SENTINET

API Security Management

SENTINET

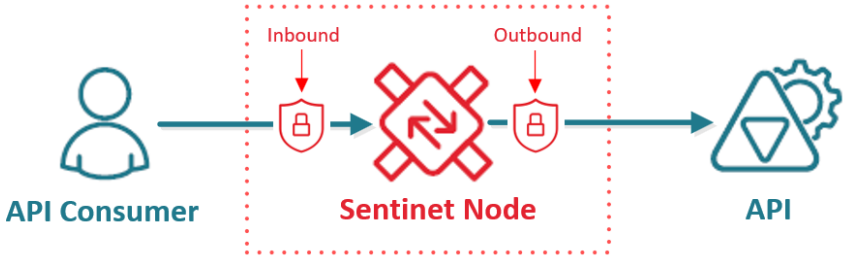
Nevatech

Contents

Introduction

Nevatech Sentinet™ API Management helps developers build, provide and consume APIs using both industry standard and custom security models. Developers can delegate some, or all of the responsibilities to handle security on behalf of the API Provider or API Consumer applications to Sentinet. These API Security Management capabilities provided by Sentinet tremendously reduce time and efforts on developing, testing and operating APIs in secure environments.

Sentinet manages security independently at both the Inbound and the Outbound message flows (see diagram below), when passing through Sentinet Nodes (API Gateways), therefore creating the opportunity to pass through security and/or mediate (translate) security between API Consumers and backend APIs.



Security Models

Inbound or outbound message flows can implement and enforce many different security authentication models with different user credentials and security token types. These can be industry standard authentication schemes and security tokens, as well as custom security models. Sentinet enforces both authentication and authorization to ensure complete end-to-end security.

Authentication

Sentinet supports standard and custom authentication schemes for both RESTful APIs and SOAP services. Tables below provide high-level overview of available options.

For RESTful APIs		
Security Token Type	Authentication Model	Security Level
Username/Password	Basic Authentication	Transport
Username/Password	Windows Integrated	Transport
Username/Password	Custom	Transport, Message
X.509 Certificate	Single-sided SSL	Transport
X.509 Certificate	Mutual SSL	Transport
JWT	OAuth/OpenID Connect	Transport
Kerberos, NTLM	Windows Integrated	Transport
API Keys	Custom	Transport, Message
Custom Tokens	Custom	Transport, Message

For SOAP Services		
Security Token Type	Authentication Model	Security Level
Username/Password	Basic Authentication	Transport
Username/Password	WS-Security	Message (XML SOAP Header)
Username/Password	Windows Integrated	Transport
Username/Password	Custom	Transport, Message
X.509 Certificate	Single-sided SSL	Transport
X.509 Certificate	Mutual SSL	Transport
X.509 Certificate	WS-Security	Message (XML SOAP Header)
Kerberos, NTLM	Windows Integrated	Transport
Kerberos, NTLM	Windows Integrated	Message (XML SOAP Header)
SAML	WS-Security	Message (XML SOAP Header)
JWT	OAuth/OpenID Connect	Transport

Authorization

Sentinet provides unique capabilities to create simple to complex Authorization/Access Rules. These can be configured graphically using the Sentinet Console and its Access Rules Designer with a drag-and-drop user interface. Sentinet remotely and securely delivers designed Access Rules to the Sentinet Nodes (API Gateway), where they are executed at runtime to enforce Authorization logic. A Sentinet Access Rule is a combination of Access Rule conditions, that ultimately grant or deny access to an API or some of its parts (ex. operations or endpoints). Available Access Rule conditions are listed below:

1. Logical **Any** (or), **And All** (and) and **Not** (not).
2. Username/Password identity
3. Windows Active Directory user identity
4. Windows Active Directory Group membership
5. Claims validation (ex: validation of claims in JWT tokens issued by OAuth servers, such as Azure Active Directory, Google, Twitter, Facebook, Salesforce, or any other OAuth server conforming to the OAuth specifications).
6. Request URL validation that can validate any parts of the request URL including paths and query parameters (ex. API keys as query parameters)
7. HTTP Headers validation
8. HTTP Method validation
9. Message body validation using Regular expression
10. Message body validation using XPath
11. Date/Time schedule validation
12. Allowed or restricted client IP addresses validation
13. Access validation by Operation(s') name(s).

14. Custom Authorization validation rules and conditions implemented in .NET code, and configured with Sentinet graphical Access Rules Designer.

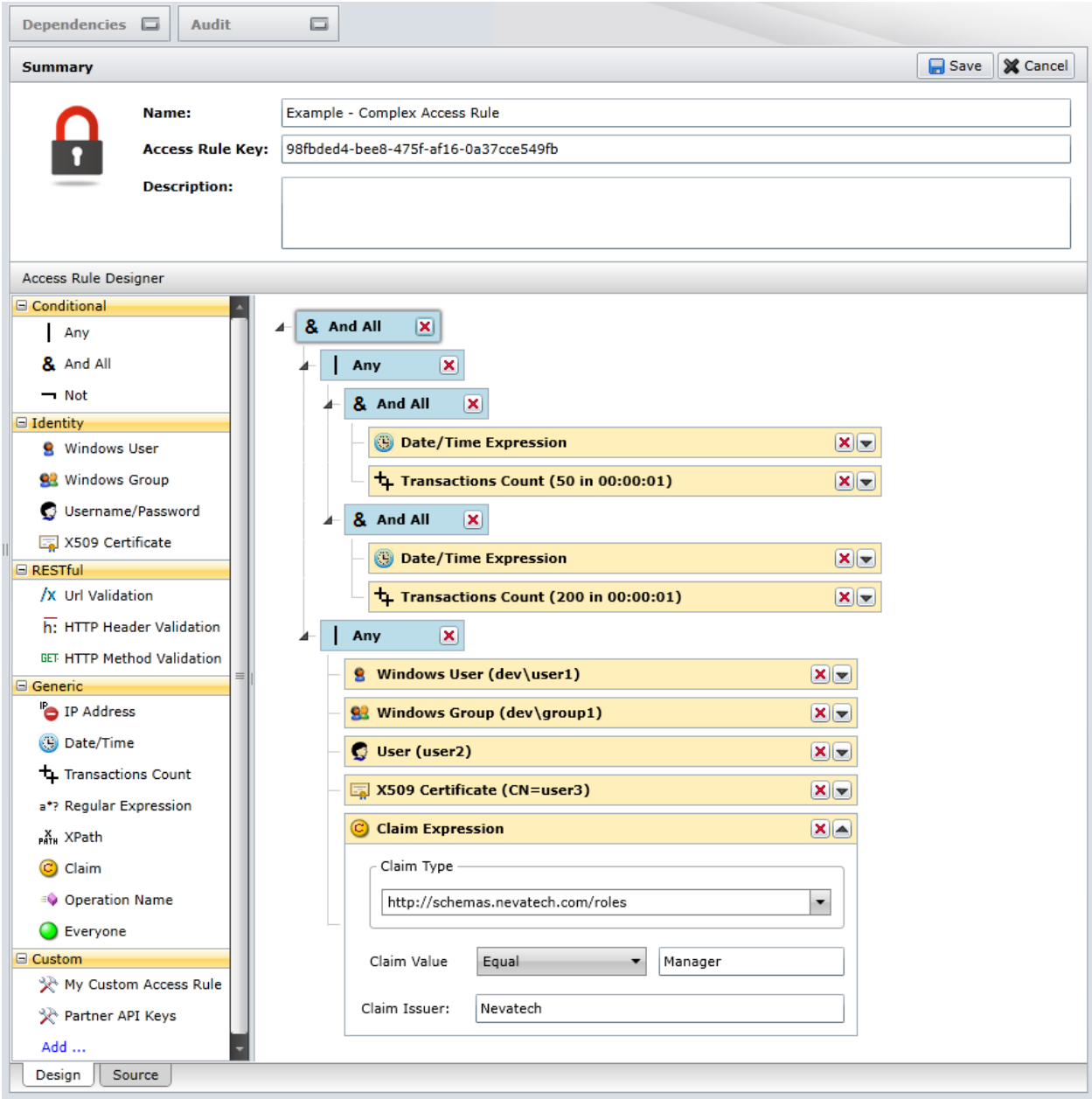
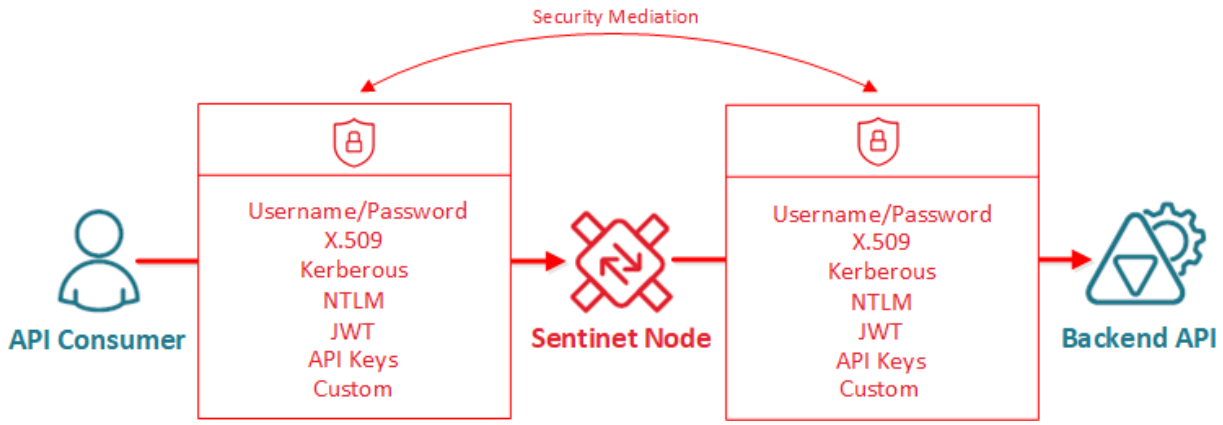


Figure. Example – Complex Access Rule configured in the graphical Access Rules Designer

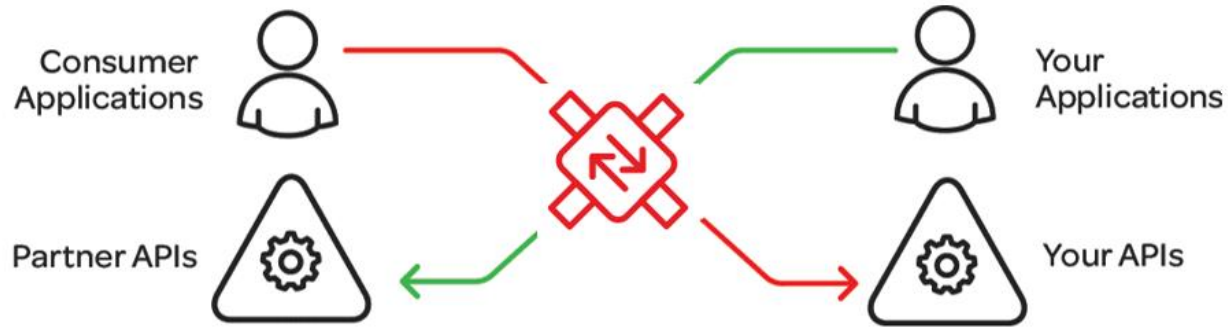
Security Mediation and Translation

Sentinet can mediate and translate the security of both request and response messages while they are passing through the Sentinet Nodes (API Gateways). Inbound and Outbound security models can be the same, or they can be very different. For example, an on-premises backend API may require Windows Integrated security authentication with local Active Directory, while it is exposed externally as an API requiring Username/Password, X.509 certificate, OAuth JWT token and/or API Keys.



Bidirectional Security Management

Sentinet's security management benefits are bidirectional. Sentinet Nodes will protect your API applications with required security, and they will help your API consumer applications to implement security required by somebody else's (for example partner) APIs.



Security Identities Management

Sentinet can either passthrough API consumer identities or convert them from one identity type into another. For example, Username/Password, Windows identities, JWT token, API Keys can all be passed through Sentinet Nodes from the API Consumer to the backend API. At the same time, with Security Mediation and Translation, Sentinet can use an inbound Username/Password to generate the outbound Kerberos token, or replace inbound claims in a JWT token with a specific X.509 certificate required by

the outbound security. Many security token types, listed in the Authentication section above, can interchangeably replace one another, while the messages are being processed by the Sentinet Nodes.