|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Iptables + NAT  http://upload.wikimedia.org/wikipedia/commons/thumb/3/35/Tux.svg/512px-Tux.svg.png  Iptables + NAT (suite)  http://upload.wikimedia.org/wikipedia/commons/thumb/3/35/Tux.svg/512px-Tux.svg.png  Iptables + NAT (suite)  http://upload.wikimedia.org/wikipedia/commons/thumb/3/35/Tux.svg/512px-Tux.svg.png  Iptables + NAT (suite)  http://upload.wikimedia.org/wikipedia/commons/thumb/3/35/Tux.svg/512px-Tux.svg.png  Iptables + NAT (suite)    http://upload.wikimedia.org/wikipedia/commons/thumb/3/35/Tux.svg/512px-Tux.svg.png  Iptables + NAT (suite)    http://upload.wikimedia.org/wikipedia/commons/thumb/3/35/Tux.svg/512px-Tux.svg.png  Iptables + NAT (suite)    http://upload.wikimedia.org/wikipedia/commons/thumb/3/35/Tux.svg/512px-Tux.svg.png  Iptables + NAT (suite)  http://upload.wikimedia.org/wikipedia/commons/thumb/3/35/Tux.svg/512px-Tux.svg.png |  | **Mise en place de NAT sous Linux avec iptables**  La plupart des entreprises possèdent un nombre limité d'adresses IP « aiguillables » (routable) de l'extérieur provenant de leur fournisseur d’accès Internet. De ce fait, les administrateurs réseau doivent trouver d'autres moyens pour partager l'accès aux services Internet sans donner d'adresses IP publiques limitées à chaque nœud sur le réseau local.  L'utilisation d'adresses IP privées est la manière la plus utilisée afin de permettre à tous les nœuds d’un réseau local d'accéder correctement aux services du réseau (interne et externe).  Les passerelles de périphérie (comme les serveurs mandataires NAT) permettent de relayer des transmissions sortantes vers Internet ou d’aiguiller des paquets provenant de l’extérieur vers un nœud du réseau local.  **Configuration des interfaces**   |  |  | | --- | --- | | **aa.aa.aa.aa** |  | | **bb.bb.bb.bb** |  | | **cc.cc.cc.cc** |  | | **dd.dd.dd.dd** |  | | **ee.ee.ee.ee** |  | | **ff.ff.ff.ff** |  |   Ce tutoriel démontre, étape par étape, comment mettre en place la translation d'adresses réseau (NAT) sous Linux avec *iptables*.  À la fin de l’exercice votre système va fonctionner comme une passerelle et pourra fournir un accès Internet à de multiples hôtes du le réseau local (LAN) en utilisant une seule adresse IP publique.  **Exigences matérielles et/ou logiques** 1. Un serveur physique ou virtuel avec 2 (deux) cartes d'interface réseau (NIC) ; 2. Une distribution Linux ; 3. *iptables*. 4. Un client pour vérifier le bon fonctionnement de la passerelle  **Définitions de base**   * **aa.aa.aa.aa** est l’adresse IP du réseau étendu (WAN) et  **bb.bb.bb.bb**  est le masque de sous-réseau du réseau étendu (WAN); * **cc.cc.cc.cc** est l'adresse IP du réseau local (LAN) (par exemple 192.168.0.1 ou 10.0.0.1)  et  **dd.dd.dd.dd** (LAN) est le masque de sous-réseau du réseau local (par exemple 255.255.255.0) ; * **ee.ee.ee.ee**  est la passerelle par défaut pour la connexion Internet; * **ff.ff.ff.ff** est l’adresse du serveur DNS ; * eth0 est le nom de l’interface réseau reliée au réseau étendu (WAN); * eth1 est le nom de l’interface réseau reliée au réseau local (LAN).   **Mise en place étape par étape**  **Étape 1 Vérification si les deux interfaces réseau sont bien reconnues par Linux et sont entièrement fonctionnelles**  Pour visualiser si les interfaces réseau sont fonctionnels …  **dmesg | grep *eth0* dmesg | grep *eth1***  Le résultat de la commande peut varier, mais dans la plupart des cas, il devrait ressembler à ce qui suit:  *eth1: RealTek RTL8139 au 0xe0830000, 00:30:04 f: 3b: af: 45, IRQ 19 eth1: Identifié 8139 type de puce 'RTL-8100B/8139D' eth0: link up, 100Mbps, full-duplex, lpa 0x41E1*   Une sortie similaire devrait être pour les cartes réseau eth0 et eth1.  Pour vérifier que les cartes réseau sont reconnues par Linux en tant que dispositifs de réseautage…  **ifconfig *eth0* ifconfig *eth1***  Le résultat de la commande peut varier, mais dans la plupart des cas, il devrait ressembler à ce qui suit:  *eth0 Link encap: Ethernet HWaddr 00:50:56: C0: 00:08  adr inet6: fe80 :: 250:56 ff: fec0: 8/64 Portée: Lien  UP BROADCAST RUNNING MULTICAST MTU: 1500 Metric: 1  RX paquets: 0 erreurs: 0: 0 overruns: 0 trame: 0  TX paquets: 41 erreurs: 0: 0 overruns: 0 porteuses: 0  collisions: 0 txqueuelen: 1000  Octets reçus: 0 (0.0 b) TX bytes: 0 (0.0 b)*    **Étape 2  Configuration de l'interface WAN (eth0) pour obtenir une connexion Internet**  **ifconfig *nnn* aa.aa.aa.aa netmask bb.bb.bb.bb** Exemple **ifconfig eth0 10.30.242.200 netmask 255.255.255.0**  Vous pouvez également modifier les paramètres de l’interface du réseau étendu (WAN) à l’aide du fichier de configuration ***/etc/sysconfig/network-scripts/ifcfg-xxx*** ou ***/etc/network/interfaces***.  L’adresse IP du réseau étendu (WAN) et le masque doivent être fournie par votre fournisseur d’accès Internet.    **Étape 3 Mise en place des paramètres de l’interface réseau étendu qui s'appliqueront après le démarrage du serveur**   Pour les distributions telles que RedHat, Fedora, Centos le fichier de configuration eth0 est situé dans ***/etc/sysconfig/network-scripts/ifcfg-xxx****.*  Pour les distributions telles que Debian, Ubuntu et Mint le fichier de configuration eth0 est situé dans ***/etc/network/interfaces****.*  Pour éditer des fichiers de configuration utiliser le traitement de texte *nano*.  Après avoir édité ***/etc/sysconfig/network-scripts/ifcfg-nnn*** le résultat devrait ressembler à ceci…  *DEVICE = nnn ONBOOT = yes BOOTPROTO = static IPADDR = aa.aa.aa.aa # EX. 10.30.242.200 NETMASK = bb.bb.bb.bb # EX. 255.255.255.0 GATEWAY = ee.ee.ee.ee # EX. 10.30.242.200 HWADDR = f 00:30:04: 3b: af: 45 # adresse MAC (entrée facultative)*  Après avoir édité ***/etc/network/interfaces*** le résultat devrait ressembler à ceci…  *Address 10.30. GATEWAY = ee.ee.ee.ee # EX. 10.30.242.200 HWADDR = f 00:30:04: 3b: af: 45 # adresse MAC (entrée facultative)*  **Étape 4 Configuration de l'interface LAN (eth1) pour obtenir une connexion Internet**   Après avoir édité ***/etc/sysconfig/network-scripts/ifcfg-eth1*** le résultat devrait ressembler à ceci…  *DEVICE = eth1 ONBOOT = yes BOOTPROTO = static IPADDR = cc.cc.cc.cc # EX. 192.168.125.1 NETMASK = dd.dd.dd.dd # EX. 255.255.255.0 HWADDR = 00:50:08 d: D1: 24: db # Adresse MAC de l’interface réseau local (entrée facultative)*  **Étape 5 (facultative) Définition des noms de domaine des serveurs**  Après avoir édité ***/etc/resolv.conf*** le résultat devrait ressembler à ceci  *nameserver 203.145.184.13 nameserver 203.145.184.12*  **Étape 6 Activation du la redirection IP**  **cd /proc/sys/net/ipv4/  echo 1 > ip\_forward** [[1]](#footnote-1)  **Étape 7 Mise en place du service NAT avec iptables**   Pour supprimer les éventuelles règles existantes de chaque table *iptables [[2]](#footnote-2)*.  **Iptables -F iptables -t nat -F iptables -t mangle -F**   |  |  | | --- | --- | | Commutateur | Signification | | -t | spécifie la table qui sera l’objet de l’action : (nat pour la translation et mangle pour le type de paquets) | | -F | signifie *Flush* (vider) le contenu existant. | | Important: Linux est sensible à la casse (MAJ / min) lors du passage de paramètres. | |   Pour activer la fonctionnalité de NAT...  **Iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE iptables -A FORWARD -i eth1 -j ACCEPT**   |  |  | | --- | --- | | Commutateur | Signification | | -t | spécifie la table qui sera l’objet de l’action : (nat pour la translation et mangle pour le type de paquets) | | -F | signifie *Flush* (vider) le contenu existant. | | -A | signifie *Append* (ajout) | | POSTROUTING | modifie le paquet avant sa sortie du système après être passé par le module d’aiguillage | | -o | Indique l’interface de sortie (out) | | MASQUERADE | indique le camouflage de l’adresse IP source avec l’interface par lequel les paquets IP sortent | | FORWARD | signifie faire suivre | | -I | Indique le nom de l’interface qui reçoit les paquets | | -j | précise l’action qu’il faut faire si le paquet correspond à la règle | | ACCEPT | signifie accepter | | Important: Linux est sensible à la casse (MAJ / min) lors du passage de paramètres. | |   Dans la table du NAT (-t nat), ajouter une règle (-A) après le routage (POSTROUTING) pour tous les paquets qui sortent par eth0 (-o eth0) qui stipule de camoufler la connexion (-j MASQUERADE). POSTROUTING permet aux paquets d'être modifiés lorsqu'ils quittent le périphérique externe de la passerelle.  Avant de redémarrer le service *iptables*, afin de s’assurer que les modifications ont été prises en compte, il est préférable de sauvegarder votre configuration actuelle.  **iptables-save > iptable.rule**  Par la suite, on redémarre le service.  **service iptables restart**  Enfin, suite au redémarrage du service, on recharge la configuration car cette dernière a pu être modifiée lors du lancement du service.  **iptables-restore < iptable.rule**  **Étape 8 Configuration des clients du réseau local (LAN) pour accéder à Internetà partir de la passerelle**  *Adresse IP du même réseau que cc.cc.cc.cc MSR : dd.dd.dd.dd Serveur DNS : ff.ff.ff.ff  Passerelle cc.cc.cc.cc*   Exemple: *Adresse IP: 192.168.0.7 MSR: 255.255.255.0 Serveur DNS: 209.160.67.13 Passerelle: 192.168.0.1*  **Pour en faire un peu plus…**  S’il existe un serveur sur le réseau interne que l’on souhaite le rendre disponible de manière externe, il faut utiliser la cible -j DNAT de la chaîne PREROUTING dans NAT pour spécifier une adresse IP et un port de destination où les paquets entrants demandant une connexion à votre service interne peuvent être retransmis.  Par exemple, si on souhaite retransmettre des requêtes HTTP au serveur HTTP Apache dédié sur 172.31.0.23, il faut saisir la commande suivante :  **iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to 172.31.0.23:80**  Cette règle spécifie que la table NAT utilise la chaîne intégrée PREROUTING pour retransmettre les requêtes HTTP entrantes exclusivement à l'adresse IP de destination listée de 172.31.0.23.  **Références pour la rédaction de ce document** <http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-fr-4/s1-firewall-ipt-fwd.html> <http://www.howtoforge.com/nat_iptables> <http://www.bctes.com/nat-linux-iptables.html> |
|  |  |  |

1. Pour activer la redirection d'IP, il est également possible d’exécuter la commande suivante :

   **sysctl -w net.ipv4.ip\_forward=1**

   Si cette commande est exécutée via une invite du shell, le paramètre est alors oublié après un redémarrage.

   Il est aussi possible de définir la retransmission de façon permanente en éditant le fichier ***/etc/sysctl.conf***. Il faut alors trouvez et modifiez la ligne suivante, en remplaçant 0 par 1 :

   **net.ipv4.ip\_forward = 0**

   Enfin, il faut exécuter la commande suivante pour activer les changements dans le fichier ***sysctl.conf*** :  
   **sysctl -p /etc/sysctl.conf** [↑](#footnote-ref-1)
2. Les commandes suivantes peuvent être aussi utilises :  
   **iptables --flush   
   iptables --table nat –flush  
   iptables --delete-chain** [↑](#footnote-ref-2)