

## Re: ISA and PIX 506

**Source:** <http://www.tech-archive.net/Archive/ISA/microsoft.public.isa.configuration/2005-01/0055.html>

---

**From:** Stuart Mackie [MCP, MSP] ([newsgroups\\_at\\_---REMOVE\\_THIS---stu.uk.com](mailto:newsgroups_at_---REMOVE_THIS---stu.uk.com))

**Date:** 01/09/05

Date: Sun, 9 Jan 2005 11:54:31 -0000

Hi Scott. Answers in-line below.

> *Recently, the client decided that they wanted to be protected by putting a  
> Pix in the mix in front of the ISA ( Upgrade to ISA 2004) so he would have  
> two firewalls protecting the network.  
> Here is the problem, when we put the Pix (501) at Site "A" and one at Site  
> "B" the tunnel between the ISA servers was disconnected. The Pix's were  
> configured to do a VPN between locations with a 3 Des encryption. In order  
> for users at Site "A" to login, we had to create a VPN from ISA to ISA, so  
> you ended up with a PIX tunnel packaged into a ISA tunnel to the other  
> ISA. A  
> lot of encryption that degraded the connection and performance.  
> So, in this situation, what is the best way to get users from Site "A" to  
> get authentication from Site "B" without having dual tunnels between the  
> networks. They would like to use ISA at both locations with a Dual NIC  
> format.*

When you added the PIX firewalls did you make any configuration changes to the ISA servers to accomodate the PIX acting as the end point rather than ISA ? It's likely you were nearly there but didn't tell ISA how to route the traffic to the other network.

> *The other issue is, if a remote user (IE sales person) uses the Cisco VPN  
> client to connect to Site "B", what would have to happen next ( or config)  
> to  
> allow access to the Internal network.  
> Here is what we would like to  
> Site "A" Site  
> "B"  
> network -->ISA -->Pix 501-->Internet - - - -->Pix  
> 501 -->ISA -->network*

Is this remote user behind the PIX at Site "B" or is this a roaming user or a home user connecting in remotely ? If this was a user at Site B they shouldn't be using the VPN client to connect to site A internally :) But if they are a remote user out of the office you would have a number of options as to how to do this. Since you have two ISA servers but only one DC at this point, you would have to decide whether you only use the PIX at Primary

Site A for roaming user VPN connections otherwise any user connecting to Site B PIX will have to go through two tunnels since your DC is at site A, although their data may be at site B. Depending on which way you went with (see comments below for adding second DC), you would need to configure the PIX firewall to allow dynamic VPN connections with the appropriate settings (e.g. 3DES with DH Group 2 and SHA). Your ISA server would then need to be configured to recognise the subnet used by remote VPN users as part of the internal network to provide connectivity and routing.

> *So some questions are:*

- > *1. With this setup, what is the best way to configure Pix and ISA so users*
- > *at Site "A" can get authenticated to Site "B"?*

There are pros and cons of using ISA – ISA and ISA – PIX – PIX – ISA, but IMO what you decided to do by adding the PIX as the end point is the better choice. To resolve your problems you need to remove the VPN tunnel between ISA and ISA leaving just the PIX – PIX VPN tunnel. You then need to create a destination set on each ISA server with the IP/Subnet of the remote network (the IP/Subnets must be different between Site A and Site B i.e. 10.0.0.1–255.255.255.0 on A and 10.0.1.1–255.255.255.0 on B). You would then create a new Static Route in ISA using this destination set to instruct ISA server how to route traffic destined for the remote network. Finally you would add the remote network subnet into the LAT (Local Address Table) in ISA so that ISA treats the remote network as part of the local network. There may be security advantages in not adding the remote network to the LAT on each server and configuring access rules to allow only access to specific ports so that although you want both networks connected as one local network, only allowing access to specific ports/resources could provide security between branches. In saying depending on what ports/resources are required, configuration could be lengthy and you may end up opening most ports up.

#### ISA Site A

Local Network 10.0.0.1–255.255.255.0

Remote Network Destination Set 10.0.1.1–255.255.255.0

#### ISA Site B

Local Network 10.0.1.1–255.255.255.0

Remote Network Destination Set 10.0.0.1–255.255.255.0

You would also have to examine your PIX Configuration to check it is configured correctly not only in terms of encryption but to handle the different subnets.

The one other suggestion I would make is to add a Domain Controller at Site B. This provides a number of advantages.

Firstly and the main reason you would cut down traffic over the tunnel if users can authenticate locally. If you were using folder redirection and roaming profiles you could configure Site B users data to be stored on the DC at Site B and similar for Site A. You could then configure replication for the data to run during the evening or when the offices are quite to

replicate the data for backup to the opposite site.

Secondly you can configure replication so that if one DC was to go down all your users would still have access by using the remaining DC. This idea could be slightly flawed if your ISA servers are also your DCs since if your DC goes down its likely the whole server would be down and you wouldn't have any routing between the networks :) Although, at least with DCs at either site if a failure were to occur, only one site would be affected rather than the whole organisation.

Finally when accomodating roaming users you would have the choice of Site A users connecting to Site A via VPN when travelling and Site B to Site B since their profiles and data would likely be stored in their respective local site reducing the need to pull information across the tunnel. From an admin point of view configuring and supporting two VPN connection points may provide additional issues. You also haven't mentioned what type of connection is being used between Site A and B which would have an influence on some of these decisions.

> 2. *How could someone from Site "B" use Cisco VPN to connect to anther site > that uses Cisco VPN. ( Yes the second would need a VPN Concentrator).*

You phrased this slightly differently to the above VPN user, is this a different issue to the Remote Salesman ? As long as your ISA policy allows this type of outgoing connection and the remote VPN Concentrator is configured correctly for the VPN connection you shouldn't have any problems. Due to NAT being used on your connection the remote Cisco end point e.g. PIX, Concentrator etc would have to be configured to accomodate NAT Traversal if not already configured. If you have everything configured correctly already and are having problems, it may be worth checking the port requirements of the Cisco Client and how it initiates the connections.

Hopefully this helps you get your configuration up and running. If you have any more problems or questions please post back.

--

Hth,  
Stuart Mackie [MCP, MSP]  
www.stu.uk.com