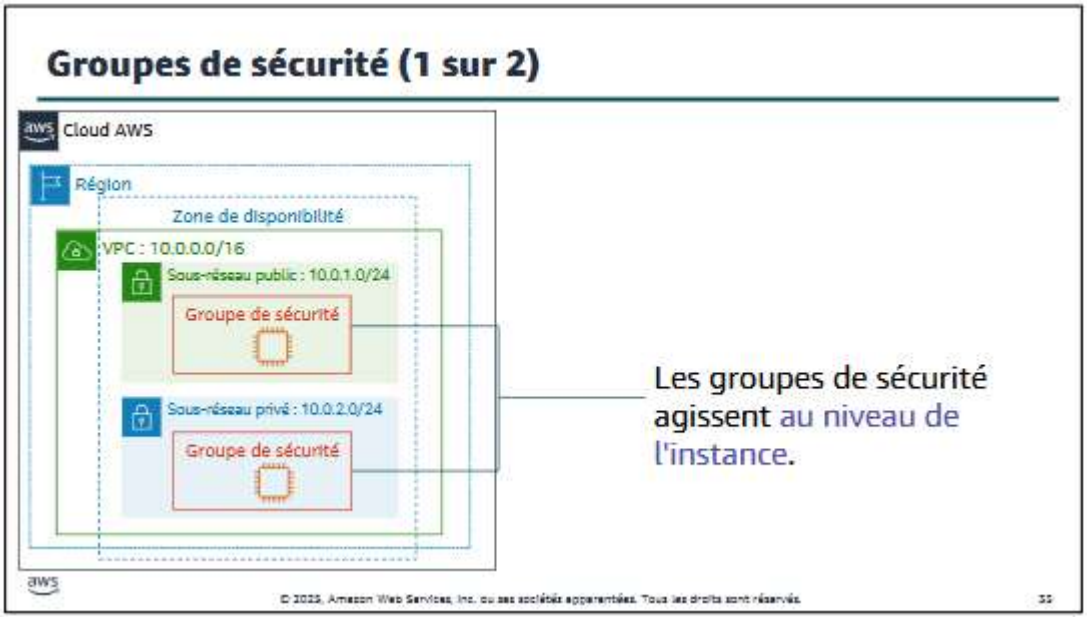
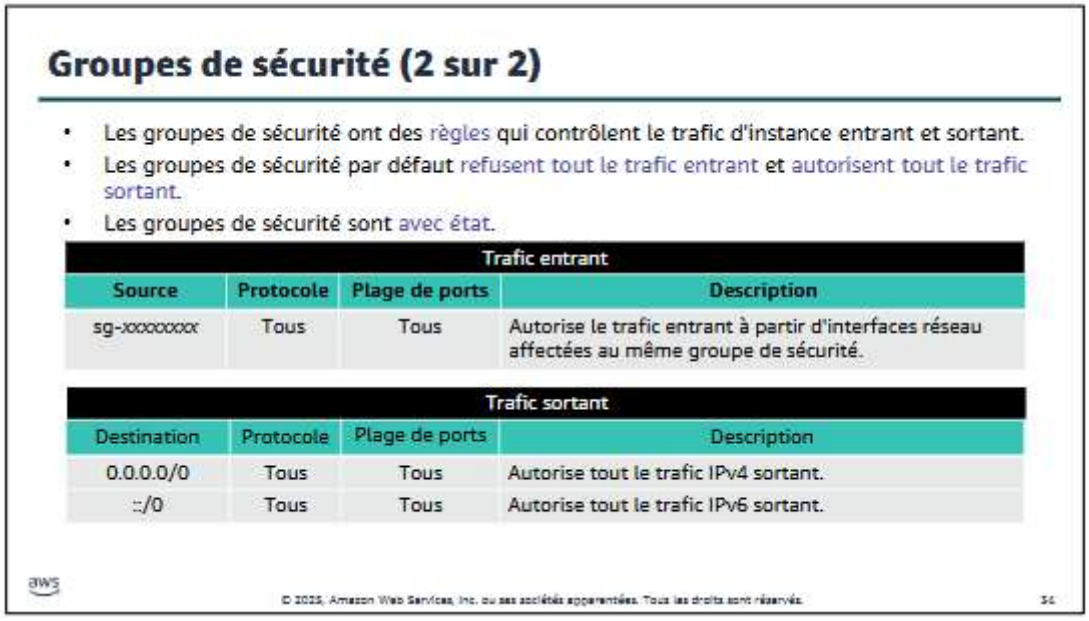
Sécurité de VPC



Un **groupe de sécurité** agit en tant que pare-feu virtuel pour votre instance et contrôle le trafic entrant et sortant. Les groupes de sécurité agissent au niveau de l'instance et non au niveau du sous-réseau.

Par conséquent, chaque instance dans un sous-réseau de votre VPC peut être affectée à un ensemble différent de groupes de sécurité

Au niveau le plus basique, un groupe de sécurité n'est autre qu'une méthode de filtrage du trafic vers vos instances.



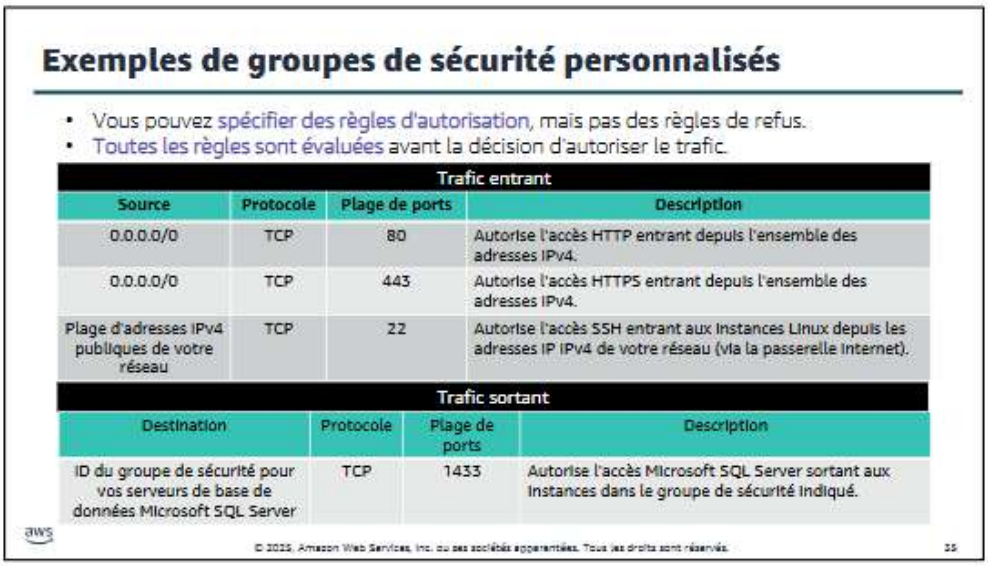
Les **groupes de sécurité** ont des **règles** qui contrôlent le trafic d'instance entrant et sortant.

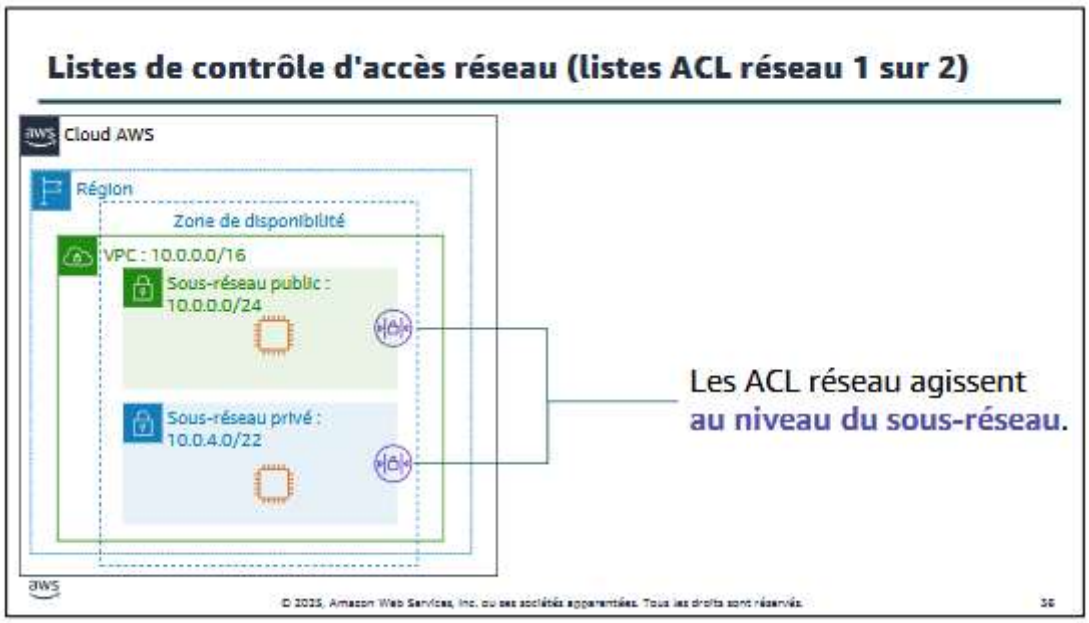
Lorsque vous créez un groupe de sécurité, il ne comporte pas de règles entrantes. Par conséquent, aucun trafic entrant issu d'un autre hôte de votre instance n'est autorisé tant que vous n'avez pas ajouté de règles entrantes au groupe de sécurité.

Par défaut, un groupe de sécurité inclut une règle sortante qui autorise tout le trafic sortant. Vous pouvez retirer la règle et ajouter des règles sortantes qui n'autorisent qu'un trafic sortant spécifique. Si votre groupe de sécurité ne contient pas de règles sortantes, aucun trafic sortant provenant de votre instance n'est autorisé.

Les groupes de sécurité sont avec **état**, ce qui signifie que les informations d'état sont conservées même après le traitement d'une demande. Dès lors, si vous envoyez une demande à partir de votre instance, le trafic de la réponse pour cette demande est autorisé, indépendamment des règles entrantes du groupe de sécurité.

Les réponses au trafic entrant autorisé sont autorisées à acheminer le trafic sortant, quelles que soient les règles de trafic sortant.

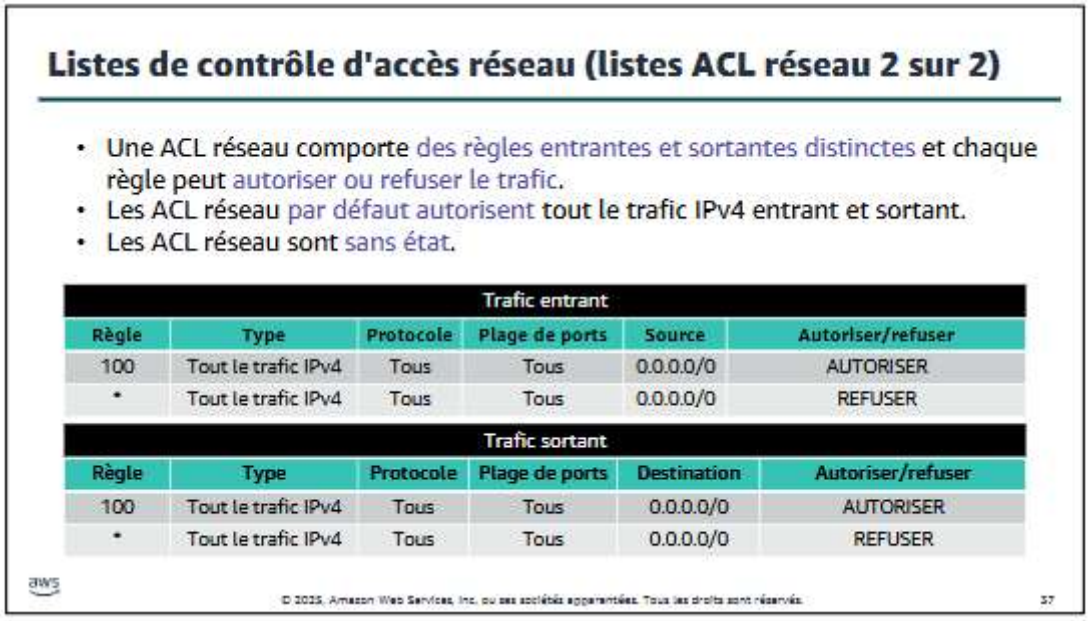




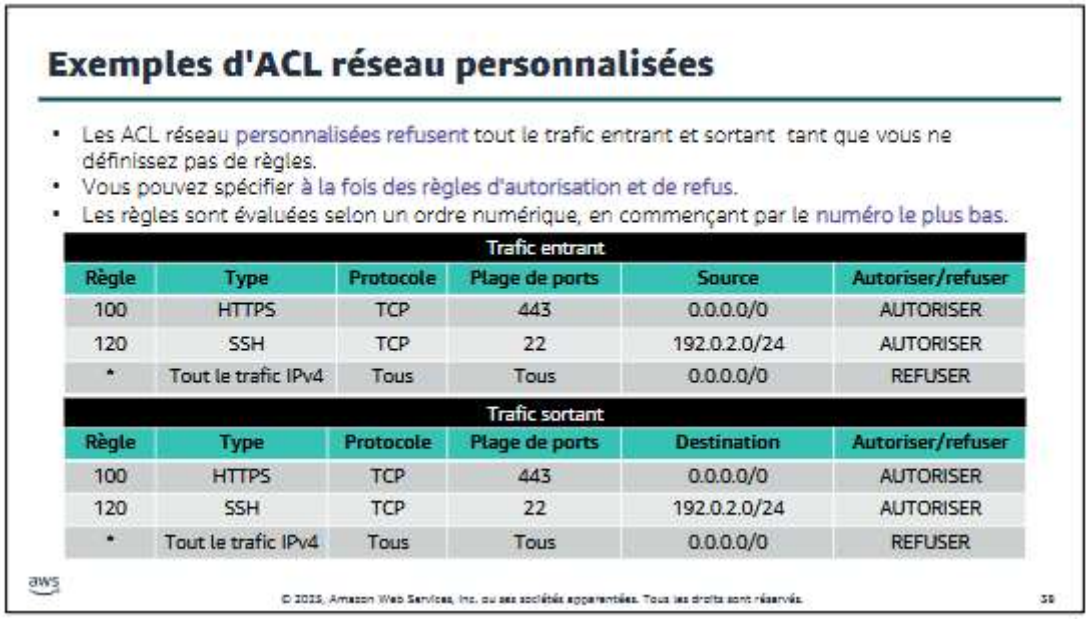
Une liste de contrôle d'accès réseau (ACL réseau) est une couche de sécurité facultative pour un Amazon VPC. Elle agit comme un pare-feu pour contrôler le trafic entrant et sortant d'un ou de plusieurs sous-réseaux.

Pour ajouter une autre couche de sécurité à votre VPC, vous pouvez configurer des ACL réseau avec des règles similaires à vos groupes de sécurité.

Chaque sous-réseau de votre VPC doit être associé à une liste ACL réseau. Si vous n'associez pas explicitement un sous-réseau à une ACL réseau, le sous-réseau est automatiquement associé à l'ACL réseau par défaut. Vous pouvez associer une ACL réseau à plusieurs sous-réseaux. Toutefois, un sous-réseau ne peut être associé qu'à une seule ACL réseau à la fois. Lorsque vous associez une ACL réseau à un sous-réseau, l'association précédente est supprimée.



Une ACL réseau comporte des règles entrantes et sortantes distinctes et chaque règle peut autoriser ou refuser le trafic. Votre VPC est automatiquement associée à une ACL réseau par défaut, que vous pouvez modifier. Par défaut, il autorise tout le traficIPv4 entrant et sortant, ainsi que le traficIPv6, le cas échéant. Le tableau présente une ACL réseau par défaut. Les ACL réseau sont sans état, ce qui signifie qu'aucune information sur une requête n'est conservée après son traitement.



Vous pouvez créer une ACL réseau personnalisée et l'associer à un sous-réseau. Par défaut, chaque ACL réseau personnalisée rejette tout le trafic entrant et sortant jusqu'à ce que vous ajoutiez des règles. Une ACL réseau contient une liste numérotée de règles évaluées dans l'ordre, en commençant par la règle dont le nombre est le plus bas. Les règles déterminent si le trafic est autorisé à l'intérieur ou à l'extérieur d'un sous-réseau associé à l'ACL réseau. Le nombre le plus élevé

que vous pouvez utiliser pour une règle est 32766. AWS vous recommande de créer des règles par incréments (par exemple, des incréments de10 ou100) afin de pouvoir insérer de nouvelles règles là où vous en aurez besoin ultérieurement.

Groupes de sécurité par rapport aux ACL réseau

Attribut	Groupes de sécurité	Listes ACL réseau
Portée	Au niveau de l'instance	Au niveau du sous-réseau
Règles prises en charge	Règles d'autorisation uniquement	Règles d'autorisation et de refus
État	Avec état (le trafic de retour est automatiquement autorisé, quelles que soient les règles)	Sans état (le trafic de retour doit être explicitement autorisé par les règles)
Ordre des règles	Les règles sont évaluées avant la décision d'autoriser le trafic	Les règles sont évaluées selon un ordre numérique avant la décision d'autoriser le trafic

aws