

## RE: Firewall and DMZ topology

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-06/0244.html>

---

**From:** Morgado Alain (*amorgado\_at\_AeroKool.com*)

**Date:** 06/11/03

To: security-basics@securityfocus.com

Date: Wed, 11 Jun 2003 10:54:34 -0400

What is a soho?

-----Original Message-----

From: Christopher Ingram [mailto:cmi@crystalsands.net]

Sent: Tuesday, June 10, 2003 3:01 PM

To: security-basics@securityfocus.com

Subject: Re: Firewall and DMZ topology

First I apologize if someone already followed up with the same answer I'm about to give. I've getting a ton of Out Of Office, unknown user, and account full messages since I first posted here and its made a mess of things on this end.

Also, when I say firewall, I mean Router + Firewall.

The point of a DMZ is to isolate it as much as possible from the rest of your network. Should whatever resides in it become compromised, the attacker cannot spread his influence across the network. Also, simply having the address of a public server of a company will make finding the address of the other hosts very simple. This can be quite cost prohibitive for smaller companies, but the larger a corporation is (in terms of its network) the more they can benefit from the 2 uplink setup. With all that said, the original question said SOHO, so I realize this would never be a real solution.

Keeping SOHO in mind, we can look at the rest of the options more carefully. If the DMZ resides between the public Internet and the internal network, compromising the DMZ will mean any traffic passing to and from the local network to the Internet is sniffable. If this is not an issue (No sensitive information at all will pass through here including e-mails with corporate secrets, and online shopping and banking (yes, even with SSL)) then that may work fine.

Assuming that this isn't acceptable, the inline method (every box has 2 NICs chained together) can be ruled out.

Should the DMZ be behind the LAN and not split off at the firewall, it

## SecurityFocus BASICS: RE: Firewall and DMZ topology

would have to be on the same NIC the LAN uses on the firewall. Splitting that one port among several clients in the LAN and the DMZ would require a switch or a hub, and that opens the door to sniffing as well. Only this time, all traffic on the LAN can be sniffed, not just Internet <-> LAN traffic.

The three NIC method (Internet -> Firewall -> LAN, DMZ) is decent and probably best situation if the implementing person/staff has the skill and time to devote to it. No offense, but this didn't appear to be the case. In the original question, this was ruled out due to costs.

Considering that the setup would only cost a few hundred dollars at most, it seems that the person/staff responsible for this does not have sufficient resources to properly implement and maintain this. This 3 NIC firewall would require constant maintenance because, as it will most likely run a full fledged OS, it is susceptible to attack, resulting in the scenario I described in the beginning of this post.

I recommended splitting the LAN and DMZ using a simple SOHO hardware router because a decent one can be found on eBay for around \$40. I know because I bought one 2 weeks ago. Considering how difficult it is to compromise one of those, it can serve the purpose of the 3 NIC firewall for a much lower cost.

On Monday, June 9, 2003, at 08:53 PM, Chris Berry wrote:

>> *From: Christopher Ingram <cmi@crystalsands.net>*  
>> *So, the below setup is not decent for a corporate LAN. Ideally, the*  
>> *DMZ should sit on a separate connection to the Internet from the rest*  
>> *of the network, using a different ISP and therefore, different IP*  
>> *block. This provides the most isolation.*  
>  
> *I'm afraid I don't see how that:*  
>  
> *internet --> Firewall --> Lan*  
>  
> *internet --> Firewall --> DMZ*  
>  
> *would be any more secure than this:*  
>  
> *internet --> Outer Firewall --> DMZ --> Inner Firewall --> LAN*  
>  
> *or this:*  
>  
> *internet --> Firewall --> LAN*  
> *--> DMZ*  
>  
> *which are the setups that I've seen. Can you give some*  
> *justification/explanation on why you think that would be better?*  
>  
> *Chris Berry*  
> *compjma@hotmail.com*

RE: Firewall and DMZ topology

SecurityFocus BASICS: RE: Firewall and DMZ topology

- > *Systems Administrator*
- > *JM Associates*
- >
- > *"All I want is a few minutes alone with the source code for the*
- > *universe and a quick recompile."*
- >
- >
- > 

---
- > *STOP MORE SPAM with the new MSN 8 and get 2 months FREE\**
- > <http://join.msn.com/?page=features/junkmail>
- >
- >
- >

- > 

---
- > *Evaluating SSL VPNs' Consider NEOTERIS, chosen as leader by top*
- > *analysts!*
- > *The Gartner Group just put Neoteris in the top of its Magic Quadrant,*
- > *while InStat has confirmed Neoteris as the leader in marketshare.*
- > *Find out why, and see how you can get plug-n-play secure remote*
- > *access in*
- > *about an hour, with no client, server changes, or ongoing maintenance.*
- > *Visit us at: <http://www.neoteris.com/promos/sf-6-9.htm>*
- >

>

Evaluating SSL VPNs' Consider NEOTERIS, chosen as leader by top analysts!  
The Gartner Group just put Neoteris in the top of its Magic Quadrant,  
while InStat has confirmed Neoteris as the leader in marketshare.

Find out why, and see how you can get plug-n-play secure remote access in  
about an hour, with no client, server changes, or ongoing maintenance.

Visit us at: <http://www.neoteris.com/promos/sf-6-9.htm>

Evaluating SSL VPNs' Consider NEOTERIS, chosen as leader by top analysts!  
The Gartner Group just put Neoteris in the top of its Magic Quadrant,  
while InStat has confirmed Neoteris as the leader in marketshare.

Find out why, and see how you can get plug-n-play secure remote access in  
about an hour, with no client, server changes, or ongoing maintenance.

Visit us at: <http://www.neoteris.com/promos/sf-6-9.htm>