

CHAPTER 5: NONSECURE ENDPOINTS

.....

Use enforcement rules to ensure protected computers comply with your security policies regarding anti-virus and other types of software. If a protected computer does not comply with one or more enforcement rules, you can restrict the connection using restriction firewall rules.

Objective

By the end of this chapter, you will have met the following objective:

1. Create rules to secure remote endpoint PCs.



Key Terms

- Observe rule
- Warn rule
- Enforce rule



UNDERSTANDING ENFORCEMENT RULES

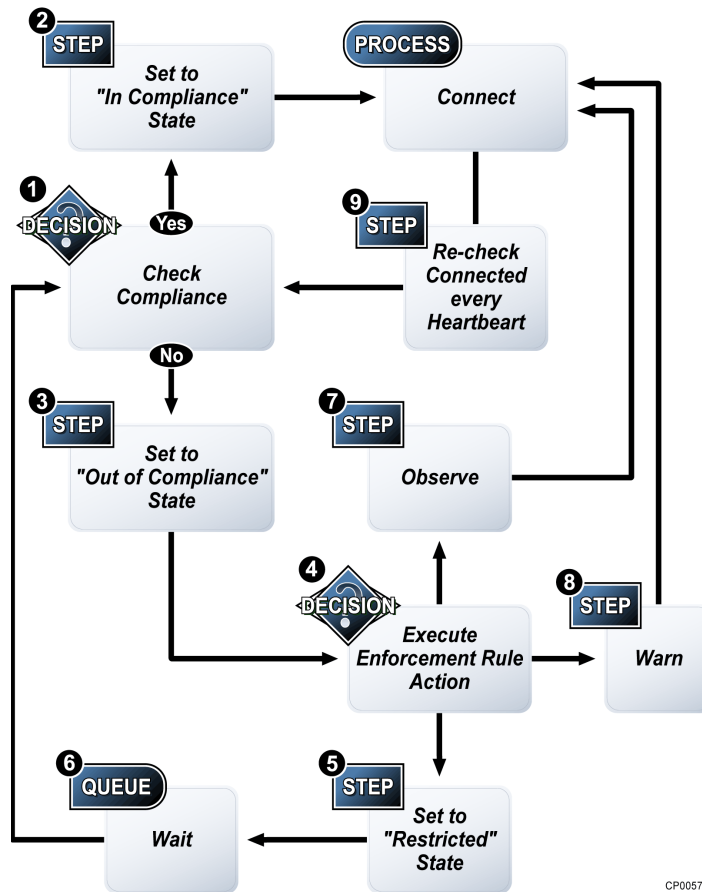
Enforcement rules determine whether the Integrity client can establish and maintain a session with Integrity Advanced Server and your internal network. The Integrity client periodically checks the protected computer for the enforcement rule conditions you set.

Integrity Advanced Server allows you to create the following types of enforcement rules to secure a protected computer:

- General enforcement rules that require or prohibit specific file or program configurations; for example, if you create a rule requiring a specific Registry key on Windows NT computers, users establishing a session from a Windows NT computer must have that Registry key. Users logging in from Windows NT computers that do not have the Registry key are then treated as being out of compliance with the rule.
- Anti-virus provider rules that require a specific anti-virus program, version, and configuration on the endpoint; for example, if you configured a rule requiring McAfee VirusScan Version 4.2 or higher, users logging in from computers that do not have this software are then treated as being out of compliance with the rule.
- Client rules that require an Integrity client on the endpoint computer; for example, if you create a rule requiring Integrity Agent version 6.0, users must have that version of Integrity Agent. Users that do not have Integrity Agent, or who have the wrong version, are then treated as being out of compliance with the rule.
- Rule groups that require compliance with a single rule in the group; with a rule group, the computer must be in compliance with at least one of the rules in the group. For example, if you configure a group with rules that require McAfee VirusScan, Symantec Norton AntiVirus, or Trend Micro PC-cillin, as long as the protected computer complies with one of those rules, the user is treated as being compliant with the rule.

How Enforcement Rules Work

Integrity client regularly checks the protected computer to ensure that it complies with all enforcement rules in the assigned security policy. If the user's computer becomes out of compliance with the enforcement rule's conditions, the Integrity client executes the enforcement action specified by the rule. The following figure shows the enforcement process:



CP00574

How Enforcement Rules Work



1. Integrity client checks the protected computer against all enforcement rules in the assigned security policy, including anti-virus provider rules and groups. The protected computer is found to be either in or out of compliance with the rules.
2. If the protected computer complies with all enforcement rules, the Integrity client sets the state to “In Compliance” and the connection can proceed.
3. If the protected computer is in violation of one or more enforcement rules, the Integrity client sets the state to “Out of Compliance.”
4. After the protected computer has been out of compliance for the number of specified heartbeats, the Integrity client executes the action specified in the enforcement rule. You can set the Integrity client to observe, warn, or restrict computers that are out of compliance.
5. If you have set the enforcement rule to “Restrict”, the protected computer will be restricted according to the restriction rules you created for the enforcement rule. The Integrity client will set the state to “Restricted”.
6. When a protected computer is restricted, the Integrity client rechecks every minute to see if the computer is back in compliance with the enforcement rules. When the computer is compliance, the Integrity client sets the compliance state to “In Compliance” and sends a sync to the server to immediately reestablish full access.
7. If you set the enforcement rule to “Observe”, the computer is allowed to connect and the event is logged.
8. If you set the enforcement rule to “Warn”, the computer is allowed to connect, the event is logged, and the user sees an alert that describes the security violation and provides a link to remediation information. You can set up remediation resources for endpoints that Integrity Advanced Server has warned or restricted. Warned users must apply the remediation resources manually. Restricted users can apply the resources manually, or you can configure Integrity Advanced Server to run the resources automatically.

9. Connected computers are rechecked every heartbeat to ensure that they remain compliant.



There is a delay between the time the protected computer becomes noncompliant and the point at which the connection is restricted. The delay is equal to the number of heartbeats you specify before restriction, multiplied by the time interval you set for the heartbeats. Observe and warn rules execute on the next heartbeat after noncompliance.

What the Restricted User Experiences

When a protected computer is out of compliance with an enforcement rule, the following occurs:

1. Integrity client executes the rule action. The user session is affected as follows:
 - Observed users can access the protected network. Observed users receive no alert.
 - Warned users receive an alert, but can still access the protected network. If you have configured a remediation resource for the rule, Integrity includes the resources (for example, a link or an executable file) in the alert message.
 - Restricted users can access only the part of your network you specify using restriction rules. Generally, you will restrict users to just the Sandbox server, where they can get remediation information. If you have configured a remediation resource for the rule, Integrity Advanced Server includes the resource (for example, a link or an executable file) in the alert message. If you have configured it to do so, Integrity Advanced Server applies the resource automatically.

Warning and restriction alerts include:

- Default or optional customized text explaining the rule action.
- The rule name.
- Any additional customized text you defined in the policy (optional).
- A help link that opens the Sandbox page you created for that enforcement rule.



Restriction Alert

2. If the user clicks the help link, one of the following Sandbox pages appears:
 - **REQUIRE** appears when users are not compliant with an enforcement rule that requires a specific program, registry keys/values, or files/properties.
 - **PROHIBIT** appears when users are not compliant with an enforcement rule that prohibits a specific program, registry keys/values, or files/properties.
 - **AV_COMPLIANCE** appears when users are not compliant with an anti-virus provider rule.
 - **GROUP** appears when users are not compliant with at least one of the rules in a group.
3. When the user becomes compliant, Integrity client no longer restricts the session, and the user can access the protected network.

Minimizing Support

Enforcement rules can cut off users from the network resources they need when they are out of compliance. Therefore, it is important to provide easy means for the user to become compliant, thereby minimizing any support requirements related to enforcement rules.

PROVIDING REMEDIATION RESOURCES FOR USERS

When implementing enforcement rules, provide adequate resources and information on the enforcement alerts and Sandbox pages, to enable warned and restricted users to become compliant. There are two ways to configure remediation resources:

1. In the enforcement rule, you can specify a remediation resource that users can download and install themselves. For restricted users, you have the option of configuring Integrity Advanced Server to run remediation resources automatically.
2. In the enforcement Sandbox pages (REQUIRE, PROHIBIT, AV_COMPLIANCE, and GROUP)

USING RULES THAT OBSERVE OR WARN

An important strategy for smoothly implementing enforcement rules is to first create rules that observe or warn, but do not restrict noncompliant computers. This helps identify any frequently occurring noncompliant conditions in your network, before restricting users as a result of those conditions. When you configure an enforcement rule to observe, the Integrity client logs noncompliance events and reports them to Integrity Advanced Server. The user session is not restricted.



Configure **“observe” rules** for centrally managed software that users do not install themselves. That way, you will be able to tell which users need the software, without inconveniencing users with compliance issues they cannot solve for themselves.



When you configure an enforcement rule to warn, Integrity client displays an Alert message that directs the user to remediation resources. Integrity client logs the event, but allows the user full access to the protected network.



Configure “**warn**” rules for software that users are responsible for installing and maintaining themselves.

After deploying a policy with an observe or warn rule, use the Enforcement report in the Reports module of Integrity Advanced Server to track the number of users affected by the rule. By tracking which users are noncompliant and the frequency of noncompliance, and by seeing how long it takes users to come into compliance, you can gauge the effectiveness of your policy and remediation resources.



To log enforcement-related events, configure the Client Alerts and Logging on the Client Settings tab of the security policy.

When you are satisfied that your rule and resources will enhance security without unduly increasing your support burden, change the action indicator in the rule from Observe (or Warn) to Restrict, and redeploy the policy. Note that for rules that restrict, you can configure Integrity Advanced Server to apply remediation resources automatically.

To set the enforcement action for a rule, in the Rule Action area of the enforcement rule, choose one of the following:

- Observe clients that don't comply
- Warn clients that don't comply
- Restrict clients that don't comply

Use the Enforcement Manager to create rules that can be used in security policies to:

- Require or prohibit specific conditions, such as files, programs, or Windows Registry keys and values, on the protected computer.
- Require specific anti-virus programs and definition files on the protected computer.
- Require a specific type and version of Integrity client on the protected computer.

Enforcement-Rule Workflow

1. Set up an enforcement rule for each set of conditions you want to enforce in the Enforcement Rules Manager, including setting up the alert-message text.
2. Customize the following Sandbox pages:
 - **AV_COMPLIANCE** for anti-virus rules
 - **PROHIBIT** for enforcement rules that prohibit programs, files, and/or keys
 - **REQUIRE** for enforcement rules that require programs, files, and/or keys
 - **GROUP** for enforcement/anti-virus rule groups that require one program
3. Assign the enforcement rules to a security policy.
4. Deploy the policy and assign it to endpoint users.

Cooperative Enforcement

Use the Cooperative Enforcement feature to ensure that endpoint computers remotely connecting to your network:

- Are running an Integrity client.
- Have a specific policy.
- Comply with the security policy assigned to them.



Using the Cooperative Enforcement feature, you can restrict or terminate the VPN session for any endpoint computer that is out of compliance.



If you are using a Check Point InterSpect internal security gateway, you can also have intra-LAN cooperative enforcement.

SUPPORTED GATEWAYS AND CLIENTS

Integrity Advanced Server can perform Cooperative Enforcement protection with the following gateways and clients:

- Check Point's VPN-1 SecureClient and VPN-1 NGX, using Secure Configuration Verification (SCV)
- Check Point InterSpect internal security gateways
- Cisco VPN 3000 Series Concentrator
- Nortel Contivity VPN switch with TunnelGuard, Firmware version 4.80 or later



If you use an unsupported gateway, Integrity Advanced Server can monitor Integrity client events and user status, but will not be able to restrict access at the gateway level. You must use enforcement rules in conjunction with Restriction Firewall rules to restrict endpoint users in this case.

For most supported gateways, you must configure Integrity first, then configure the gateway. The exception is Check Point InterSpect, which you must configure *before* you configure Integrity.

▪ *Understanding Enforcement Rules*

-
-
-
-