

JUNIPER SESSION SMART NETWORKING ADVANCED SECURITY PACK DATASHEET

Product Overview

The Juniper Session Smart Router's Advanced Security Pack integrates security functionality into the routing fabric. The unique, state-of-the-art security offering provides:

URL filtering to prevent access to and from specific sites and to meet special business requirements

An **Intrusion Detection and Prevention System (IDS/IPS)** to protect against advanced malicious attacks.

An extensive Intrusion Detection and Prevention (IDP) signature database for state-of-the-art protection against the most up-to-date vulnerabilities.

Product Description

[Juniper® SD-WAN driven by Mist AI™](#) has built-in capabilities to provide sophisticated security services from every router in the network. The solution uses the Session Smart™ Router (SSR) and includes deny-by-default access based on application policies that ensure zero-trust access control to the networking fabric.

Built on Juniper's patented [Secure Vector Routing \(SVR\)](#) technology, this guaranteed secure coupling of users and their applications is unique in the industry. The tunnel-free protocol enables a 30% to 50% reduction in bandwidth costs, and includes an adaptive encryption feature, ensuring that the user experience is not sacrificed as a result of needless double encryption and overhead.

Juniper® Session Smart™ Router's [Advanced Security Pack](#) (Figure 1) integrates further security functionality into the routing fabric:

- URL filtering prevents access to and from specific sites and to meet special business requirements.
- An Intrusion Detection and Prevention System (IDS/IPS) protects against advanced malicious attacks.



Figure 1: Foundational SSR router security and the Advanced Security Pack

These features eliminate the need for additional security appliances at the branch, providing this enhanced functionality within the Juniper Mist ecosystem of Wired, Wireless, and SD-WAN. If more cloud-integrated security is needed, customers have the option of adding the [Juniper Secure Edge](#) to the environment.

Features and Benefits

The IDS/IDP and URL filtering functionality in the Advanced Security Pack is made possible with the following features:

- Policy establishment maps the policies for networks and their users to applications and destinations; this ensures that applications can only be accessed by permitted users
- Event filtering and capturing provides information on attacks and their threat levels; operators are continually aware of current security attacks and threats

- Signature database mapping provides further information on vulnerabilities, along with how to apply appropriate protections

Wherever you are in your security journey with AI-Driven SD-WAN, Session Smart Networking functions will add the needed features for your evolving needs.

Establishing Policies

With the Advanced Security Pack, policies are established for all network users and outside resources; examples include applications, services, and web sites (Figure 2).

NAME	NETWORK / USER (MATCHING ANY)	ACTION	APPLICATION / DESTINATION (MATCHING ANY)	IDP
AcceptableUse	Corp	Block	All-Categories	Strict
CorporateAccess	Corp	Allow	DataCenter	None
Malware	Corp	Block	Malware	Strict
POS-EdgeCompute-POS-Server	POS	Allow	EdgeCompute-POS-Server	None
POS-EdgeCompute	POS	Allow	EdgeCompute	None
SocialMediaCorp	Corp	Block	SocialMedia	Strict

Figure 2: Policy to Restrict Social Media Access for Corporate Employees

Filtering and Capturing Events

The Advanced Security Pack filters and captures relevant events (Figure 3).

Time	Device Name	Site	Source Address	Source Port	Source Interface	Destination Address	Destination Port	Destination Interface	Attack Name	Threat Severity	Action
3/17/2023, 11:58:47 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	58266	ge-0-1	35.182.119.134	554	ge-0-2	HTTP_INVALID_METHOD_HTTP-VER	Major	close
3/17/2023, 11:58:47 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	58266	ge-0-1	35.182.119.134	554	ge-0-2	HTTP_INVALID_METHOD_HTTP-VER	Minor	close
3/17/2023, 11:58:47 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	58264	ge-0-1	35.182.119.134	554	ge-0-2	HTTP_INVALID_METHOD_HTTP-VER	Major	close
3/17/2023, 11:58:47 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	58264	ge-0-1	35.182.119.134	554	ge-0-2	HTTP_INVALID_METHOD_HTTP-VER	Minor	close
3/17/2023, 11:58:47 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	58250	ge-0-1	35.182.119.134	554	ge-0-2	HTTP_INVALID_METHOD_HTTP-VER	Major	close
3/17/2023, 11:58:47 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	58250	ge-0-1	35.182.119.134	554	ge-0-2	HTTP_INVALID_METHOD_HTTP-VER	Minor	close
3/17/2023, 11:58:10 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	37444	ge-0-1	35.182.119.134	7070	ge-0-2	TROJANBACKORFICE-BO2K-CONNECT	Major	close
3/17/2023, 11:56:39 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	50232	ge-0-1	35.182.119.134	554	ge-0-2	HTTP_INVALID_METHOD_HTTP-VER	Minor	close
3/17/2023, 11:56:39 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	47252	ge-0-1	35.182.119.134	7070	ge-0-2	HTTP_INVALID_METHOD_HTTP-VER	Major	close
3/17/2023, 11:56:39 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	47224	ge-0-1	35.182.119.134	7070	ge-0-2	HTTP_INVALID_METHOD_HTTP-VER	Minor	close
3/17/2023, 11:56:39 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	50216	ge-0-1	35.182.119.134	554	ge-0-2	HTTP_INVALID_METHOD_HTTP-VER	Major	close
3/17/2023, 11:56:39 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	47224	ge-0-1	35.182.119.134	7070	ge-0-2	HTTP_INVALID_METHOD_HTTP-VER	Minor	close
3/17/2023, 11:56:39 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	50216	ge-0-1	35.182.119.134	554	ge-0-2	HTTP_INVALID_METHOD_HTTP-VER	Minor	close
3/17/2023, 11:56:39 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	38654	ge-0-1	35.182.119.134	554	ge-0-2	HTTP_INVALID_METHOD_HTTP-VER	Major	close
3/17/2023, 11:56:39 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	38648	ge-0-1	35.182.119.134	554	ge-0-2	HTTP_INVALID_METHOD_HTTP-VER	Minor	close
3/17/2023, 11:56:39 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	38648	ge-0-1	35.182.119.134	554	ge-0-2	HTTP_INVALID_METHOD_HTTP-VER	Minor	close
3/17/2023, 11:56:39 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	38636	ge-0-1	35.182.119.134	554	ge-0-2	HTTP_INVALID_METHOD_HTTP-VER	Minor	close
3/17/2023, 11:56:39 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	38636	ge-0-1	35.182.119.134	554	ge-0-2	HTTP_INVALID_METHOD_HTTP-VER	Major	close
3/17/2023, 11:56:14 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	42084	ge-0-1	35.182.119.134	7070	ge-0-2	TROJANBACKORFICE-BO2K-CONNECT	Major	close
3/17/2023, 11:56:43 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	50592	ge-0-1	35.182.119.134	554	ge-0-2	HTTP_INVALID_METHOD_HTTP-VER	Minor	close
3/17/2023, 11:56:43 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	60950	ge-0-1	35.182.119.134	7070	ge-0-2	HTTP_INVALID_METHOD_HTTP-VER	Minor	close
3/17/2023, 11:56:38 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	37028	ge-0-1	35.182.119.134	554	ge-0-2	HTTP_INVALID_METHOD_HTTP-VER	Major	close
3/17/2023, 11:56:38 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	37028	ge-0-1	35.182.119.134	554	ge-0-2	HTTP_INVALID_METHOD_HTTP-VER	Minor	close

Figure 3: Captured Events from IDP and URL Filtering

Matching Against a Signature Database

These events may be matched against a signature database that contains definitions of attack objects and application signatures defined in the form of an IDP policy rule set (Figure 4). This rule set is updated regularly by automatically downloading the latest definitions and application signatures.

Signature Detail	
Short Name	TROJAN:BACKORFICE-BO2K-CONNECT
Severity	Major
Recommended	False
Recommended Action	Drop
False Positive	Unknown
Category	TROJAN
Standard Ports	TCP/6000-10000,31337
Keywords	2000 Back CVE-1999-0660 Client Connection Orifice bid:1648
Release Date	10/16/2003
Signature Version	3336
Supported Platforms	mx-12.3 mx-19.3 mx-19.4 snx-12.3 snx-19.3 snx-19.4 snx-branch-12.3 snx-branch-19.3 snx-branch-19.4 vmx-19.3 vmx-19.4 vnx-12.3 vnx-19.2 vnx-19.4 vnx3bsd-19.2 vnx3bsd-19.4

Figure 4: IPS signature for a detected vulnerability

The SSR router is thus able to provide cutting-edge security solutions for your network. When vulnerabilities are discovered, you can either have your router alerted to the vulnerability or block the traffic. This provides you with the network protection you require, without the need to purchase specialized appliances that add complexity.

Meeting You Where You Are

Juniper Networks wants to meet you where you are when it comes to your network security. The Advanced Security Pack can thus be installed standalone or alongside a Juniper Networks® [SRX Series Firewall](#) at your branch or data center.

The Advanced Security Pack can also be used to help you with your [SASE Journey](#) giving you protection in the branch or data center before easily offloading that traffic to an SSE such as the [Juniper Secure Edge](#).

Ordering Information

To order the Advanced Security Pack and access software licensing information, please visit the How to Buy page at <https://www.juniper.net/us/en/how-to-buy/form.html>.

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions, and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable, and secure networks to move at the speed of business.

Corporate and Sales Headquarters

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA

Phone: 888.JUNIPER (888.586.4737)

or +1.408.745.2000

www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.
Boeing Avenue 240 1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands

Phone: +31.207.125.700

