

ISA and ACK segments filtering

Source:

<http://www.tech-archive.net/Archive/BackOffice/microsoft.public.backoffice.smallbiz2000/2004-10/0346.html>

From: Fred Blum (*h.f.blum_at_marketconnectnospam.nl*)

Date: 10/07/04

Date: Thu, 7 Oct 2004 14:58:40 +0200

Does ISA filter only SYN/ACK segments? or also ACK segments? Can this be configured?

>From a paper bt Arne Vidstrom:

Ordinary packet filtering firewalls rely on the fact that a session always starts with a SYN segment from the client. Thus, they apply their rule sets on all SYN segments, and simply assume that any ACK segments are part of an established session. More advanced firewalls apply their rule sets on all segments, including ACK segments. Some firewalls are configurable, so you can choose between the two ways to handle ACK segments. The reason to configure a firewall not to apply the rule set on ACK segments is work load. While a session can contain thousands or millions of ACK segments, it only contains one SYN segment. This way you can decrease the work load on the firewall considerably, and save money on expensive hardware. Remember, you cannot establish a TCP session against an ordinary system through any of these two kinds of firewalls if they are set up to block incoming connections.

When ACK Tunneling can be applied

Consider the following case. You have a firewall that doesn't apply its rule set on ACK segments. The rules are to block UDP and ICMP completely, to block all incoming TCP connections, and to allow all outgoing connections. Also to block any other protocols. The attacker sends a trojan by mail to a user on the inside of the firewall. The user runs the trojan.

Now what? How can the attacker on the outside contact the trojan on the inside? There are at least two ways. Either the trojan makes a connection to some computer on the outside, and accepts commands and sends the results through this connection. Another way is to use ACK Tunneling.

So how does ACK Tunneling work? The client part of the trojan uses only ACK segments to communicate with the server part, and vice versa. Now the segments pass straight through the firewall. As long as the attacker knows the IP of the target system, it doesn't matter if his/her own IP is dynamic.

And even if the target IP changes with time the attacker could use a special scanner to scan for the trojan – straight through the firewall.

The trojan doesn't have to contain any link to the attacker. And the person connecting to it might not even know who sent the trojan to the user. It would be just like scanning for NetBus over a whole network hoping it's running on some of the systems. Of course the attacker might be traced through sniffing and tracing the ACK segments. On the other hand there is a great possibility that the firewall won't log these even if it's configured to log all outgoing connections, because it probably only logs the starting SYN segment.

TIA,

Fred Blum