

Application Note

Trend Micro Policy Based Host Check

Denzil Wessels
Technical Marketing Engineer



Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
408 745 2000 or 888 JUNIPER
www.juniper.net

Part Number: 350031-001

Contents

| | |
|--|---|
| Contents | 2 |
| Executive Summary | 4 |
| Trend Micro Office Scan Version Check..... | 5 |
| Trend Micro OfficeScan Realtime Scan | 6 |
| Host Checker Policies Applied to Authentication Realm..... | 7 |

Executive Summary

Host Checker can be configured using Policy Based host checks to require that Trend Micro OfficeScan is running and up to date before allowing a user to connect to the IVE.

This can be done with two checks.

1. Check to see if the software and signatures are up to date.
2. Check to see if the real time scan option is enabled and the process is running.

Trend Micro Office Scan Version Check

This policy verifies that OfficeScan is up to date with the version specified by the administrator. This includes checking for the virus pattern version, and the scanning engine version.

Pattern Version Check

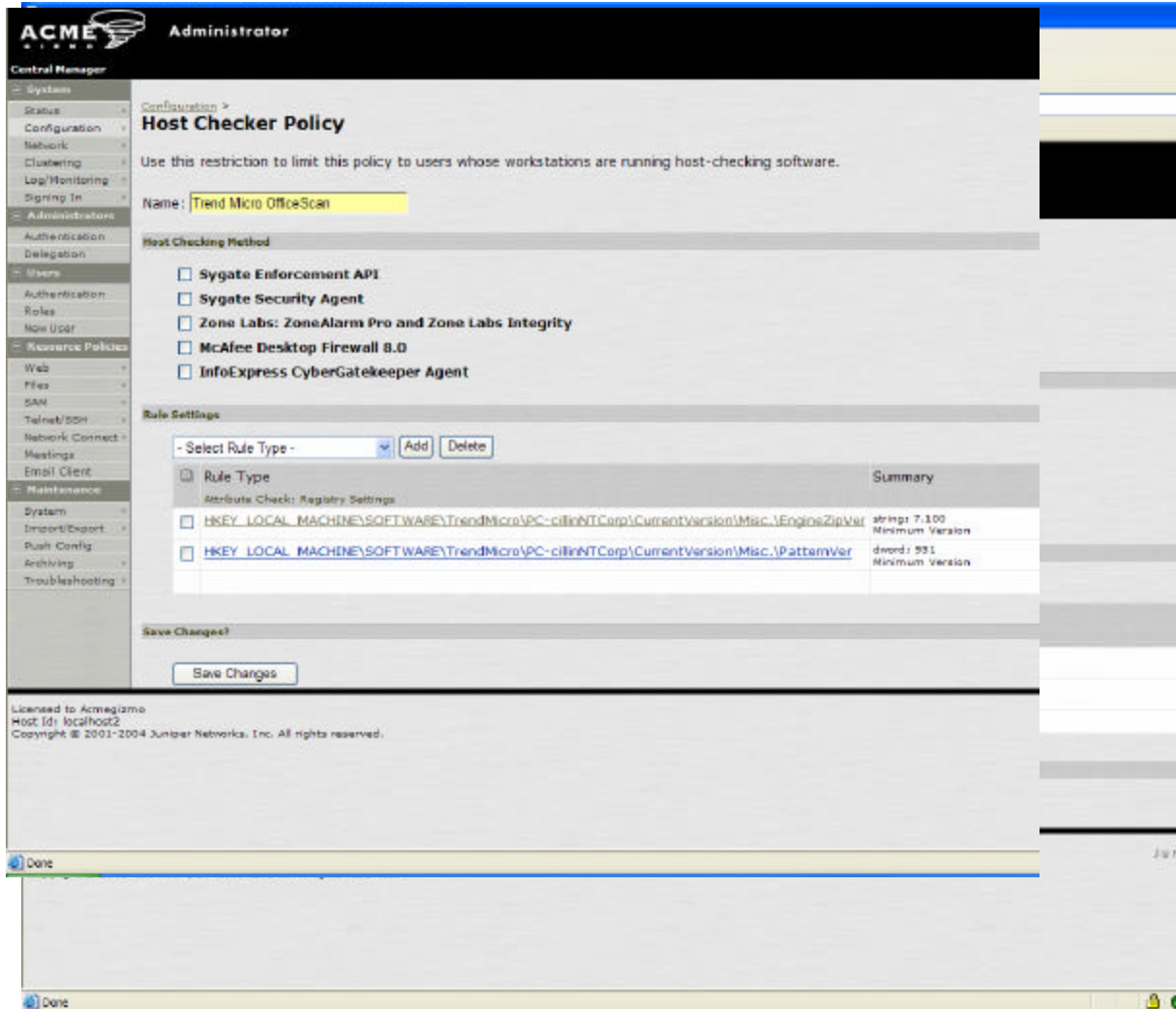
Attribute Check: Registry Settings

HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc.\PatternVer dword; 951

Engine Version Check

Attribute Check: Registry Settings

HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc.\EngineZipVer string; 7.100



The screenshot shows the ACME Administrator interface for configuring a Host Checker Policy. The policy name is "Trend Micro OfficeScan". Under "Host Checking Method", several options are listed with checkboxes: Sygate Enforcement API, Sygate Security Agent, Zone Labs: ZoneAlarm Pro and Zone Labs Integrity, McAfee Desktop Firewall 8.0, and InfoExpress CyberGatekeeper Agent. The "Rule Settings" section includes a table with the following data:

| Rule Type | Summary |
|--|----------------------------------|
| Attribute Check: Registry Settings | |
| HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc.\EngineZipVer | string: 7.100 Minimum Version |
| HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc.\PatternVer | dword: 951 Minimum Version |

At the bottom of the interface, there is a "Save Changes?" section with a "Save Changes" button. The footer of the interface contains the following text: "Licensed to Acmeqizmo, Host Id: localhost2, Copyright © 2001-2004 Juniper Networks, Inc. All rights reserved."

Trend Micro OfficeScan Realtime Scan

This policy verifies that OfficeScan is currently enabled and running on the workstation.

It can also verify that it is the correct version using an MD5 sum.

Host Check to look for the NTRTScan process

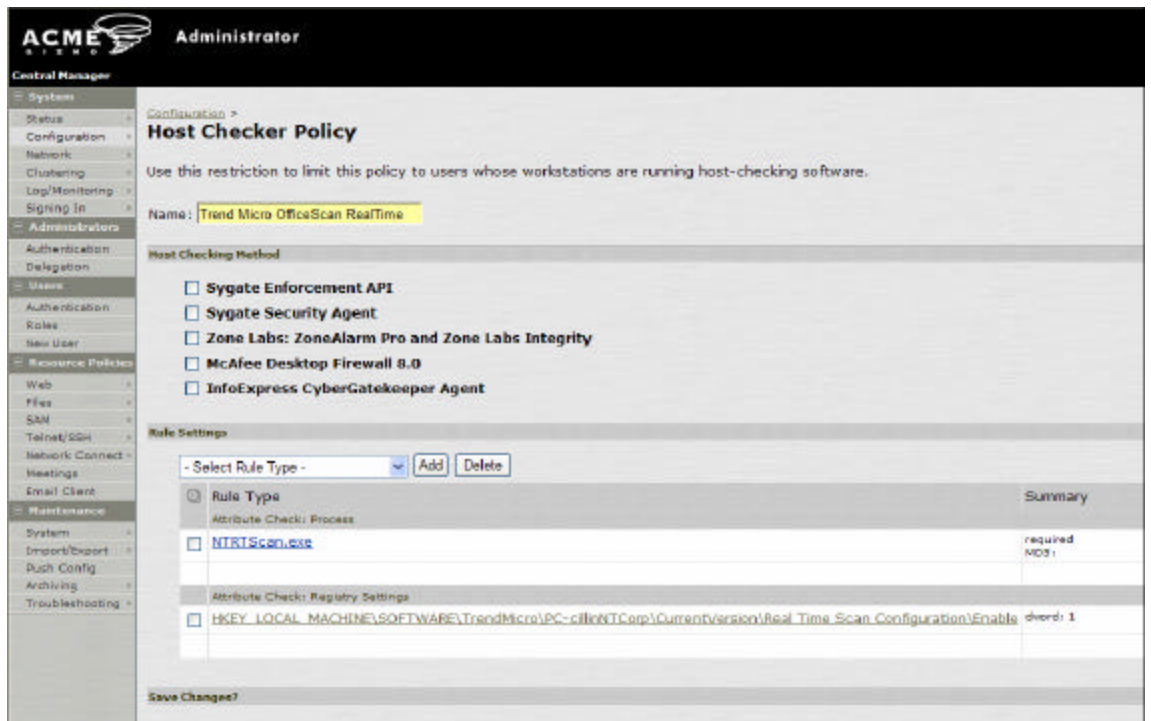
Attribute Check: Process

NTRTScan.exe required MD5:

Host Check to ensure that Real Time scan is enabled

Attribute Check: Registry Settings

HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\Real Time Scan Configuration\Enable dword: 1



The screenshot shows the ACME Administrator interface for configuring a Host Checker Policy. The policy name is "Trend Micro OfficeScan RealTime". Under "Host Checking Method", several options are listed with checkboxes: Sygate Enforcement API, Sygate Security Agent, Zone Labs: ZoneAlarm Pro and Zone Labs Integrity, McAfee Desktop Firewall 8.0, and InfoExpress CyberGatekeeper Agent. The "Rule Settings" section shows a table of rules:

| Rule Type | Summary |
|--|---------------|
| Attribute Check: Process | |
| <input type="checkbox"/> NTRTScan.exe | required MD5: |
| Attribute Check: Registry Settings | |
| <input type="checkbox"/> HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\Real Time Scan Configuration\Enable | dword: 1 |

At the bottom of the configuration page, there is a "Save Changes?" button.

Host Checker Policies Applied to Authentication Realm

This is a screen shot of all the above Host Checker policies being applied to an authentication realm.

An administrator would go to Users...Authentication...”realm name”...Authentication Policy...Host Checker

They would select the available policy and click the add button. This will add it to the list of checked policies.

