思科认证:Cisco路由器上如何防止DDoS攻击Cisco认证考试
 1、使用 ip verfy unicast reverse-path 网络接口命令 这个功能检查每一个经过路由器的数据包。在路由器的CEF（Cisco Express Forwarding）表该数据包所到达网络接口的所有路由项中，如果没有该数据包源IP地址的路由，路由器将丢弃该数据包。例如，路由器接收到一个源 IP地址为1.2.3.4的数据包，如果CEF路由表中没有为IP地址1.2.3.4提供任何路由（即反向数据包传输时所需的路由），则路由器会丢弃它。 单一地址反向传输路径转发（Unicast Reverse Path Forwarding）在ISP（局端）实现阻止SMURF攻击和其它基于IP地址伪装的攻击。这能够保护网络和客户免受来自互联网其它地方的侵扰。使用Unicast RPF需要打开路由器的"CEF swithing"或"CEF distributed switching"选项。不需要将输入接口配置为CEF交换（switching）。只要该路由器打开了CEF功能，所有独立的网络接口都可以配置为其它交换（switching）模式。RPF（反向传输路径转发）属于在一个网络接口或子接口上激活的输入端功能，处理路由器接收的数据包。 在路由器上打开CEF功能是非常重要的，因为RPF必须依靠CEF。Unicast RPF包含在支持CEF的Cisco IOS 12.0及以上版本中，但不支持Cisco IOS 11.2或11.3版本。 2、使用访问控制列表（ACL）过滤RFC 1918中列出的所有地址 参考以下例子： interface xy ip access-group 101 in access-list 101 deny ip 10.0.0.0 0.255.255.255 any access-list 101 deny ip 192.168.0.0 0.0.255.255 any access-list 101 deny ip 172.16.0.0 0.15.255.255 any

access-list 101 permit ip any any 3、参照RFC 2267，使用访问控制列表（ACL）过滤进出报文 参考以下例子： -- ISP端边界路由器 -- 客户端边界路由器 -- ISP端边界路由器应该只接受源地址属于客户端网络的通信，而客户端网络则应该只接受源地址未被客户端网络过滤的通信。以下是ISP端边界路由器的访问控制列表（ACL）例子： access-list 190 permit ip any access-list 190 deny ip any any [log] interface ip access-group 190 in 以下是客户端边界路由器的ACL例子： access-list 187 deny ip any access-list 187 permit ip any any access-list 188 permit ip any access-list 188 deny ip any any interface ip access-group 187 in ip access-group 188 out 如果打开了CEF功能，通过使用单一地址反向路径转发（Unicast RPF），能够充分地缩短访问控制列表（ACL）的长度以提高路由器性能。为了支持Unicast RPF，只需在路由器完全打开CEF；打开这个功能的网络接口并不需要是CEF交换接口。 4、使用CAR（Control Access Rate）限制ICMP数据包流量速率 参考以下例子： interface xy rate-limit output access-group 2020 3000000 512000 786000 conform-action transmit exceed-action 0drop access-list 2020 permit icmp any any echo-reply 请参阅IOS Essential Features 获取更详细资料。 5、设置SYN数据包流量速率 interface rate-limit output access-group 153 45000000 100000 100000 conform-action transmit exceed-action 0drop rate-limit output access-group 152 1000000 100000 100000 conform-action transmit exceed-action 0drop access-list 152 permit tcp any host eq www access-list 153 permit tcp any host eq www established 在实现应用中需要进行必要的修改， 替换： 45000000为最大连接带宽 1000000为SYN

flood流量速率的30%到50%之间的数值。 burst normal（正常突变）和 burst max（最大突变）两个速率为正确的数值。 注意，如果突变速率设置超过30%，可能会丢失许多合法的SYN数据包。使用"show interfaces rate-limit"命令查看该网络接口的正常和过度速率，能够帮助确定合适的突变速率。这个SYN速率限制数值设置标准是保证正常通信的基础上尽可能地小。 警告：一般推荐在网络正常工作时测量SYN数据包流量速率，以此基准数值加以调整。必须在进行测量时确保网络的正常工作以避免出现较大误差。 另外，建议考虑在可能成为SYN攻击的主机上安装IP Filter等IP过滤工具包。 6、搜集证据并联系网络安全部门或机构 如果可能，捕获攻击数据包用于分析。建议使用SUN工作站或Linux等高速计算机捕获数据包。常用的数据包捕获工具包括TCPDump和snoop等。基本语法为： tcpdump -i interface -s 1500 -w capture_file snoop -d interface -o capture_file -s 1500 本例中假定MTU大小为1500。如果MTU大于1500，则需要修改相应参数。将这些捕获的数据包和日志作为证据提供给有关网络安全部门或机构。 更多优质资料尽在百考试题论坛 百考试题在线题库 思科认证更多详细资料 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com