网络地址转换技术

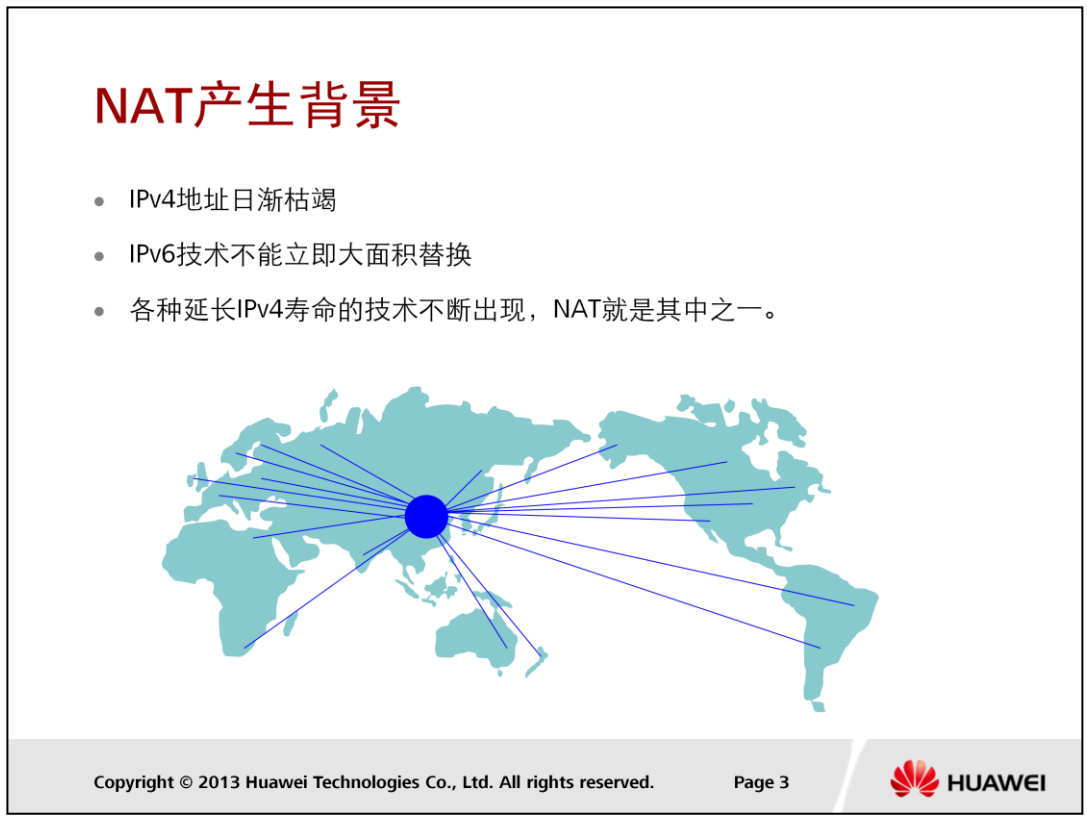
www.huawei.com

HUAWEI

目标

- 学完本课程后，您将能够:
  - 掌握NAT的技术原理
  - 掌握NAT几种应用方式
  - 掌握防火墙的NAT配置

目录



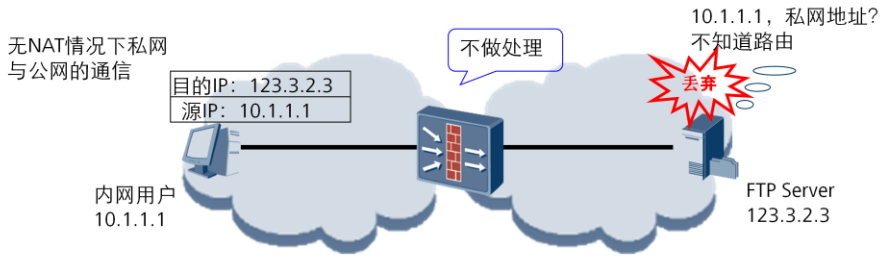
早在上世纪90年代初，有关RFC文档就提出IP地址耗尽的可能性。基于TCP/IP协议的Web应用使互联网迅速扩张，IPv4地址申请量越来越大。互联网可持续发展的问题日益严重。中国的运营商每年向ICANN申请的IP地址数量为全球最多。曾经有专家预言，根据互联网的发展速度，到2011年左右，全球可用的IPv4地址资源将全部耗尽。

IPv6的提出，就是为了从根本上解决IPv4地址不够用的问题。IPv6地址集将地址位数从IPv4的32位扩展到了128位。对于网络应用来说，这样的地址空间几乎是无限大。因此IPv6技术可以从根本上解决地址短缺的问题。但是，IPv6面临着技术不成熟、更新代价巨大等尖锐问题，要想替换现有成熟且广泛应用的IPv4网络，还有很长一段路要走。

既然不能立即过渡到IPv6网络，那么必须使用一些技术手段来延长IPv4的寿命。而技术的发展确实有效延缓了IPv4地址的衰竭，专家预言的地址耗尽的情况并未出现。其中广泛使用的技术包括无类域间路由（CIDR， Classless Inter-Domain Routing）、可变长子网掩码（VLSM， Variable Length Subnet Mask）和网络地址转换（NAT， Network Address Translation）。

为什么需要NAT?

- NAT技术主要应用是实现大量的私网地址对少量公网地址的转换。保障通信在基础上节约IP地址资源。
- 私网地址不能在公网中路由，否则将导致通信混乱



HUAWEI

私网地址出现的目的是为了实现地址的复用，提高IP地址资源的利用率，为了满足一些实验室、公司或其他组织的独立于Internet之外的私有网络的需求，RFCA（Requests For Comment）1918为私有使用留出了三个IP地址段。具体如下：

- A类IP地址中的10.0.0.0～10.255.255.255（10.0.0.0/8）
- B类IP地址中的172.16.0.0～172.31.255.255（172.16.0.0/12）
- C类IP地址中的192.168.0.0～192.168.255.255（192.168.0.0/16）

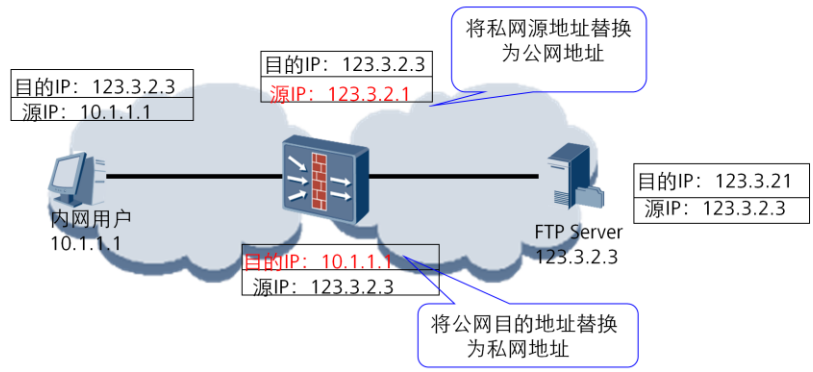
上述三个范围内的地址不能在Internet上被分配，因而可以不必申请就可以自由使用

内网使用私网地址，外网使用公网地址，如果没有NAT将私网地址转换为公网地址，会造成通信混乱，最直接的后果就是无法通信。

使用私网地址和外网进行通信，必须使用NAT技术进行地址转换，保证通信正常。

NAT技术的基本原理

- NAT技术通过对IP报文头中的源地址或目的地址进行转换，可以使大量的私网IP地址通过共享少量的公网IP地址来访问公网。



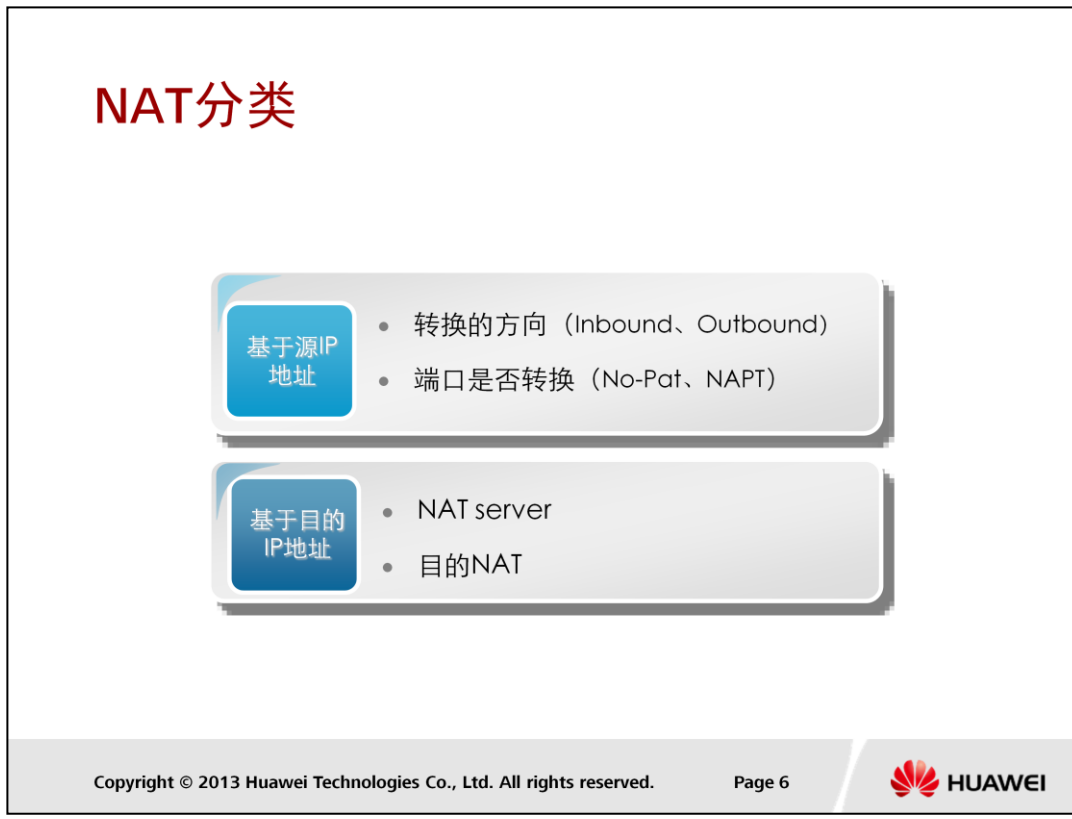
NAT是将IP数据报文报头中的IP地址转换为另一个IP地址的过程，主要用于实现内部网络（私有IP地址）访问外部网络（公有IP地址）的功能。从实现上来说，一般的NAT转换设备（实现NAT功能的网络设备）都维护着一张地址转换表，所有经过NAT转换设备并且需要进行地址转换的报文，都会通过这个表做相应的修改。

地址转换的机制分为如下两个部分：

- 内部网络主机的IP地址和端口转换为NAT转换设备外部网络地址和端口。
- 外部网络地址和端口转换为NAT转换设备内部网络主机的IP地址和端口。

也就是<私有地址+端口>与<公有地址+端口>之间相互转换。

NAT转换设备处于内部网络和外部网络的连接处。内部的PC与外部服务器的交互报文全部通过该NAT转换设备。常见的NAT转换设备有路由器、防火墙等。



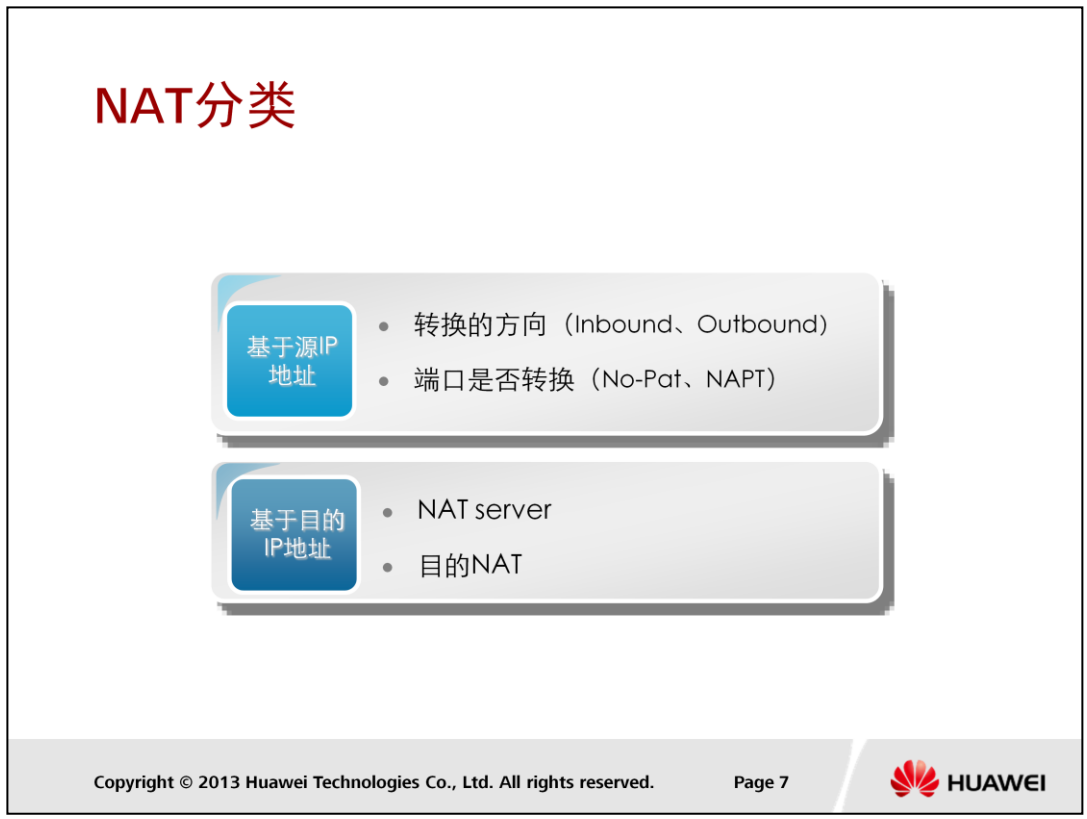
NAT功能包括对源IP地址进行转换，和对目的IP地址进行转换两种方式。

其中，基于源IP地址的转换可以从以下两个方面进行划分：

- 转换的方向。按照转换的方向可以将源IP地址转换划分为以下两类：
  - Inbound方向：数据包由低安全级别的安全区域向高安全级别的安全区域方向传输时，基于源IP地址进行的转换。
  - Outbound方向：数据包由高安全级别的安全区域向低安全级别的安全区域方向传输时，基于源IP地址进行的转换。
- 端口是否转换。按照端口是否转换可以将源IP地址转换划分为以下两类：
  - No-PAT(Port Address Translation)方式的NAT：主要用于一对一的IP地址的转换，端口不进行转换。
  - NAPT(Network Address Port Translation)方式的NAT：主要用于多对一或多对多的地址转换，转换时地址和端口号同时进行转换。

按照功能不同，可以将基于目的IP地址的转换分为以下两类：

- NAT Server：主要应用于实现私网服务器以公网IP地址对外提供服务的场景。
- 目的NAT：主要应用于实现手机用户上网时，手机的缺省WAP网关与所在地运营商的实际WAP网关不一致，导致需要修改报文的目的网关地址的场景。



在某些场景下，既要对源IP地址进行转换，又要对目的IP地址进行转换，被称为双向NAT。常见的场景包括：

- NAT Inbound和NAT Server一起使用：主要用于简化配置NAT Server时的路由配置。
- 域内NAT和NAT Server一起使用：主要应用于实现私网用户以公网地址访问属于同一安全区域的私网服务器的场景。

NAT技术除了可以实现地址复用，节约宝贵IP地址资源的优点外，还有其他一些优点，NAT技术的发展，也不断吸收先进的理念，总的来说，NAT的优点和不足如下：

- NAT的优点

可以使一个局域网中的多台主机使用少数的合法地址访问外部的资源，也可以设定内部的WWW、FTP、Telnet等服务提供给外部网络使用，解决了IP地址日益短缺的问题。

对于内外网络用户，感觉不到IP地址转换的过程，整个过程对于用户来说是透明的。

对内网用户提供隐私保护，外网用户不能直接获得内网用户的IP地址、服务等信息，具有一定的安全性。

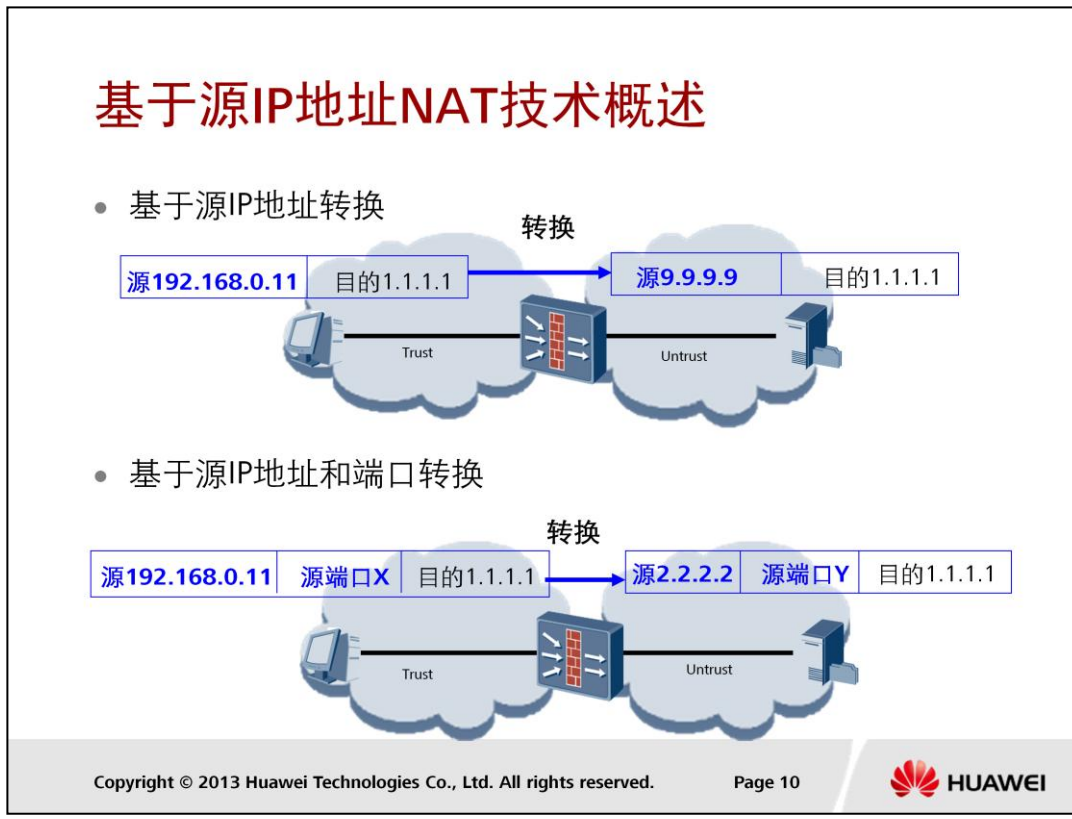
通过配置多个相同的内部服务器的方式可以减小单个服务器在大流量时承担的压力，实现服务器负载均衡。

- NAT的不足

由于需要对数据报文进行IP地址的转换，涉及IP地址的数据报文的报头不能被加密。在应用协议中，如果报文中有地址或端口需要转换，则报文不能被加密。例如，不能使用加密的FTP连接，否则FTP的port命令不能被正确转换。

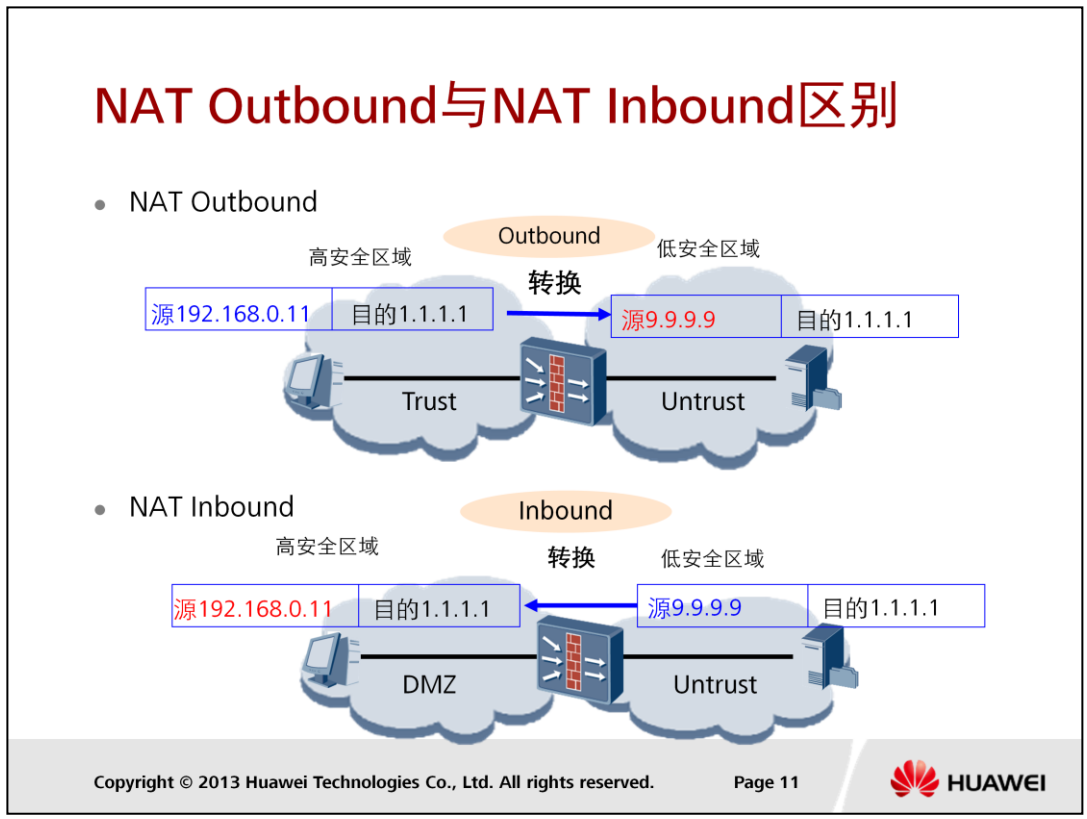
网络监管变得更加困难。例如，如果一个黑客从内网攻击公网上的一台服务器，那么要想追踪这个攻击者很难。因为在报文经过NAT转换设备的时候，地址经过了转换，不能确定哪台才是黑客的主机。

目录

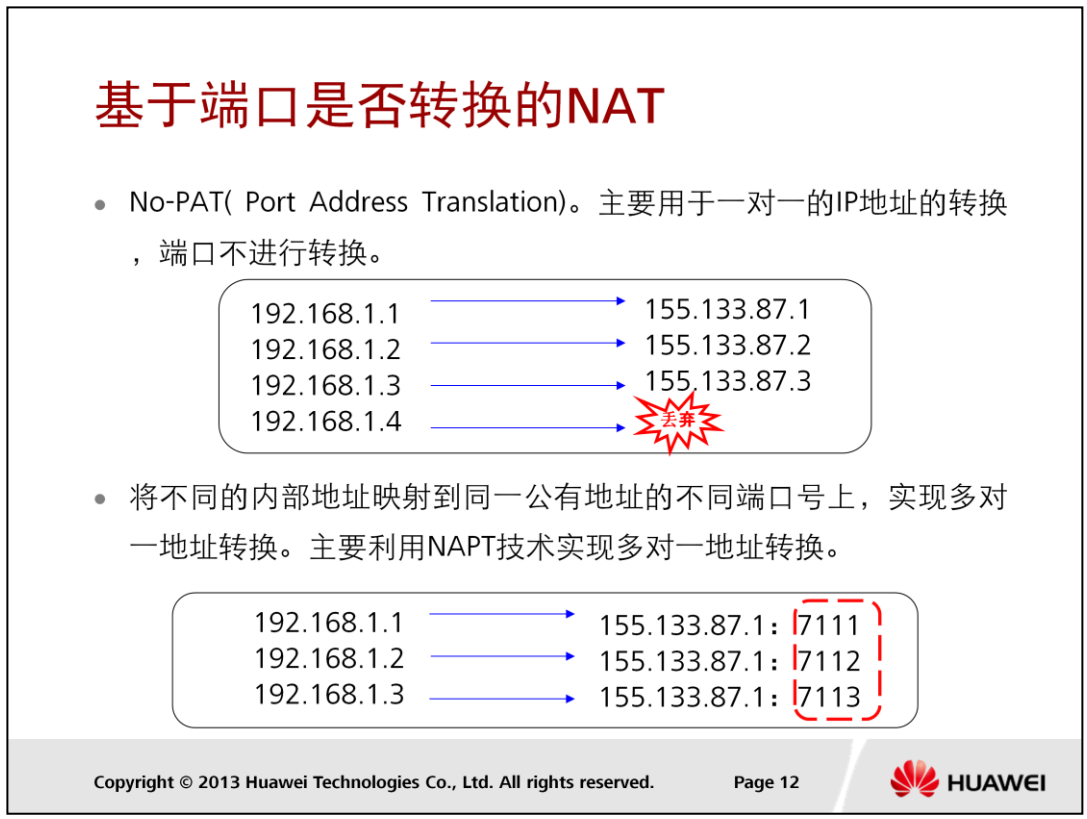


基于源IP地址的NAT是指对发起连接的IP报文头中的源地址进行转换。它可以实现内部用户访问外部网络的目的。通过将内部主机的私有地址转换为公有地址，使一个局域网中的多台主机使用少数的合法地址访问外部资源，有效的隐藏了内部局域网的主机IP地址，起到了安全保护的作用。由于一般内网区域的安全级别比外网高，所以这种应用又称为NAT Outbound。

基于源IP地址和端口转换，一般情况下源端口X=源端口Y，即保持原端口信息，并表现在会话表项。此种转化方式需保证会话表项的唯一性。



NAT Outbound与NAT Inbound区别，主要在于基于源IP地址转换是由高优先级至低优先级，还是低优先级至高优先级。他们的共同点都是进行源IP地址转换。



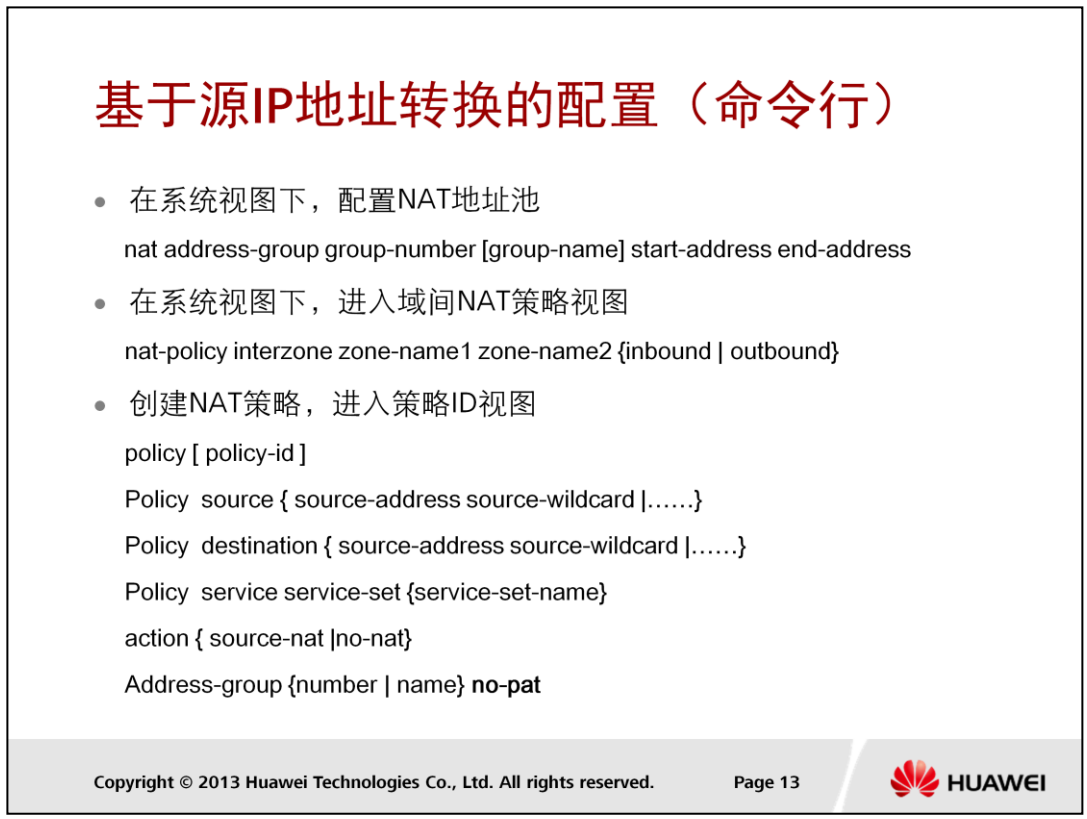
NAT No-PAT可以称为“一对一地址转换”，在地址转换过程中，数据包的源IP地址由私网地址转换为公网地址，但端口号不做转换。

例如，地址池中的公网IP地址只有两个。由于一台私网主机在借用其中的一个公网IP访问公网时，会占用这个IP的所有端口。因此，这种情况只允许最多有两台私网主机同时访问公网，其他的私网主机要等到其中一台主机不再访问公网，它占用的公网IP地址被释放后，才可以再进行NAT访问公网。

网络地址端口转换（NAPT， Network Address Port Translation）也能实现并发的地址转换。它允许多个内部地址使用一个公有地址访问Internet，也可称之为“多对一地址转换”或 “地址复用”。

NAPT是一种利用第四层信息来扩展第三层地址的技术，一个IP地址有65535个端口可以使用。理论上来说，一个地址可以为其他65535个地址提供NAPT转换，NAPT还能将来自不同内部地址的数据报文映射到同一公有地址的不同端口号上，因而仍然能够共享同一地址，对比一对一或多对多地址转换。这样极大的提升了地址空间，增加了IP地址的利用率。 因此NAPT是最常用的一种地址转换方式。

在NAPT方式中，还可以直接借用设备与外网相连的接口的IP地址作为转换后的IP地址，这种借用接口IP做NAT的应用又称为easy-ip。直接借用接口IP地址作为公网地址的情况下，不需要创建NAT地址池。



NAT地址池是指用NAT转换时用于分配的公网IP地址范围。进行转换时，设备会从该地址池中随机选择一个地址，用于替换报文中的源IP地址。不进行端口转换。

进入NAT域间进行NAT转换的源IP地址所在的两个安全区域，域间的方向的选择与包过滤一致，当源地址所在安全区域的优先级比目的地址所在安全区域高，则应选择outbound，反之，则应选择inbound。在NAT No-pat应用中，需要进行NAT转换的源IP地址是内网用户的IP地址，所以此处的流的方向应该是从内网流入外网。外网安全区域的安全级别一般比内网低，所以这里一般选择outbound。

同一个域间NAT策略视图下可配置多个NAT策略。缺省情况下，越先配置的策略，优先级越高，越先匹配报文。

NAPT与NAT No-pat主要区别在于，NAPT除了转换源IP地址外，还进行端口转换，即不需要配置no-pat参数。

在NAPT情况下，若直接使用设备与外网相连的接口的IP地址作为转换后的源IP地址，可执行命令**easy-ip** *interface-type interface-number*，配置NAT策略直接引用接口IP地址。

NAT 地址池

- NAT地址池是一些连续的IP地址集合，当来自私网的报文通过地址转换到公网IP时，将会选择地址池中的某个地址作为转换后的地址
  - 创建NAT地址池的命令为：

    nat address-group *group-number* [*group-name*] *start-address end-address* [**vrrp** *virtual-router-ID*]

  - nat address-group 0 pool0 192.168.1.1 192.168.1.100

HUAWEI

NAT地址池中的地址可以是一个公网IP地址，也可以是多个公网IP地址。

在配置基于源IP地址的NAT与域内NAT时，需要首先配置NAT地址池，然后将NAT地址池与policy绑定，通过选择不同的参数，实现不同功能的NAT。

在配置NAT地址池的时候，地址池中的地址个数不能超过4096。当地址个数超过256时，该地址池只能被No-PAT的方式引用。

当某地址池已经和policy关联时，不允许删除这个地址池。

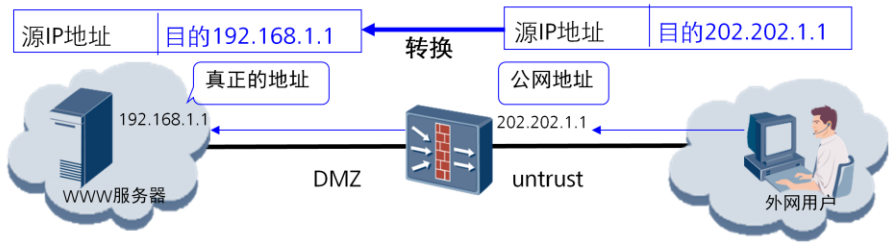
配置NAT地址池时，应将上网接口地址和地址池配置在同一网段，即和分配的公网IP地址在同一网段；如果地址池所在网段与上网接口不在同一个网段，注意需要在USG的下一跳路由器上配置到地址池的路由。

当设备同时应用于双机热备组网时，如果NAT地址池地址与VRRP备份组虚拟IP地址不在同一网段，不需要配置vrrp关键字；如果NAT地址池中的地址与VRRP备份组虚拟IP地址在同一网段，需要配置vrrp关键字，且*virtual-router-id*为NAT出接口对应的VRRP备份组的ID。否则可能导致业务中断。

目录

NAT Server-内部服务器

- 内部服务器(Nat Server)功能是使用一个公网地址来代表内部服务器对外地址。



- 在防火墙上，专门为内部的服务器配置一个对外的公网地址来代表私网地址。对于外网用户来说，防火墙上配置的外网地址就是服务器的地址。

HUAWEI

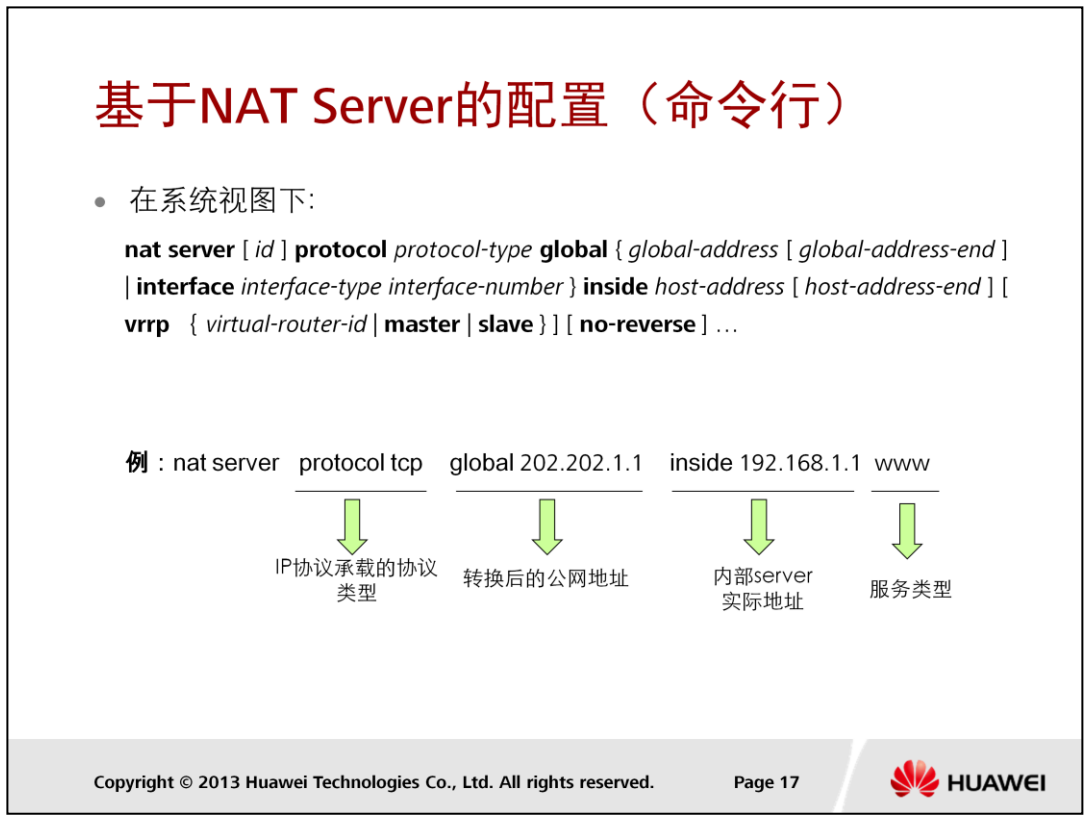
NAT Server，即内部服务器。NAT隐藏了内部网络的结构，具有“屏蔽”内部主机的作用。但是在实际应用中，可能需要提供给外部一个访问内部主机的机会，如提供给外部一台WWW的服务器，而外部主机根本没有指向内部地址的路由，因此无法正常访问。这时可以使用内部服务器（Nat Server）功能来实现这个功能应用。

使用NAT可以灵活地添加内部服务器。例如：可以使用202.202.1.1等公网地址作为Web服务器的外部地址，甚至还可以使用202.202.1.1 :8080这样的IP地址加端口号的方式作为Web的外部地址。

外部用户访问内部服务器时，有如下两部分操作：

- 防火墙将外部用户的请求报文的目的地址转换成内部服务器的私有地址。
- 防火墙将内部服务器的回应报文的源地址（私网地址）转换成公网地址。

防火墙支持基于安全区域的内部服务器。例如，当需要对处于多个网段的外部用户提供访问服务时，防火墙结合安全区域配置内部服务器可以为一个内部服务器配置多个公网地址。通过配置防火墙的不同级别的安全区域对应不同网段的外部网络，并根据不同安全区域配置同一个内部服务器对外的不同的公网地址，使处于不同网段的外部网络访问同一个内部服务器时，即通过访问对应配置的公网地址来实现对内部服务器的访问能力。



NAT Server是最常用的基于目的地址的NAT。当内网部署了一台服务器，其真实IP是私网地址，但是希望公网用户可以通过一个公网地址来访问该服务器，这时可以配置NAT Server，使设备将公网用户访问该公网地址的报文自动转发给内网服务器。

针对配置NAT Server ，有以下不同类型：

对所有安全区域发布同一个公网IP，即这些安全区域的用户都可以通过访问同一个公网IP来访问内部服务器。

与发布不同的公网IP相比，发布同一个公网IP地址时多了个参数*no-reverse*。配置不带*no-reverse*参数的**nat server**后，当公网用户访问服务器时，设备能将服务器的公网地址转换成私网地址；同时，当服务器主动访问公网时，设备也能将服务器的私网地址转换成公网地址。

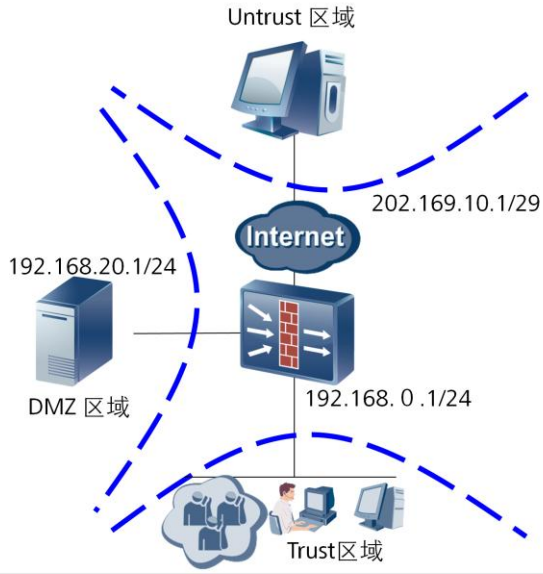
参数*no-reverse*表示设备只将公网地址转换成私网地址，不能将私网地址转换成公网地址。当内部服务器主动访问外部网络时需要执行outbound的nat策略，引用的地址池里必需是nat server配置的公网IP地址，否则反向NAT地址与正向访问的公网IP地址不一致，会导致网络连接失败。

多次执行带参数*no-reverse*的**nat server**命令，可以为该内部服务器配置多个公网地址；未配置参数*no-reverse*则表示只能为该内部服务器配置一个公网地址。

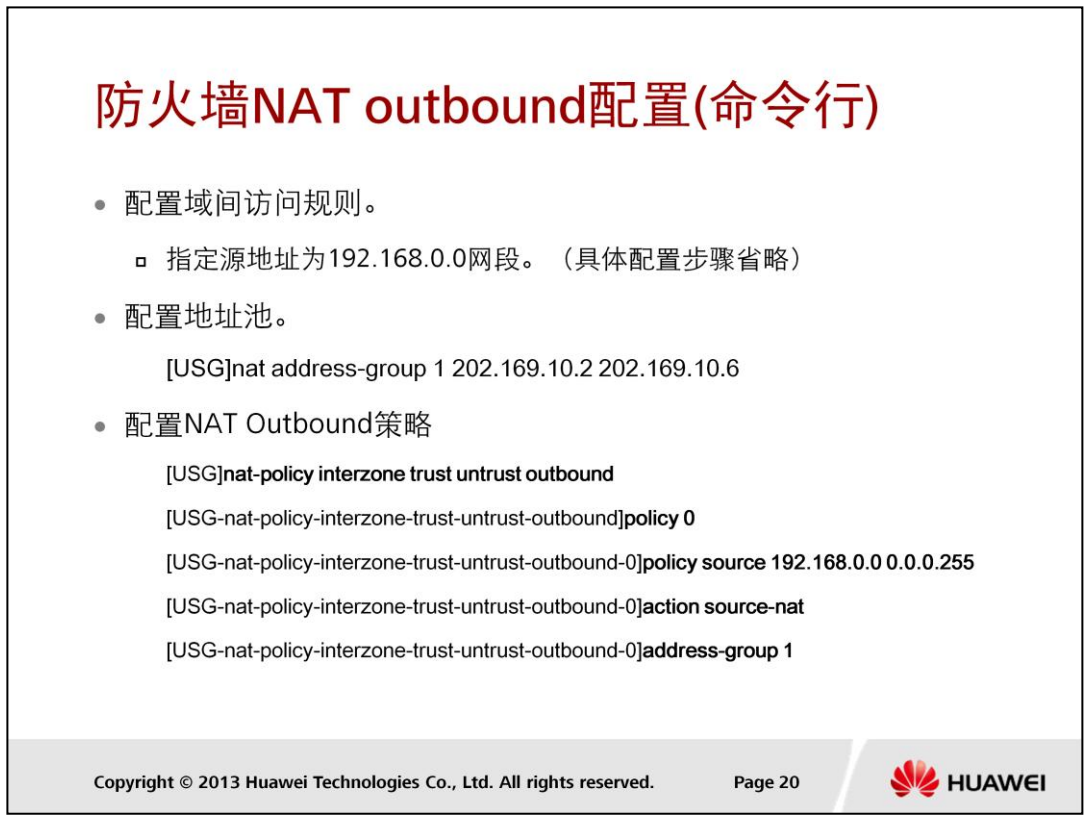
针对不同的安全区域发布不同的公网IP，即不同安全区域的用户可以通过访问不同的公网IP来访问内部服务器。适用于内部服务器向不同的运营商网络提供服务，且在每个运营商网络都拥有一个公网IP的情况。

目录

NAT典型应用场景配置举例



- **应用场景分析**
  - NAT Outbound应用
  - NAT Server应用



域间访问规则配置命令参考：

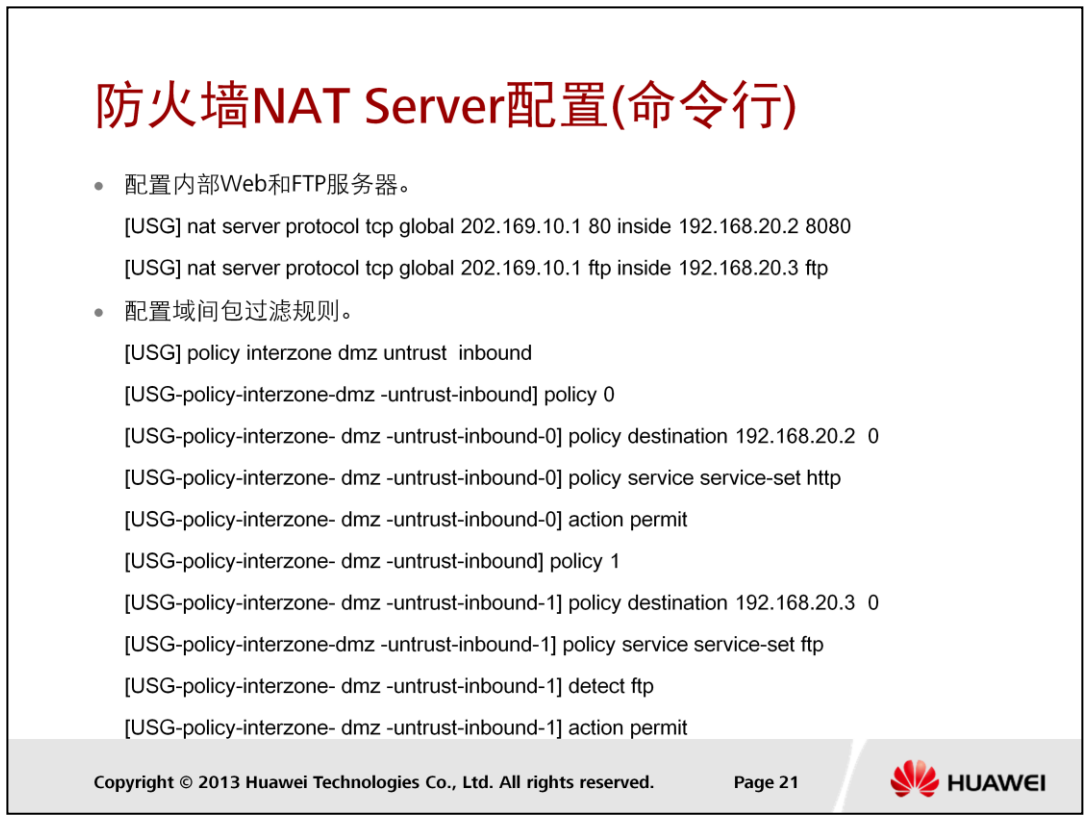
[USG]policy interzone trust untrust outbound

[USG-policy-interzone-trust-untrust-outbound]policy 0

[USG-policy-interzone-trust-untrust-outbound-0]policy source 192.168.0.0 0.0.0.255

[USG-policy-interzone-trust-untrust-outbound-0]action permit

配置NAT outbound，是为了实现内网员工对外部网络进行访问时进行NAT地址转换，数据流向是从高安全级别到低安全级别，因此源地址应该为内部网络的地址网段。而为内网用户分配的地址池，应该为外网地址网段用于对internet资源进行访问。

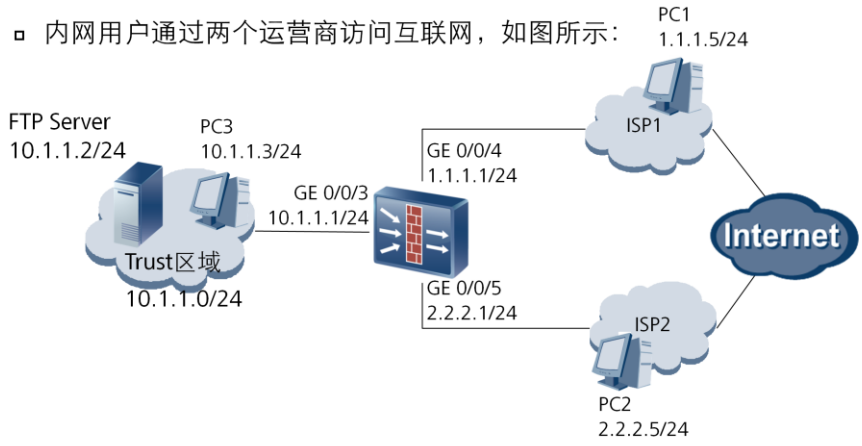


USG上同时配置NAT和内部服务器时，内部服务器优先级较高，首先起作用。

多个不同内部服务器使用一个公有地址对外发布时，可以多次使用 nat server 命令对其进行配置。配置参数 zone，可以使内部服务器访问该 zone 时候做 NAT 服务器逆向转换。当一个用户和内部服务器处于同一安全区域时，USG统一安全网关允许该用户使用内部服务器的公网IP地址访问该内部服务器。允许外部网络访问的内部服务器通常置于 USG 统一安全网关的 DMZ安全区域。不建议配置允许这个安全区域中的设备主动向外发起连接。当统一安全网关同时应用于双机热备组网时，如果转换后的 NAT 服务器地址与 VRRP备份组虚拟 IP地址不在同一网段，则不必配置携带 vrrp关键字的 nat server 命令。如果转换后的 NAT 服务器地址与 VRRP备份组的虚拟 IP地址在同一网段，则需要配置相关命令，且 virtual-router-ID为统一安全网关 NAT 服务器出接口对应的 VRRP备份组的ID。

NAT双出口场景配置举例

- 组网需求
  - 两个不同运营商用户需要访问同一内网服务器资源；
  - 内网用户通过两个运营商访问互联网，如图所示：



在该例中，企业从每个运营商处都获取到了一个公网IP地址，为了保证所有用户的访问速度，需要让不同运营商的用户通过访问相应的运营商的IP来访问企业提供的服务，而不需要经过运营商之间的中转。同时，对于企业内网的用户也可以通过两个运营商所提供的网络访问到internet资源。

ISP1和ISP2作为internet运营商，两者都连接internet并可以互通。

NAT 双出口实例配置思路

HUAWEI

NAT Outbound双出口配置1（命令行）

- 创建安全区域。 为ISP1和ISP2分别创建一个安全区域。

  [USG] **firewall zone name ISP1**

  [USG-zone-isp1] **set priority 10**

  [USG] **firewall zone name ISP2**

  [USG-zone-isp2] **set priority 20**

- 配置各接口的IP地址，并将其加入相应的安全区域。 （配置省略）
- 配置域间安全转发策略。开启内网到ISP1和ISP2区域的outbound方向策略

  [USG] **policy interzone trust isp1 outbound**

  [USG-policy-interzone-trust-isp1-inbound] **policy 0**

  [USG-policy-interzone-trust-isp1-inbound-0] **policy source 10.1.1.0 24**

  [USG-policy-interzone-trust-isp1-inbound-0] **action permit**

HUAWEI

配置各接口的IP地址，并将其加入安全区域。 配置命令参考：

[USG] interface GigabitEthernet 0/0/3

[USG-GigabitEthernet0/0/3] ip address 10.1.1.1 24

[USG] interface GigabitEthernet 0/0/4

[USG-GigabitEthernet0/0/4] ip address 1.1.1.1 24

[USG-GigabitEthernet0/0/4] quit

[USG] interface GigabitEthernet 0/0/5

[USG-GigabitEthernet0/0/5] ip address 2.2.2.1 24

[USG]firewall zone trust

[USG-zone-trust]add interface gigabitetherent 0/0/3

[USG]firewall zone isp1

[USG-zone-isp1]add interface gigabitetherent 0/0/4

[USG]firewall zone isp2

[USG-zone-isp2]add interface gigabitetherent 0/0/5

NAT Outbound双出口配置2（命令行）

- 配置静态路由，保证路由可达 。

  假设通过ISP1和ISP2访问internet资源的下一跳地址分别为1.1.1.2/24和2.2.2.2/24。

  （具体步骤省略）

- 配置NAT Outbound策略 （isp2策略步骤省略）

  [USG]**nat-policy interzone trust isp1 outbound**

  [USG-nat-policy-interzone-trust-untrust-outbound]**policy 0**

  [USG-nat-policy-interzone-trust-untrust-outbound-0]**action source-nat**

  [USG-nat-policy-interzone-trust-untrust-outbound-0]**easy-ip GigabitEthernet 0/0/4**

静态路由配置命令参考：

[USG] ip route-static 0.0.0.0 0.0.0.0 1.1.1.2

[USG] ip route-static 0.0.0.0 0.0.0.0 2.2.2.2

NAT Server双出口配置1（命令行）

- 配置域间安全转发策略。开启ISP1和ISP2区域到内网的inbound方向策略。（ISP2的配置与ISP1相似，具体配置省略）

[USG] **policy interzone trust isp1 inbound**

[USG-policy-interzone-trust-isp1-inbound] **policy 0**

[USG-policy-interzone-trust-isp1-inbound-0] **policy destination 10.1.1.2 0**

[USG-policy-interzone-trust-isp1-inbound-0] **policy service service-set ftp**

[USG-policy-interzone-trust-isp1-inbound-0] **action permit**

配置接口IP地址、接口加域配置命令参考：

<USG> system-view

[USG] interface GigabitEthernet 0/0/3

[USG-GigabitEthernet0/0/3] ip address 10.1.1.1 24

[USG-GigabitEthernet0/0/3] quit

[USG] interface GigabitEthernet 0/0/4

[USG-GigabitEthernet0/0/4] ip address 1.1.1.1 24

[USG-GigabitEthernet0/0/4] quit

[USG] interface GigabitEthernet 0/0/5

[USG-GigabitEthernet0/0/5] ip address 2.2.2.1 24

[USG-GigabitEthernet0/0/5] quit

[USG] firewall zone dmz

[USG-zone-dmz] add interface GigabitEthernet 0/0/3

[USG-zone-dmz] quit

[USG] firewall zone untrust

[USG-zone-untrust] add interface GigabitEthernet 0/0/4

[USG-zone-untrust] add interface GigabitEthernet 0/0/5

[USG-zone-untrust] quit

NAT Server双出口配置2（命令行）

- 创建内网服务器的公网IP与私网IP的映射关系。

  [USG] **nat server zone isp1 protocol tcp global 1.1.1.1 ftp inside 10.1.1.2 ftp**

  [USG] **nat server zone isp2 protocol tcp global 2.2.2.1 ftp inside 10.1.1.2 ftp**

- 在ISP1、ISP2与DMZ的域间配置NAT ALG，使服务器可以正常对外提供FTP服务。

  [USG] **firewall interzone dmz isp1**

  [USG-interzone-dmz-isp1] **detect ftp**

  [USG-interzone-dmz-isp1] **quit**

  [USG] **firewall interzone dmz isp2**

  [USG-interzone-dmz-isp2] **detect ftp**

  [USG-interzone-dmz-isp2] **quit**

在本例中，ISP1和ISP2可以划为同一安全区域也可以设置为不同的安全区域。在这种时候，需要采用nat server zone 方式可以使防火墙识别报文“来自”或者“去往”的域，对报文的目的地址和源地址通过nat server所创建的地址映射关系进行转换。

总结

- NAT的技术原理
- NAT几种应用方式
- 防火墙NAT典型场景配置

Thank you

www.huawei.com