

## Re: [Firewalls] Checkpoint FW-1 – Static NAT

*Source:* <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-10/6274.html>

---

*From:* me ([me@nottoday.org](mailto:me@nottoday.org))

*Date:* 08/03/02

From: me <[me@nottoday.org](mailto:me@nottoday.org)>

Date: Sat, 03 Aug 2002 02:34:15 GMT

you can do this with NG FP1 or FP2

There are 3 user defined services in FireWall-1 NG FP1 / FP2:

http\_mapped  
ftp\_mapped  
smtp\_mapped

These services perform port mapping. By editing the service, the destination port and IP address of a connection can be changed.

Create the following rules in the Policy Editor:

Rule #1

SOURCE: Any

DESTINATION: FW-1\_object

SERVICE: mapped service (ie. http\_mapped, ftp\_mapped, or smtp\_mapped)

ACTION: accept

Rule #2

SOURCE: Any

DESTINATION: internal Workstation object

SERVICE: actual service (ie. http, ftp, smtp)

ACTION: accept

Edit the properties of the "http\_mapped" service to point to the IP address of an internal http server using a private address. If port 8000 on the FireWall Module (gateway) is to be mapped to port 80 on the internal web server 10.9.8.7, proceed as follows:

On the Policy Editor

1. Select Manage > Services.
2. In the Services window, select http\_mapped.
3. Click Edit.
4. In the User Defined Service Properties window, click on Advanced in the General tab.
5. In the Advanced Other Service Properties window, change the

contents of the Match field from:

```
SRV_REDIRECT(8080,0.0.0.0,80)
```

to:

```
SRV_REDIRECT(8000,10.9.8.7,80)
```

After installing the new policy on the target Firewall Module, an http request may be sent whose destination address is port 8000 on the Firewall Module, and be transparently connected directly to the http server.

No NAT needs to be configured for this to work. The internal "mapped" host can be non-routable.

Note: There has to be at least one Network Address Translation (NAT) rule in the rulebase for this to work. However, the NAT rule does not necessarily have to apply to this connection.

To create a "mapped" service, create a new service of type "Other" in the following way:

On the Policy Editor

1. Select Manage > Services.
2. In the Services window, click the New button and select Other from the drop down list.
3. In the User Defined Service Properties window, configure the General tab fields as follows:

Name: mapped\_service

IP Protocol: 6

4. Click the Advanced button.
5. In the Advanced Other Service Properties window, configure the Match field with the following syntax:

Match: SRV\_REDIRECT(<incoming destination port>,<IP to forward to>,<new destination port>)

The following is an example configuration of the Match field:

```
Match: SRV_REDIRECT(8080,10.1.1.250,80)
```

The same technique works for SMTP and FTP, with the exception that FTP data connections of a redirected FTP request will not be implicitly allowed, and must be accepted explicitly by the Rule Base. In fact, the underlying macro SRV\_REDIRECT can be used in user-defined services to redirect any simple TCP service from the FireWall Module to an internal server running on any TCP port.

On Wed, 24 Jul 2002 16:17:51 GMT, "Bill Lavalette"

<[bill@cyberbase7.com](mailto:bill@cyberbase7.com)> wrote:

>Brandon –

>

>No... in order to use static Nat the ip can not be part of the hide Nat  
>pool. The best thing is if you could swing a few more real ips this will  
>solve a lot of problems for you. what you might want to do is add a  
>additional nic to the firewall and use that as a natted DMZ then you can  
>statically Nat your servers. also do not forget to add in the arp info for  
>routing.

>

>at the very least 1 more real IP for this third interface then you can map  
>your mail,web,ftp etc through this.

>

>Hope this helps

>

>Bill

>

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

>From: [firewalls-admin@section5.cyberbase7.com](mailto:firewalls-admin@section5.cyberbase7.com)

>[mailto:[firewalls-admin@section5.cyberbase7.com](mailto:firewalls-admin@section5.cyberbase7.com)]On Behalf Of Brandon

>Creekmore

>Sent: Wednesday, July 24, 2002 10:59 AM

>To: [firewalls@section5.cyberbase7.com](mailto:firewalls@section5.cyberbase7.com)

>Subject: [Firewalls] Checkpoint FW-1 – Static NAT

>

>

>I'm trying to setup a very common, and simple static NAT configuration with  
>Checkpoint FW-1, but I am having problems getting it to work.

>

>I have two interfaces on my firewall. One to the internet, and the other to  
>my internal LAN. I am doing basic NAT to allow my internal LAN to access  
>the internet.

>

>My firewall only has 1 public IP address to the internet due to IP  
>limitation, so would it still be possible to forward services from my  
>firewall to my internal mail, ftp, etc?? If so, can anyone point me to some  
>good documentation on the proper way to configure this, as I havent had much  
>luck. Thanks.

>

>–Brandon

>

>

>

>Firewalls mailing list

>[Firewalls@section5.cyberbase7.com](mailto:Firewalls@section5.cyberbase7.com)

><http://section5.cyberbase7.com/mailman/listinfo/firewalls>

---

• Next message: "ZAF 3.1.291 and VSDATA95 – Windows protection error"

comp.security.firewalls: Re: [Firewalls] Checkpoint FW-1 – Static NAT

- ***Previous message:*** : "Re: Linksys BEFSR41 to Netscreen VPN problem."
- ***In reply to:*** Bill Lavalette: "RE: [Firewalls] Checkpoint FW-1 – Static NAT"
- ***Next in thread:*** Alan Strassberg: "Re: Checkpoint FW-1 – Static NAT"
- ***Messages sorted by:*** [ date ] [ thread ] [ subject ] [ author ] [ attachment ]