Integration Guide

Office 365

Revised: 21 January 2016

About This Guide

Guide Type

Documented Integration —WatchGuard or a Technology Partner has provided documentation demonstrating integration

Guide Details

WatchGuard provides integration instructions to help our customers configure WatchGuard products to work with products created by other organizations. If you need more information or technical support about how to configure a third-party product, see the documentation and support resources for that product.

Office 365 Integration Overview

Many organizations are moving their core email infrastructure to cloud-based email services such as Office 365 / Exchange Online. To maintain control and security of your cloud-based email communications, we recommend you route your email connections through your Firebox SMTP-proxy before they connect to cloud services. This integration is limited to SMTP connections only. Email retrieved through POP-3 clients will be secured in a future release of Fireware OS.

Platform and Software

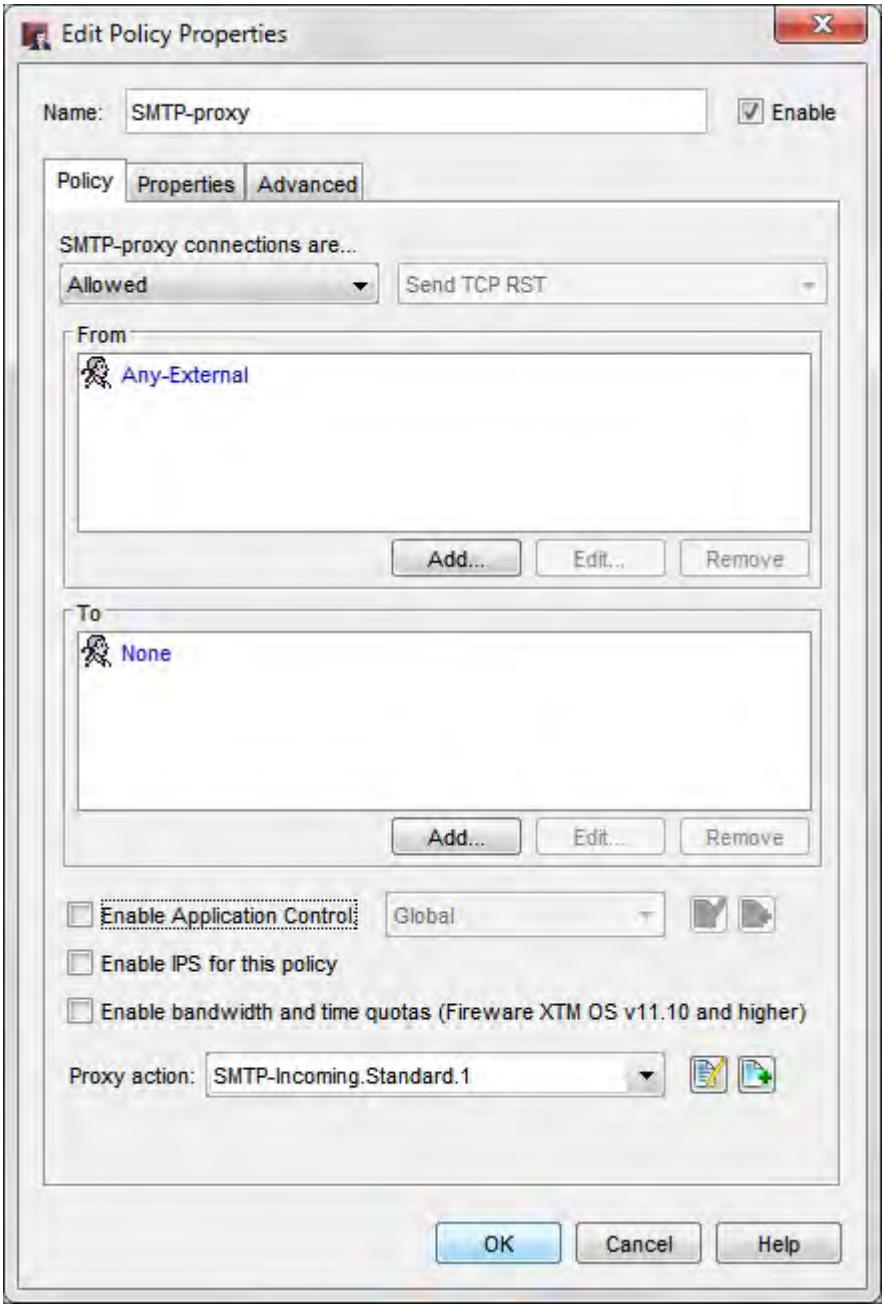
The hardware and software used to complete the steps outlined in this document include:

- Firebox or WatchGuard XTM device installed with Fireware v11.10.2 Update 1 or higher
- Office 365 in the cloud

Configuration

To secure your cloud-based email communications, you must use an SMTP-proxy policy in your Firebox configuration.

1. Connect to your Firebox and open Policy Manager.
2. Add an incoming SMTP-proxy policy.

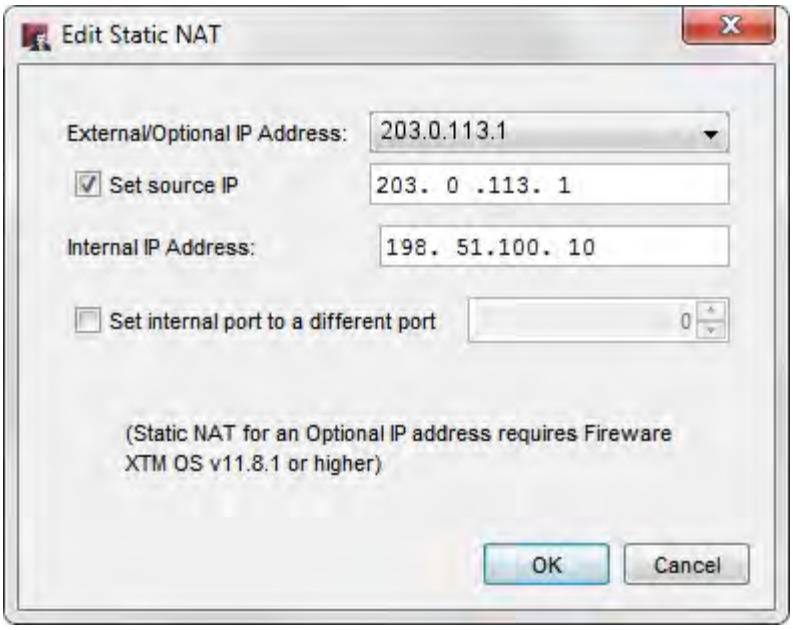


3. In the **From:** field of your policy, select **Any-External**.
4. In the **To:** field of your policy, add an **SNAT** entry.
5. In the **Set source IP** field, configure the source IP address as the external IP address of your Firebox. The responses from the cloud-based email server will be sent to this address and not the client that initiated the request.
6. In the **Internal IP Address** text box, type the IP address of your cloud-based email server.

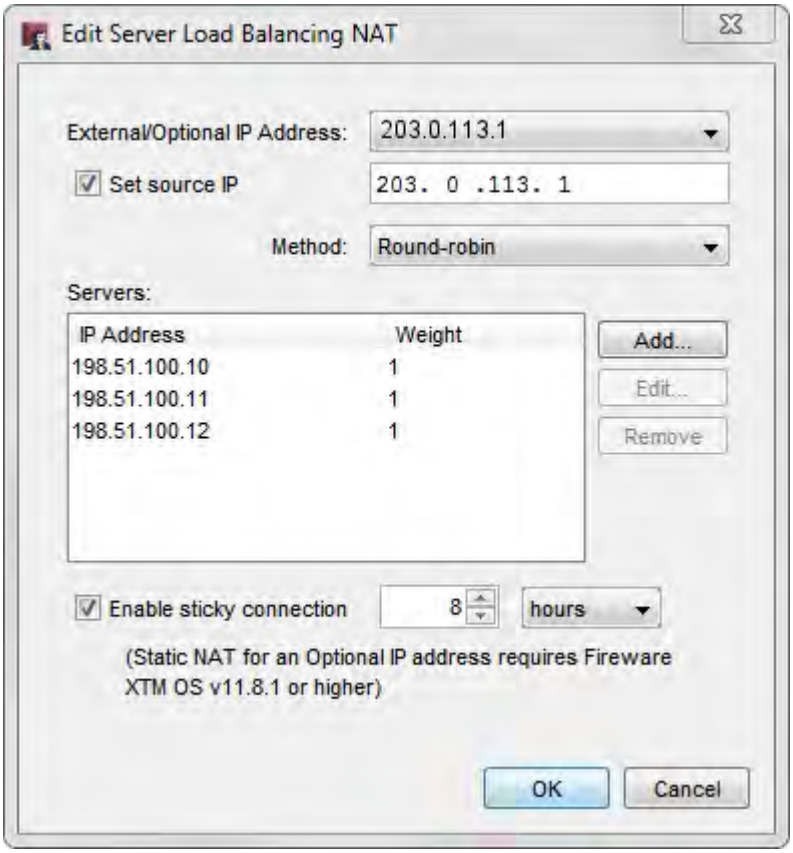
If your cloud-based email server uses multiple IP addresses, you can create an SNAT rule for each address if you have enough external IP addresses available on your Firebox to support this configuration.

If you have only one external IP address, you can apply a server load balancing configuration through SNAT and add the IP addresses of the cloud-based email server.

Note: Mail will not be delivered if your provider changes the IP address of the cloud-based email server.



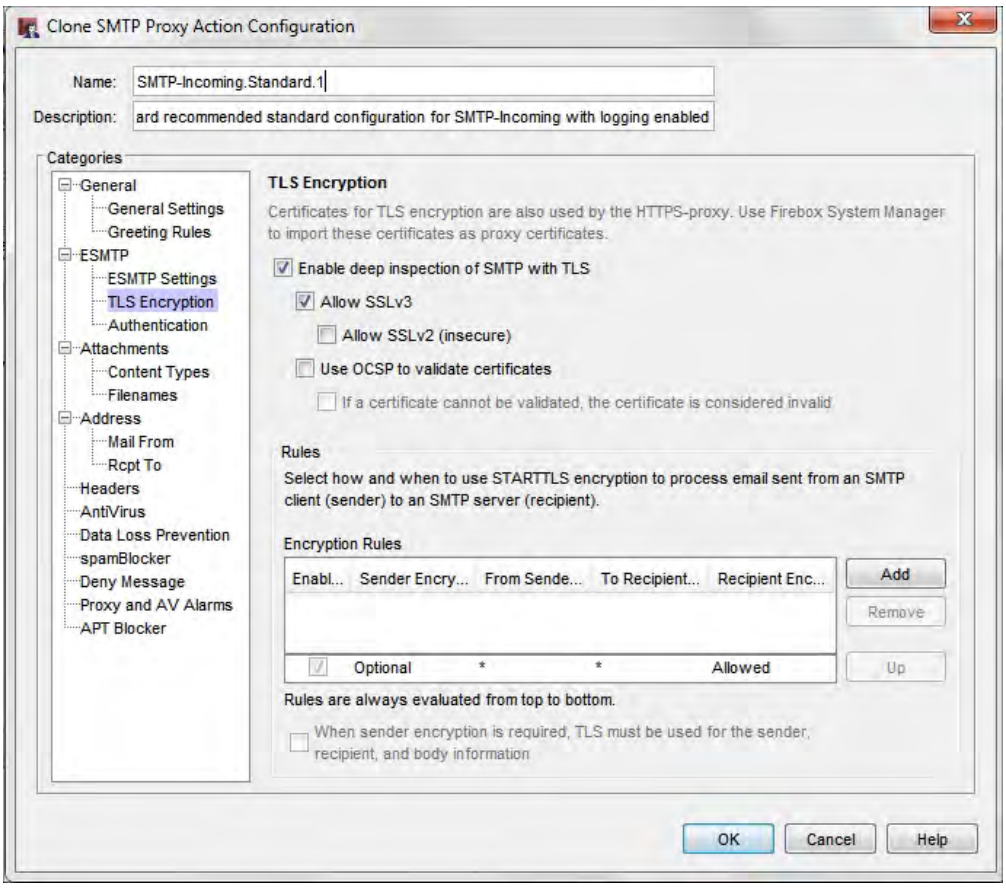
Single IP address in an SNAT rule



Multiple IP addresses in a Server Load Balancing NAT configuration

After you apply this configuration, you can configure your proxy security settings for email services, including spamBlocker, Gateway Anti-Virus, and APT Blocker.

To make full use of this configuration, you must enable deep inspection of SMTP traffic because communications will primarily be sent using TLS over SMTP. In some cases, you may have to enable SSLv3 for compatibility with older mail servers.


Clone SMTP Proxy Action Configuration
Name: SMTP-Incoming.Standard.1
Description: ard recommended standard configuration for SMTP-Incoming with logging enabled
Categories
General
General Settings
Greeting Rules
ESMTP
ESMTP Settings
TLS Encryption
Authentication
Attachments
Content Types
Filenames
Address
Mail From
Rcpt To
Headers
AntiVirus
Data Loss Prevention
spamBlocker
Deny Message
Proxy and AV Alarms
APT Blocker
TLS Encryption
Certificates for TLS encryption are also used by the HTTPS-proxy. Use Firebox System Manager to import these certificates as proxy certificates.
Enable deep inspection of SMTP with TLS
Allow SSLv3
Allow SSLv2 (insecure)
Use OCSP to validate certificates
If a certificate cannot be validated, the certificate is considered invalid
Rules
Select how and when to use STARTTLS encryption to process email sent from an SMTP client (sender) to an SMTP server (recipient).
Encryption Rules
Enabl... Sender Encry... From Sende... To Recipient... Recipient Enc...
Optional * * Allowed
Add
Remove
Up
Rules are always evaluated from top to bottom.
When sender encryption is required, TLS must be used for the sender, recipient, and body information
OK
Cancel
Help