Les différents moyens de reconnexion à Nuabee

Test de PRA · https://preview.nuabee.fr/documents/les-differents-moyens-de-reconnexion-a-nuabee/

Moyens de reconnexion à l’environnement PRA Nuabee

Dans le cadre des tests de PRA ou lors d’une crise réelle, Nuabee met à disposition plusieurs moyens de reconnexion permettant d’accéder à l’environnement de secours hébergé dans le cloud.

Ces solutions couvrent différents besoins : interconnexion réseau site-à-site, accès utilisateur, mobilité, accès technique de secours et interconnexion privée. Le choix du mode de reconnexion dépend de l’architecture du client, des contraintes de sécurité, des performances attendues et du contexte (test ou crise réelle).

Chaque solution fait l’objet d’une documentation dédiée détaillant son fonctionnement et ses prérequis.

Solution	Type d’accès	Cas d’usage principaux	Utilisation en test	Utilisation en crise
VPN IPsec	Site à site (réseau)	Interconnexion sécurisée entre le site client et le PRA	(exceptionnel)	
NCA (Nuabee Cloud Access)	Appliance réseau	Accès réseau simple depuis site de repli		
Appliances de sécurité	Pare-feu / VPN / sécurité	Reproduire l’architecture de sécurité	(exceptionnel)	

SoftEther (VPN utilisateurs)	VPN utilisateur	Accès utilisateur / mobilité		
CAV-MPLS (Cloud Avenue)	Interconnexion privée MPLS	Lien privé haute disponibilité avec PRA	(exceptionnel)	
Machine de rebond	Accès RDP intermédiaire	Accès technique sécurisé au PRA		⚠ (pré-crise)
VNC console Nuabee	Accès console technique	Dépannage bas niveau		⚠ (secours)

VPN Ipsec

Explication et contexte

Le VPN IPsec est une solution de connexion sécurisée permettant d'établir un tunnel chiffré entre l'infrastructure du client et l'environnement de secours PRA de Nuabee via Internet.
Il permet de rétablir les flux réseau de manière sécurisée, comme si les deux environnements étaient interconnectés sur un même réseau privé.

Cas d'usage

Le VPN IPsec est utilisé **uniquement en cas de crise réelle PRA**, afin de permettre la reconnexion sécurisée de l'infrastructure du client vers l'environnement de secours cloud, dans le but de rétablir l'accès aux ressources critiques.

Ressources complémentaires

Cette méthode nécessite la configuration d'équipements compatibles IPsec côté client et côté Nuabee.

➡ Les paramètres techniques détaillés sont décrits dans la documentation
https://nuabee.fr/documents/vpn-ipsec-reconnexion-client/

NCA (Nuabee Cloud Access)

Explication et contexte

La NCA (Nuabee Cloud Access) est une appliance réseau fournie et préconfigurée par Nuabee, permettant d'établir automatiquement une connexion sécurisée entre l'espace de repli du client et l'environnement de reprise PRA hébergé dans le cloud.

Une fois connectée à un accès Internet, la NCA établit le tunnel VPN vers l'environnement PRA sans configuration côté client. Elle fournit un accès réseau simple et sécurisé aux ressources restaurées, via ports Ethernet et/ou Wifi.

La NCA est administrée, supervisée et maintenue à distance par Nuabee.

Cas d'usage

La NCA est utilisée :

- lors des différents tests annuels de PRA, afin de permettre l'accès à l'environnement de secours,
- lors d'une crise PRA réelle, pour assurer la reprise de l'activité admin/User depuis un espace de repli.

Ressources complémentaires

➡ Les détails techniques et prérequis sont disponibles dans la documentation:

- Présentation: https://nuabee.fr/documents/nuabee-cloud-access-nca/
- Mode opératoire: https://nuabee.fr/documents/mode-operatoire-nca/
- Prérequis paramétrages : https://nuabee.fr/documents/prerequis-nca/

Appliances de sécurité

Explication et contexte

Dans le cadre de la solution PRA, Nuabee peut intégrer des appliances de sécurité dans l'environnement de secours afin de reproduire ou maintenir le niveau de sécurité du système

d’information du client.

Ces appliances permettent d’assurer des fonctions critiques telles que le pare-feu, le VPN, la détection/prévention d’intrusion (IDS/IPS) ou d’autres services de sécurité nécessaires à la continuité d’activité. Nuabee propose notamment l’intégration d’une appliance standard (OPNsense) ainsi que la prise en charge d’autres appliances de sécurité compatibles (Fortinet, Palo Alto, Stormshield, Sophos, etc.).

Les appliances sont provisionnées dans l’espace PRA et peuvent être restaurées rapidement en cas d’activation, afin de garantir une reprise sécurisée et conforme à l’architecture du client.

Cas d’usage

Les appliances de sécurité sont utilisées :

- lors des tests de PRA, afin de valider le bon fonctionnement des règles de sécurité et des flux réseau dans l’environnement de secours,
- lors d’une crise PRA réelle, pour rétablir une architecture de sécurité équivalente à la production et permettre une reprise d’activité sécurisée.

Ressources complémentaires

➡ Les modalités complètes de prise en charge et les appliances compatibles sont décrites dans la documentation **https://nuabee.fr/documents/traitements-appliances-securite-pra-nuabee/**

➡ Gestion du trafic Nord/Sud : https://nuabee.fr/documents/gestion-trafic-firewall-nord-sud/

Softether

Explication et contexte

La solution SoftEther permet de fournir un accès VPN sécurisé aux utilisateurs, via le client natif Windows, afin de se connecter à l’environnement PRA de Nuabee.(Possible aussi avec les OS Linux)

Cette solution est particulièrement adaptée aux scénarios de reconnexion utilisateur en mobilité ou lorsque la mise en place d’une interconnexion réseau site-à-site (IPsec ou NCA) n’est pas possible. Elle repose sur un tunnel VPN chiffré, établi à la demande, permettant un accès sécurisé

aux ressources hébergées dans l'environnement de secours.

La solution SoftEther est pilotée et sécurisée par Nuabee, et permet une mise en œuvre rapide côté utilisateur.

Cas d'usage

La solution SoftEther est utilisée :

- pour permettre la reconnexion des utilisateurs en mobilité lors des tests de PRA,
- pour fournir un accès sécurisé aux utilisateurs lors d'une crise PRA réelle,
- pour des scénarios de reconnexion à la demande, lorsque les autres moyens de reconnexion (IPsec, NCA) ne sont pas adaptés ou disponibles.

Ressources complémentaires

➡ Les modalités d'accès, d'installation et de configuration sont détaillées dans la documentation **https://nuabee.fr/documents/acces-pra-securise-via-vpn-softether/**

Documentation utilisateur: https://nuabee.fr/documents/acces-pra-securise-via-vpn-softether/

Machine rebond

Explication et contexte

La machine de rebond est une machine virtuelle Windows déployée dans l'environnement PRA de Nuabee, disposant d'un accès sécurisé à l'espace de secours.

Elle sert de point d'accès intermédiaire permettant aux équipes autorisées de se connecter en RDP à cette machine, puis d'accéder aux serveurs et ressources restaurés dans l'environnement PRA. Ce mécanisme permet un accès contrôlé à l'environnement, sans exposition directe des ressources internes sur Internet.

La machine de rebond est principalement utilisée à des fins de validation, de contrôle et d'administration de l'environnement PRA.

➡ Les modalités techniques de création et de configuration sont décrites dans la documentation interne: https://nuabee.fr/documents/machine-rebond/

Cas d’usage

La machine de rebond est utilisée :

- lors des tests annuels de PRA, pour valider l’accessibilité et le bon fonctionnement de l’environnement de secours,
- en amont d’une crise PRA réelle, pour effectuer une vérification rapide de l’environnement avant la reconnexion des utilisateurs.

VNC depuis votre console Atlas

Explication et contexte

La console Nuabee permet d’accéder directement aux machines restaurées dans l’environnement PRA via une prise en main à distance en VNC, depuis le centre de commande.

Ce mode d’accès ne nécessite aucun accès réseau spécifique côté client. Il s’effectue directement depuis l’interface Nuabee et permet une connexion de secours aux machines, indépendamment des services RDP ou de la connectivité réseau classique.

Cette fonctionnalité est principalement destinée aux opérations techniques et de dépannage.

➡ L’accès VNC est disponible directement depuis la console Nuabee, dans le centre de commande.

Documentation: https://nuabee.fr/documents/vnc-via-console-nuabee/

Cas d’usage

L’accès VNC depuis la console Nuabee est utilisé :

- lors des tests de PRA, pour dépanner une machine lorsque celle-ci est injoignable en RDP,
- pour effectuer des opérations de debug ou de vérification bas niveau sur une machine restaurée,
- de manière ponctuelle, en raison d’une ergonomie limitée pour un usage utilisateur standard.

MPLS BVPN – CAV

Explication et contexte

La solution CAV-MPLS repose sur une interconnexion privée via le réseau MPLS d'Orange (Cloud Avenue), permettant de relier directement l'infrastructure du client à l'environnement PRA de Nuabee.

Nuabee a déployé une passerelle dédiée sur Cloud Avenue (site de Chartres), permettant l'acheminement sécurisé des flux MPLS entre le réseau du client et l'environnement de secours. Cette architecture permet une reconnexion sans passer par Internet, avec des performances, une stabilité et un niveau de sécurité renforcés.

La solution CAV-MPLS s'intègre dans l'architecture réseau existante du client et nécessite une coordination avec Orange pour la mise en place, la validation (VABF) et les tests de bascule.

➡ Les modalités de déploiement, de validation et de test sont détaillées dans la documentation (VABF) pour chacun de nos clients

Cas d'usage

La solution CAV-MPLS est utilisée :

- lors des tests de PRA, afin de valider la bascule des flux MPLS vers l'environnement de secours,
- lors d'une crise PRA réelle, pour assurer une reprise d'activité avec interconnexion privée, sans dépendance à Internet.