

User-Role-Based Policy Feature Overview

The user role-based policy feature depends on integration with the Juniper Networks IC Series Unified Access Control appliance. This feature requires collaboration with the UAC administrator.

The user role-based policy feature enables you to specify user roles as match criteria in IDP rulebase and application policy enforcement (APE) rulebase rules. Matching based on user role rather than IP address both simplifies and finely tunes your rules. In many networks, the IP address is dynamically assigned. To protect your network, you would have to cast a wide net for traffic sources. In most cases, you would specify a subnet mask or specify **Any** source (in the latter case, this means you really are not matching on source). For the purpose of intrusion detection and prevention, a wide net is not necessarily a bad thing: you do want to inspect any session that could potentially contain an attack. Use of role-based rules with a terminal match, however, will improve performance by providing faster matching with specific source targets and rulebase termination. In addition, you are likely to find that user role-based logs are easier to analyze because they provide visibility into the user role associated with an attack event or application usage.

UAC integration with IDP Series appliances also improves end user experience authenticating to your network. In a UAC deployment, you use the Host Checker feature to quarantine users with vulnerable hosts. Instead of using a firewall to shut down access to network resources, you can use IDP security policies to enable access and inspect the traffic to guard against threats.

In the APE rulebase, role-based rules are indispensable to supporting the business cases that demand a nuanced approach to application policy enforcement. They enable you to enforce business policies such as “Contractors, Part-Time, and Temporary employees may not use peer-to-peer filesharing applications; full-time employees may use them, but only with a limited pool of bandwidth.”

To deploy the user role-based feature:

1. Read the release notes for the IDP and UAC releases to verify version compatibility requirements.
2. Deploy a UAC solution for user access to the network. For details, see the *Unified Access Control Administration Guide*.
3. Use the UAC user interface to create the user roles you want to use in your security policy:
 - For security rules, you want to leverage results of the Host Checker to map users to roles that identify vulnerabilities, such as “Laptop Users,” “Unauthorized Instant Messenger Installed,” or “Windows XP Patch Required.”
 - For application policy enforcement rules, you want to map users to roles that reflect the business rule, such as Contractor, Part-Time, and Temporary.

For details, see the *Unified Access Control Administration Guide* or UAC online Help.

4. Configure communication between the UAC appliance and the IDP appliance so you can use the IDP role-based policy feature:
 - From the IDP side, you use the Appliance Configuration Manager (ACM) to generate a one-time password the UAC appliance can use to connect to the IDP appliance.
 - From the UAC side, you configure the connection to the IDP appliance, specifying the IP address, port 7103, and the one-time password.

For details, see the UAC online Help.

5. Use the IDP appliance command-line interface to verify integration. You can use CLI commands to verify connectivity with the IC Series device and to display the user session table, which is populated by the IC Series appliance.

For details, see the *IDP Administration Guide*.

6. In NSM, create a security policy with role-based rules. The roles you specify are the roles created and managed in UAC.
7. Push the security policy from NSM to the IDP appliance.

Related Topics The following related topic is included in the *IDP Concepts and Examples Guide*:

- Understanding Communication Between IDP Series and IC Series Appliances
- IDP Rulebase Example: User-Role-Based Policies
- APE Rulebase Example: Limiting Bandwidth to Instant Messaging and Peer-to-Peer Traffic in the Enterprise
- APE Rulebase Example: Using User-Role-Based Rules to Support Tiered Subscriptions

The following related topic is included in the *IDP Administration Guide*:

- Specifying Rule Match Conditions (NSM Procedure)

Published: 2010-01-12