WatchGuard

Configuration Example

Set Up a Public Web Server Behind a Firebox

Example configuration files created with *— WSM v11.10.1*

Revised *— 7/21/2015*

Use Case

In this configuration example, an organization wants to set up a public web server on a protected network behind the firewall. They want to direct incoming website traffic from the Internet to the private address of this web server. They also want local users on their own internal network to use the public URL to browse to this website.

> *This configuration example is provided as a guide. Additional configuration settings could be necessary, or more appropriate, for your network environment.*

Solution Overview

When a computer sends traffic over the Internet to a server or another computer, it uses an IP address to identify the server, and a TCP or UDP port number to identify the process on the server that receives the data. Port 80 is used for HTTP traffic.

Network Address Translation (NAT) refers to any of several forms of IP address and port translation. Static NAT, also known as port forwarding, is a port-to-host NAT. When a packet comes in to a port on a Firebox interface, a static NAT action can change the destination IP address to a different IP address and port behind the firewall. Static NAT also operates on traffic sent from networks that your Firebox protects.

This solution uses a static NAT action in an HTTP-proxy policy to forward incoming traffic on port 80 to the private IP address of the web server located behind the Firebox. This is transparent to the Internet user.

How It Works

The web server has a private IP address and is connected to a network behind an optional interface of the Firebox. In the public DNS record for this web server, the IP address associated with the web server is the external IP address of the Firebox.

The Firebox configuration includes an HTTP-proxy policy to handle all incoming port 80 traffic. The policy configuration contains a static NAT action that tells the device to forward all incoming port 80 traffic to the private IP address of the web server on the optional network.

When an Internet user browses to the URL of the web server, the traffic comes in to the external interface of the Firebox on port 80. The HTTP-proxy policy receives the traffic and uses the IP address specified in the static NAT action to forward that web traffic to the web server.

Requirements

A Firebox

This configuration example is for a Firebox that runs Fireware OS v11.7.2. In versions of Fireware XTM earlier than 11.4.x the static NAT configuration looks slightly different than what is shown here.

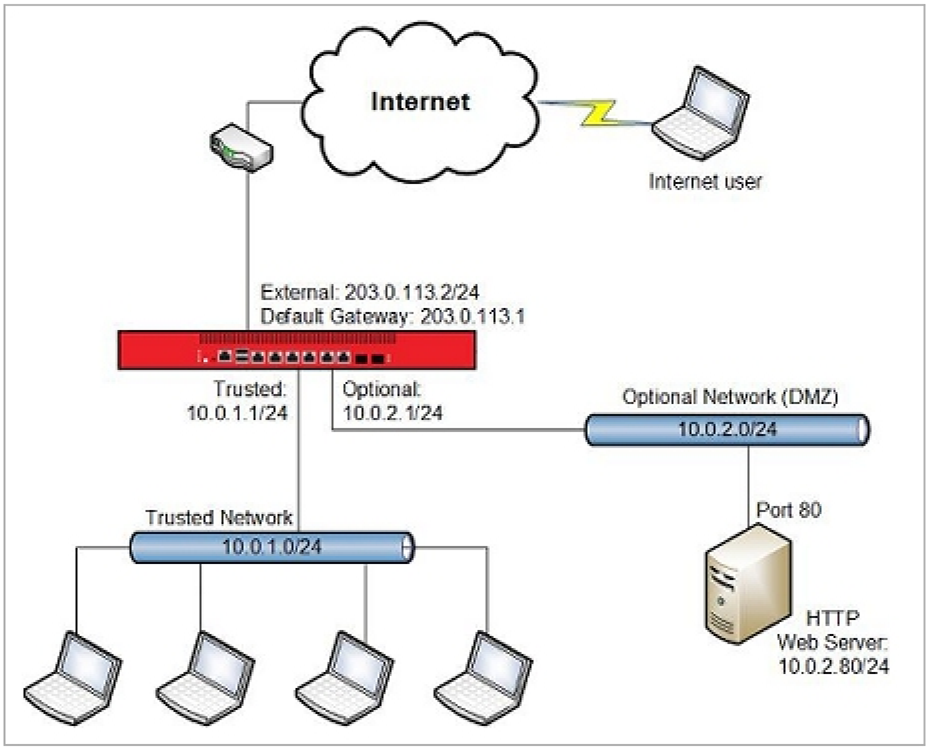
A web server

An HTTP server configured as a public web server with a private IP address.

We recommend that you do not connect publicly accessible servers, such as a web server, FTP server, or mail server, to the same network that connects to internal users or other non-public network resources. Because these servers are publicly accessible, they represent a potential vulnerability to your internal network. Instead, connect these publicly accessible servers to a separate network from your other internal network resources and users. In this example, the web server is part of a network connected to a Firebox configured as *Optional*, sometimes called the optional network.

Configuration Example

In this use case, the web server is located behind the Firebox on the optional network.



The Firebox and the web server use these IP addresses:

	Site A
External interface IP address	203.0.113.2/24
Default Gateway IP address	203.0.113.1
IP address of the Firebox interface connected to the trusted network	10.0.1.1/24
IP address of the Firebox interface connected to the optional network	10.0.2.1//24
IP address of the web server on the optional network	10.0.2.80/24

Example Configuration File

For your reference, we have included an example configuration file with this document. To examine the details of the example configuration file, you can open it with Policy Manager. The name of the configuration file is `snat_web_server.xml`.

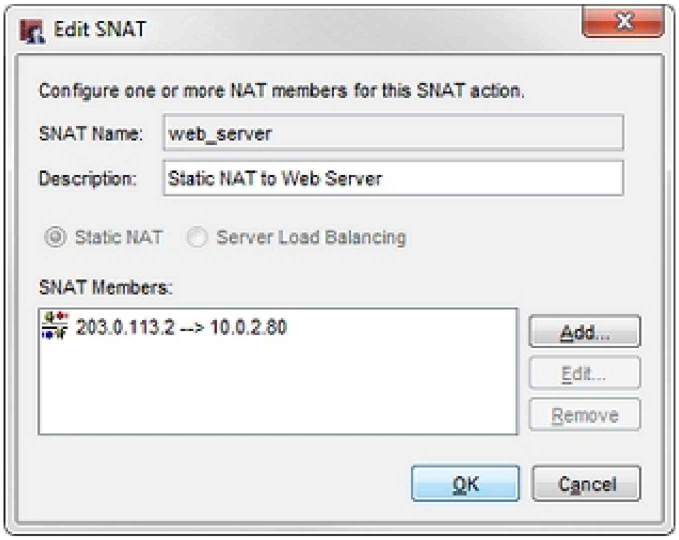
Configuration Explained

Static NAT Action

The example configuration file contains a static NAT action, also known as an SNAT action, to forward traffic from the public IP address of the Firebox external interface to the private IP address of the web server.

To see the static NAT action:

1. Start Policy Manager for the Firebox.
2. Select **Setup > Actions > SNAT**.
3. Open the **web_server** action.
   The Edit SNAT dialog box appears.



Configure one or more NAT members for this SNAT action.

SNAT Name: web_server

Description: Static NAT to Web Server

● Static NAT ○ Server Load Balancing

SNAT Members:

203.0.113.2 --> 10.0.2.80

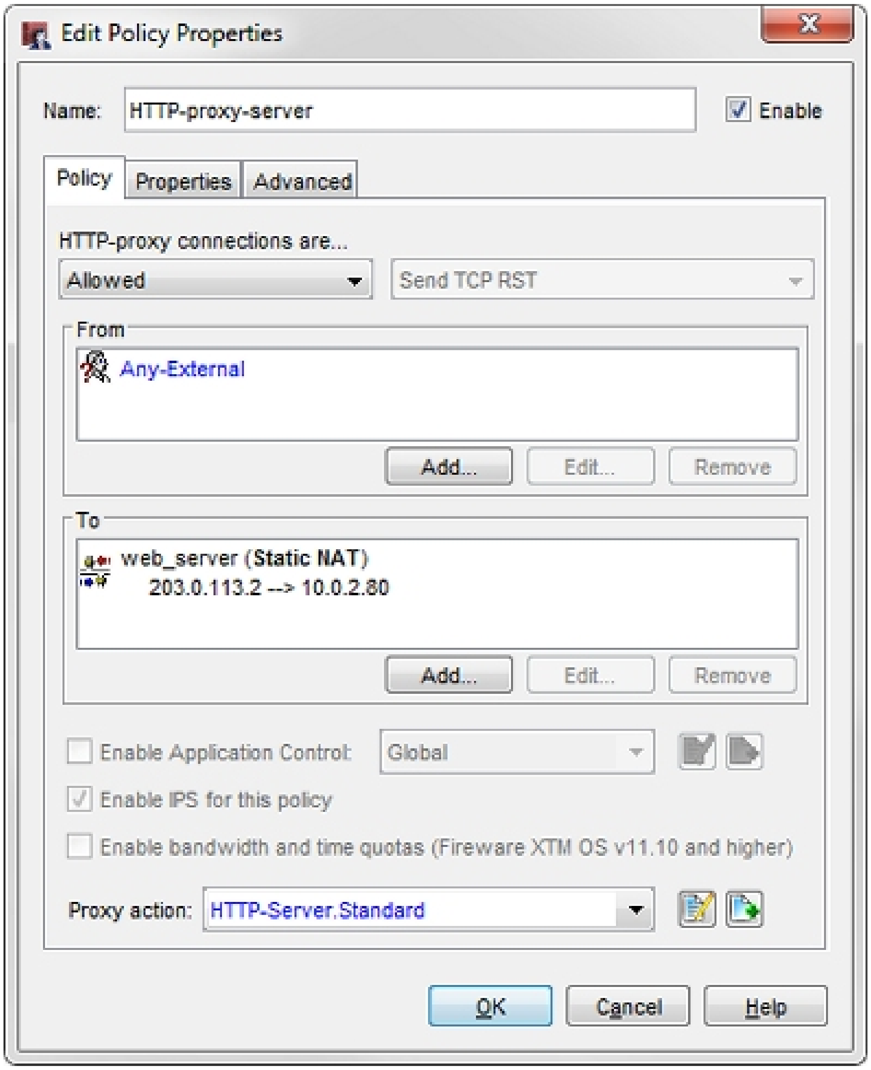
The static NAT action forwards packets addressed to the Firebox external interface IP address (203.0.113.2) to the private IP address of the web server (10.0.2.80). You can also see and edit this static NAT action from within policies where it is used.

HTTP-Proxy Policy for Incoming Traffic to the Web Server

By default, the Firebox does not allow incoming traffic from the external interface to the trusted or optional networks. To allow the traffic to your web server, you must add either an HTTP packet filter or HTTP-proxy policy . We recommend you use the HTTP-proxy policy because it monitors the commands used in the connection to make sure they are in the correct syntax and order, and uses deep packet inspection to help protect your HTTP server from attacks. For each proxy policy, you assign a proxy action that contains rules about what kind of content to allow. The rules in the HTTP-Server proxy action are good defaults for traffic to an internal web server.

To see the HTTP-proxy policy:

1. Open the example configuration file in Policy Manager.
2. Double-click the **HTTP-proxy-server** policy to open it.



Name: HTTP-proxy-server ☑ Enable

HTTP-proxy connections are... Allowed | Send TCP RST

From
Any-External

To
web_server (Static NAT)
203.0.113.2 --> 10.0.2.80

□ Enable Application Control: Global

☑ Enable IPS for this policy

□ Enable bandwidth and time quotas (Fireware XTM OS v11.10 and higher)

Proxy action: HTTP-Server.Standard

Make sure you understand these settings:

From

The **From** section contains the **Any-External** alias, because this policy handles traffic that comes in to the web server from the external interface.

To

The **To** section contains the static NAT action that forwards packets addressed to the Firebox external interface IP address (203.0.113.2) to the private IP address of the web server (10.0.2.80).

Proxy action

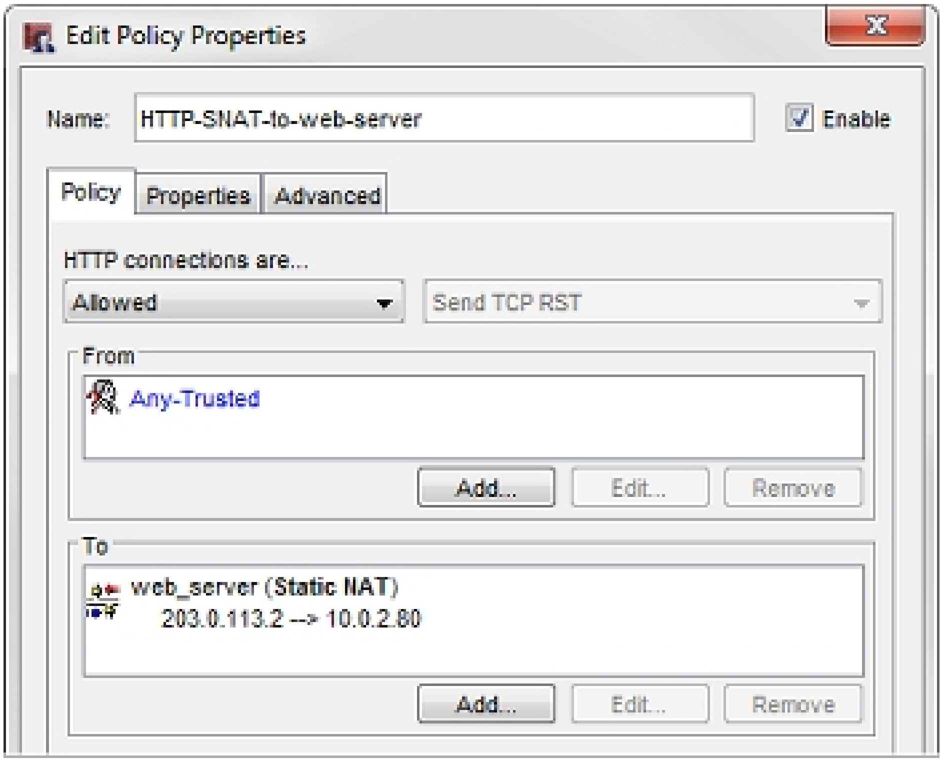
The **Proxy action** is set to **HTTP-Server.Standard**. The default settings in the HTTP-server proxy action are the recommended default settings for traffic to a web server.

HTTP Policy to Allow Internal Users to Use the Public Web Server URL

The example configuration contains an HTTP policy to allow the internal users to browse to the web server by its public domain name, such as www.example.com. The HTTP policy handles traffic from the trusted network to the local web server. This policy includes the same static NAT action as in the HTTP-proxy-server policy. Because this policy handles only internal traffic, there is no need for deep packet inspection, so we use the HTTP packet filter policy instead of the HTTP-Proxy policy.

To see the HTTP NAT policy for this example:

1. Open the example configuration file in Policy Manager.
2. Double-click the **HTTP-SNAT-to-web-server** policy to open it.



Edit Policy Properties

Name: HTTP-SNAT-to-web-server ☑ Enable

HTTP connections are... Allowed

From: Any-Trusted

To: web_server (Static NAT)
203.0.113.2 --> 10.0.2.80

This policy includes:

From

The **From** section of the policy allows traffic from **Any-Trusted**.

To

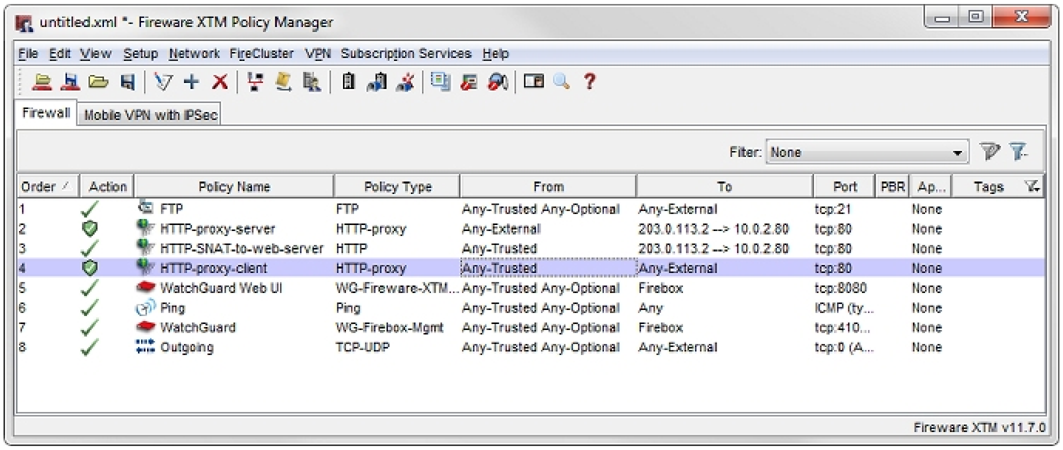
The **To** section contains the same static NAT action to forward packets addressed to the Firebox external interface IP address (203.0.113.2) to the private IP address of the web server (10.0.2.80).

This policy uses the static NAT action for traffic from users on the trusted network.

> *If the network has a local DNS server with a split DNS configuration, you can add a DNS record to the internal zone to map the public domain name of the web server to its private IP address. If you do this, the HTTP policy with the SNAT action is not necessary.*

HTTP-Proxy Policy for Outbound Web Requests

The example configuration file also includes an HTTP-proxy policy to control outbound web server access. This is not related to configuration of the web server on the optional network, but is a policy you would typically use to apply HTTP-proxy settings to outbound HTTP access for users on the trusted network. This policy allows HTTP traffic from Any-Trusted to Any-External. In the example configuration file, that policy is named **HTTP-proxy-client**.


untitled.xml *- Fireware XTM Policy Manager
File Edit View Setup Network FireCluster VPN Subscription Services Help
Firewall
Mobile VPN with IPSec

Filter: None

Order	Action	Policy Name	Policy Type	From	To	Port	PBR	Ap...	Tags
1	✓	FTP	FTP	Any-Trusted Any-Optional	Any-External	tcp:21		None	
2	🛡	HTTP-proxy-server	HTTP-proxy	Any-External	203.0.113.2 --> 10.0.2.80	tcp:80		None	
3	✓	HTTP-SNAT-to-web-server	HTTP	Any-Trusted	203.0.113.2 --> 10.0.2.80	tcp:80		None	
4	🛡	HTTP-proxy-client	HTTP-proxy	Any-Trusted	Any-External	tcp:80		None	
5	✓	WatchGuard Web UI	WG-Fireware-XTM...	Any-Trusted Any-Optional	Firebox	tcp:8080		None	
6	✓	Ping	Ping	Any-Trusted Any-Optional	Any	ICMP (ty...		None	
7	✓	WatchGuard	WG-Firebox-Mgmt	Any-Trusted Any-Optional	Firebox	tcp:410...		None	
8	✓	Outgoing	TCP-UDP	Any-Trusted Any-Optional	Any-External	tcp:0 (A...		None	

Fireware XTM v11.7.0

Conclusion

In this configuration example, the Internet user browses to 203.0.113.2, or to a URL that resolves to that IP address. The traffic enters the Firebox external interface on port 80. The HTTP-proxy-server policy inspects the incoming traffic on the external interface and forwards that traffic to the HTTP server on the private network address, 10.0.2.80. Responses from the web server appear to the Internet user to come from IP address 203.0.113.2.

This configuration example demonstrates how to use static NAT to send web traffic to an HTTP server on a protected network. You can also use static NAT in other policies to redirect incoming traffic to other internal servers, such as an FTP server or an SMTP email server.

For more information about static NAT, see the *Fireware Help*.

About this Configuration Example

This configuration example is provided as a guide. Additional configuration settings could be necessary, or more appropriate, for your network environment.

For complete product documentation, see the *Fireware Help* on the WatchGuard website at: http://www.watchguard.com/help/documentation/.

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Copyright, Trademark, and Patent Information

About WatchGuard

WatchGuard offers affordable, all-in-one network and content security solutions that provide defense-in-depth and help meet regulatory compliance requirements. The WatchGuard Firebox line combines firewall, VPN, GAV, IPS, spam blocking and URL filtering to protect your network from spam, viruses, malware, and intrusions. The XCS line offers email and web content security combined with data loss prevention. WatchGuard extensible solutions scale to offer right-sized security ranging from small businesses to enterprises with 10,000+ employees. WatchGuard builds simple, reliable, and robust security appliances featuring fast implementation and comprehensive management and reporting tools. Enterprises throughout the world rely on our signature red boxes to maximize security without sacrificing efficiency and productivity.

For more information, please call 206.613.6600 or visit www.watchguard.com.

Address

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

Support

www.watchguard.com/support
U.S. and Canada +877.232.3531
All Other Countries +1.206.521.3575

Sales

U.S. and Canada +1.800.734.9905
All Other Countries +1.206.613.0895