As for blocking all of 18. instead of a more specific 18.55.5., 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, [Author] wrote:

> [http://]

> [Author] commented on OPS-1845:

> Given that [Author] 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 [Author] 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 [Author]-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: [Redacted]
Assignee: [Redacted]
Priority: Urgent

[Redacted] is asking that the MIT range be restored. [Redacted] 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.

>