape 2 du présent laboratoire (231, 232, 233)

Sur votre poste externe

Connecter en VPN à l'aide de votre utilisateur personnel

Faire un ipconfig/all dans une invite de commande

Qu'avez-vous comme adresse et expliquer sa provenance ? 

Déconnectez-vous de l'accès VPN et faire un ipconfig/all

Étape 6 (Individuellement)
Configuration utilisateur – Refus

Sur votre serveur personnel

À partir d'une console «UOAD» modifier les propriétés de votre utilisateur personnel.

Dans l'onglet «Appel entrant»,

- Refuser l'accès

Sur votre poste externe

Connecter en VPN à l'aide de votre utilisateur personnel

Que se passe-t-il ? 

Étape 7 (Individuellement)
Configuration utilisateur – Via les GPO

Sur votre serveur personnel

À partir de la console «UOAD» modifier les propriétés de votre utilisateur personnel.

Dans l'onglet «Appel entrant»,

- Cocher «Contrôler l'accès via la stratégie d'accès à distance»

Pour rendre l'exercice plus personnel, vous allez vous créer un nouveau groupe «grVotrePrénom»

- Mettre votre utilisateur personnel membre de ce groupe

À partir de la console Serveur NPS (Network Policy Server) en sélectionnant l'ordinateur qui est votre routeur

On peut installer la console par l'ajout de la fonctionnalité «Outils d'administration de serveur distant», «Outils d'administration de rôles», «Outils de le stratégie réseau et des services d'accès»

Il est aussi possible de faire ce travail directement sur le routeur

Les paramètres mis dans cette console influence le comportement du routeur

Attention vous y verrez aussi les stratégies de vos collègues

Dans la section «Stratégies»

- Dans la section «Stratégies réseau» dans le menu contextuel, créer une nouvelle stratégie d'accès distant
- Écran Nom et type
  - Nom : «Accès - votre prénom»
  - Type de serveur d'accès réseau : «Serveur d'accès à distance (VPN-Dial up)»
- Écran Condition
  - Bouton «Ajoutez»
  - Choisir «Groupes d'utilisateurs»
  - Ajouter votre groupe «grVotrePrénom»
- Écran Autorisation d'accès
  - Sélectionner : Accès accordé
- Écran Méthodes d'authentification
  - Ajouter dans «Types de protocoles EAP «Microsoft : Mot de passe sécurisé (EAP-MSCHAP version2)
  - Vous pouvez décocher «Authentification chiffrée Microsoft (MS-CHAP)»
- Écran Contraintes : ne rien changer
- Écran Paramètres, ne rien changer

N.B. Votre nouvelle stratégie devrait apparaître en début de liste

Sur votre poste externe

Connecter en VPN à l'aide de votre utilisateur personnel

Que se passe-t-il ?

Étape 8 – Synthèse

Refaire une configuration d'accès VPN pour un utilisateur créé dans un laboratoire précédent. La configuration devra avoir les caractéristiques suivantes :

- Une adresse réservée
- Accès accordé via une stratégie d'accès distant
- Uniquement pour cet utilisateur
- Durant les heures de cours du lundi
- N.B. Cet utilisateur devrait être membre de votre nouveau groupe

L'accès devra être testé d'un poste d'une équipe différente de celui utilisé précédemment.