Administrator Guide

Firewall Rules for Monitoring Point Deployment

Last updated: September 7, 2018

Prepared by: Mike Marzec (mmarzec@appneta.com),

AppNeta Technical Account Manager

2 Copley Place, Boston, MA | 800-890-1553 | www.fuze.com

Introduction

This document provides details about firewall rules for monitoring point deployment.

Table of contents

Executive Summary

In order for your monitoring point to access APM and perform the monitoring you require, you must configure your firewall rules to allow this access. At a minimum, the monitoring point must be able to connect to the APM servers. Additional configuration beyond this is based on your monitoring needs.

Links

A few reference links to AppNeta documentation are listed here, as they augment the content described in this document: AppNeta APM documentation regarding tests or diagnostics that can be executed from the MP.

Delivery diagnostics - diagnostic tests

Voice tests / assessments - voice delivery

Video tests - video delivery

Firewall Configuration

Typical nis.config

NIS Address: fuze.pm.appneta.com

NIS Ports: 80,8080

NIS Protocol: TCP

SSL: true

Site Key: <various>

Connection Relay Addresses: pvc-scr-1.pathviewcloud.com:443

Server IPs

The Fuze or Fuze's client monitoring points need to be allowed to connect to the following servers, with the listed associated IPs:

Upgrade server -- appliance-repo.pm.appneta.com : 13.32.205.172, 13.32.205.211, 13.32.205.53, 13.32.205.173

NIS or Primary Server -- fuze.pm.appneta.com : 23.21.57.177

Capture Server -- cap-07.pm.appneta.com : 54.83.35.39

APM Servers

All APM servers

Outbound	TCP	80, 8080, 443	fuze.pm.appneta.com

Connect to all APM servers. This rule can be substituted for all the rules in this table.

Assigned server

Outbound	TCP	80, 8080	fuze.pm.appneta.com

A monitoring point attempts to connect to APM on port 80, then on port 8080. Whether you are connecting directly or through a proxy, you must allow outbound TCP connections to your assigned server on one or both of these ports. To determine the URL of your assigned APM server, Log in to APM. The server URL is in the browser address bar.

Relay server

Outbound	TCP	443	mp-relay.pm.appneta.com

A monitoring point first tries to connect to your assigned APM server on port 80, then on port 8080. If it cannot (for example, when your security policy disallows HTTPS) the monitoring point attempts to connect to APM via an SSL relay server. In this case, you must allow outbound TCP connections on port 443 to this server.

Capture server

Outbound	TCP	443	cap-07.pm.appneta.com, pvc-cap7.pathviewcloud.com

Capture servers receive Usage monitoring records and packet captures, and provide a reverse proxy for SSL connections from the APM server to monitoring points. You must allow outbound TCP connections on port 443 to all of these servers.

Upgrade repository

Outbound	TCP	80	appliance-repo.pm.appneta.com

You must allow outbound TCP connections on port 80 to this server so that your monitoring point can download new software versions.

Outbound	TCP	80, 443	mp-repo-proxy.pm.appneta.com

You must allow outbound TCP connections on port 80 and 443 to this server so that your monitoring point can download new software versions.

Outbound	TCP	80, 443	s3.amazonaws.com

(Optional) You may allow outbound TCP connections on port 80 and 443 to this server in case the monitoring point is ever unable to connect to mp-repo-proxy.pm.appneta.com.

Proxy server

Outbound	e.g., permit tcp host device-ip host proxy-ip eq proxy-port

If HTTP traffic is directed to a proxy server, make sure that no ACLs prevent the monitoring point from connecting to it. This might be the case if the monitoring point is deployed in a subnet reserved for network infrastructure rather than end-stations. If the proxy service requires authentication, it must use either basic or digest authentication; NTLM and Kerberos are not supported. See the proxy setup page: physical and virtual monitoring points or software monitoring points (software sequencers).

NTP server

Inbound + Outbound UDP 123 Addresses for all NTP servers you want to access.

The monitoring point needs a inbound and outbound connections for NTP to ensure precise timestamping.

DNS server

Outbound UDP 53 All addresses

DNS is required for hostname to IP resolution.

Web Admin

Outbound TCP 443 cap-07.pm.appneta.com, pvc-cap7.pathviewcloud.com

When you access Web Admin via the Manage Monitoring Points page, a capture server provides a reverse proxy so that your connection remains secure.

Delivery monitoring

Outbound TCP 443 All Addresses

Allow TCP 443 so that the monitoring point can perform TCP traceroute on single- and dual-ended paths.

Inbound + Outbound ICMP Message types used: Echo Request, Echo Reply, Time Exceeded, and Destination Unreachable

ICMP is used for Delivery monitoring on single- and dual-ended paths, so it is essential that these messages are allowed.

Inbound + Outbound UDP 3239 All Addresses

Allow UDP 3239 inbound so that monitoring points can coordinate dual-ended monitoring. Allow UDP 3239 outbound so that monitoring points can coordinate dual-ended monitoring and perform

UDP traceroute.

Inbound + Outbound UDP 45056-49151 All Addresses

Allow inbound and outbound UDP messages on this range so that monitoring points can perform single- and dual-ended monitoring, continuous monitoring traceroute using the port-unreachable method, voice tests, and QoS alerting. You can also customize this range.

Outbound UDP 49152-65535 All Addresses

APM sends UDP packets to ports in the stated range as part of QoS diagnostics, path MTU determination, and network discovery. ICMP port-unreachable messages are expected in response. Keep in mind that path targets must actually respond with an ICMP port-unreachable for any of these processes to be successful.

Outbound UDP 161 All Addresses

Allow outbound UDP messages on port 161 so that monitoring points can query network devices via SNMP.

Path Plus

Outbound ICMP Message types used: Echo Request, Echo Reply.

ICMP is used for pings in Path Plus.

Outbound UDP 7 All Addresses

UDP port 7 is used for traceroute in Path Plus.

Outbound TCP 53 All Addresses

TCP and UDP messages on port 53 are used for nslookup in Path Plus.

Outbound UDP 53

Outbound TCP 3236 All Addresses

Allow outbound TCP and UDP messages on port 3236 so that PathTests can target monitoring points. The source and target monitoring points coordinate on TCP 3236 before and after tests, so it must be opened even if the testing protocol is UDP.

Outbound UDP 3236

Voice/Video

Inbound + Outbound UDP 3239 All Addresses

Monitoring points coordinate over UDP 3239 for voice and video tests. Allow outbound access for source monitoring points and inbound access for target monitoring points.

Inbound + Outbound UDP 5060 All Addresses

Video and voice tests can use one of two signaling protocols: SIP uses port 5060, and H.323 uses port 1720. If you need to use different ports for signaling, open a support ticket.

Inbound+ Outbound UDP 1720

Inbound + Outbound UDP 45056-49151 All Addresses

For video and voice tests, RTP and RTCP automatically select ports between 45056-49151.

Experience monitoring

Outbound TCP 80, 443 All Addresses

Outbound TCP connections on port 80 are essential to Experience monitoring. Allow outbound connections on port 443 if a workflow includes logging in to the target site.

SNMP

Outbound UDP 162 All Addresses

(Optional) You may allow outbound UDP messages on port 162 so that monitoring points can send SNMP notifications.

Fuze, Inc

2 Copley Place, Suite 7000

Boston MA 02116

800.890.1553