

# Exchange 2000 in the Enterprise: Tips and Tricks Part One

*Tim Mullen* 2003-01-02

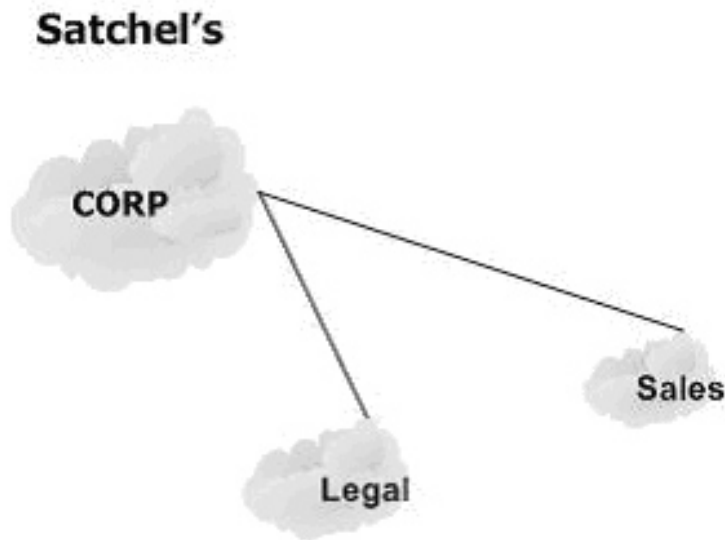
What is the best way to deploy Exchange 2000 in your enterprise? There is, of course, no right answer to that - but hey, I needed an intro.

The Mighty Chris Webber covered securing Exchange 2000 in a DMZ configuration in a series of [SecurityFocus articles](#) that makes for great reading. In this two-part article we will discuss an alternate configuration in which we will utilize Microsoft's Internet Security and Acceleration (ISA) Server, a third party SMTP Gateway (Trend Micro's Internet Messaging Security Suite) and Exchange 2000. This sort of configuration is flexible enough to be used in smaller installations that do not use a DMZ, or as part of the DMZ configuration itself.

Email seems simple on the surface, but securing a messaging topology is a complex task. We must consider attacks against the mail services themselves, malicious content within the mail, security issues with remote and Web access, and even information leakage via mail headers. Our goal in the following examples is to address as many of these concerns as possible while maintaining a system that is not a nightmare to administer. So let's get to it.

## Topology

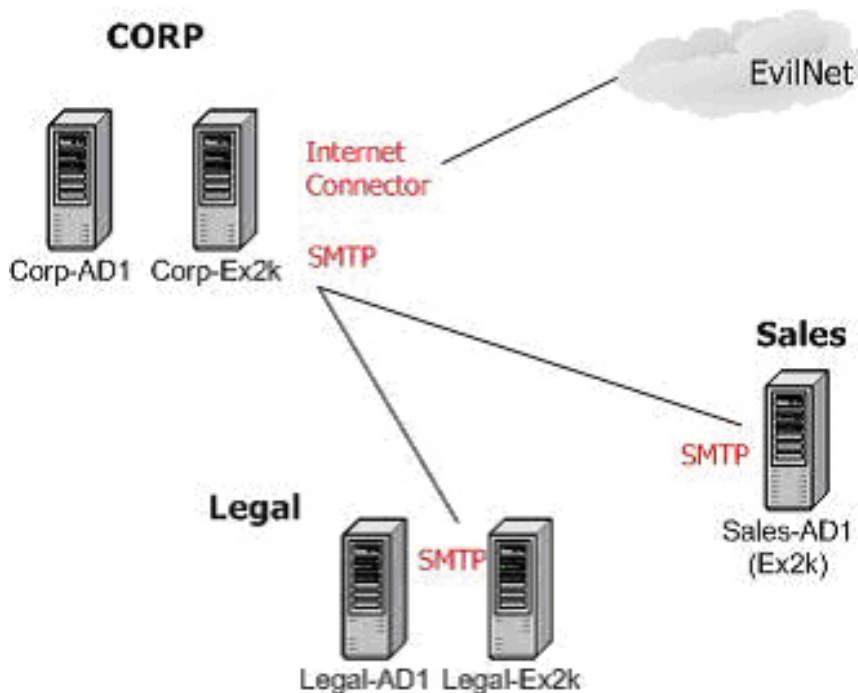
Our fictitious company, Satchel's, makes Hillary Rosen dolls that wear little "Berman for President" T-shirts and sing *Danke Schoen* when you pull the string. Orders are flooding in. To keep things simple, we've got three sites to worry about: the main facility, the sales offices, and, most importantly, the legal department. Here's the layout:



It's pretty basic. The main Internet connection runs out of Corp, with Sales and Legal coming in via a frame relay PVC or maybe a DSL VPN - that part doesn't really matter for this example, as long as it is a persistent connection with decent bandwidth.

First for the messaging infrastructure. Meeting with the best practices of active directory and domain controller placement, we'll have a controller at each site. Keeping with real-life deployment, the Sales site controller will also run Exchange 2000, even though we all know better. The Corp and Legal sites will be running Exchange 2000 member servers. Let's get those in place and get Internet mail going.

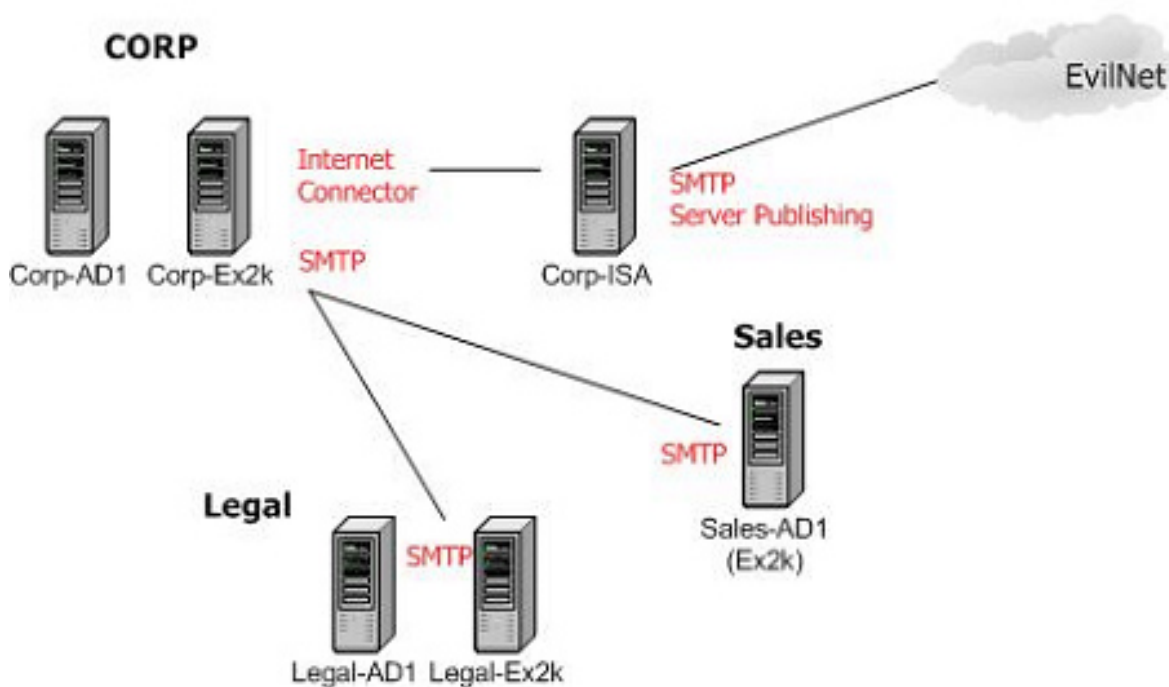
## Satchel's



This is a pretty common topology - the router or firewall allows TCP 25 into the SMTP service of Corp-Ex2k, which accepts incoming email. (There is no reason to get into the varied ways of doing this, as we're going to change it in the next step.) Exchange Server configuration and user mailbox information is stored in Active Directory, which is used to route the mail items to the appropriate boxes (both for internal and Internet mail). Likewise, outbound mail from each site is routed to the correct site/mailbox or, in the case of Internet mail, out the Internet Connector on Corp-Ex2k.

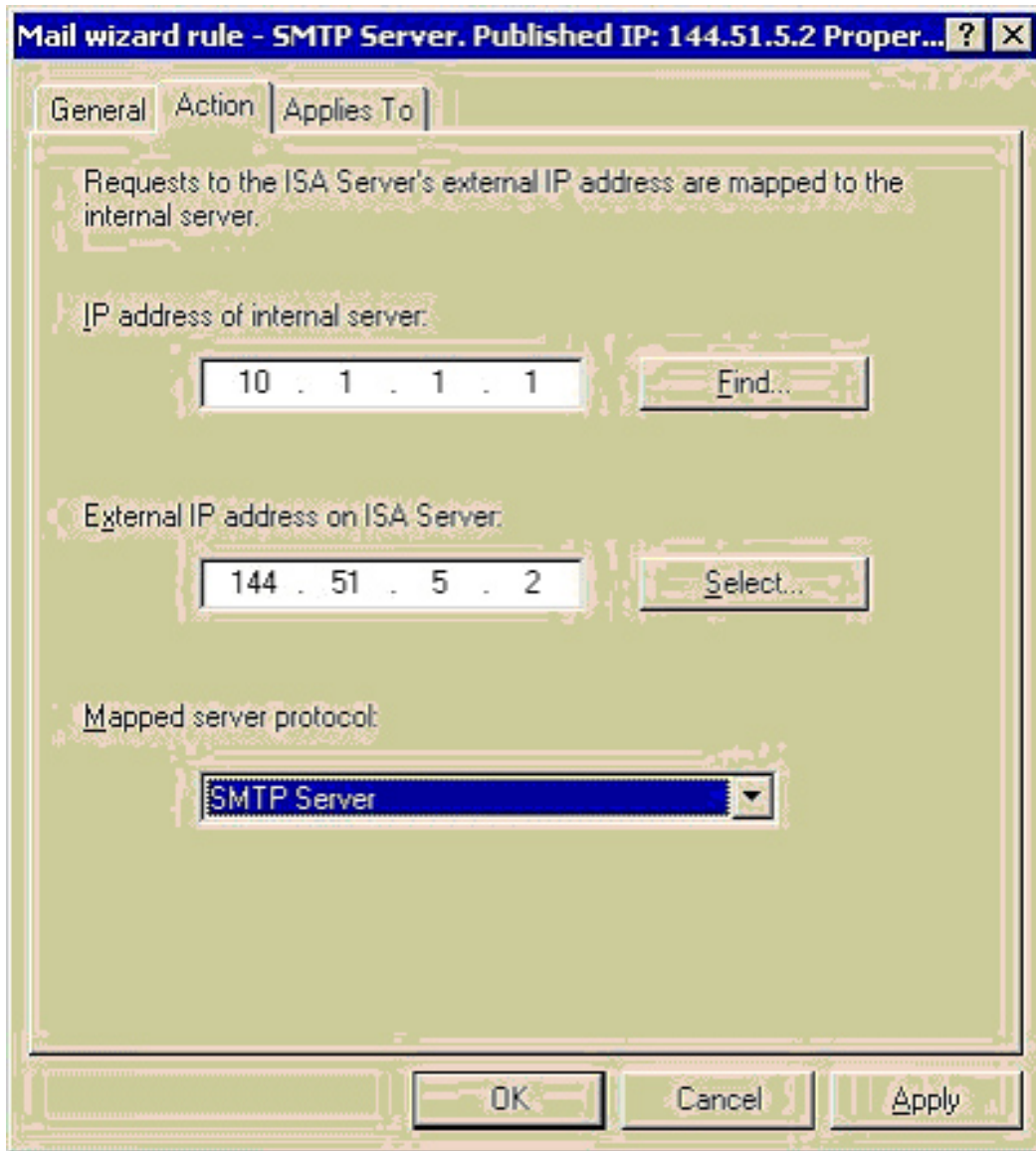
The problems here are obvious - outside attackers can make direct contact with Corp-Ex2k and there is no server-based content or virus checking going on. The first thing to do is to remove Corp-Ex2k from all direct access and put him behind something robust- that is where ISA Server comes into play:

## Satchel's

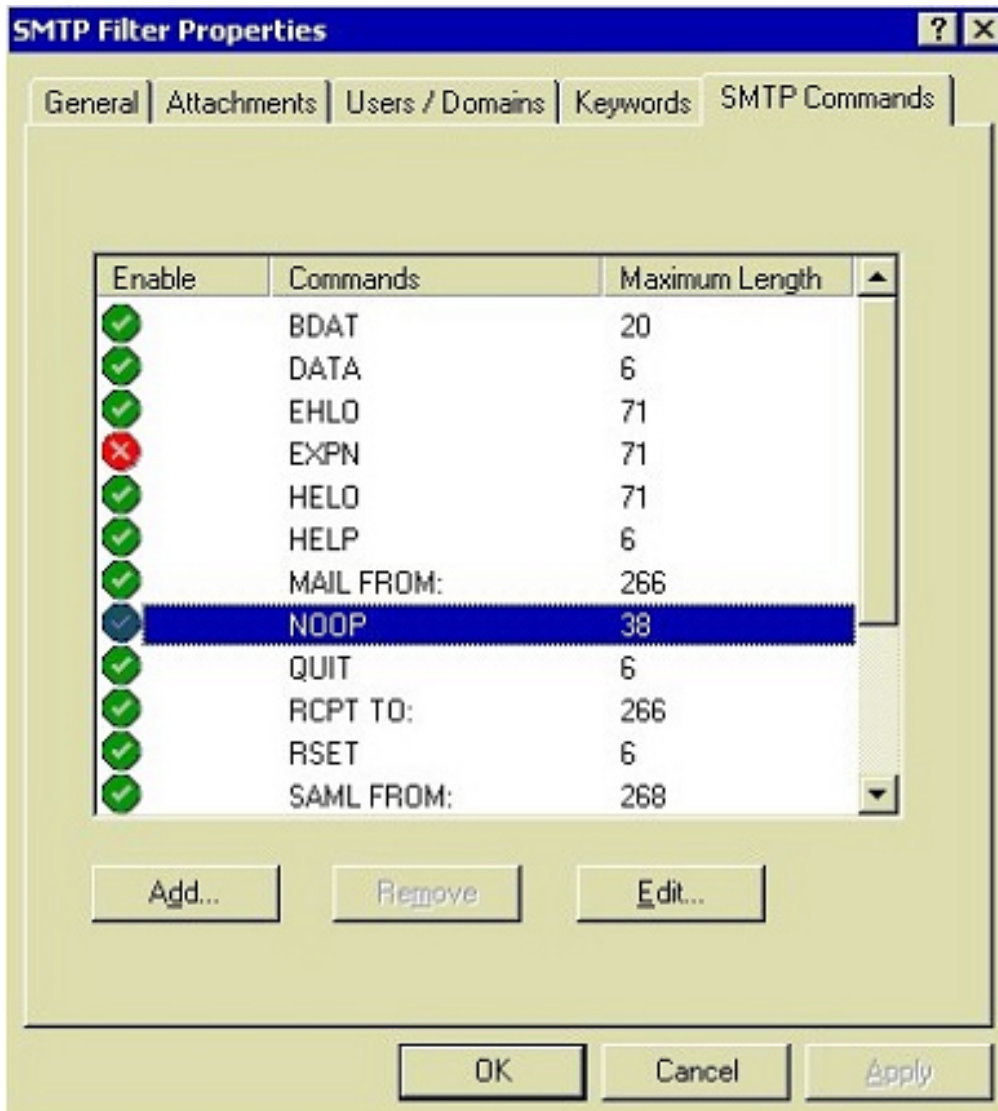


With the addition of an ISA server between Corp-Ex2k and the Internet, we can keep Corp-Ex2k entirely within our private address space and abstract it a bit from the Internet.

ISA Server is performing two roles for us now. Firstly, via a Server Publishing wizard called "Secure Mail Server," we are publishing the SMTP Service from the external interface of the ISA Server to the otherwise unreachable internal Corp-EX2k machine. We'll create a Server Publishing Rule that will "map" a particular Protocol Definition, in this case SMTP Server (Inbound TCP 25), from a public IP and publish it to an internal unit:



Secondly, we can now filter SMTP commands at the application level through the ISA box by using the SMTP Application Filter, one of many application filters built into ISA Server. Here are the properties for the SMTP Filter:



This configurable filter allows you to select which SMTP commands you wish to enable, and the maximum length in bytes each command is allowed. This will prevent potential abuse from overly long commands and overflow attempts. There is also a POP intrusion detection filter designed to protect against POP buffer overflow attempts (created for Microsoft by ISS), but it is not configurable.

You will notice that NOOP is highlighted in the above screenshot of the SMTP Filter properties. I have changed it from its default of 6 bytes (4 Char + CR LF) to 38 bytes- this is because I have seen other Exchange servers (both 5.5 and 2000) pad their NOOP (which stands for No Operation) commands with 25 or more bytes of 0x20 characters. In these cases, the default 6-byte command filter would block the command, and it would cause mail delivery problems from those hosts. A maximum length of 38 bytes has worked just fine for me ever since.

OK. Though we have abstracted the Corp-Ex2k from the Internet and now have an application filter in place, I still have a problem with the outside world being able to issue commands

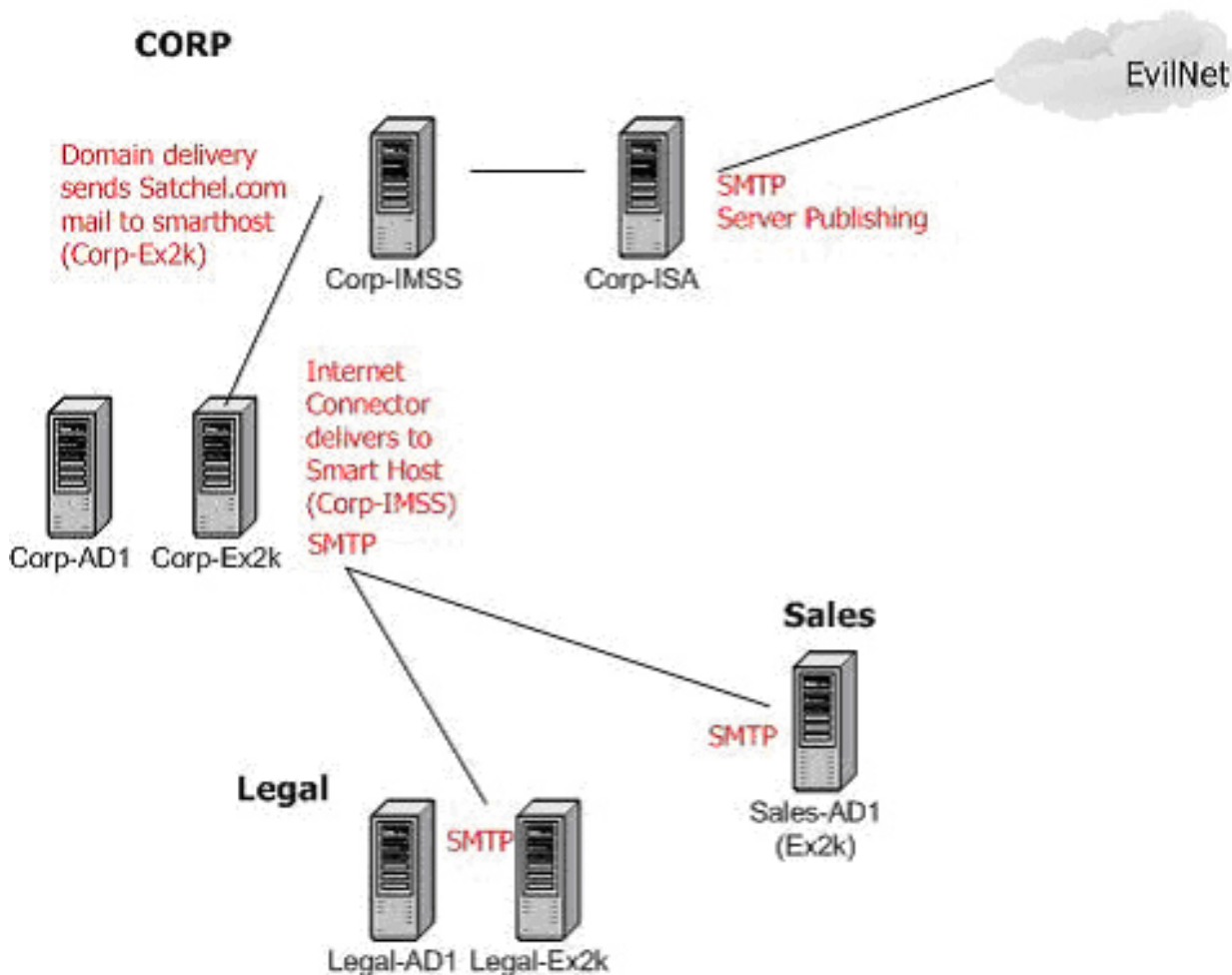
against the Exchange SMTP service itself. Telnetting to port 25 on the external interface of Corp-ISA still gives us:

```
220 corp-ex2k.satchels.com Microsoft ESMTTP MAIL Service, Version:
5.0.2195.5329 ready at Mon, 23 Dec 2002 14:00:00 -0500
```

Anyone can sit on top of the service and dump commands into it. Though we are filtering the command set through the ISA server, it is the element of the unknown that concerns me: we just don't know what vulnerabilities the future may present, and the possibility of a compromised Exchange server is just too much of a risk. I also don't like anyone being able to ID the server banner that easily.

This is a perfect time to introduce our SMTP Gateway, which will not only completely remove Corp-Ex2k from all outside access, but it will give us our much needed content and virus scanning. The gateway product is really your preference, but in this example we'll install [Trend Micro's IMSS](#) on a stand-alone server and set it up as follows:

## Satchel's



Like most SMTP gateway products, IMSS allows us to easily customize the server banner so that we don't immediately own up what products we are using. Something like this gives an attacker much less information to work with:

```
220 mail.satchels.com YoMommaMail(c) Ver 9.2 ready Mon, 23 Dec 2002 14:00:00 -0500
```

Now we have a decent messaging topology. We have an enterprise firewall protecting our corporate assets, which is also publishing SMTP traffic (after filtering SMTP commands) to our internal IMSS server, which then scans the message for viruses, any content or spam filtering you have enabled, strips attachments, etc. [Note that the ISA SMTP Filter can also strip attachments-- it is up to you what system(s) you want to perform this function on.] Corp-IMSS performs domain-based delivery to route all mail bound for Satchels.com to Corp-Ex2k as a Smart Host.

Corp-Ex2k will then route the mail to the appropriate mailbox. Outbound Internet mail routed

through Corp-Ex2k will all be delivered to Corp-IMSS as a Smart Host, at which point DNS-based delivery will take over.

We've got application level filtering, virus protection, content management, robust firewall configuration, isolation of services, and a good set up.

Now that we've got the infrastructure built, it is time to offer up access to mail content for our users on the Web via Outlook Web Access, which we will cover in our next segment. In addition to OWA considerations, we'll talk a bit about what information you might be giving out in your email headers, and ways to mitigate possible information leakage.

We'll see you then.

To read Part Two of this article, click [here](#).

*Timothy M. Mullen is CIO and Chief Software Architect for AnchorIS.Com, a developer of secure, enterprise-based accounting software. This article is an exclusive excerpt from Tim Mullen's upcoming Blackhat Win2K training, "Microsoft Ninjitsu: Securely Deploying Microsoft Technologies."*

[Privacy Statement](#)

Copyright 2006, SecurityFocus