！！补充

案例1：NAT BYPASS

没有设置NAT BYPASS 配置（假设NAT 和VPN 在一起）

假设FA0/0 是OUTSIDE，FA0/1 是INSIDE

NAT 部分

interface fa 0/1

ip nat inside

!

int fa 0/0

ip nat outside

!

access-list 1 permit 10.0.0.0 0.255.255.255

改成

**ip access-list ex NAT**

**deny ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255**

**permit ip 10.1.1.0 0.0.0.255 any**

!

ip nat inside source list 1 interface fa 0/0 overload

**ip nat inside source list NAT interface fa0/0 overload**

!

VPN 部分

crypto isakmp policy 1

authen pre

encry aes

hash sha

group 5

!

crypto key cisco address a.b.c.d

!

ip access-list ex VPN-T

permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255

!

crypto ipsec transform-set R1-TR esp-aes esp-sha

!

crypto map R1-MAP 1 ipsec-isakmp

set peer a.b.c.d

set transform-set R1-TR

match address VPN-T

!

int fa 0/0

crypto map R1-MAP