JUNIPER NETWORKS

Junos® OS

Unified Access Control Solution Guide for SRX Series Services Gateways

Release

Junos Pulse Access Control Service 4.2/Junos OS 12.1

Published: 2012-04-03

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Junos OS United Access Control Solution Guide for SRX Series Services Gateways

Revision History
March 2012—Initial release

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

SOFTWARE LICENSE

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions. Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details. For complete product documentation, please see the Juniper Networks website at www.juniper.net/techpubs.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Guide

This preface provides the following guidelines for using this guide:

SRX Series and Junos Pulse Access Control Service Documentation and Release Notes

For a list of related SRX Series documentation, see http://www.juniper.net/techpubs/hardware/srx-series-main.html .

For a list of related Junos Pulse Access Control Service documentation, see http://www.juniper.net/techpubs/hardware/srx-series-main.html .

If the information in the latest release notes differs from the information in the documentation, follow the *Junos OS Release Notes* or the *Junos Pulse Access Control Service Release Notes*.

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

Juniper Networks supports a technical book program to publish books by Juniper Networks engineers and subject matter experts with book publishers around the world. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration using the Junos operating system (Junos OS) and Juniper Networks devices. In addition, the Juniper Networks Technical Library, published in conjunction with O'Reilly Media, explores improving network security, reliability, and availability using Junos OS configuration techniques. All the books are for sale at technical bookstores and book outlets around the world. The current list can be viewed at http://www.juniper.net/books .

Objectives

This guide describes how to use and configure key security features on SRX Series Services Gateways running Junos OS in conjunction with Junos Pulse Access Control Service. It provides conceptual information, suggested workflows, and examples where applicable.

Audience

This manual is designed for anyone who installs, sets up, configures, monitors, or administers an SRX Series Services Gateway running Junos OS in conjunction with Junos Pulse Access Control Service. The manual is intended for the following audiences:

- Customers with technical knowledge of and experience with networks and network security, the Internet, and Internet routing protocols
- Network administrators who install, configure, and manage Internet routers

Supported Routing Platforms

This manual describes features supported on the SRX Series Services Gateways running Junos OS in conjunction with Junos Pulse Access Control Service.

Document Conventions

Table 1 on page viii defines the notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page ix defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces important new terms. • Identifies book names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS System Basics Configuration Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; interface names; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Enclose optional keywords or variables.	**stub** <**default-metric** *metric*>**;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** (***string1*** **|** ***string2*** **|** ***string3***)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	**community name members [** ***community-ids*** **]**

Indention and braces ({ })	Identify a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

J-Web GUI Conventions

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/ . If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need postsales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf .
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/ .
- JTAC Hours of Operation —The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Find product documentation: http://www.juniper.net/techpubs/

- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/ .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, visit us at http://www.juniper.net/support/requesting-support.html

Acquiring User Role Information from an Active Directory Authentication Server

Networks have used the IP address as a way of identifying users and servers. The strategy is based on the assumption that users or groups of users connect to the network from fixed locations and use one device at a time.

Wireless networking and mobile devices require a different strategy. Individuals can connect to the network using multiple devices simultaneously. The way in which devices connect to the network changes rapidly. It is no longer possible to identify a user with a group of statically allocated IP addresses.

In Junos OS Release 12.1 and later, user role firewall security policies let you classify traffic based on the roles to which a user is assigned. Based on match criteria, which includes the user's role, you create policies to apply services that allow or block access to resources. The user role firewall is similar to the identity-based network access control (NAC) solution available with UAC on the SRX Series device. A user role firewall, however, does not require the Junos Pulse/Odyssey installation, and it supports agentless transparent authentication.

User role information can be collected in several ways: locally on the SRX Series device, from a Junos Pulse Access Control Service device, or by relaying authentication data from a third-party authentication server through a Junos Pulse Access Control Service device to the SRX Series device.

Incorporating a third-party authentication server into a user role firewall configuration can also provide single sign-on (SSO) support. This allows a browser-based user to authenticate once and have that authentication communicated to other trusted servers in the domain as needed.

Requirements

This solution uses the following hardware and software components:

- One MAG Series Junos Pulse Gateway device with software release 4.2 or later
- The MAGx600-UAC-SRX license installed on the MAG Series device
- One SRX Series device with Junos OS Release 12.1 or later
- One Microsoft Active Directory server using version 2008

NOTE: **Microsoft Windows 2003 is also compatible with this functionality, but terminology, pathways, and settings might differ from what is presented in this document.**

Before you begin:

- Ensure that the MAG Series device is configured as an Access Control Service and is accessible to the network. See the *MAG Series Junos Pulse Gateway Hardware Guide* for configuration details.
- Ensure that the MAGx600-UAC-SRX license is installed on the MAG Series device.
- Ensure that the SRX Series device is configured and initialized with Junos OS version 12.1 or later.
- Ensure that the Active Directory authentication server is configured for standard Junos Pulse Access Control Service authentication. See your third-party documentation.
- Ensure that the administrator has the appropriate capabilities for configuring the roles, users, and device interactions.

Overview

In this solution an SRX Series device obtains user role information dynamically from a Microsoft Active Directory authentication server. Authentication verification and user role information from the Active Directory server is relayed by the Access Control Service on the MAG Series device to the SRX Series device.

Users within the same domain are connected to a LAN segment. They are associated with user role groups, such as developer or manager, depending on their work in the organization. When a user authenticates to the AD authentication server, the user should be able to access protected resources without having to authenticate a second time.

The SRX Series device is configured as an enforcer for the MAG Series device. It receives user role information from the MAG Series device and applies user role firewall policies accordingly to incoming and outgoing traffic.

When the SRX Series device has no user role information for a user, the user's browser is redirected to the MAG Series device. Transparently to the user, the MAG Series device requests verification from the browser. The browser retrieves a token from the Active Directory server confirming authentication and passes it to the MAG Series device. With the information provided by the token, the MAG Series device retrieves user role information for the user from the Active Directory server and creates an authentication table entry consisting of the current IP address and the user role data. The MAG Series device pushes the updated table to the SRX Series device and redirects the browser back to the SRX to request access again. This time, the table does contain user role information which is then retrieved and used as part of the match criteria for applying user role firewall services.

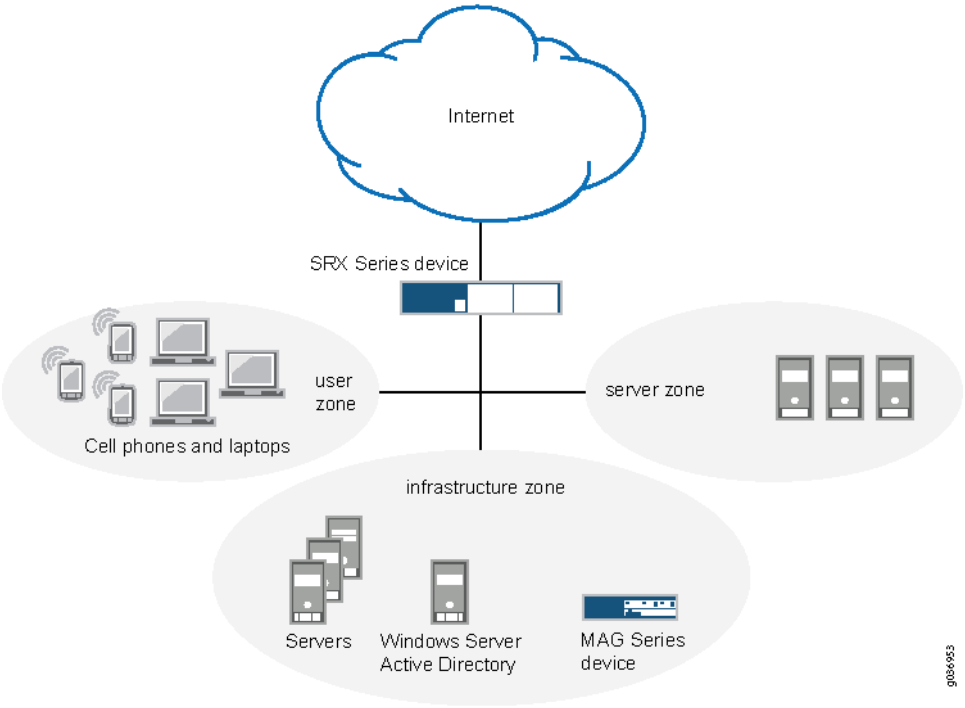
The user is not aware of the process unless the Active Directory server has no current authentication for the user. When that is the case, the server prompts the user for name and password. Once authentication occurs, the server returns a token to the browser.

The procedure documented here initially configures the MAG Series device as the authenticator. The configuration is later modified to retrieve authentication information from the AD server. This solution uses SPNEGO negotiation and Kerberos authentication

to secure communications among the SRX device, the MAG Series device, the browser, and the authentication server.

Topology

Figure 1: Single Sign-On Support Topology



A user's request to access another resource is controlled by roles and groups associated with the user. For example, a user belonging to a group of developers named Dev might have access to a particular test server. The same user might also be the manager and belong to the Mgr group that can access certain HR resources. A contractor working for this manager might require access to the test server as well but not to the HR resources. In this case, the user would be added to the Dev group and perhaps a Contractor group, but not the Mgr group.

User role firewall policies defined on the SRX Series device control the groups and user roles that can access various resources. In this configuration, if user role data does not exist for a user requesting access, a policy redirects the user's browser to the MAG Series device to authenticate the user and retrieve any associated user role data.

A token exchange among the Access Control Service, the browser, and the Active Directory server remains transparent to the user while it verifies the user's authentication. The exchange uses SPNEGO negotiation and Kerberos authentication for encrypting and decrypting messages among the devices.

With information obtained from the response token, the MAG Series device retrieves the user's roles and groups directly from the Active Directory server. It then creates an authentication table entry and passes it to the SRX Series device.

Configuration

Configure the devices for this solution by performing the following tasks.

- Connect the SRX Series device and the MAG Series device in an enforcer configuration.
- Configure the Access Control Service on the MAG Series device for local user authentication and verify that authentication information is transferred between the devices.
- Configure a captive portal policy on the SRX Series device to redirect any unauthenticated user to the Access Control Service and verify that redirection is functioning properly.
- Configure the Microsoft Active Directory authentication server to interact with the Access Control Service and the endpoints.
- Reconfigure the Access Control Service for remote authentication by the Active Directory server and redefine Active Directory groups for the SRX Series device.
- Configure endpoint browsers for the SPNEGO protocol

NOTE: **Configuring the Access Control Service using local authentication is not necessary for this solution. However, by configuring local authentication first you can verify the captive portal interaction between the MAG Series device and the SRX Series device.**

The following solution requires you to navigate various levels in the configuration hierarchy on the SRX Series device. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the *Junos OS CLI User Guide*.

Connecting the SRX Series Device to the Access Control Service

Step-by-Step Procedure

In an enforcer configuration, the Access Control Service on the MAG Series device and the SRX Series device communicate over a secure channel. When the SRX Series device first connects with the Access Control Service, the devices exchange information to ensure secure communication. Optionally, you can use digital security certificates as an enhanced mechanism for establishing trust.

See the *Unified Access Control Administration Guide* for details about configuring certificate trust between the SRX Series device and the Access Control Service.

To connect the SRX Series device and the Access Control Service on the MAG Series device:

1. Configure the SRX Series device.
   a. Configure the zones and interfaces of the devices.

      user@host# set security zones security-zone user interfaces ge-0/0/0
      user@host# set security zones security-zone infrastructure interfaces ge-0/0/1
      user@host# set security zones security-zone untrust interfaces ge-0/0/2

b. Configure the IP addresses of the interfaces.

```
user@host# set interfaces ge-0/0/0 unit 0 family inet address 10.12.12.1/24
user@host# set interfaces ge-0/0/1 unit 0 family inet address 10.0.0.20/24
user@host# set interfaces ge-0/0/2 unit 0 family inet address 1.1.1.1/24
```

c. Identify the Access Control Service as a new Infranet Controller, and configure the interface for the connection to it.

```
[edit]
user@host# set services unified-access-control infranet-controller mag123
  address 10.0.0.22
user@host# set services unified-access-control infranet-controller mag123
  interface fxp0.0
```

d. Specify the password for securing interactions between the Access Control Service and the SRX Series device.

```
[edit]
user@host# set services unified-access-control infranet-controller mag123
  password "InSub321"
```

NOTE: The same password must be configured on both devices.

e. (Optional) Specify the full name of the Access Control Service certificate that the SRX Series device must match during connection.

```
user@host# set services unified-access-control infranet-controller mag123
  ca-profile ca-mag123-enforcer
```

f. If you are done configuring the SRX Series device, enter commit from configuration mode.

2. Configure the Access Control Service from the administrator console on the MAG Series device.

a. Navigate to the Infranet Enforcer page, and click **New Enforcer**.

b. Select **Junos**, enter the password set previously on the SRX Series device (InSub321), and enter the serial number of the SRX Series device.

c. Click **Save Changes**.

Results When both devices are configured, the SRX Series device connects automatically to the Access Control Service.

- From the Access Control Service, select **System>Status>Overview** to view the status of the connection to the SRX Series device. The diode in the display is green if the connection is functioning. To display additional information, click the device name.
- From operational mode on the SRX Series device, confirm your connection by entering the **show services unified-access-control status** command. If the output does not display

the intended configuration, repeat the instructions in this section to correct the configuration.

user@host> **show services unified-access-control status**

```
Host          Address         Port   Interface     State
mag123        10.0.0.22       11123  fxp0.0        connected
```

Configuring the Access Control Service for Local User Authentication

Step-by-Step Procedure

When a user is authenticated, the Access Control Service on the MAG Series device updates its authentication table with the IP address and associated roles of the user, and pushes the updated table to the SRX Series device. If this user data is deleted or modified, the Access Control Service updates the authentication table with the new information and again pushes it to the SRX Series device.

To test the successful transfer and content of the authentication table, this task configures the Access Control Service on the MAG Series device for local authentication. Within this configuration you can test the user role firewall from the SRX Series device without affecting other network operations. A later task modifies this configuration to provide user role retrieval from the remote Active Directory server.

NOTE: **It is not a requirement to configure the Access Control Service for local user authentication. It is provided so that you can test each task in the configuration.**

To configure the Access Control Service for local authentication:

1. Define roles on the Access Control Service.
   a. From the administrator console of the Access Control Service, select **Users>User Roles>New User Role**.
   b. Enter **dev** as the role name.

      In this solution, use the default values for other role settings.
   c. Click **Save Changes**.

NOTE: **This solution assumes that the MAGx600-UAC-SRX license is installed on the Access Control Service. If the full-feature license is installed, you will need to disable OAC Install and enable Agentless Access.**

2. Configure the default authentication server.
   a. Select **Authentication>Auth. Servers**.

b. Select **System Local**. This establishes the MAG Series device as the default authentication server.

3. Create users.
   a. Select the **Users** tab, and click **New**.
   b. Create **user-a** by entering the following details.
      - Username
      - User's full name
      - Password
      - Password confirmation
   c. Repeat the previous step to create **user-b**.
   d. Click **Save Changes**.
4. Create a realm.
   a. Select **Users>User Realms>New User Realm**.
   b. Enter **REALM6** as the realm name.
   c. Select **System Local** in the Authentication box.
   d. Click **Save Changes**.
5. From the same page, create role mapping rules.
   a. Select the **Role Mapping** tab, and click **New Rule**.
   b. Define two rules with the following details.
      - Enter username user-a, and assign it to role dev.
      - Enter username user-b, and assign it to role dev.
   c. Click **Save Changes**.
6. Set up the default sign-in page.
   a. Select **Authentication>Signing In>Sign-in Policies**.
   b. Click the default **Sign-in policy (*/)**.
   c. In the **Sign-in URL** box, enter the IP address of this device.
   d. In **Authentication realm, Available realms**, select REALM6.
   e. Click **Save Changes**.

Results Verify the results of the configuration. If the output does not display the intended configuration, repeat the instructions in this section to correct the configuration.

1. Verify that local authentication on the Access Control Service is functioning properly.
   - Open a browser window from an endpoint in the network.
   - Enter the fully qualified domain name for the Access Control Service.

     The default sign-in page should display.
   - Sign in as user-a, and provide the defined password.
2. From operational mode on the SRX Series device:
   a. Confirm that the authentication table on the SRX Series device was updated with **user-a**.

      user@host> **show services unified-access-control authentication-table**

      ```
      Id    Source IP       Username     Age      Role identifier
      1     172.24.72.79    user-a       0        0000000001.000005.0
      Total: 1
      ```

   b. Confirm that the correct role has been associated with the role identifier.

      user@host> **show services unified-access-control roles**

      ```
      Name                Identifier

      dev                 0000000001.000005.0
      ```

   c. List all roles associated with user-a.

      user@host> **show services unified-access-control authentication-table detail**

      ```
      Identifier: 1
        Source IP: 172.24.72.79
        Username: user-a
        Age: 0
        Role identifier       Role name
          0000000001.000005.0 dev
      ```

Configuring Redirection from the SRX Series Device to the Access Control Service

Step-by-Step Procedure

Local authentication, as configured in the previous task, requires users to log on to the Access Control Service directly to gain access to network resources. The SRX Series device can be configured to automatically redirect the browser of an unauthenticated user to the Access Control Service if a user requests access to a protected resource directly. You can define a user role firewall policy to redirect an unauthenticated user to a captive portal on the Access Control Service for sign-in.

NOTE: Other services, such as IDP, UTM, AppFW, and AppQoS, can be configured as well as the UAC captive portal implementation. The solution focuses on captive portal for authentication for user role implementation only.

To configure redirection from the SRX Series device to the Access Control Service:

1. From configuration mode on the SRX Series device, configure the profile for the captive portal acs-device.

```
[edit]
user@host# set services unified-access-control captive-portal acs-device
    redirect-traffic unauthenticated-user
```

2. Add either the redirection URL for the Access Control Service or a default URL.

```
[edit]
user@host# set services unified-access-control captive-portal acs-device
redirect-url https://%ic-url%/?target=%dest-url%&enforcer=%enforcer-id%
```

   This command specifies the default target and enforcer variables so that the browser is returned to the SRX Series device after authentication.

3. Allow traffic to the Acitve Directory (AD) server, the Access Control Service, and the other infrastructure servers.

```
[edit]
user@host# set security policies from-zone user to-zone infrastructure policy
    Allow-AD-UAC match source-address any
user@host# set security policies from-zone user to-zone infrastructure policy
    Allow-AD-UAC match destination-address any
user@host# set security policies from-zone user to-zone infrastructure policy
    Allow-AD-UAC application any
user@host# set security policies from-zone user to-zone infrastructure policy
    Allow-AD-UAC then permit
```

4. Configure a security policy that redirects HTTP traffic from zone user to zone untrust if the source-identity is unauthenticated-user.

```
[edit]
user@host# set security policies from-zone user to-zone untrust policy user-role-fw1
    match source-address any
user@host# set security policies from-zone user to-zone untrust policy user-role-fw1
    match destination-address any
```

```
user@host# set security policies from-zone user to-zone untrust policy user-role-fw1
  match application http
user@host# set security policies from-zone user to-zone untrust policy user-role-fw1
  match source-identity unauthenticated-user
```

5. Configure the action to be taken when traffic matches the criteria for user-role-fw1.

   In this case, traffic meeting the specified criteria is allowed access to the UAC captive portal defined by the acs-device profile.

```
user@host# set security policies from-zone user to-zone untrust policy user-role-fw1
  then permit application-services uac-policy captive-portal acs-device
```

6. Configure a security policy allowing access to any HTTP traffic from zone user to zone untrust.

```
[edit]
user@host# set security policies from-zone user to-zone untrust policy user-role-fw2
  match source-address any
user@host# set security policies from-zone user to-zone untrust policy user-role-fw2
  match destination-address any
user@host# set security policies from-zone user to-zone untrust policy user-role-fw2
  match application http
user@host# set security policies from-zone user to-zone untrust policy user-role-fw2
  match source-identity any
user@host# set security policies from-zone user to-zone untrust policy user-role-fw2
  then permit
```

NOTE: It is important to position the redirection policy for unauthenticated users before a policy for “any” user so that UAC authentication is not shadowed by a policy intended for authenticated users.

7. If you are done configuring the policies, commit the changes.

```
[edit]
user@host# commit
```

Results Confirm your configuration with the following procedures. If the output does not display the intended configuration, repeat the instructions in this section to correct the configuration.

1. From configuration mode, confirm your captive portal profile configuration by entering the **show services** command.

```
[edit]
user@host# show services
```

```
...
unified-access-control {
 captive-portal acs-device {
  redirect-traffic unauthenticated;
  redirect-url https://%ic-url%/?target=%dest-url%&enforcer=%enforcer-id%
...
```

2. From configuration mode, confirm your policy configuration by entering the **show security policies** command.

   user@host# **show security policies**

```
...
from-zone user to-zone infrastructure {
 policy Allow-AD-UAC  {
  match {
   source-address any;
   destination-address any;
   application any;
  }
  then {
   permit
  }
 }
}
from-zone user to-zone untrust {
 policy user-role-fw1 {
  match {
   source-address any;
   destination-address any;
   application http;
   source-identity unauthenticated-user
  }
  then {
   permit {
    application-services {
     uac-policy {
      captive-portal acs-device;
     }
    }
   }
  }
 }
}
from-zone user to-zone untrust {
 policy user-role-fw2 {
  match {
   source-address any;
   destination-address any;
   application http;
   source-identity any
  }
  then {
   permit
  }
 }
}
...
```

3. Verify that the redirection policy is functioning correctly.

   a. Open a browser window from a second endpoint in the network.

   b. Enter a third-party URL, such as www.google.com.

      The default sign-in page from the Access Control Service prompts for a user and password.

c. Enter the username **user-b** and its password.

The browser should display the requested URL.

NOTE: If a pop-up blocker is set on the endpoint, it could interfere with this functionality.

d. From operational mode on the SRX Series device, verify that the authentication data and roles from the Access Control Service were pushed to the SRX Series device successfully.

user@host> **show services unified-access-control authentication-table**

```
Id     Source IP       Username     Age      Role identifier
1      172.24.72.79    user-a       0        0000000001.000005.0
2      172.24.72.87    user-b       0        0000000001.000005.0
Total: 2
```

Configuring Active Directory Settings

Step-by-Step Procedure

SPNEGO negotiation and Kerberos authentication are transparent to the user and network administrator, but certain configuration options enable the use of these protocols. This section identifies configuration requirements when using Active Directory as the authentication server. To interact in SPNEGO negotiation, the Access Control Service requires a keytab file created by Active Directory. Refer to your third-party documentation for more information about enabling SPNEGO and Kerberos usage.

This section is not intended to be a tutorial for Active Directory. However, there are specific configuration details required for this solution. See your third-party documentation to set up Active Directory as a domain controller.

To configure the Active Directory authentication server:

1. Add a DNS entry as the UAC service account in the **Forward Lookup Zones**. In this way clients can refer to the MAG Series device by name or by IP address.

   This UAC service account name will be used in the next section when reconfiguring the UAC service on the MAG Series device.

2. Single sign-on authentication requires that the UAC service account password never expires. To modify user settings:

   a. From the Active Directory Users and Computers application in DNS, select **Users>New>User** and select the UAC service account created in step 1.

   b. Select the **Account** tab.

   c. In user settings, click **Password Never Expires**.

3. On the Domain Controller, open a command line, and enter the **ktpass** command to create the SPNEGO keytab file.

The keytab file created on the Active Directory server contains the full service principal name (SPN) and other encryption information from the server. The keytab file is then uploaded to the Access Control Service on the MAG Series device. This shared information identifies one device to the other whenever encrypted messages and responses are sent.

Use the following syntax.

ktpass -out *output-file-name* -mapuser *uac-service-acccount-name* -prin *service://fqdn@REALM*

ktpass—Third-party Kerberos utility that maps an SPN to a user, in this case, to the UAC service account. The executable is available for download. Refer to your third-party documentation for the source for this utility.

-out *output-file-name*—The name for the SPNEGO keytab file you are creating.

-mapuser *uac-service-acccount-name*—The name of the UAC service account created in step 1.

-prin *service://fqdn@REALM*—The service principal name. The Kerberos authentication uses the SPN in its communication. It does not use an IP address.

service—The HTTP service.

fqdn—The hostname of the Junos Pulse Access Control Service. The *service://FQDN* portion of the name is provided by the Access Control Service when registering with the Active Directory server.

REALM—The realm of the Active Directory authentication server. It is the same as the domain name. The Kerberos realm name is always in uppercase letters following the recommendation in RFC 1510. This affects interoperability with other Kerberos-based environments.

The following command creates an SPNEGO keytab file named ic.ktpass.

ktpass -out ic.ktpass -mapuser icuser@UCDC.COM -princ HTTP/mag123.ucdc.com@UCDC.COM -pass Doj73096

This file is copied to the Access Control Service on the MAG Series device in the next section when SPNEGO is configured for remote authentication.

Reconfiguring Remote Authentication on the Access Control Service

Step-by-Step Procedure

This section reconfigures the Access Control Service on the MAG Series device to query the remote Active Directory server instead of the local authentication table when authenticating a user. The following steps add services and authentication options to the Access Control Service on the MAG Series device. The configuration of the SRX Series device remains unchanged.

When you reconfigure the realm's authentication server, the Access Control Service displays all roles or groups from the configured domain controller and its trusted domains. Establishing role mapping rules equates the authentication server's roles or groups to those defined on the Access Control Service.

To reconfigure remote authentication on the Access Control Service:

1. From the administrator console of the Access Control Service on the MAG Series device, select **Authentication>Auth. Servers**.
2. Choose the **Active Directory/Windows NT** server type, and click **Add New Server**.
3. Enter the profile of the new authentication server.
   a. Name the Active Directory server.
   b. Enter its NetBIOS domain name in the domain box.

NOTE: You might receive the following message: "Either the server is not a domain controller of the domain, or the NetBIOS name of the domain is different from the Active Directory (LDAP) name." This message is informational and does not affect the processing of the authentication.

   c. Enter the Kerberos Realm name.

      The Kerberos realm name is the FQDN of the Active Directory domain. For example, if "juniper" is the domain or NetBIOS name, juniper.net is the Kerberos realm name.

   d. In the Domain Join Configuration section, enter the Username and password of the UAC services account which has permission to join computers to the Active Directory domain.
   e. Select the Save credentials box.
   f. Enter the Container name.

      This is the name of the container in Active Directory where you created the UAC services account for the Access Control Service.

   g. Enter the Computer Name.

Specify the machine ID that the Access Control Service uses to join the specified Active Directory domain as a computer. This name is derived from the licence hardware ID of the Access Control Service in the following format: 0161MT2L00K2C0.

h. Verify that the join operation has succeeded.

The Join Status indicator provides a color-coded status for the domain join operation as follows:

- Gray: Not started
- Yellow: In progress
- Red: Failed to join
- Green: Joined the domain

i. Select **Kerberos** and **NTLM v2** as the authentication protocols.

j. In the Trusts section, select the Allow trusted domains box.

k. Select **Enable SPNEGO**.

l. Use the Browse button to upload the keytab file that you created in the previous section.

m. Click **Save Changes** and **Test Configuration**.

4. Ensure that SSO is enabled.

a. Select **Users>User Realms** and the realm name.

b. Select the Active Directory server name from the **Auth Server** list.

c. Select the **Authentication Policy** tab.

d. Verify that the **SSO** option is selected.

e. Click **Save Changes**.

5. Create role-mapping policies for groups acquired from the authentication server.

Groups from the Active Directory authentication server need to be mapped to roles on the Access Control Service. You first need to create roles, and then map one or more groups to the appropriate role.

a. Select the Role Mapping tab.

b. Click **New Rule**, enter a role name, and click **Save Changes**.

You do not need to add users to the role. Create as many roles as needed to map the groups from the Active Directory authentication server.

c. Click **Groups**, and select **Search** to list the groups defined in the domain controller.

d. Select the group names that you want to map to the new role.

e. Repeat steps b through d to create and map other groups.

f. Click **Save Changes**.

Configuring Endpoint Browsers for the SPNEGO protocol

Step-by-Step Procedure

Ensure that endpoint browsers have SPNEGO enabled. For further information, see your third-party documentation.

- Internet Explorer

  From **Security>Local Intranet>Sites>Advanced** add the trusted URL.

  IE performs SPNEGO without any further endpoint configuration but the user is prompted for a username and password. The username and password can be cached.

  To provide single sign-on support, an Internet Explorer configuration can be pushed by configuring a group policy on the Active Directory server. See your third-party documentation for further information.

  Integrated Windows Authentication must be enabled. Use the **Tools>Internet Options>Advanced>Security>Enable Integrated Windows Authentication** path to verify that IWA is enabled.

- Firefox (Windows and MacOS)

  The configuration is in a hidden location. For the URL, type **about:config** and search for the word **trusted**. The required key is the comma separated parameter named **network.negotiate-auth.trusted-uris**.

  NOTE: You need to specify the URL of the resource (in this solution, the FQDN or domain controller value UCDC.com).

- Chrome

  Use the Internet Explorer setting. From **Security>Local Intranet>Sites>Advanced** add the trusted URL.

  An internet Explorer configuration can also be pushed by configuring a group policy on the Active Directory server. This configuration is honored by Chrome.

After successful authentication, the standard agentless page is shown along with a second window with the protected resource (unless a pop-up blocker prevents this).

Related Documentation

- *Junos OS Security Configuration Guide*
- *Junos OS CLI Reference*
- *Junos Pulse Access Control Service Administration Guide*