FortiNAC

Control Manager Proxy

Version: 9.1, 9.2, 9.4

Date: December 6, 2023

Rev: D

FORTINET DOCUMENT LIBRARY
http://docs.fortinet.com

FORTINET VIDEO GUIDE
http://video.fortinet.com

FORTINET KNOWLEDGE BASE
http://kb.fortinet.com

FORTINET BLOG
http://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
http://support.fortinet.com

FORTINET COOKBOOK
http://cookbook.fortinet.com

NSE INSTITUTE
http://training.fortinet.com

FORTIGUARD CENTER
http://fortiguard.com

FORTICAST
http://forticast.fortinet.com

END USER LICENSE AGREEMENT
http://www.fortinet.com/doc/legal/EULA.pdf

Contents

Overview

Some large enterprises do not allow individual FortiNAC appliances internet access. This prohibits weekly OS and antivirus updates to this CA appliance. However, they do allow the Control Manager internet access.

This document provides guidance on configuring FortiNAC appliances to download any or all of the following from the Control Manager:

- Auto-Definitions
- Software updates
- Agent packages
- CentOS updates
- License Entitlements and IoT data collection

This configuration minimizes internet access of the managed FortiNAC appliances.

Procedure Overview

1. Configure Control Manager: Configure the Control Manager to download the appropriate updates and proxy using squid service.
2. Configure Managed FortiNAC Servers: Configure to download updates from Control Manager.

Requirements

- FortiNAC 8.8.3 or higher
- CentOS based appliances (not supported on appliances running FortiNAC-OS)
- Appliances are managed by a Control Manager
- Control Manager has internet access

Procedure

Configure Control Manager

Squid Service

Configure the squid service on the Control Manager. This enables the Control Manager to proxy to the PODs.

1. Login to the Control Manager CLI as root.
2. Type

   yum update

   yum --enablerepo=base,updates install squid

3. Edit **/etc/squid/squid.conf**
4. Add ACL for the Control Manager's local subnet.

   acl localnet src <subnet>/<mask>

   Example:

   ```
   acl localnet src 192.168.0.0/16
   ```

5. Enable squid service.

   systemctl enable squid
6. Start squid.

   systemctl restart squid
7. Confirm squid is running.

   systemctl status squid

   Example output:

   ```
   squid.service - Squid caching proxy
      Loaded: loaded (/usr/lib/systemd/system/squid.service; enabled;
      vendor preset: disabled)
      Active: active (running) since Thu 2018-09-20 10:07:23 UTC; 5min ago
    Main PID: 2005 (squid)
      CGroup: /system.slice/squid.service
              ├─2005 /usr/sbin/squid -f /etc/squid/squid.conf
              ├─2007 (squid-1) -f /etc/squid/squid.conf
                 └─2008 (logfile-daemon) /var/log/squid/access.log
   ```

8. Verify the port squid is using.

   netstat -tulnp | grep squid
9. Note this port value as it will be used when configuring the FortiNAC servers.

System Updates

Configure the Control Manager to download the Auto-Definitions, software updates and agent packages from the download site.

1. Login to Control Manager Administration UI.
2. Navigate to **System > Settings > Updates > System**
3. Configure to download updates from **fnac-updates.fortinet.net**
4. Configure other parameters as desired. For options see section System update in the Administration Guide.
5. Navigate to **System > Scheduler**
6. Modify the time and frequency the Auto-Definition Update scheduled task is run.

   Important: This task must run before the scheduled updates for the managed appliances. Otherwise, the PODs will be a week behind in updates. For modification instructions, see section Modify a task in the Administration Guide.

Configure Managed FortiNAC Servers

The following must be done on all FortiNAC servers managed by the Control Manager.

System Updates

Configure FortiNAC server to download Auto-Definitions, software updates and agent packages from the Control Manager:

1. Login to the managed FortiNAC server Administration UI.
2. Navigate to **System > Settings > Updates > System**
3. Configure to download updates from Control Manager using the table below.

Host	Control Manager IP address
Auto-Definition Directory	/bsc/campusMgrUpdates
Product Distribution Directory	/bsc/campusMgrUpdates
Agent Distribution Directory	/bsc/campusMgr/agent/packages
User	Control Manager CLI user (admin or root)
Password	Control Manager CLI password
Protocol	SFTP

4. Click **Test** to check that the settings allow connection to the Control Manager.
5. Click **Save Settings**.
6. Navigate to **System > Scheduler**
7. Modify the time and frequency the Auto-Definition Update scheduled task is run.

   Important: This task must run after the Control Manager Auto-Definitions Updates. Otherwise, the PODs will be a week behind in updates. For modification instructions, see the following Administration Guide section (right click and open in new tab): Modify a task.

Enable Proxy Function

Enable proxy function, specifying the squid service port. The License Entitlements, IoT data collection and the updates configured for /bsc/campusMgrUpdates in the previous step will start using the proxy.

1. Navigate to **System > Settings > System Communication > Proxy Settings**
2. Click **Enable Proxy Configuration**.
3. Under the **HTTP Proxy** section, configure the following:
   - **Host**: The hostname or address of the Control Manager
   - **Port**: <squid service port>
   - **Authentication**: Disabled
4. Click **Save Settings**.

   For details on fields in this view, see the following Administration Guide section (right click and open in new tab): Proxy settings.

Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.