Pulse Policy Secure

UAC Solution Guide for SRX Series Services Gateways

Product Release 5.1

Document Revision 1.0
Published: 2015-02-10

Pulse Secure, LLC
2700 Zanker Road, Suite 200
San Jose, CA 95134
http://www.pulsesecure.net

Pulse Policy Secure UAC Solution Guide for SRX Series Services Gateways

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

END USER LICENSE AGREEMENT

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

Table of Contents

List of Figures

List of Tables

About This Guide

Objectives

This guide describes basic configuration procedures for Pulse Policy Secure (UAC) interoperability with the Junos Enforcer.

Audience

This guide is designed for network administrators who are configuring and maintaining a Pulse Policy Secure Series Device. To use this guide, you need a broad understanding of networks in general and the Internet in particular, networking principles, and network configuration. Any detailed discussion of these concepts is beyond the scope of this guide.

Documentation Conventions

Table 1 on page 9 defines the notice icons used in this guide. Table 2 on page 9 defines text conventions used throughout this documentation.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that may result in loss of data or hardware damage.
	Warning	Alert regarding risk of personal injury or death.
	Laser warning	Alert regarding risk of personal injury from a laser.

Table 2: Text Conventions

Convention	Description	Examples
Bold text	Represents keywords, scripts, and tools in text. Represents a GUI element that the user selects, clicks, checks, or clears.	Specify the keyword exp-msg. Run the install.sh script. Use the pkgadd tool. To cancel the configuration, click Cancel.
Bold text like this	Represents text that the user must enter.	user@host# set cache-entry-age *cache-entry-age*

Fixed-width text like this	Represents information as displayed on your terminal's screen, such as CLI commands in output displays.	nic-locators {
		login {
		resolution {
		resolver-name /realms/
		login/A1;
		key-type LoginName;
		value-type SaeId;
		}

Regular sans serif typeface	Represents configuration statements. Indicates SRC CLI commands and options in text. Represents examples in procedures.	System Idap server{ Stand-alone; • Use the request sae modify device failover command with the force option user@host# . . .
Italic sans *serif typeface*	Represents variables in SRC CLI commands.	user@host# set local-address *local-address*
Angle brackets	In text descriptions, indicate optional keywords or variables	Another runtime variable is <gfwif>

Key name	Indicates the name of a key on the keyboard	Press Enter
Key names linked with a plus sign (+)	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b
Italic *typeface*	Emphasizes words. Identifies book names. Identifies distinguished names. Identifies files, directories, and paths in text but not in command examples.	There are two levels of access: *user* and *Privileged*. *SRC-PE Getting Started Guide.* *o=Users, o=UMC* The */etc/default.properties* file.
Backslash	At the end of a line, indicates that the text wraps to the next line.	Plugin.radiusAcct-1.class=\ net.pulsesecure.smgt.sae.plugin\ RadiusTrackingPluginEvent
Words separated by the | symbol	Represent a choice to select one keyword or variable to the left or right of this symbol. (The keyword or variable may be either optional or required.)	diagnostic | line

Documentation

For a list of related Pulse Policy Secure documentation, see http://www.pulsesecure.net/support. If the information in the latest Pulse Policy Secure Release Notes differs from the information in the documentation, follow the Pulse Policy Secure Release Notes.

Obtaining Documentation

To obtain the most current version of all Pulse Secure technical documentation, see the products documentation page at http://www.juniper.net/techpubs.

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@pulsesecure.net

Requesting Technical Support

Technical product support is available through the Pulse Secure Global Support Center (PSGSC).

- Product warranties—For product warranty information, visit http://www.pulsesecure.net/support
- PSGSC hours of operation—The PSGSC 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, the Pulse Secure Global Support Center (PSGSC) that provides you with the following features:

- Find CSC offerings: http://www.pulsesecure.net/support
- Search for known bugs: http://www.pulsesecure.net/support
- Find product documentation: http://www.pulsesecure.net/support
- Find solutions and answer questions using our Knowledge Base: http://www.pulsesecure.net/support
- Download the latest versions of software and review release notes: http://www.pulsesecure.net/support
- Search technical bulletins for relevant hardware and software notifications: http://www.pulsesecure.net/support
- Open a case online in the CSC Case Management tool: http://www.pulsesecure.net/support

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: http://www.pulsesecure.net/support

Opening a Case with PSGSC

- You can open a case with PSGSC on the Web or by telephone.
- Use the Case Management tool in the CSC at http://www.pulsesecure.net/support
- Call 1-888-314-5822 (toll-free in the USA, Canada, and Mexico).
- For international or direct-dial options in countries without toll-free numbers, see: http://www.pulsesecure.net/support

PART 1

Active Directory and SPNEGO Concepts

CHAPTER 1

Using Pulse Policy Secure with the SRX Series Device and Active Directory

User Role Firewall Policies

NOTE: For this service, the Junos Enforcer is an SRX Series device.

UAC Release 4.2 introduces two new features that can be used with a MAGx600-UAC-SRX license:

- A user role firewall policy that does not require an agent on endpoints that provides user role support on the SRX Series device for specific applications.
- Active Directory support that allows authenticated users with Kerberos single sign on (SSO) to access different resources without passing through Pulse policy Secure for re-authentication.

In a standard Pulse Policy Secure (UAC) deployment, users authenticate to the MAG Series Junos Pulse Gateway device (MAG Series) or an IC Series device through a sign-in page, and typically download a client, or are provisioned with agentless access through a browser.

With a MAGx600-UAC-SRX license, you can use the SRX Series device and the MAG Series device or the IC Series device to authorize users at Layer 7 using a Kerberos ticket.

NOTE: For purposes of this documentation, the MAG Series device is referenced.

You can use SRX Series user role policies with or without the MAGx600-UAC-SRX license as an alternative to resource access policies with a standard UAC license.

You create user role policies for a group on the SRX Series device. This allows you to match policies to a subset of users to specific resources or services.

You create realms and roles on the MAG Series device, and then assign users to roles through role mapping. When a SRX Series device connects with a MAG Series device, the roles you have configured are pushed to the firewall. Role-based policies on the SRX Series device match users with resources. For example, a policy could state that engineers from a particular group, or role, have access to a specific set of servers.

NOTE: You can also use SRX Series device user role policies without the MAGx600-UAC-SRX license. There is no single sign-on capability without the license.

This topic provides an overview of the solution. For complete details see UAC Solution Guide for SRX Series Services Gateways.

Related Documentation

Licensing Restrictions and Disabled Features on page 15

Supported Versions on page 20

Licensing Restrictions and Disabled Features

The following licenses are available for the Pulse Policy Secure as a policy decision point with the SRX Series device:

- MAGx600-UAC-SRX-250U (250 users)
- MAGx600-UAC-SRX-500U (500 users)
- MAGx600-UAC-SRX-5KU (5,000 users)
- MAGx600-UAC-SRX-15KU (15,000 users)
- MAGx600-UAC-SRX-EVAL (250 users, eight week evaluation)
- The following admin UI pages are hidden when the MAGx600-UAC-SRX license is applied:
- UAC: Infranet Enforcer: IPsec Routing, IP Address Pools
- Authentication Servers: all are hidden except for Active Directory and local authentication
- Endpoint Security and Host Checker

- UAC: Network Access (Layer 2 options)
- UAC: Host Enforcer
- IF-MAP Federation
- Junos Pulse and Odyssey Access Client installation option
- Agent settings for user roles

To learn more about these features please see the referenced topics in this guide. Note the following licensing restrictions:

- When a MAGx600-UAC-SRX license is attempted to be installed, no other licenses may exist (license count must be zero).
- When a MAGx600-UAC-SRX license is installed, no other licenses can be applied.
- The exception to the first two requirements is to allow installation of additional MAGx600-UAC-SRX licenses (user count is additive).
- There is no change to the default behavior in a cluster. The user count is shared and added across nodes, so the licenses should be installed in a way that balances the user count (in the event a node goes down).

NOTE: You can upgrade to a full-featured UAC by applying the appropriate license, but you must first remove the MAGx600-UAC-SRX license.

Related Documentation Configuration Summary on page 20

Terminology for Active Directory SPNEGO Authentication with User Role Policies

This section details terminology that is applicable for using Active Directory with the MAG Series device to permit single sign-on for users.

NOTE: Only Internet Explorer, Firefox (Windows and MacOS), and Google Chrome browsers are supported with SPNEGO.

Term	Description
Generic Security Service Application Program Interface (GSS-API)	The GSS-API is a generic API for performing client-server authentication. Every security system has a unique API, and the effort involved with adding different security systems to applications is extremely difficult with the variation between security APIs. With a common API, enterprises can write to the generic API, and work with any number of security systems.

	The GSS-API is included with most Kerberos 5 distributions. If a particular application or protocol supports GSS-API, then Kerberos is supported.
Simple and Protected GSS-API Negotiation (SPNEGO)	A security mechanism that enables GSS-API peers to determine whether their credentials support a common set of one or more GSS-API security mechanisms. If so, it invokes the normal security context establishment for a selected common security mechanism. This is most useful for applications that depend on GSS-API implementations and share multiple mechanisms between the peers. You must enable SPNEGO for supported browsers.
Keytab	A keytab is a file that contains pairs of Kerberos principals and encrypted keys (derived from the Kerberos password). You use this file to log in to a Kerberos system without being prompted for a password. You upload the keytab file when you create the Active Directory instance on the Pulse Connect Secure device and enable SPNEGO.
Key Distribution Center (KDC)	Part of a system intended to reduce the risk of exchanging keys. A KDC consists of an authentication server and a Ticket Granting Server (TGS).
Service Principal Name (SPN)	An SPN is the name by which a client uniquely identifies an instance of a service, in this case a Pulse Policy Secure. If you install multiple instances of a service on computers throughout a forest, each instance must have its own SPN. A given service instance can have multiple SPNs if there are multiple names that clients might use for authentication. An SPN includes the hostname of the Pulse Policy Secure device.

NOTE:

A running domain controller is required for this solution.

You must create a machine account or user account.

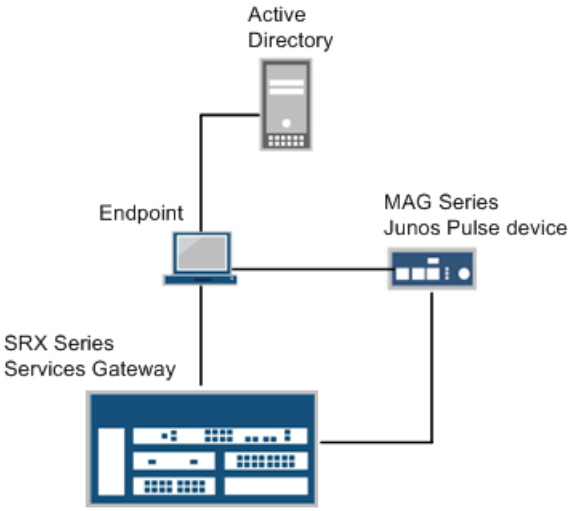
You must create a KTPass (keytab) token and import it into the Mag Series device.

Related Documentation

Configuration Summary on page 20

User Authentication Sequence for Active Directory

Figure 1: Example Configuration



The sequence that permits users to access protected resources is as follows:

- The Pulse Policy Secure device connects to the SRX Series device and pushes all of the configured roles to the firewall.
- The user endpoint connects to the domain by authentication with the Domain Controller.
- The user attempts to access an HTTP resource protected by the SRX Series device.
- There is initially no auth table entry for the user, so the SRX Series device sends a drop notification to the Pulse Policy Secure device, and the endpoint is redirected (via a HTTP Error 302 - Moved temporarily) through a captive portal.
- The endpoint sends an HTTP GET request to the Pulse Policy Secure device for authentication.
- The Pulse Policy Secure device sends the endpoint an HTTP Error 401 Unauthorized with a SPNEGO challenge.
- The endpoint retrieves a service ticket from the key distribution center for a service principle name (SPN) that matches the Pulse Policy Secure device hostname.
- The endpoint resubmits an HTTP GET request to the Pulse Policy Secure device with a SPNEGO authentication token.
- After successful SPNEGO authentication, a session is created on the Pulse Policy Secure device, and an auth table entry is pushed to the SRX Series device.

NOTE: The Pulse Policy Secure device permits single sign on by implementing the Kerberos protocol and SPNEGO.

The Pulse Policy Secure device redirects the endpoint back to the protected resource, and the endpoint successfully accesses the protected resource.

NOTE: The end user should disable pop-up blockers for the browser. The browser must be left open to ensure continued access to the protected resources.

This service enhances integration with Active Directory. When the Pulse Policy Secure challenges the endpoint with a 401 error for SPNEGO authentication, the endpoint requests a ticket from Active Directory.

The SPN used for the ticket is the Pulse Policy Secure hostname. The SPN used by the browser is in the form http/hostname. For this transaction to be successful, the SPN must be registered with Active Directory as an HTTP service using the hostname (FQDN).

NOTE: The MAG Series device hostname must be used for the SPN.

The SPN created on the Pulse Policy Secure is composed as service/<FQDN>@<REALM>.

A sample SPN: HTTP/users.resources.company.com@TESTLAB.COMPANY.COM.

When a ticket arrives in an HTTP header for validation, the SPN is used to load the password from the keytab file. This password is then used to validate the ticket.

Supported Versions

The Junos Enforcer is an SRX Series device. The Pulse Policy Secure runs on the MAG Series device or the IC Series device.

To use the SRX Series device with the Pulse Secure Access Control device for Layer 7 protection, the SRX Series device must have JunosOS Release 12.1 or greater, and the Pulse Policy Secure must have Release 4.2 or greater.

Related Documentation Licensing Restrictions and Disabled Features on page 15

CHAPTER 2

Configuring the Pulse Policy Secure Device for User Access

Configuration Summary

Following is an overview of the configuration details for this solution:

- Ensure that your Active Directory server is properly set up with a domain. Add a user and SPN that match the MAG Series device hostname. Do not select "User must change password at next logon.

  NOTE: If you are not using Active Directory as an authentication server, users must log in through the MAG Series device portal. See About Sign-In Policies.

- Set up and install the SRX Series device. See the applicable hardware guide at: http://www.juniper.net/techpubs.
- Set up the MAG Series device. See http://www.juniper.net/support/products/mag/ for hardware installation and initial network configuration.
- Connect the MAG Series device and the Junos Enforcer. See Configuring the Junos Enforcer to Communicate with the Access Control Service.
- Configure an Active Directory instance on the MAG Series device. See Using Active Directory.
  - Enable Kerberos for users.
  - Enable SPNEGO for supported browsers. Supported browsers include:
    - Internet Explorer 5.5 and later
    - Firefox 1.0 and later
    - Apache Mozilla 1.7.3 and later

- Upload a keytab file through the Active Directory configuration page in the admin console.

NOTE: Task Guidance, on the Pulse Policy Secure admin console can guide you through the basic configuration steps. Refer to the referenced topics for more detailed information.

(Optional) Configure another type of authentication server. Note that SSO is not an option unless Active Directory is used. See AAA Server Overview.

- Configure Roles on the MAG Series device. See Understanding User Roles.
- Configure Realms on the MAG Series device. See Specifying Role Mapping Rules for an Authentication Realm.
- Configure Security Policies on the SRX Series device.
- Configure Captive Portal on the SRX Series device. The MAG Series device address must match the AD SPN. See Understanding the Infranet Enforcer Captive Portal Feature.

Related Documentation User Authentication Sequence for Active Directory on page 18

Configure an Active Directory Instance on Pulse Policy Secure

To define an Active Directory server:

1. Specify a **Name** to identify the server instance.
2. Enter the **Domain**. This is the NetBIOS domain name for the organization. The NetBIOS short name can be found within Active Directory, under Users and Computers.
3. Enter the Kerberos **Realm** name. This name should be the same as the domain name in all capital letters.
4. In the Domain Join Configuration section, enter your **Username**. This is required if a machine account has not already been created.
5. Enter the corresponding **Password**.
6. Select the **Save credentials** check box. If you do not save these credentials, they are not remembered after the domain join.
7. Enter the **Container Name**. This is the name of the container in active directory in which to create the machine name.
8. Enter the **Computer Name**. The computer name field is where you specify the name that the IC Series device uses to join the specified Active Directory domain as a computer. Otherwise, leave the default identifier that uniquely identifies your system.

You may notice that the computer name is prepopulated with an entry in the format vc0000HHHHHHHH, where HHHHHHHH is a hex representation of the IP address of the IC Series device. With unique name (either the one provided by default or one of your choice) you can more easily identify your systems in the Active Directory. For example, the name can be something like vc0000a1018dF2.

In a clustered environment with the same Active Directory authentication server, this name is also unique among all cluster nodes. The IC Series device displays all of the identifiers for all attached cluster nodes.

9. The **Join Status** check box.
10. Specify the authentication protocol you are using by selecting the following check boxes:
    - **Kerberos** - This is the most secure method and is required for Kerberos Single Sign-on authentication.
    - **Enable NTLM protocol** - (This is required for password management.) Kerberos authentication is attempted first. Select one of the following options as the fallback protocol.
        - **NTLMv2** - This is a moderately secure method required for MS-CHAP authentication.
        - **NTLMv1** - This is a less secure method which you can select for existing legacy servers.
11. In the Trusts section, select the **Allow trusted domains** check box if you are allowing members of trusted domains to authenticate.
12. In the **Nested Group Search Depth** field, enter the maximum number of levels to search through when flattening nested group memberships. Note that the higher the number you use here the more impacted performance may be.
13. In the SPNEGO Single Sign On section, select the **Enable SPNEGO** check box to use the Pulse Policy Secure user role firewall policy feature. Enable SPNEGO if you are configuring the SSO feature for users. The option to upload a keytab file appears.
14. Upload the keytab that you created on the Active Directory server.
15. Click **Save Changes**.
16. Verify that you have made a successful connection with the Active Directory server by clicking the **Test Configuration** button.

CHAPTER 3

Active Directory and Kerberos

Active Directory Integration Notes

On Active Directory, there are two steps that must be performed:

- Create a dedicated user for the SPN.

NOTE: You must set a password for the user. User must change password on next logon should not be enabled, and Password never expires should be enabled.

- Add the SPN to this user using 'ktpass.exe' (this will generate the keytab).

NOTE:
The SPN must be added in this format: HTTP/hostname@REALM. The SPN is case sensitive. Note the order of upper case, lower case and upper case.
For Active Directory 2008, the commands 'ktpass' and 'setspn' are already installed. For Active Directory 2003, an add-on pack is required.
Before adding the SPN, it's a good idea to make sure it doesn't already exist. This will help avoid ticket decryption issues on Pulse Policy Secure.
On the endpoint, the MAG Series device must be added as a trusted host (with Internet Explorer or Firefox). This can also be done with an Active Directory group policy. Without this, the browser will not participate in SPNEGO.
On the MAG Series device, you must upload the keytab file and verify that the diode turns green (indicating a successful join). SPNEGO does not work unless the diode is green.

Sample Active Directory Commands

To search for a particular SPN:

C:\>setspn -Q HTTP/dev94.abc-domain.lab.test.com

To search for all the SPNs of user 'spnuser': C:\>setspn -L spnuser

To delete this SPN of user 'spnuser':

C:\>setspn -d HTTP/dev94.abc-domain.lab.test.com spnuser

In this example, the MAG Series device FQDN is: xyz.abc-domain.lab.test.com and the AD realm is: ABC-DOMAIN.LAB.JUNIPER.NET. This adds an SPN to the user:

Additional Information

The 'kerbtray.exe' program is helpful for viewing and deleting Kerberos tickets on the endpoint. Old tickets must be purged from the endpoint if SPNs are updated or passwords are changed (assuming the endpoint still has a cached copy of the ticket from a prior SPNEGO request to the MAG Series device. During testing, you should purge tickets before each authentication request.

A similar program to 'kerbtray.exe' is klist.exe. This is a command line program to view and purge tickets. This can be downloaded from Microsoft's site.

When troubleshooting, Juniper Network recommends that you restart the browser between auth requests to avoid cache issues.

If Internet Explorer pops-up a Windows dialog box during authentication, this signifies that the IC isn't trusted for SPNEGO. You should add the MAG Series device FQDN under Options -> Security -> Local Intranet -> Sites -> Advanced.

In Firefox, you can install the 'Live HTTP Headers' plug-in to monitor HTTP traffic. You should verify that the ticket is being sent as base64 data. To add the MAG Series device as a trusted host in Firefox, load URL about: config in the address window and set: network.negotiate-auth.trusted-uris.

User Log Messages on the MAG Series Device

Table 3: Understanding Log Messages Related to Active Directory and SPNEGO

Log Message: AUT30832 2012-01-30 08:41:15 - asgic15 - [10.64.105.112]System(Users)[]-Kerberosticket decodefailure(An unsupported mechanism was requested) AUT30845 2012-01-30 08:41:15 - asgic15 - [10.64.105.112] System(Users)[] - SPNEGO SSO: received 56 bytes in HTTP header 'Authorization' from 10.64.105.112	Possible Causes: The SPN does not exist on Active Directory. Note the small number of bytes sent (56). This value is normally closer to 2K bytes.
Log Message: AUT30831 2012-01-30 08:44:45 - asgic15– [10.64.105.112] System(Users)[] - Cannot load SPN 'HTTP/icvip.juniper.net@JUNIPER.NET' from keytab file (No principal in keytab matches desired name)	Possible Causes: This log indicates that the Pulse Policy Secure requested from the browser was not found in the keytab
Log Message:AUT30832 2012-01-30 09:52:15 - asgic15 -	Possible Causes: This log may indicate that the SPN was updated on Active Directory, but Pulse Policy

[10.64.105.112] System(Users)[] - Kerberos ticket decode failure (Unknown code FF 163)	Secure is still using an older keytab
Log Message:AUT30832 2012-01-30 08:34:58 - asgic15 - [10.64.105.112] System(Users)[] - Kerberos ticket decode failure (Unknown code FF 161)	Possible Causes: The Active Directory user's password associated with the SPN has changed. Pulse Policy Secure cannot join the domain; the diode must be green (if you are using Windows 2008).

Index