

RE: Symantec Ghost & ISA 2004

Source: <http://www.tech-archive.net/Archive/ISA/microsoft.public.isa/2004-11/0374.html>

From: StevenM (*StevenM_at_discussions.microsoft.com*)

Date: 11/22/04

Date: Mon, 22 Nov 2004 03:59:03 -0800

Hi Jason,

I've just run up against the same problem, again – for a school (ten schools in fact, as I intend to roll this out for nine others in my cluster also once the bugs are all out).

I pretty much ran through the same process as you documented, came up with a similar rule set through trial and error, and got the same non-working result. I'm not sure about ISA 2K4's internal workings in handling high level plain english policies, but it may be that allowing all traffic from/to all networks (including local host) may only be effective for TCP sessions, not UDP flows.

You are quite right, ISA 2K4 doesn't behave anything like ISA 2K. Nowhere near as instinctive to set up for a single interface Web Proxy, particularly if it is a DC/DHCP/DNS/SMB/CIFS/RIS/SAVEntServer/GhostEntConsole/YouNameIt box like we run in the schools.

In checking through the logs I find that the system/firewall policies I came up with do seem to (and at first blush probably should) cover all the services listed above, as there are very few Deny entries coming through the monitoring log now other than for unauthenticated Web Proxy Access (which suits me fine).

The one hard nut that remains uncracked is to sort out Ghost 8.0 Console/Client imaging/cloning jobs, which get caught in an endless transmit/acknowledge loop immediately before the Ghost Client proper kicks in and the file transfer begins.

Have spent about half a day on the problem so far and found the knowledge base article up on Symantec's site entitled "How the Ghost Console and Client communicate over the network", which gives a full run down on the various Console/Client communications and associated protocols. Haven't had time to turn the information into anything useful yet. Reading through the article and what you've done so far, it appears you are on the right track.

FYI, the article URL is

<http://service1.symantec.com/SUPPORT/ghost.nsf/d87bb6ce0bde286d88256d6a00452701/65f62a3671db55e288256c>

Of course, you may have uncovered this for your self by now. If not, hope it is of some use.

Cheers,

Steve.

"Jason" wrote:

- > *G'day All,*
- >
- > *My problem is this; ISA2000, Symantec Ghost & Symantec Anti Virus*
- > *Enterprise worked fine on the same machine with a single network adapter.*
- > *This is for a school so please no replies saying move ghost to another*
- > *machine. Send the funds for a new machine and the building works to add*
- > *space then I'll accept that answer :p*
- >
- > *Now I upgraded the firewall to ISA 2004 that works fine so for uniformity I*
- > *decided to upgrade the ISA2000 (proxy only) server which also has Symantec*
- > *Ghost & Symantec Anti Virus Enterprise installed.*
- >
- > *Now my problems begin :(Symantec Ghost no longer works!*
- >
- > *This is what I've done so far.*
- > *I ran the single network adapter template wizard (default setting)*
- > *I created a rule in the firewall policy:*
- > *Rule 1*
- > *Action: Allow*
- > *Protocols: All outbound traffic*
- > *From / listener: All Networks (and localhost)*
- > *To: All Networks (and localhost)*
- > *Condition: All Users*
- >
- > *I figured that this would allow all users and traffic. This didn't work so*
- > *i added a rule to allow the ports that were being blocked and what i could*
- > *see that ghost was trying to use.*
- >
- > *Rule 2*
- > *Action: Allow*
- > *Protocols:*
- > *TCP/UDP 1345–1347 inbound outbound, receive send*
- > *TCP 1024–49151 inbound outbound*
- > *UDP 1024–49151 receive send*
- > *From / listener: All Networks (and localhost)*
- > *To: All Networks (and localhost)*
- > *Condition: All Users*
- >
- > *Rule 3*
- > *Default block all.*

>
> *Still doesn't work after two days of trying to figure this out, below is a*
> *copy of the firewall logs i hope this will help.*
>
> *computer date time IP protocol source destination original client*
> *IP source network destination network action status*
> *rule application protocol bidirectional bytes sent bytes*
> *sent intermediate bytes received bytes received intermediate*
> *connection time connection time intermediate source proxy*
> *destination proxy source name destination name username agent*
> *session ID connection ID interface IP header protocol*
> *payload*
> *FS002 30/9/2004 01:03:03 TCP 10.254.0.96:1025 10.254.0.11:1347*
> *10.254.0.96 Internal Local Host Denied 0xc0040017 -*
> *FS002 30/9/2004 01:03:16 UDP 10.254.0.96:1346 10.254.0.11:1347*
> *10.254.0.96 Internal Local Host Terminate 0x80070057 Allow All*
> *FS002 30/9/2004 01:03:17 TCP 10.254.0.96:1025 10.254.0.11:1347*
> *10.254.0.96 Internal Local Host Denied 0xc0040017 -*
> *FS002 30/9/2004 01:03:17 TCP 10.254.0.96:1025 10.254.0.11:1347*
> *10.254.0.96 Internal Local Host Denied 0xc0040017 -*
> *FS002 30/9/2004 01:03:24 TCP 10.254.0.96:1025 10.254.0.11:1347*
> *10.254.0.96 Internal Local Host Denied 0xc0040017 -*
> *FS002 30/9/2004 01:03:39 TCP 10.254.0.96:1025 10.254.0.11:1347*
> *10.254.0.96 Internal Local Host Denied 0xc0040017 -*
> *FS002 30/9/2004 01:03:39 TCP 10.254.0.96:1025 10.254.0.11:1347*
> *10.254.0.96 Internal Local Host Denied 0xc0040017 -*
> *FS002 30/9/2004 01:03:45 TCP 10.254.0.96:1025 10.254.0.11:1347*
> *10.254.0.96 Internal Local Host Denied 0xc0040017 -*
> *FS002 30/9/2004 01:04:00 TCP 10.254.0.96:1025 10.254.0.11:1347*
> *10.254.0.96 Internal Local Host Denied 0xc0040017 -*
> *FS002 30/9/2004 01:04:02 TCP 10.254.0.96:1025 10.254.0.11:1347*
> *10.254.0.96 Internal Local Host Denied 0xc0040017 -*
>
> *Thanks to all that reply!!*
>
> *Cheers*
>
> *Jason*
>