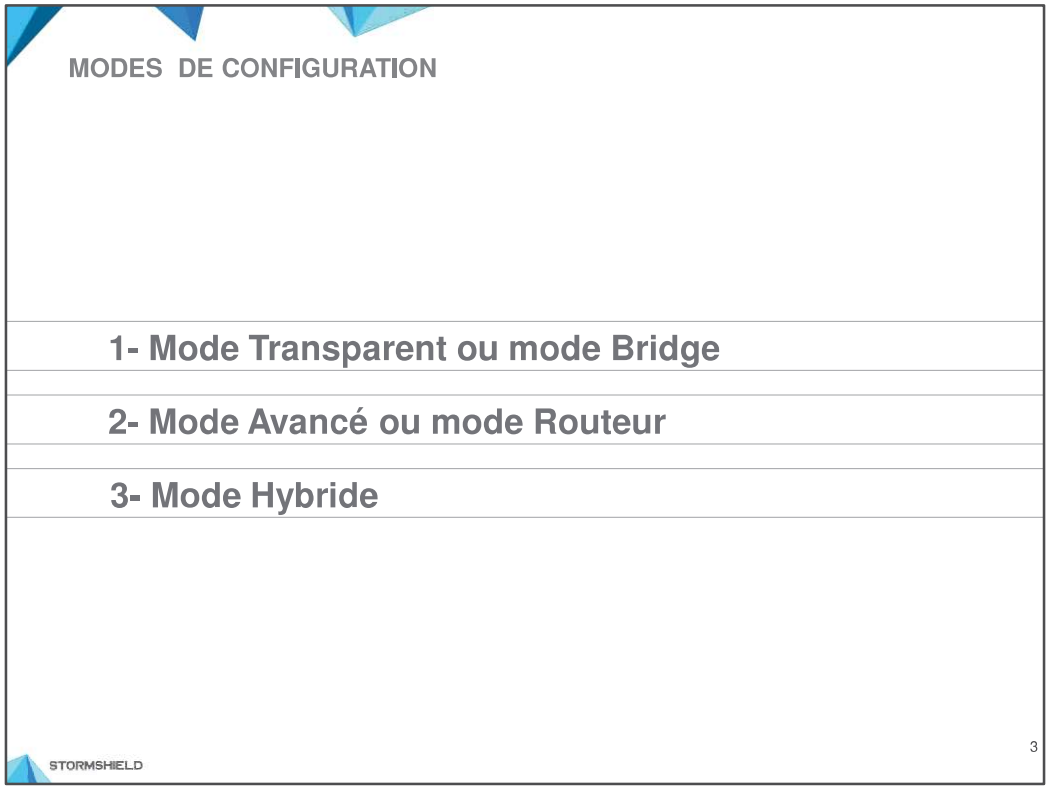
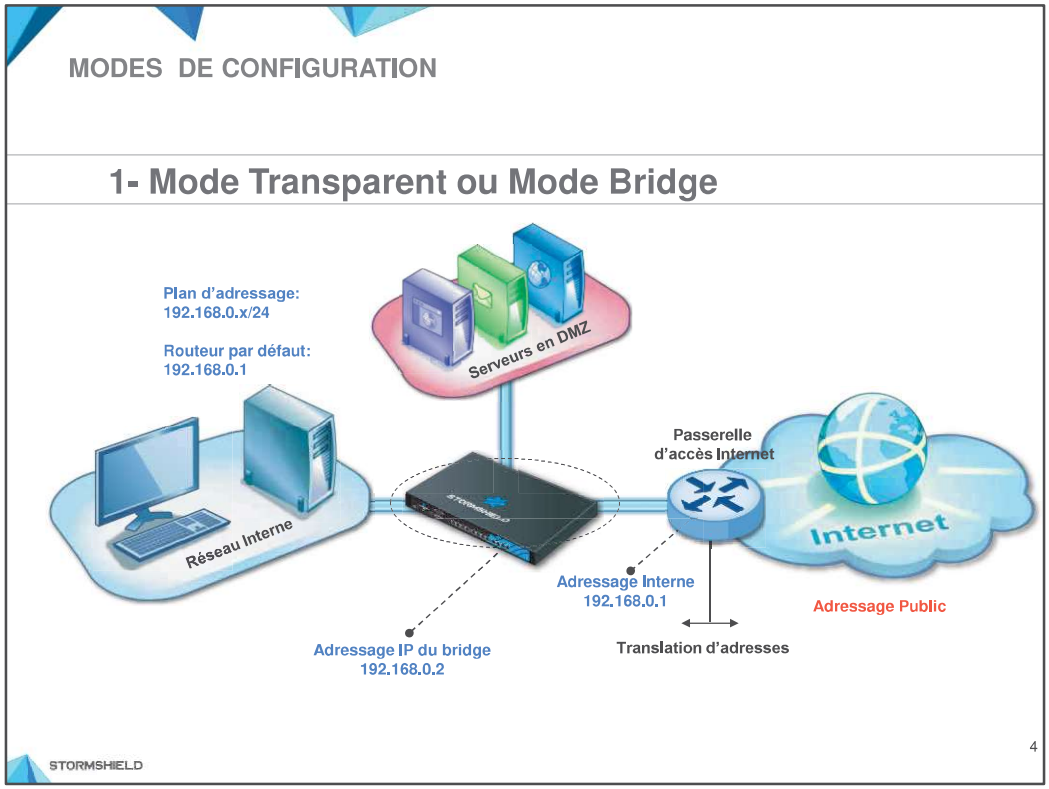


Trois modes de configuration existent sur l'ensemble de la gamme Stormshield Network Security:

- Mode transparent ou mode Bridge,
- Mode avancé ou mode routeur,
- Mode hybride.

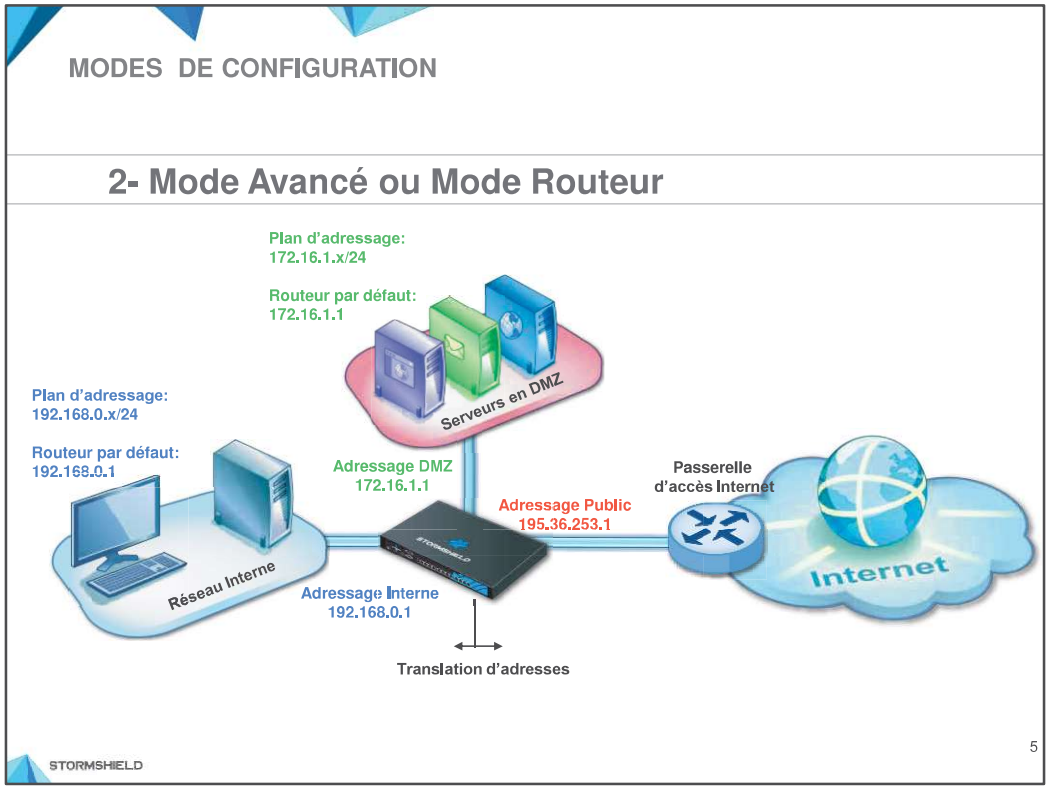
Il est important de noter qu'il n'existe pas d'assistant pour la configuration de ces modes, il s'agit uniquement d'une dénomination. La mise en œuvre de chacun des modes s'effectue suivant le besoin, en configurant les interfaces réseaux et les règles de translation.



Grâce au mode transparent, le firewall Stormshield Network s'intègre aisément dans un réseau existant sans devoir en modifier sa configuration.
La particularité de ce mode est que toutes les interfaces du firewall sont incluses dans un bridge qui porte une adresse IP du réseau local (IP utilisée pour accéder à l'interface d'administration du firewall). Ceci permet d'avoir plusieurs réseaux physiques (un réseau par interface) partageant le même réseau logique.

La communication entre les réseaux physiques et la passerelle d'accès Internet se fait en mode bridge (niveau 2) sans soustraire les flux transitant entre les interfaces aux contrôles du firewall (filtrage, analyse ASQ, etc.).

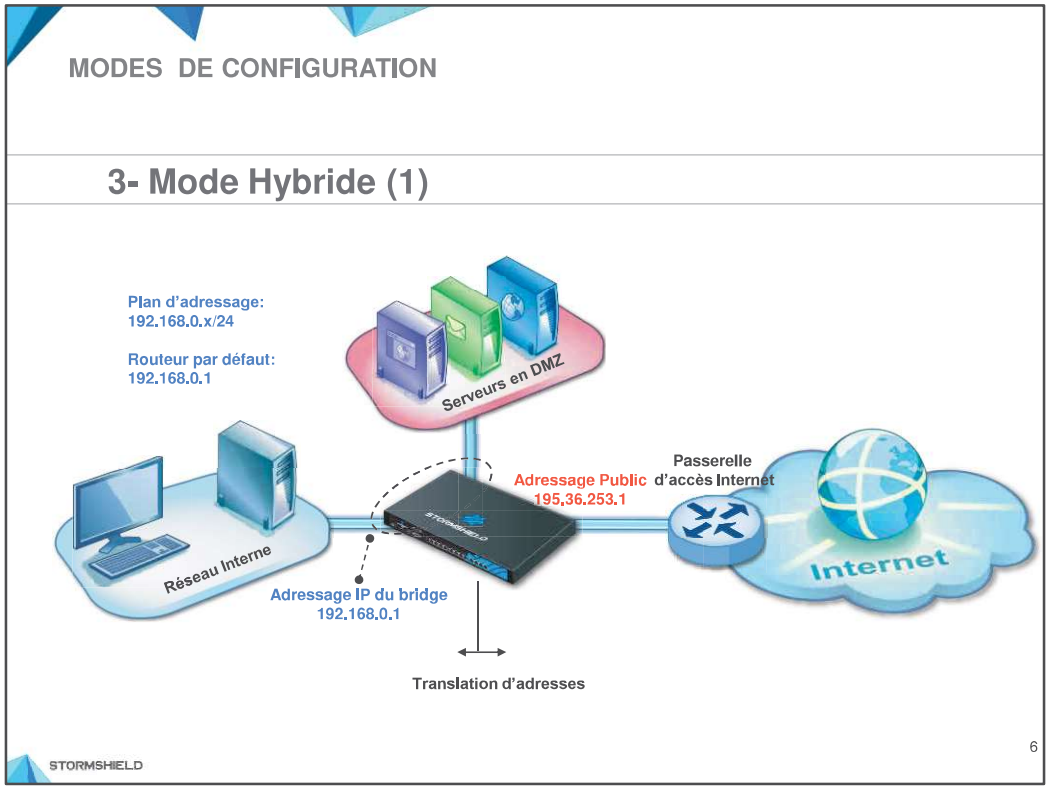
Dans la figure ci-dessus, le réseau local utilise une plage d'adresses privée 192.168.0.0/24 et accède à Internet via une passerelle qui assure la translation d'adresses. Le firewall Stormshield Network est positionné en coupure des connexions entre les machines du réseau local et la passerelle d'accès à Internet.



Dans le mode avancé, le firewall fonctionne comme un routeur en gérant plusieurs réseaux logiques (adresses réseaux). Chaque interface est configurée avec un réseau IP particulier, ce qui permet une segmentation du réseau aux niveaux physique et logique.
Dans l'image ci-dessus, le réseau local est composé de deux réseaux logiques : un réseau pour les machines internes et un réseau pour les serveurs en DMZ. Chaque réseau est connecté au firewall via une interface possédant un plan d'adressage IP spécifique. L'adresse IP publique est configurée directement sur une interface externe du firewall.

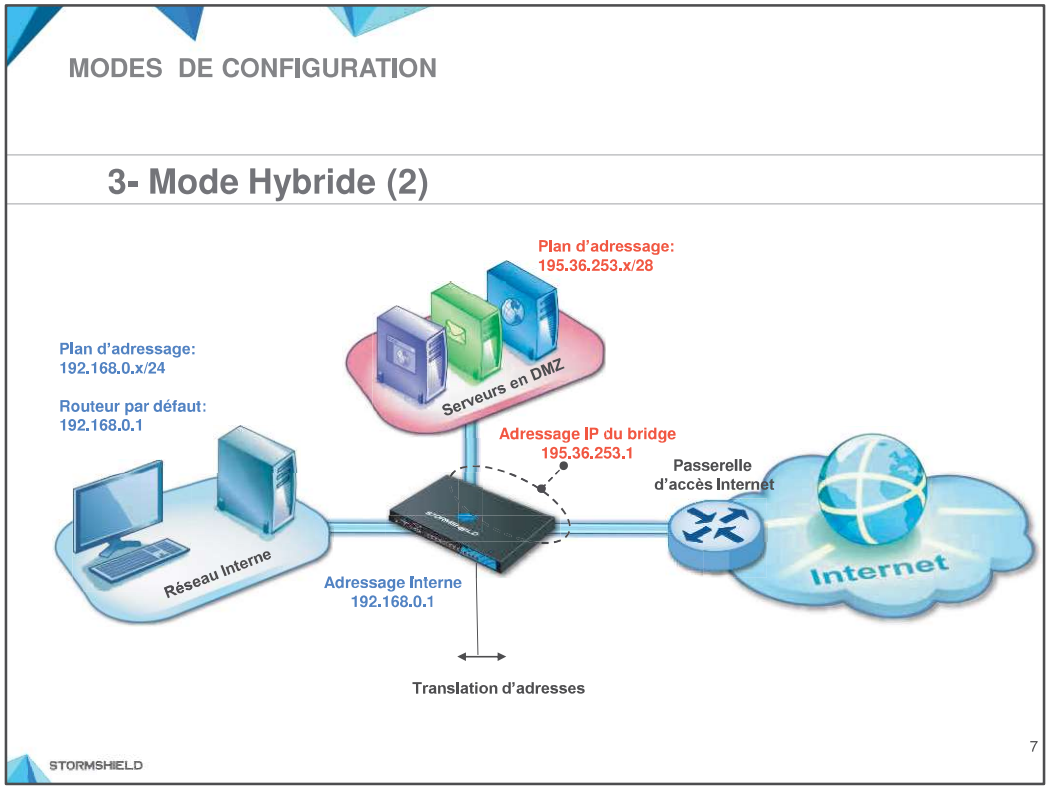
Dans ce mode, l'UTM Stormshield Network doit gérer les mécanismes de translation d'adresse pour assurer l'accès à Internet au réseau local.

Ce sera mis en oeuvre pour l'activité 4



Le mode hybride est une combinaison des modes bridge et avancé. Le principe est d'avoir plusieurs interfaces dans un bridge (même plan d'adressage) et d'autres interfaces indépendantes avec des plans d'adressages différents.

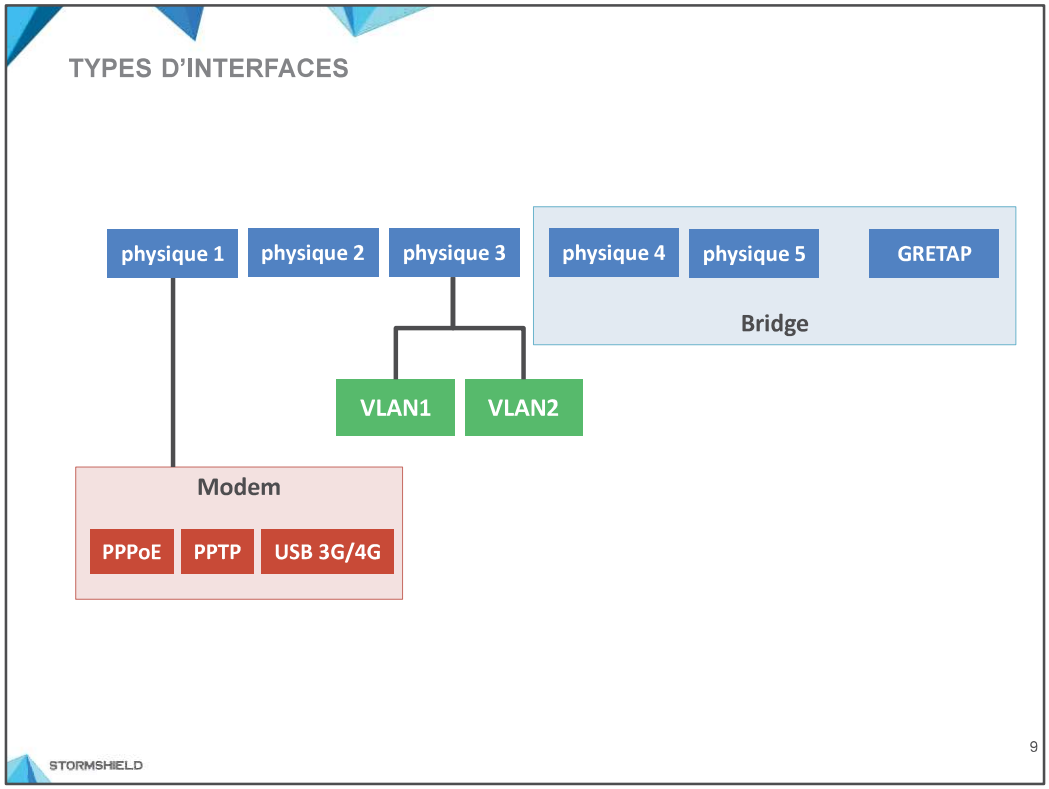
Dans ce mode nous pouvons avoir deux cas de figure. Le premier est illustré ci-dessus. Le réseau des machines internes et le réseau des serveurs en DMZ partagent le même plan d'adressage et ils sont connectés au firewall via des interfaces appartenant au même bridge. La translation d'adresse doit être configurée sur le firewall pour que le réseau local (réseau du bridge) accède à Internet via l'interface externe, configurée avec une adresse IP publique.



Le deuxième cas de figure est illustré ci-dessus. Le réseau des serveurs en DMZ est configuré avec un plan d'adressage IP public. Chaque serveur disposera donc d'une IP publique distincte.

Ce réseau est connecté au firewall par une interface incluse dans le même bridge que l'interface externe où est connecté le routeur d'accès Internet. Les serveurs en DMZ accèdent à Internet via le bridge et aucune translation d'adresse n'est nécessaire (les connexions restent néanmoins soumises aux directives de filtrage et autres analyses applicatives de l'UTM).

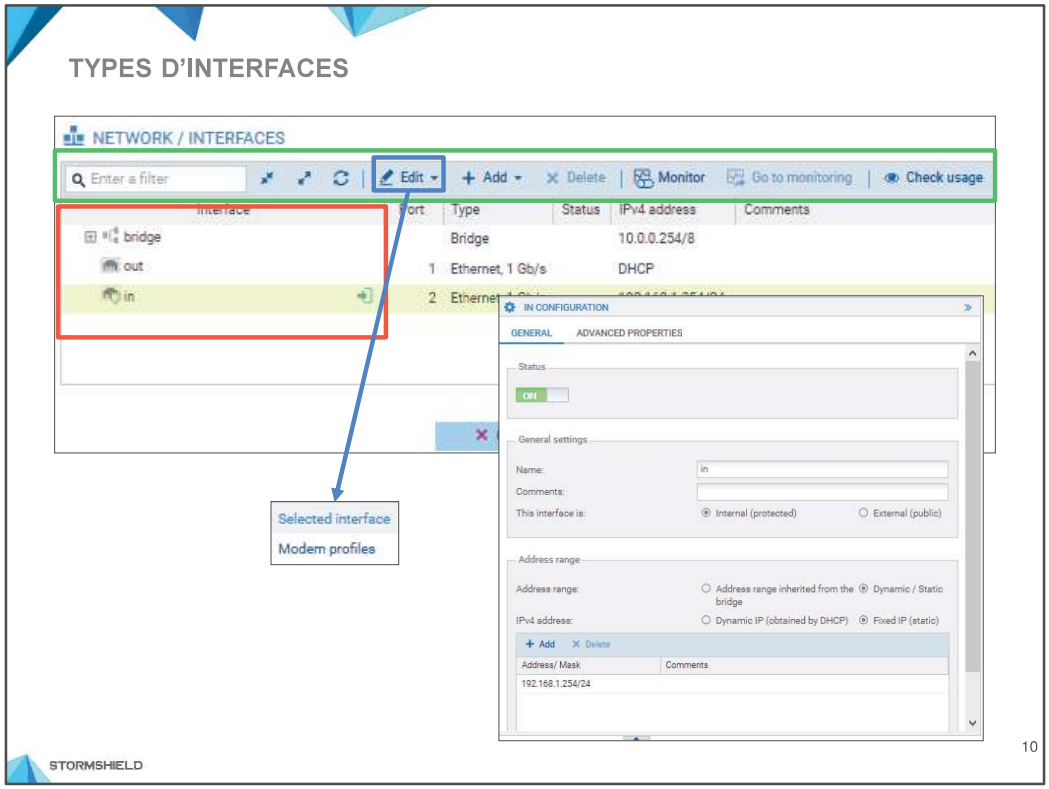
Le réseau des machines internes possède un plan d'adressage privé. Il est connecté au firewall via une interface n'appartenant pas au bridge. Par conséquent, la translation d'adresse doit être configurée pour lui permettre un accès à Internet.



Il existe 5 types d'interfaces sur le firewall :

- **Les interfaces physiques** : Le nombre d'interfaces dépend du modèle du firewall,
- **Les interfaces bridges** : association de plusieurs interfaces physiques ou VLAN. Le nombre de bridges dépend du modèle du firewall. (rappel : dans la configuration usine, toutes les interfaces appartiennent à un seul et même bridge),
- **Les interfaces VLAN** : Segment réseau attaché à une interface physique de l'UTM et caractérisée par un tag et un plan d'adressage spécifique. Le nombre maximal d'interfaces VLAN dépend du modèle du firewall,
- **Les interfaces Modem** : Ce type d'interface permet la prise en charge d'une connexion entre le firewall et un modem (ADSL, RNIS, RTC, …). Les types de connexions possibles sont : PPPoE, PPTP.
- **Les interfaces GRETAP :** Interface d'encapsulation qui permet de relier deux réseaux distants au niveau 2 (bridge). Pour cela, elle permet d'encapsuler des paquets Ethernet à l'intérieur de paquets IP via le protocole GRE. Les machines des deux réseaux distants communiqueront comme s'ils faisaient partie du même LAN.

Cela peut être un projet intéressant en faisant passer le traffic GRETAP dans un tunnel VPN IPsec pour assurer une confidentialité des flux.

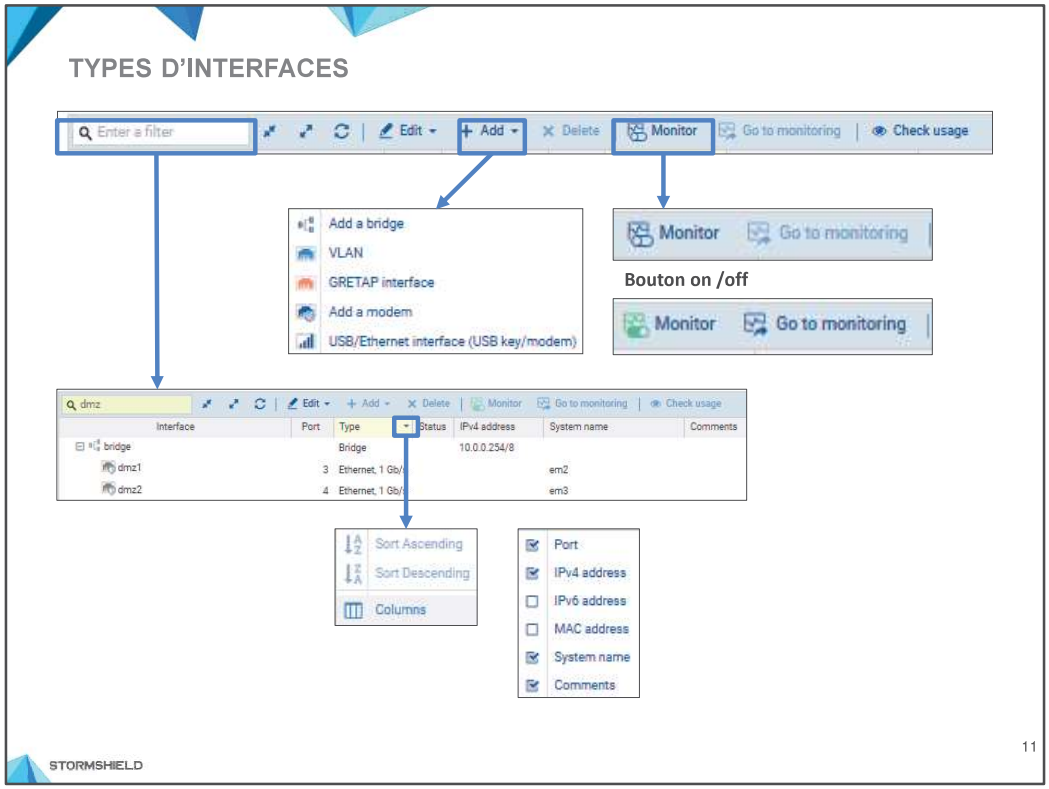


La configuration des interfaces s'effectue dans le menu **CONFIGURATION ⇒ Réseau ⇒ Interfaces**. Le menu est constitué de deux parties :

- L'en-tête (encadré vert) : offre les fonctionnalités de base pour la gestion des interfaces.
- La liste des interfaces (encadré rouge) : affiche toutes les interfaces (physique, bridge, vlan, modem) du firewall. Il est possible de faire un glisser-déposer sur les interfaces pour modifier leur configuration. Par exemple, l'ajout d'une interface à un bridge peut se faire en glissant l'interface physique et en la déposant sur l'interface bridge. L'action inverse est possible pour retirer une interface d'un bridge.

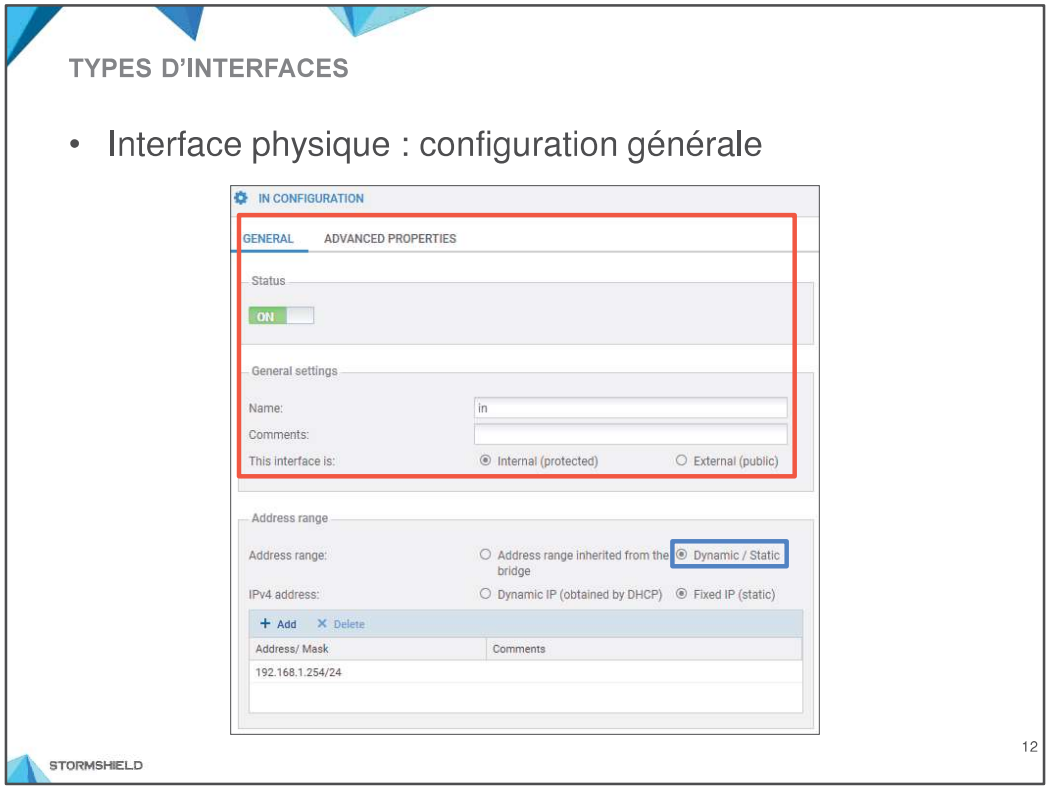
Pour configurer une interface (encadré bleu), vous pouvez double cliquer sur sa ligne en surbrillance ou cliquer sur le bouton **Edition**. La fenêtre d'édition est composée de deux onglets pour tous les types d'interface.
Les deux flèches en haut à droite de la fenêtre permettent de confirmer les modifications effectuées et de fermer la fenêtre d'édition.

NOTE : l'icône visible dans l'écran ci-dessus indique que l'administrateur est connecté au firewall via l'interface correspondante.



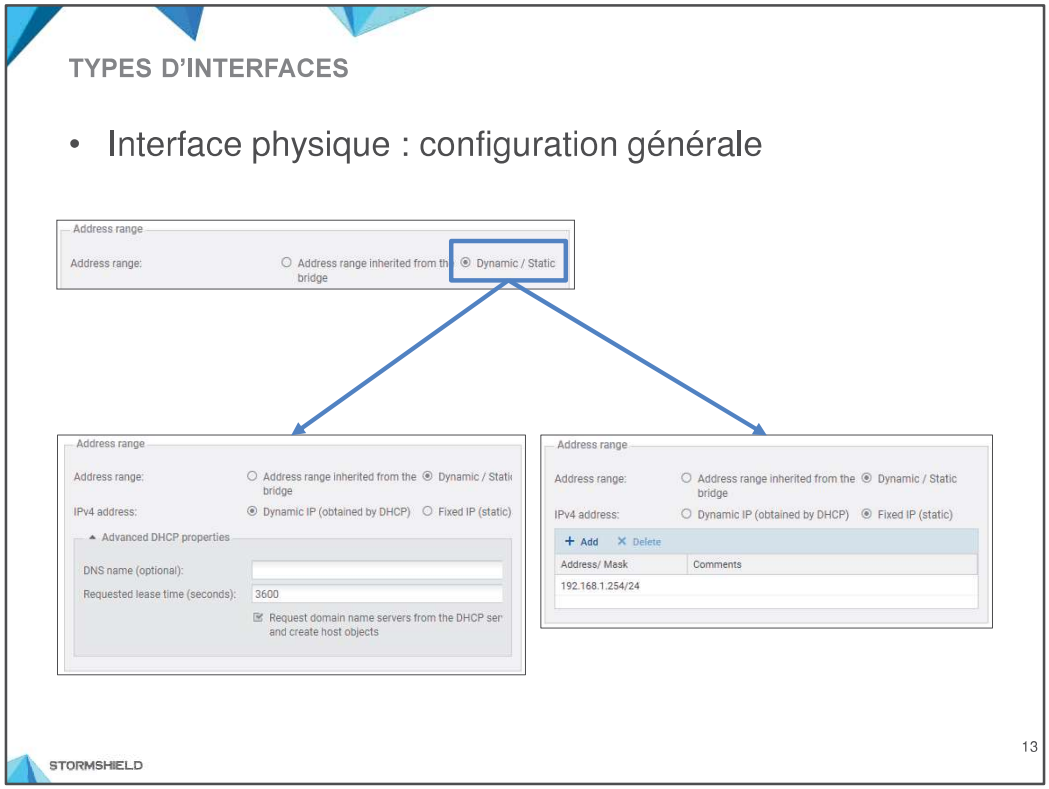
L'en-tête contient :

- **Filtre** : recherche des interfaces par une partie ou par la totalité des champs : nom, adresse IP ou commentaire,
- **Edition** : ouverture de la fenêtre de configuration de l'interface courante ou de l'un des 2 profils « Modem »,
- **Ajouter** : ajout d'une nouvelle interface de type Bridge, VLAN, Modem (ou USB Modem) ou GRETAP,
- **Supprimer** : suppression de l'interface sélectionnée. Un message d'alerte s'affiche si l'interface est utilisée dans un menu de configuration. Malgré ce message, la suppression peut être forcée,
- **Superviser** et **Accéder à la supervision** : activation ou désactivation de la supervision d'une interface pour vérifier l'utilisation de la bande passante et le nombre de connexions,
- **Vérifier l'utilisation** : afficher les menus de configuration dans lesquels l'interface est utilisée. Le résultat de cette vérification s'affiche dans l'encadré de gauche en-dessous de l'icône favoris ★



Une interface physique porte au moins une adresse IP, dynamique ou statique (encadré bleu), les paramètres dans l'encadré rouge sont détaillés ci-après :

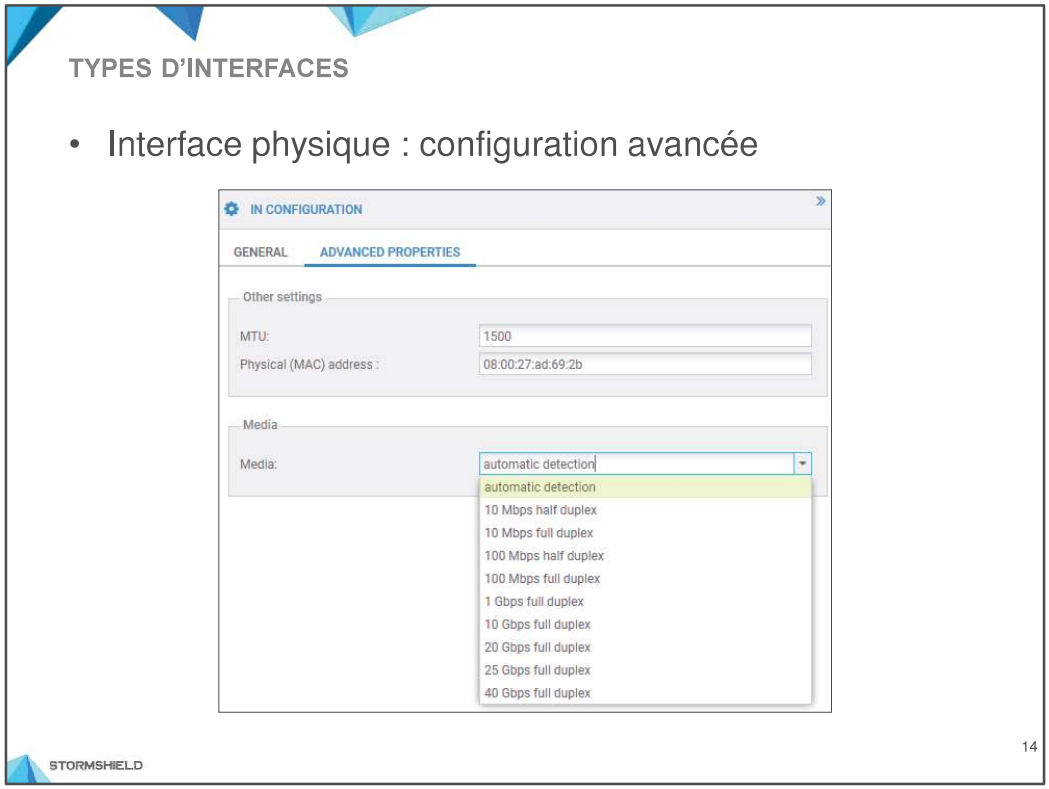
- **État** : interface activée ou désactivée
- **Nom** : Le nom de l'interface est obligatoire, c'est un nom logique différent du nom système de l'interface,
- **Commentaire** : paramètre facultatif pour ajouter toute remarque informative au sujet de l'interface sélectionnée,
- **Cette interface est** :
  - **interne (protégée)** : Une interface protégée n'accepte que les paquets provenant d'un plan d'adressage connu, tel qu'un réseau directement connecté ou un réseau défini par une route statique. Cette protection comprend une mémorisation des machines connectées à cette interface (protégeant ainsi contre l'usurpation d'identité), et permet de générer les règles de filtrage implicites lors de l'activation de certains services du firewall (par exemple SSH). Une icône représentant un bouclier est apposée à toute interface protégée.
  - **externe (publique)** : Indique que l'interface est dépourvue des protections d'une interface protégée et peut donc recevoir des paquets provenant de n'importe quel plan d'adressage (qui ne font pas partie des plans d'adresses des interfaces internes). Ce type d'interface est utilisé principalement pour connecter le firewall à Internet.



Les paramètres dans l'encadré **Plan d'adressage** sont détaillés ci-après :

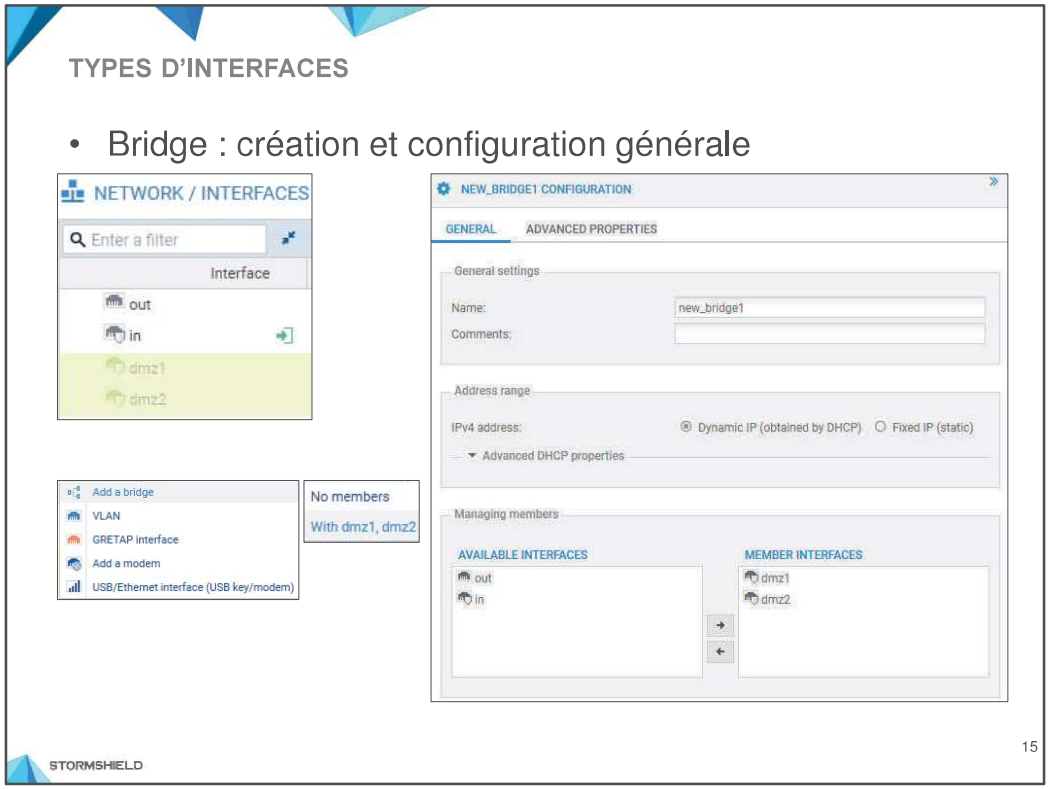
- **Adressage** : choix entre les deux possibilités suivantes :
  - **Plan d'adressage hérité du bridge** : se reporter à la section bridge plus loin dans ce chapitre,
  - **Dynamique/statique** : la définition du type d'adresse est précisée sur la ligne suivante : Adresse IPv4.
- **Adresse IPv4** : choix entre les deux possibilités suivantes :
  - **IP dynamique** (obtenue par DHCP). Un menu de configuration DHCP avancée s'affiche :
    - **Nom DNS (facultatif)** : Indique le nom de domaine envoyé au serveur DHCP,
    - **Durée de bail demandée (secondes)** : Permet de configurer la durée du bail DHCP demandée au serveur DHCP,
    - **Demander les serveurs DNS au serveur DHCP et créer les objets machine** : le nom des objets créés est Firewall_<nom_interface>_dns_1, Firewall_<nom_interface>_dns_2, etc.
  - **IP fixe (statique)** : La sélection de cette option indique que l'interface possède une adresse IP fixe qui doit être renseignée dans la liste en-dessous, accompagnée d'un masque réseau. Le masque peut être écrit aux formats numérique ou CIDR. Plusieurs adresses IP fixes (alias) peuvent être configurées sur une interface, même si elles font partie du même réseau IP.

NOTE : aucune configuration n'est prise en considération si elle n'est pas appliquée avec le bouton **Appliquer** .



La figure ci-dessus illustre l'onglet **CONFIGURATION AVANCÉE** :

- **MTU** : indique la taille du MTU de l'interface en octets,
- **Adresse physique (MAC)** : permet de forcer l'adresse MAC d'une interface,
- **Média** : permet de choisir la vitesse du lien utilisé par l'interface. Par défaut, la vitesse est détectée automatiquement.



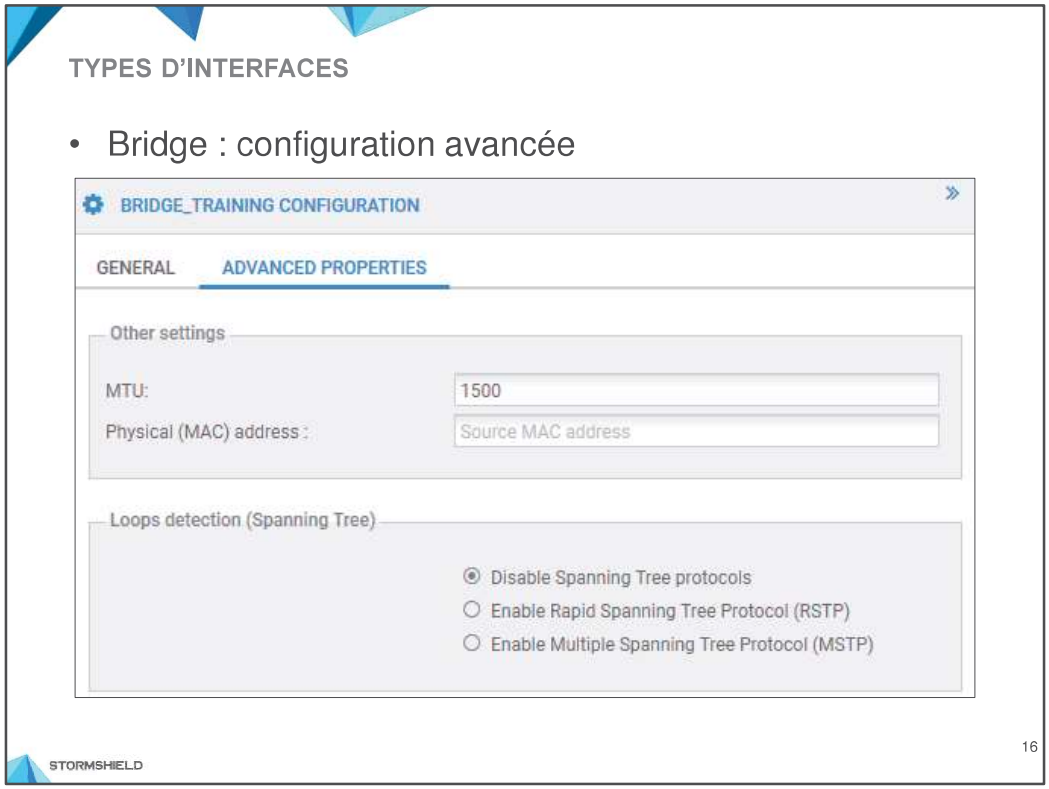
Deux méthodes sont disponibles pour la création d'un bridge :

1. Présélection des interfaces membres du bridge : les interfaces sont mises en surbrillance, la fenêtre de configuration est directement renseignée, comme ci-dessus,
2. Création d'un bridge sans interface membre, le nom du bridge dans la fenêtre de configuration reste grisé, jusqu'à ce que au moins deux interfaces soient sélectionnées comme membres du bridge.

L'onglet de **CONFIGURATION GÉNÉRALE** contient :

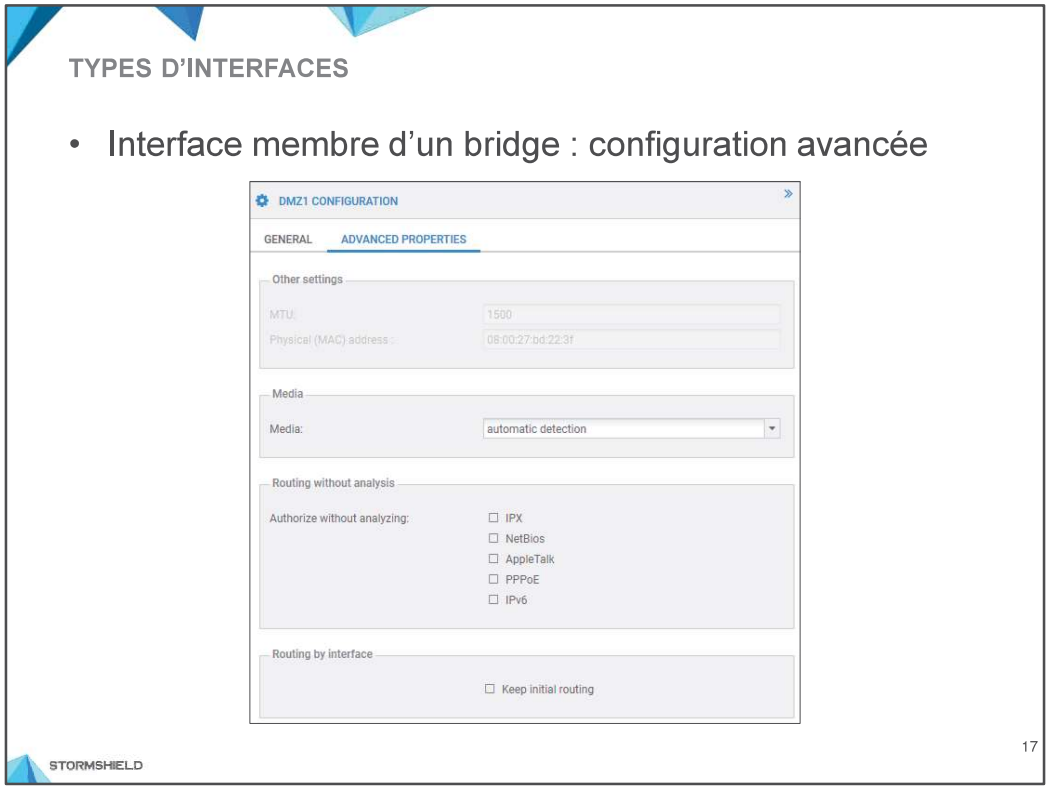
- **Paramètres généraux** : nommage de l'interface (champ obligatoire) et commentaire facultatif,
- **Plan d'adressage** : le bridge peut être configuré avec une adresse IP fixe accompagnée d'un masque réseau ou avec une IP dynamique fournie par un serveur DHCP,
- **Gestion des membres** : choix des interfaces membres du bridge, qui héritent de ses paramètres IP.

NOTE : Le nombre maximum de bridge dépend du modèle.



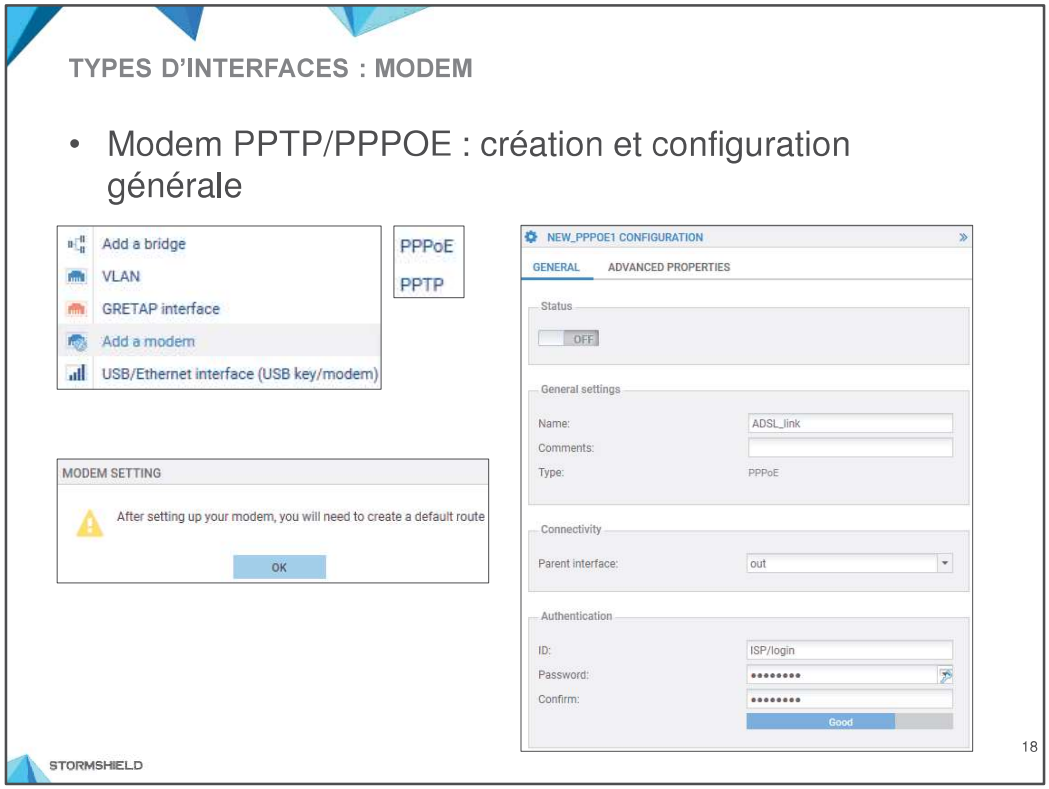
La figure ci-dessus illustre l'onglet **CONFIGURATION AVANCÉE** d'un bridge :

- **MTU** : indique la taille du MTU de l'interface en octets,
- **Adresse physique (MAC)** : permet de forcer l'adresse MAC du bridge. Toutes les interfaces membres du bridge héritent de son adresse MAC (et de son adresse IP),
- **Détection de boucles (Spanning Tree)** : permet d'activer le protocole RSTP ou MSTP pour communiquer avec les éléments de couche 2 du réseau et éviter les boucles.



La figure ci-dessus illustre l'onglet **CONFIGURATION AVANCÉE** d'une interface :

- **MTU et Adresse Physique (MAC) :** les champs sont grisés puisqu'ils sont hérités du bridge (adresse MAC commune à toutes les interfaces membres),
- **Média** : permet de choisir la vitesse du lien Ethernet utilisé par l'interface. Par défaut, la vitesse est détectée automatiquement,
- **Autoriser sans analyser** : autorise les paquets IPX (réseau Novell), NetBIOS (sur NETBEUI), AppleTalk (pour les machines Macintosh), PPPoE ou IPv6 entre les interfaces du bridge sans aucune analyse ni inspection de niveau supérieur (le firewall fonctionne comme un commutateur).
- **Préserver le routage initial** : Garde l'adresse MAC de destination des trames reçues par une interface membre du bridge et envoyée par une autre interface membre, ce qui préserve par conséquence le routage initial des paquets. Cette option facilite l'intégration transparente du firewall dans un réseau sans avoir à modifier la route par défaut des machines. **Attention** : L'activation de cette option peut avoir des effets négatifs sur certaines fonctionnalités qui nécessitent la modification des paquets par le firewall.



Le firewall peut être raccordé à différents types de modem :

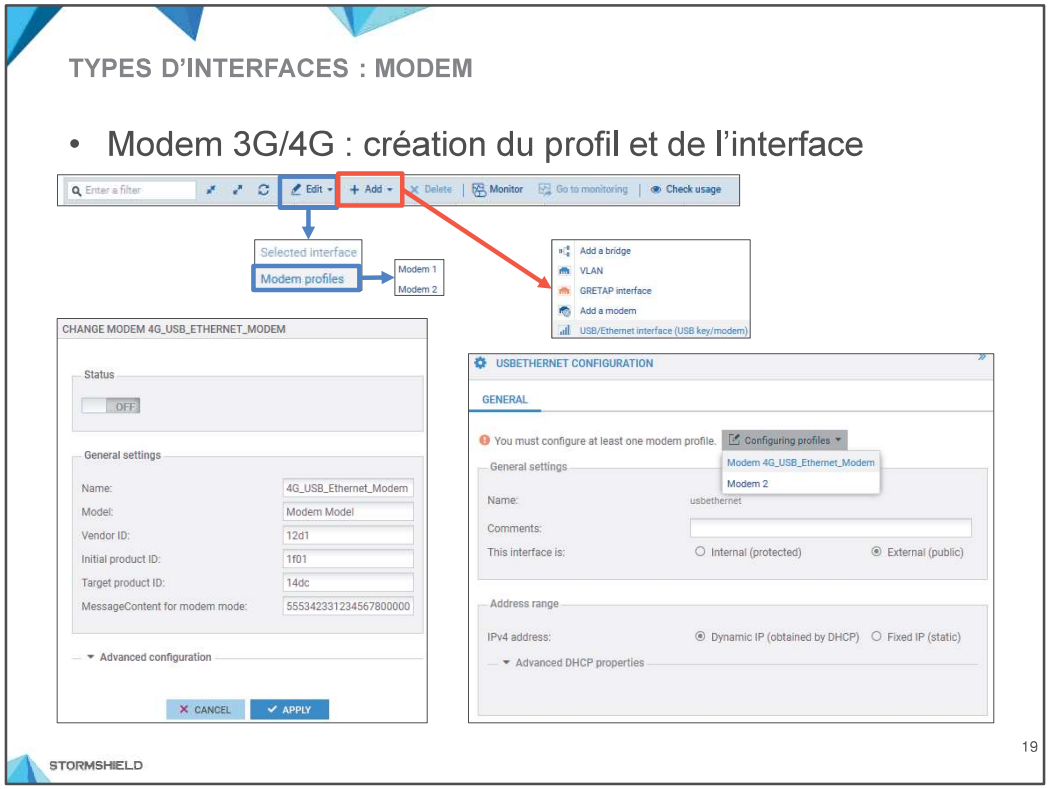
- Un modem ADSL ou câble : raccordé à une interface Ethernet (exemple montré ci-dessus),
- Un modem 3G/4G : raccordé au port USB (diapositive suivante).

Le nombre maximal de modems qui peuvent être raccordés en même temps dépend du modèle de firewall.

La figure ci-dessus illustre l'onglet **CONFIGURATION GÉNÉRALE**, affiché juste après l'avertissement qui précise qu'une route par défaut devra être créée après la configuration du modem :

- **Identification du modem** : nommage de l'interface et ajout d'un commentaire facultatif,
- **Configuration du modem** : les paramètres de ce menu changent en fonction du type du modem choisi:
  - **PPPoE**: Le modem doit être connecté à une interface externe qui doit être choisie dans le paramètre **Interface parente**,
  - **PPTP**: La négociation PPTP nécessite l'adresse IP du serveur PPTP qui doit être renseignée dans le paramètre **Adresse PPTP**,
- **Authentification** : Permet de renseigner l'identifiant et le mot de passe utilisés par la connexion modem. Ces informations sont transmises par le fournisseur d'accès.

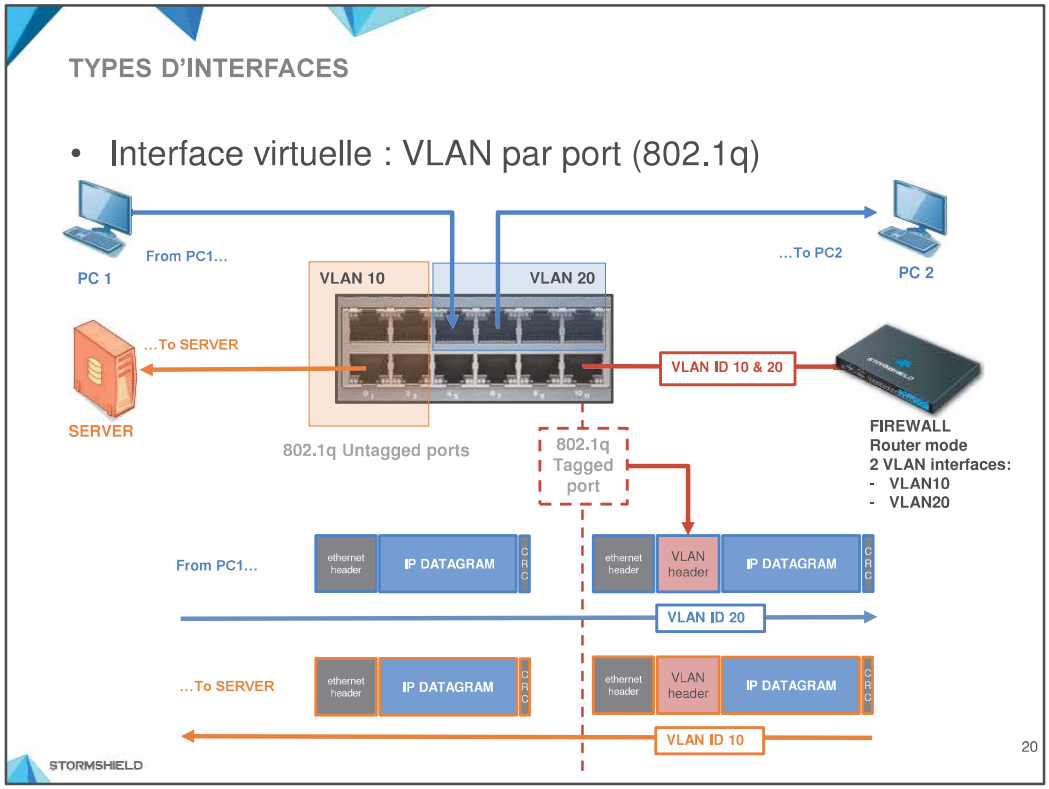
NOTE : l'onglet **CONFIGURATION AVANCÉE** d'un modem PPTP ou PPPoe permet de choisir si la connectivité est permanente où à la demande.



Il existe deux types de modems 3G/4G :

- Modem Ethernet over USB : une fois le modem connecté au firewall et configuré, c'est le modem qui porte l'adresse IP publique et opère alors comme un routeur vis-à-vis du firewall,
- Modem USB : une fois le modem connecté au firewall et configuré, c'est le firewall qui porte l'adresse IP publique.

Avant de créer l'interface modem, il faut configurer un profil selon les paramètres de configuration fournis par le constructeur du modem. Pour plus de détails, reportez-vous à la note technique : « Configurer un modem 3G/4G sur SNS ». Les éléments à préciser sur le profil sont déterminés par la procédure de la note technique.
Un redémarrage du firewall est nécessaire après la création du profil.
Après redémarrage, créez l'interface, et attachez le profil préalablement configuré à cette interface.



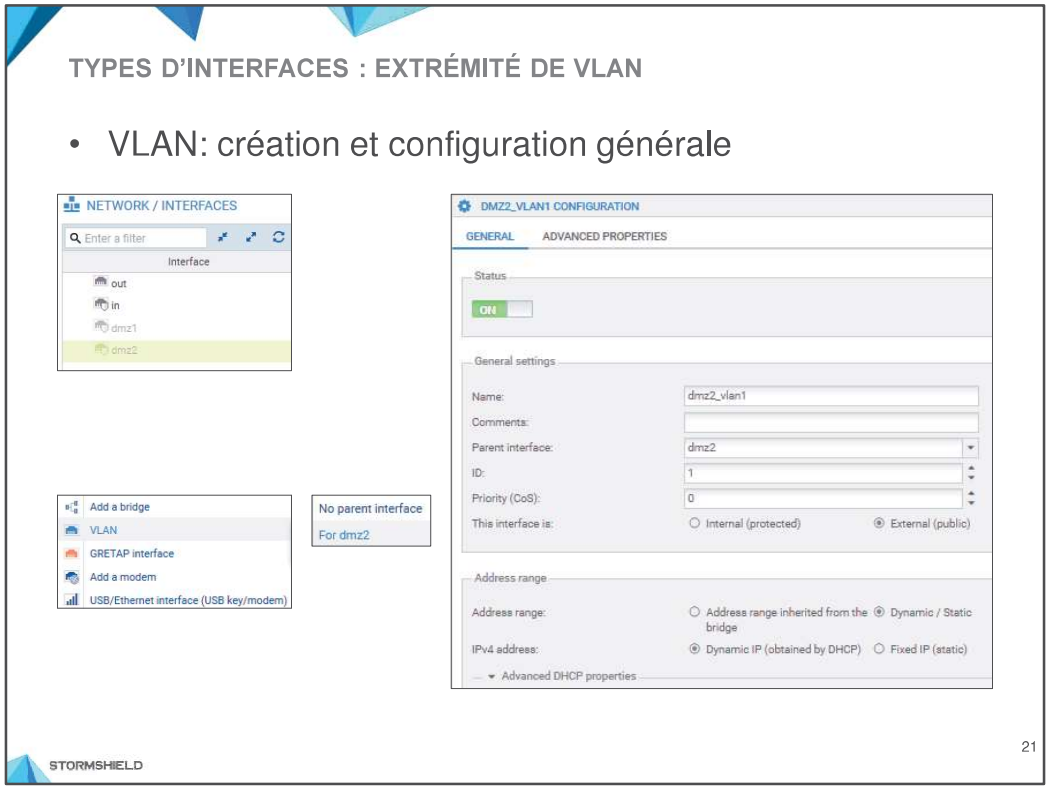
Les réseaux virtuels (VLAN : Virtual Local Area Network) introduisent la notion de segmentation virtuelle qui permet de constituer des sous-réseaux logiques au sein d'une même architecture réseau physique. Tous les équipements réseaux appartenant au même VLAN peuvent communiquer ensemble et forment un domaine de diffusion. Ainsi, l'utilisation des VLAN dans une architecture réseau améliore les performances en limitant les diffusions et offre une sécurité accrue en séparant les réseaux logiques.
Stormshield gère les VLAN normés IEEE 802.1q, pour lesquels un en-tête supplémentaire de 4 octets :

- Est ajouté par un commutateur administrable ou par le firewall à une trame Ethernet sortante sur un port étiqueté 802.1q,
- Est supprimé par un commutateur administrable ou par le firewall à une trame Ethernet entrante sur un port étiqueté 802.1q.

Cet en-tête comprend le champ VLAN id (VID) qui permet d'identifier le VLAN auquel appartient la trame. Ce champ est codé sur 12 bits. Il permet de définir jusqu'à 4094 VLAN différents (le VLANID=0 signifie que la trame n'appartient à aucun VLAN et le VLANID=4095 est réservé). L'en-tête inclut également le champ Priority ou CoS (Class of Service) sur 3 bits qui indique la priorité du paquet définie par le standard IEEE 802.1p.

Dans l'exemple ci-dessus, une trame envoyée depuis PC1 :

- Peut atteindre PC2 sans subir de modification, car les ports du commutateur sur lesquels PC1 et PC2 sont connectés appartiennent au même VLAN.
- Peut atteindre le firewall par un étiquetage 802.1q effectué par le commutateur (Ajout du VID 20).
- Ne peut pas atteindre SERVER directement, puisqu'il est dans un VLAN différent.
- Peut atteindre SERVER via routage par le firewall. Après routage, une nouvelle trame étiquetée par le firewall (Ajout du VID 10) est envoyée vers le serveur. Le commutateur supprime l'étiquette sur le port entrant et transmet la trame au serveur.



Deux méthodes sont disponibles pour la création d'un VLAN :

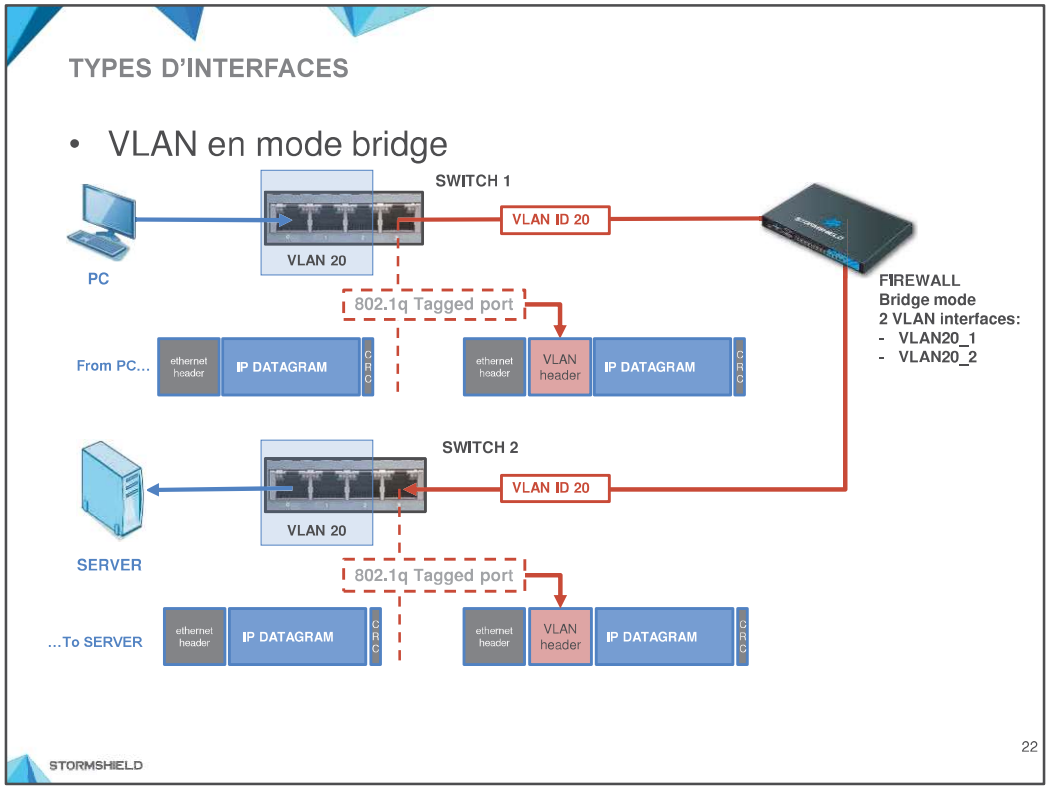
1. Présélection de l'interface parente : l'interface est mise en surbrillance, la fenêtre de configuration est directement renseignée, comme ci-dessus,
2. Création d'un VLAN sans interface parente : l'erreur « ce VLAN n'est pas associé à une interface physique » empêche la création de l'interface tant que le champ **Interface parente** n'est pas renseigné.

L'onglet de **CONFIGURATION GÉNÉRALE** contient :

- **Paramètres généraux** : nommage de l'interface (champ obligatoire) et commentaire facultatif,
- **Interface parente** : interface à laquelle sera rattaché le VLAN,
- **Identifiant de VLAN** : valeur du VLANID [1-4094],
- **Priorité (CoS)** : valeur inscrite dans le champ CoS sur tous les paquets envoyés par cette interface,
- **Cette interface est** : choix du type de l'interface, interne ou externe,
- **Plan d'adressage** : l'interface VLAN peut être configurée avec une adresse IP fixe accompagnée d'un masque réseau ou avec une IP dynamique fournie par un serveur DHCP. Elle peut également hériter de l'adresse IP d'un bridge, ce cas spécifique est détaillé sur la diapositive suivante.

NOTE :

- L'onglet **CONFIGURATION AVANCÉE** d'un VLAN permet de modifier la valeur de la MTU de l'interface,
- Dans le cas ci-dessus, l'interface parente du VLAN est désactivée, ce qui n'empêche en rien la création et le fonctionnement correct de l'interface VLAN.



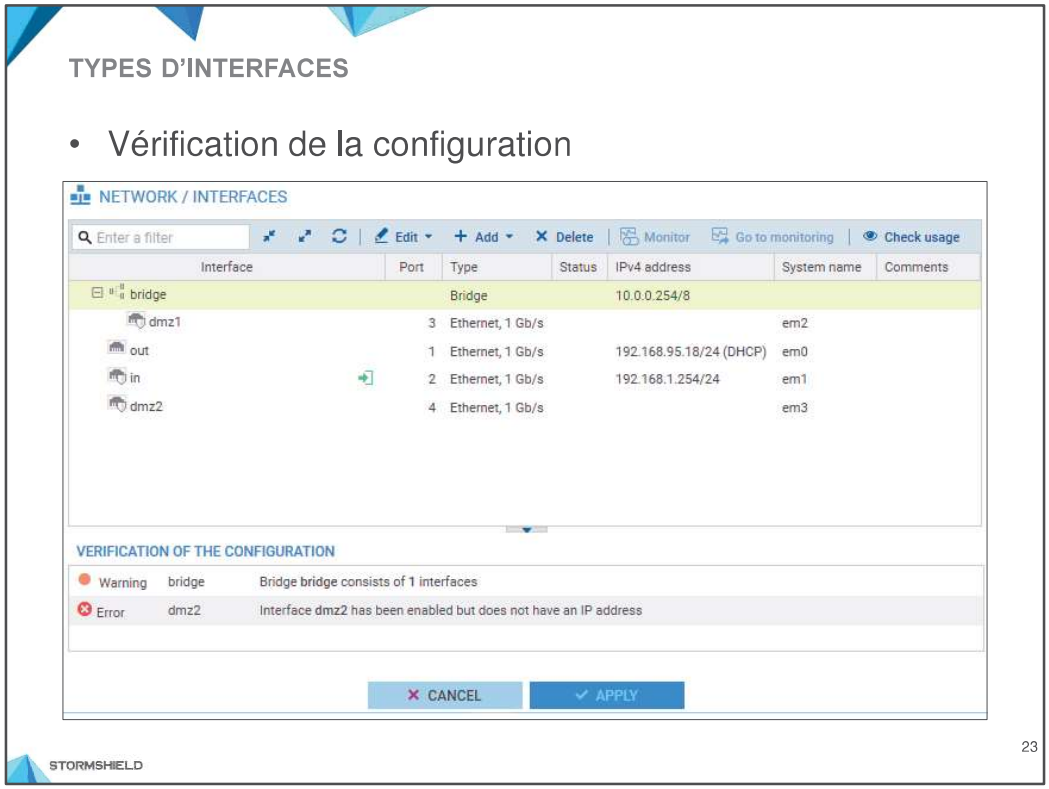
Le cas d'usage ci-dessus illustre l'ajout d'un firewall en coupure en mode bridge entre deux commutateurs existants et reliés entre eux par un lien étiqueté 802.1q. Après cet ajout, le comportement des commutateurs n'est pas modifié mais le trafic sur le VLAN est analysé par le firewall.

Les étapes de création d'un VLAN en mode bridge sont les suivantes :

1. Création de deux interfaces VLAN ayant le même identifiant (VID) sur deux interfaces parentes différentes,
2. Création d'un bridge contenant ces deux interfaces,
3. Répétition de ces deux étapes autant de fois qu'il y a de VLAN différents devant transiter par le lien entre les deux commutateurs.

Dans l'exemple ci-dessus :

1. Une trame envoyée depuis PC vers SERVER atteint le commutateur (Ajout du VID 20), puis atteint le firewall (suppression du VID 20 sur l'interface entrante),
2. Le firewall analyse le contenu de la trame,
3. La trame est étiquetée par le firewall (Ajout du VID 20 sur l'interface sortante) et envoyée vers le serveur,
4. Le commutateur supprime l'étiquette sur le port entrant et transmet la trame au serveur.



La cohérence de la configuration réseau est analysée en temps réel. Vous pouvez l'afficher en cliquant sur la flèche en bas de l'écran.

Un avertissement n'empêche pas la sauvegarde de la configuration. En revanche, une erreur bloque la sauvegarde (le bouton **Appliquer** est grisé).