

## Re: Should I still buy SBS 2003 Premium w/ ISA in light of XP SP2's ICF2?

**Source:**

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2004-08/6319.html>

---

**From:** Jeff Middleton [SBS-MVP] ([jeff\\_at\\_cfisolutions.com](mailto:jeff_at_cfisolutions.com))

**Date:** 08/19/04

Date: Thu, 19 Aug 2004 08:41:09 -0500

Hi Bret,

So many questions!

Admin rights is a very simple story. You have created an end-game scenario in which any process or application launches with the ability to access 95% of all system resources without pause by simply running in the "user context". That's a simple statement. User context in a security world is supposed to mean "user activities", but when you put that "user context" into include "administrative rights activities", 95% of the security the OS might otherwise have afforded you....you effectively defeated.

In another simple consideration, any hacker or worm/virus is seeking to gain control of something, and normally the quest in an attempt is to both propagate and escalate access level activities. Stated more simply, hackers are looking to elevate the from "user context" to "administrator context" because the Administrator accounts have "more toys" to play with, fewer restrictions on what they can do. In a well secured network, Administrative rights is something that a hacker is presumably supposed to expect to "work for" to get.

Now, I think most of this you already knew, Bret. Now let me put some of this in perspective of the nature of your questions.

In a small LAN running 5 workstations, using an SBS server as the domain management, and assuming that we are running XP2 and ISA, here's what your security profile is going to look like:

A. At the local workstation, there is a security context of:

- Various layers of "user context", accumulating up to the local Admin rights context
- Local Administrator context
- XP2 Firewall tool tuning that blocks by default, certain communication in the LAN
- XP2 Feature enhancements, delivering user preferences on annoyances,

spyware

- 3rd Party AV/malware protection
- Domain enforced security lockdown (meaning, security enforce from off the box, therefore even if you gain control of the box, you may still be subserviant to domain security overriding you, or blocking you once you attempt to use your rights elsewhere "off that box")

B. At the Domain level, there is a security context when SBS is a DC of:

- Domain Admin can remove privileges from Local Admins, but typically that's not broadly used.
- Domain Admin is typically granted Local Admin, but not constrained by reduced privs that might be enforced on the local Admins by preference.
- Domain Admin is a uniquely different account, provided that the workstations are not configured with identical matching local Admin account name/pass, in which case pass through authentication makes these accounts behave as "equals" when a user acts from one machine to another.
- Access to the SBS from the workstations is limited by unique policy settings for a Domain Controller that are elevated in security by default in Group Policy by MS, and therefore imply that a user context may be successful in doing something with "access over the network" to another workstation, that wouldn't also work with "access over the network" to the SBS as DC. Therefore, the SBS is a bit more locked out from network traffic, and a bit more locked down in general, with or without hardening beyond "out of the box" tuning.
- Flipside, as a DC, the SBS is responsible for servicing all the network requests in authentication, management, browsing...not to mention the application services. This means those ports are open for business....but it also means that they are potentially exposed if the machine is not properly patched. Lots of ports on an SBS open for business on the LAN.
- If the Internet traffic comes from a router on the LAN to a single NIC, the SBS is offering a common NIC for LAN and web traffic, and you are relying upon the firewall to block accordingly the access to workstations, and to the server. Yet, you must still have the router float traffic over to the SBS for service ports like Exchange, IIS for Remote Web Workplace. These ports will essentially see whatever traffic asks for those ports, even if it's NAT...it still comes over. Only if the router has packet-level filtering is the router going to afford protection to the SBS exposed service ports by recognizing "hey, this is coming at a valid port, but the request itself is suspicious" (more on that later)
- If the Internet traffic comes to the SBS from a 2nd NIC with the Standard Edition of SBS, the firewall protection is there as is NAT, but you don't have the same level of packet-filtering in your favor that ISA provided. Essentially, you have protection from blunt force attacks, but you lose the more sophisticated firewall features that make ISA an enterprise class firewall, vs a personal firewall like whatever we now call ICS. (more on this later)

C. At the ISA Server level, you have security context of:

- ISA provides packet-filtering...it looks not just at the port and destination, it looks at each packet to decide by rules if THAT packet can

be trusted, not can that STREAM be allowed. ISA is capable of deciding that with a stream of traffic it is willing to pass, now something is wrong and it should be blocked. It doesn't open sessions after authentication and then ignore them, it watches the entire time.

- ISA isn't just a proxy server, it's a full service firewall...rules based not just on access control, but on protocol and port filtering, user rules, group rules, destination rules....all at packet level inspection.

- ISA is a caching proxy service, so this can help with performance on certain things, but it could argued that ISA may slow down other kinds of traffic that a router wouldn't.

- ISA provides pretty detailed tracking, logs of web traffic, packet filters, all the services provided. You can audit after the fact what happened. You can see someone beating on your firewall in real-time, or in a later audit. You KNOW what is going on at the firewall.

Okay, that's my background.

If you have ISA on your SBS, you can use it to lock down traffic passing the firewall in any direction, and it doesn't matter if the user is an Administrator or not. You can set a rule that says "this specific kind of traffic is blocked, don't care who asks for it." With a rule like that, there's nothing a user on a workstation can do, even with Admin rights, they aren't going out past that rule. In fact, the Administrator can use similar stuff to prevent themselves from passing out the firewall, even from the SBS. Therefore, ISA afford the ability to ignore the concept of "admin rights" and instead look at the concept of "firewall usage based upon identity, or other factors".

ISA defines the ability to use rules that include all the AD user/group/computers identifications, then add onto that granular permissions, and granular filters. It's sooooo much more sophisticated than a typical firewall from Linksys....it's more sophisticated as a firewall than a Cisco router without a firewall specific overlay. It probably is more sophisticated (in general as a firewall) than a low to mid level security oriented firewall....except for one thing: it's running on a multi-use platform with SBS involved.

ISA on an SBS is an excellent security edge, it secures the SBS better, and it secures the network traffic better than the alternatives at the same \$1000 price. The only reason it has a caveat in SBS of "would be better" if on a standalone box is because that's just practical good sense. Think of a turtle....hides in the shell, very few places to get in, one of the holes has a nasty bite. An ISA server that provides no access (because it's dedicated) for any purpose than as firewall means it's totally locked down. That means you can use a weakness inside another service (a port ISA doesn't use, but some other service does) as a way to pry the top of the ISA server, or blow away the underlying network services (MSblast would have taken down an unpatched SBS with an attack from the LAN or internet) even if it was running ISA because the traffic would be passed! The port was open for business, and it wasn't ISA that was flawed, it was the underlying OS DCOM structure.

Where I'm bringing this to is this: Security context means that if you allow something, it's allowed...it's open for business.

At a workstation, if you allow a user to be an Administrator, they are allowed to install, shutdown, modify and create services, processes, and hacks on the OS. The administrator can grant themselves System level rights. Therefore, if you run a workstation as Administrator, any spyware or malware that isn't trapped, potentially could elevate an attack to System level in a half a heartbeat. That's System level on the local machine. But that doesn't mean the same at the next machine if one of two things is true:

1. If local Admin at one machine is not Local or Domain Admin user/pass at the next machine, the game starts over at the next machine.
2. If each machine runs a rudimentary firewall like XP SP2, then only the allowed service ports are open for business between the workstations. Unfortunately, that's typically going to mean a lot of ports are shared, but at this point, at least the attack surface is reduced to "only these open ports" as opposed to the historical Windows design of "every port I have is open."

XP SP2 reduced the attack surface inside the LAN down to a given number of ports, and you determine that by how you set the tuning on the applications.

XP SP2 reduced the attack entry points because it now looks at activities that "probably aren't authorized" and it asks the user "are you sure you want MSblast to launch from that website?"

The problem is, most users will say "Absolutely, I want to see Anna Kornikova naked" (TM: Jesper) and therefore the warning of XP SP2 didn't help for that. The user running at full Admin locally will still launch MSblast on their own machine. However, when MSblast knocks at the next box in the LAN, if the local user at Machine A isn't a Local Admin at Machine B, now the user at Machine B perhaps get's a popup "You want to see Anna naked?". In some cases, if the user's name is Sue, Barbara, Hellen (you get my drift) at least some of these users will not be interested....and MSblast is more contained than otherwise.

Meanwhile, back at the firewall, the reason that MSblast came through is because there wasn't an AV scanner in the stream, and the User context was allowed. ISA won't block MSblast coming through on the stream as a download unless you add an application to ISA that scans for viruses/hacks. By default, it doesn't...it looks for source, destination, ports, protocols, users/groups/machines, time, and rules. (Plus a little more) ISA is designed to let you add a scanner to it for this purpose, not do that job. However, MSblast is a special case.

ISA will do attachment blocking, and it can block many kinds of things based upon protocols and filters. MSblast is an odd case because of the ability to launch code living "outside" the network firewall by going to it in a stream that is allowed, or by MSblast being launched "at" an open service port that isn't protected.

Now, in the current circumstance, most malware/spyware isn't nearly as dangerous as MSblast, but the reality is that most people run with Admin rights so most of the protection at a workstation is already dropped to zero. Adding Windows XP SP2 to a workstation adds some filtering in traffic to protect your from "other machines", and it provides some tools to prevent many "transparent" attacks that a user can launch against themselves simply by not knowing that they just allowed it with their last action.

A summary then of these ideas:

If you want to secure your network, there is one thing you can do that is more effective than just about anything else: eliminate Administrator rights users.

Without Administrator rights, most users can not hurt themselves nearly as much, and many of the features of XP SP2 are even more enhanced because even if XP SP2 is willing to let you do something, the OS itself will deny it.

XP SP2 is going to improve security on any workstation, whether or not it's on the LAN or on the web because SP2 locks down things that used to be either open by default, or simply overwhelmed the user with programic self-abuse through browser actions launching themselves without restrictions.

XP SP2 should be seen as instructive....you should do both: install XP SP2 and eliminate Administrator rights. They both do the same thing....the further isolate the difference between "user context" and "system context". System context is what the OS is allowed to do. "Administrator context" is just trivially below System level. "user context" is probably about 10% of the rights of System, and 20% of the rights of Administrator (without self elevation that an Administrator can do).

Even if you give up the entire workstation, if you isolate machine to machine communication that doesn't have to happen, you knock back virus propagation tremendously. There are two ways to do that. You separate the machine by "technical access" (ports/protocol firewall, or V-LAN, or IPSEC filtering that disallows workstations to talk directly to each other), or you isolate them by "security context".

Most SBS admins are not sophisticated enough as security gurus or well enough endowed with security/network tools to isolate SBS scale networks from machine to machine context....until XP SP2. Now you can. But it won't matter nearly as much if you don't do what you can....isolate at "security context".

Security context isolation is where you force users to not have unlimited rights at all machines, even if they have them at THEIR machine. That means, you don't make Domain Users = Local Administrator at every machine. It also means you don't make:

Local Administrator Name/Pass = Domain Administrator Name/Pass

If the combination is different, it means that you can isolate what can be done even if it's allowed by "technical access" simply because "you don't have permissions".

One of those ways is to also set the same level of "security context" protection at the firewall. And now we are coming full circle, eh? If you have a firewall that works in a domain "security context" and you use it to do as much as possible at the firewall to prevent users from doing things they don't need to do, don't want to do, and shouldn't be allowed to do....you reduce the attack profile.

Most importantly, it means that if you use ISA at your perimeter, you are able to deny the ability to do things that cross the web threshold, even if a user is an Administrator. You break the chain of opportunity. Even if a user has unlimited rights to beat their machine to pulp, they don't necessarily have the option to go out on the web to get more dangerous tools....at least, not if the tools require conditions that ISA can block. In addition, the Administrator can audit what users are doing to see behavior that is dangerous, and to see slow building attacks coming in at the server regardless.

If you have ISA on the server, you can use it to protect the server better than a router would, and to provide auditing that neither a router or the connection sharing found in SBS Standard Edition provided.

ISA doesn't really supplement XP SP2...that's not the idea, even if it does work that way. As a general rule, XP SP2 is trying to close down "business ports" used only on the LAN, but the "web experience" ports are still going to be open. What ISA does in this context is to provide the Administrator with an "overrule" option related to the web, to enforce a firewall condition from the web, even if the user's XP firewall would allow it. In a sense, that means that ISA has the potential to give you better firewall blocking, if not more administratively savvy firewall tuning than the user would do for themselves. Therefore, if the only thing in front of the user running XP SP2 is a NAT router, the ISA server will potentially enhance the security.

Ultimately, the problem is that even with all this information, all this analysis, all this opportunity for improvement, you know what the typical home user does, and what the common SBS admin does?

1. Install every user as local Admin.
2. Make every user a local Admin at each station
3. Use the same username/password combo at every workstation and for the domain admin account.
4. Use All/All/All rules at the firewall for outbound
5. Never audit the firewall, or not use a firewall that allows audits
6. Trust AV to protect them passively
7. Hope that XP SP2 does a better job of adding to passive protection.