

## Re: secure server policy

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2004-07/0092.html>

---

**From:** new question ([newquestion\\_at\\_discussions.microsoft.com](mailto:newquestion_at_discussions.microsoft.com))

**Date:** 07/02/04

Date: Fri, 2 Jul 2004 06:03:04 -0700

thaks a lot ;

What is solutions to protect authentication data client to DC .

Steven Umbach" wrote:

- > *Be very careful with ipsec policies. Ipsec policies between domain members must*
- > *exempt domain controllers based on their static IP addresses or you will*
- > *experience a lot of problems. MS does not support ipsec negotiation policy*
- > *between domain members and domain controllers because of the way machine*
- > *authentication works in ipsec. See the links below for more details. --- Steve*
- >
- > <http://support.microsoft.com/?kbid=254949>
- > <http://tinyurl.com/3yvnl> -- link to a previous thread on this topic.
- >
- > *From Windows 2003 Deployment Guide :*
- > *Requiring IPSec for communication between Active Directory domain members and*
- > *domain controllers might block connections*
- > *IPSec is based on the authentication of computers on a network; therefore,*
- > *before a computer can send IPSec-protected data, it must be authenticated. The*
- > *Active Directory security domain provides this authentication using the Kerberos*
- > *protocol. Accordingly, when IKE uses Kerberos to authenticate, the Kerberos*
- > *protocol and other dependent protocols (DNS, UDP LDAP and ICMP) are used for*
- > *communication with domain controllers. Additionally, Active Directory-based*
- > *IPSec policy settings are typically applied to domain members through Group*
- > *Policy. As a result, if IPSec is required from domain members to the domain*
- > *controllers, authentication traffic will be blocked and IPSec communications*
- > *will fail. In addition, no other authenticated connections can be made using*
- > *other protocols, and no IPSec other policy settings can be applied to that*
- > *domain member through Group Policy. \*\*For these reasons, using IPSec for*
- > *communications between domain members and domain controllers is not supported\*\**
- >
- >
- > *"new question" <[newquestion\\_at\\_discussions.microsoft.com](mailto:newquestion_at_discussions.microsoft.com)> wrote in message*
- > *news:448147CF-76FE-4C37-8853-F68C60F330FD@microsoft.com...*
- > > *hi*
- > > *I experienced a problem when I deployed default secure server ipsec policy to*
- > *all my domain. Some clients didnt join after restart. We wait for very long*
- > *time. We logged local machine. And edit local policy .Assigned secure server to*

microsoft.public.win2000.security: Re: secure server policy

- > *local. And then machine restarted. Client machine logged successfull.*
- > > *I want to learn that we cant apply secure server policy to all domain ?*
- >
- >
- >