

Ang: RE: Firewall and DMZ topology

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-06/0252.html>

marcus_at_knivsta.se

Date: 06/11/03

To: Morgado Alain <amorgado@AeroKool.com>

Date: Wed, 11 Jun 2003 17:28:58 +0200

Small Office / Home Office

--

Marcus Weman (marcus@knivsta.se)

Network Engineer

Knivsta Kommun, GAS-Ek/IT

Ängbyvägen 8, 741 75 Knivsta, SWEDEN

Direct: +46 18 347103, Mobile: +46 708 216594

Phone: +46 18 347000, Fax: +46 18 380712

<http://www.knivsta.se/>

Morgado Alain <amorgado@AeroKool.com>

2003-06-11 16:54

Till

security-basics@securityfocus.com

Kopia

Ärende

RE: Firewall and DMZ topology

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

SecurityFocus BASICS: Ang: RE: Firewall and DMZ topology

NICs chained together) can be ruled out.

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