

RE: Basic Network Configuration

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-10/0303.html>

From: David Gillett (gillettdavid_at_fhda.edu)

Date: 10/15/03

To: "'Smith, KC'" <ksmith@systemsalliance.com>, <security-basics@securityfocus.com>
Date: Wed, 15 Oct 2003 10:23:23 -0700

One implements a DMZ in order to impose three sets of firewall rules:

- between the internet and the DMZ subnet
- between the internet and the trusted subnet
- between the DMZ subnet and the trusted subnet

Ignoring, for the moment, vulnerabilities in the firewall itself (more on that later), a single box with three interfaces is quite adequate to deliver this functionality at a quite reasonable cost.

If, instead, you use two boxes, your traffic between the internet and the trusted subnet incurs an extra router hop in each direction. Not a big deal, but performance purists tend to complain about firewall overheads already.

Two firewalls will not necessarily cost more than one, if you can get away with SOHO models that only have two interfaces instead of industrial-strength boxes which typically support three or more.

The usual justification for using two firewalls is that an attacker would have to get past both to get into the trusted network. You only really achieve this benefit if the boxes run different OS and firewall code, so that no single vulnerability works against both.

But if you use two boxes, then your rules that govern traffic between the internet and the trusted subnet may appear on either box -- are, in fact, the intersection of rules found on both boxes. Correctly managing such a split ruleset can be a challenge, even if both boxes use the same syntax and user interface -- which they won't, if they're distinct enough to cover against firewall vulnerabilities!

(A simple and fairly robust approach is to instantiate the full ruleset dictated by policy on both boxes.)

SecurityFocus BASICS: RE: Basic Network Configuration

Some organizations consider the additional security of using two firewalls to justify the additional cost. I suspect many then lose the addition by deploying two similar boxes because they trust them and already know how to manage them....

Others regard it as a win to get all the necessary functionality and good performance in a single inexpensive and easily-managed box.

Your choice will depend on the priorities of your organization.

David Gillett

> -----Original Message-----

> From: Smith, KC [mailto:ksmith@systemsalliance.com]

> Sent: October 14, 2003 09:40

> To: security-basics@securityfocus.com

> Subject: Basic Network Configuration

>

>

> All,

>

> Okay I know this is truly a basic question, but this is after

> all the "security-BASICS" list!

>

> Most LAN configs I've seen include two, separate pieces of

> hardware to define the DMZ. A firewall on the outside and

> another firewall or policy switch on the inside is usually

> how I've seen that handled.

>

> My new company uses 3 separate NICs in the same firewall.

> One for inbound, one for the LAN and one for the DMZ. Each

> has it's own address block.

>

> It seems like using the firewall to do this makes sense, but

> I'd appreciate some external confirmation on that.

>

> The second issue is this: is there a rule of thumb to

> determine what should and should not go in the DMZ vs. the

> LAN? It seems to me that anything that requires access from

> outside the network (Ex. DNS servers, Mail servers, demo

> servers, etc.) should go in the DMZ. True?

>

> Thanks in advance.

> KC Smith

>

>

>

>

>

>

>

FREE Whitepaper: Better Management for Network Security

Looking for a better way to manage your IP security?

Learn how Solsoft can help you:

- Ensure robust IP security through policy-based management
- Make firewall, VPN, and NAT rules interoperable across heterogeneous networks
- Quickly respond to network events from a central console

Download our FREE whitepaper at:

http://www.securityfocus.com/sponsor/Solsoft_security-basics_031015
