

Network Box advisory: 'Forgotten Security'

Part II: Routing, The Hole in the Wall

Introduction

Routing can be tricky. If you know where data is going, you're half way to resolving a large number of application problems. But understanding where data is being routed to and from is crucial in the security arena. Incorrect routing can result in security measures being bypassed or reduced to allow for badly configured networks.

This paper will investigate some of the common errors that occur and explain why they are bad practice and how they might be mitigated.

Triangular Routing

Many companies have routing where the path that data takes to arrive at a workstation differs from the path that the data takes back to the originator. If one of these paths goes through a connection tracking firewall while the other path does not, the packets will be blocked. This is because the firewall sees a return packet for a connection, but has no record of the initiating packet.

Figure 1 shows an example network that is quite common.

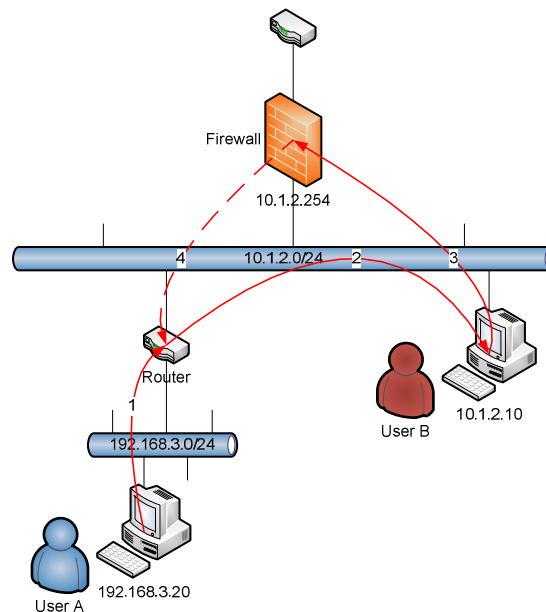


Figure 1: Triangular routing

There is a main LAN shown as 10.1.2.0/24 which is connected to a segment via a router. The remote LAN, 192.168.3.0/24, could be a branch office or maybe just a segment off the main network. User A wants to connect to a server at 10.1.2.10. So User A's PC sends a 'SYN', or its first packet, to the router, as 10.1.2.10 is not on its local LAN and the router is its default gateway. The router knows that the server is on the main LAN and routes the packet direct to the server. The server, however, does not know that the 192.168.3.0/24 network is located behind the router, so sends its reply - an 'ACK' - to the firewall, which is its default gateway. The

firewall knows that any traffic for 192.168.3.0/24 must go to the router but it sees an 'ACK' for a connection that it has seen no 'SYN' for and hence no entry in its connection tracking table. It will drop the packet.

There are a number of solutions to this problem.

- Add a route to the server that will tell it to route all 192.168.3.0/24 traffic direct to the router.
- Configure the router to send all its traffic to the firewall.

However, what often happens is that the IT department mistakes this for a firewall problem, so disables the connection tracking. This can be acceptable if the firewall is sophisticated enough to only disable connection tracking for one port and one set of systems (and the other options above are for some reason not possible). However, sometimes this action reduces a perfectly good connection tracking firewall to a packet filtering which significantly reduces security levels.

Firewalls implementing Proxy Arp

Proxy Arp is a configuration where a firewall or router can respond to arp requests on behalf of machines located 'behind' it, as shown in Figure 2 below. It is useful in a number of situations - for instance, if extra protection is required in a system but the network cannot be reconfigured to allow the firewall to go in as a network address translation (NAT) device. So in Figure 2, all internal devices are on the 10.3.4.0/24 range. The firewall will respond for machines 10.3.4.1, 10.3.4.2 and 10.3.4.3 when an arp request is made from the router at 10.3.4.252.

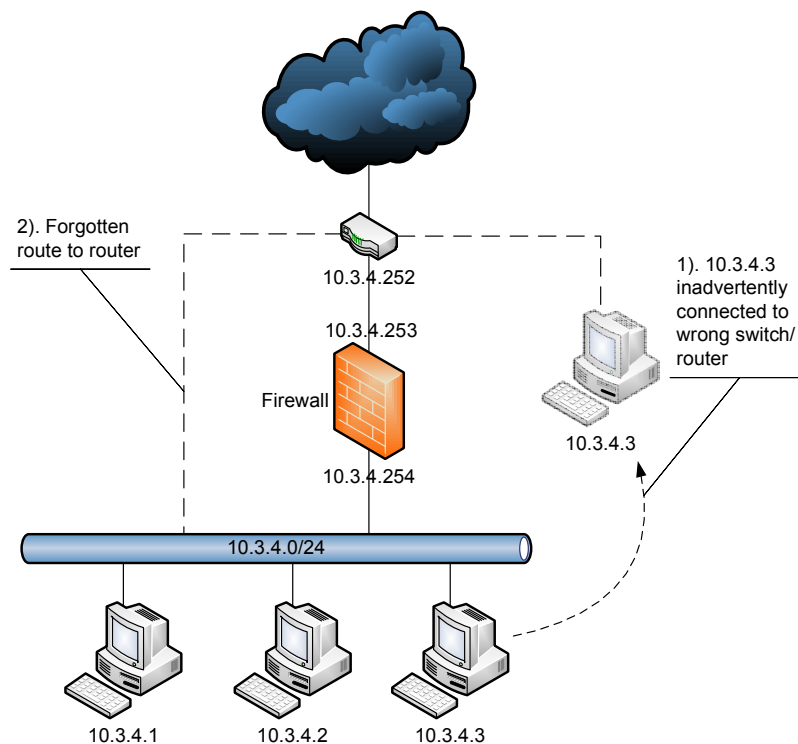


Figure 2: Proxy Arp Network

If, through some error, 10.3.4.3 was connected to the router in front (shown as '1') in the figure above), then both 10.3.4.3 and the firewall would respond to arp 'who has' requests from the router. This conflict can result in a self imposed denial of service attack. This seems like an easy problem to avoid but can happen in busy server rooms where patch panels and cabling have not been correctly labelled.

Another common error is to put the firewall in without realising that there is another route round (shown as '2') in the figure above), causing a complete conflict. In this situation, individual machines on the LAN and the firewall will respond to arp 'who has' requests.

Misdirected packets

In larger networks, packets are routed to optimise speed and loading. However, if these routing protocols are misconfigured so that all packets go the same way, then that path can become seriously overloaded, creating a bottleneck. In May 2009, Google experienced this very problem and a light-hearted explanation from Google is available here:

<http://googleblog.blogspot.com/2009/05/this-is-your-pilot-speaking-now-about.html>

There are issues that arise around dynamic routing protocols like Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP) when misconfigured, that can result in self imposed denial of service. Both OSPF and BGP were designed to improve dynamic routing in or between trusted networks. In these days of heightened security, it is important to remember that OSPF sends its passwords in plain text and BGP does not protect the integrity, freshness or source of the messages it receives. This leaves these protocols open to abuse if not protected.

Virtual Local Area Networks (VLAN)

VLANs are a great boon. They enable us to subdivide our LANs into smaller secure areas, protecting departments or different customers from each other in data centres. However, there are a number of VLAN issues that need to be guarded against.

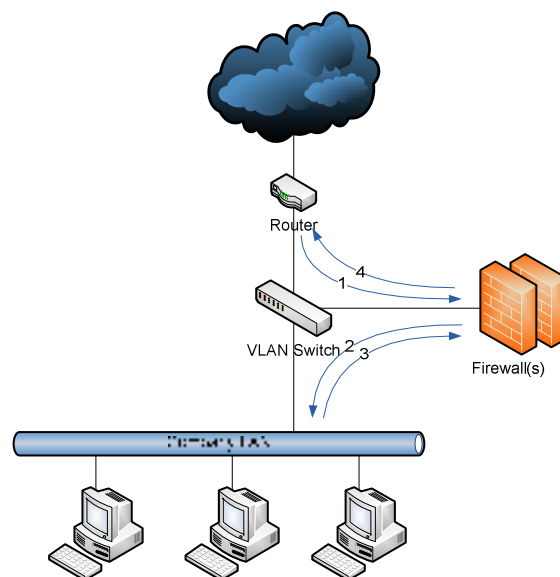


Figure 3: VLAN Switch Network

The most obvious is when the VLAN enabled switch is used for both sides of the firewall (as shown in Figure 3, below). Traffic should flow: from router to switch to firewall (step 1); to switch to LAN (step 2); then back via switch to firewall (3); and back to the Internet via the switch (4).

This is an increasingly common configuration with VLAN switches becoming ever-more popular. The obvious problem is that if an error is made, traffic does not go via the firewall but goes straight to the LAN. It is always good practice to ensure that the traffic is flowing as expected. Good firewalls will be able to show, in real time, the traffic passing through them. This allows the IT manager to check the settings on the switch. In this configuration, it is vital that the switch is hardened and maintained, always having the latest patches to ensure it is not vulnerable to attack and configured to enable only those features that are required. This last is a common omission, as switches have not required this level of attention in the past.

There are a number of other attacks that are generally the result of the switch or router not being correctly configured. For example:

VLAN Dynamic Trunking Protocol (DTP): On some switches and routers, dynamic auto trunk negotiation is enabled by default. This means that anyone with a router emulator or router can connect to a switch and negotiate a 802.1q or ISL trunk line allowing them access to every VLAN in the VTP domain.

Spanning Tree Attacks: the spanning tree election isn't authenticated and the bridge with the lowest priority always wins the election. So by becoming the root bridge, a hacker could easily cause a denial of service attack.

VLAN Hopping Attacks: by adding two VLAN tags to the same packet before transmission, when the packet hits a switch trunk the first tag is stripped off and the packet forwarded. When this packet reaches the second switch inline (where the trunk is established) it sees the tag and processes the traffic based on that information. This allows an attacker to hop between VLANs.

There are a number of other attacks against VLANs but most switches have defences against them. It is just a question of following good practice and ensuring that these defences have been implemented.

Conclusion

There are a large number of different issues with routing. As networks grow, routing becomes ever more complex and the simple examples here only scratch the surface. The important issue is to try and know how the network routes packets. Ensure that you know where they go and that they go the 'right' way. Too many networks hang together with IT managers scared to make changes as they have just managed to get the system to work more by trial and error than by planning. Routing is a security issue and should be taken as seriously as firewall configuration. This will ensure you have change control in place to validate changes and roll back errors.

References:

http://ptgmedia.pearsoncmg.com/images/9781587052569/samplechapter/1587052563_CH03.pdf