It was done before I was aware of it. I am fine with 1, OK with 3, not looking at 2 at the moment. The last time this happened, it happened Saturday and Sunday. I don't expect it to recur during the week. That said, if you guys are nervous about 1, let's go with 3, but I'd prefer 1.

-----Original Message-----
From: [mailto:*******@ithaka.org]
Sent: Tuesday, October 12, 2010 11:56 AM
To: *******
Subject: Re: Restore MIT IP Addresses

As for blocking all of 18. instead of a more specific
18.55.5.0/24, was that your idea or ?

Do let me know if you have an opinion regarding 1 vs 2 vs 3.

On 10/12/10 11:47 AM, ******* wrote:
>
> [ http://
> 
> }

> commented on OPS-1845:
> -------------------------------
> 
> Given that  is disabled, and the MIT source address group is confining MIT to this disabled VIP, I suspect that MIT is receiving no DNS responses for www.jstor.org at all.
> 
> Enabling  would put other innocent victims onto the single princeton server as well, so that doesn't seem like a very good option.
> 
> I could do any of these things:
> 1. put all of MIT back into the main pool with everyone else.
> 2. confine MIT to Princeton with a more carefully thought out method that requires a lot more configuration.
> 3. change the-confined source pool to be only the narrow 18.55.5.0/24 instead of the broad 18.0.0.0/8 (meaning that only this narrow network won't get DNS response, instead of all of MIT getting no
response).
>
>
>
>
>> Restore MIT IP Addresses
>> ______________________
>>
>> Key: OPS-1845
>> URL: http://
>> Project: Operations
>> Issue Type: Task
>> Reporter:
>> Assignee:
>> Priority: Urgent
>>
>> is asking that the MIT range be restored. asked that we take a metered approach and ease them back in if we can. I realize the whole Class A range is blocked at the firewall, but if we could enable the IPs not involved in this latest incident (aka, leave the Class C range suspended) that would be ideal in my estimation. Please advise.
>
>