





Product Overview

The Juniper Session Smart Router's Advanced Security Pack integrates security functionality into the routing fabric. The unique, state-of-theart 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 upto-date vulnerabilities.

JUNIPER SESSION SMART NETWORKING ADVANCED SECURITY PACK DATASHEET

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 <u>Secure Vector Routing (SVR)</u> 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 <u>Advanced Security Pack</u> (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 <u>Juniper Secure Edge</u> 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 Al-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).

Application Policy						
1 h						Save Canc
Search				Add App	lication Policy	Edit Applications
	NETWORK / USER (IAATCHING ANY)	ACTION	APPLICATION / DESTINATION IMATCHING ANY			
AcceptableUse	+ Corp ×	 ×>	AUP-Categories × AUP-Domains × +		•	0
CorporateAccess	+ Corp ×	$- \checkmark$	DataCenter1 × +	None	-	0
Malware	+ Corp ×	— x —>	Malware × +	Strict	-	0
POS-EdgeCompute-POS-Server	+ Pos ×	$-\!$	EdgeCompute-POS-Server ×	None	-	0
POSEdgeCompute	+ POS ×	$-\!$	EdgeCompute × +	None	-	0
SocialMediaCorp	+ Corp ×	— x —>	SocialMedia × 🕈	Strict	•	0
	https://www.internet.org/accessionalized/acce	Image: Second Se Second Second Sec	Mark Methods Markets And Algebraton Paloses Methods Markets And Constant And C	Depuny of 4 bank deplacion Prices MM ATRONK JUST SMACRAMM ATRONK ATRONK JUST SMACRAMM ATRONK JUST SMACRAM ATRONK JUST SMACRAM ATRONK JUS	Name Access Access <td>Desproy of a load Application Protest Attention Application Protest Attention Application Protest Attention Application Protest Participation Protest</td>	Desproy of a load Application Protest Attention Application Protest Attention Application Protest Attention Application Protest Participation Protest

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).

Centre WAN Edge LDP/URL Events Optimization	128 TECHNOLOGY				_		_				FRL 12:27 F
No. Str. Northers Str. Northers	ecure WAN E	dge IDP/l	JRL Events	org (Entire Or	8) 🔹 💽	URL Filtering	Hour 7 Hours 24 Hou	rs			
International Part Name	ter 9.										
D3170221.1156/744 Date data Date Additation Date Additatio						93 Total	Critical 42 Major	51 Minor 0 In	0		
D3170221.1156/744 Date data Date Additation Date Additatio											
91770221,1154/74M bali-dalla Dalla-Hittack 10.9147/100 5426 pe-1 55182,11314 554 pe-02 HTTPRULD_MITHCD_UMME Home 91770221,11546/74M bali-dalla Dalla-Hittack 10.9147/100 12.91211/114 554 pe-02 HTTPRULD_MITHCD_UMME Home 91770221,11547/4M bali-dalla Dalla-Hittack 10.9147/100 12.902 pe-1 55182,1191,114 554 pe-02 HTTPRULD_MITHCD_UMME Home 91770221,11547/M bali-dalla Dalla-Hittack 10.9147/100 12.902 pe-1 55182,1191,114 554 pe-02 HTTPRULD_MITHCD_UMME Home 91770221,115168/ M bali-dalla Dalla-Hittack 10.9147/100 12.922 pe-1 55182,1191,114 707 pe-02 HTTPRULD_MITHCD_UMME Home 91770221,115168/ M bali-dalla Dalla-Hittack 10.9147/100 12.922 pe-1 55182,1191,114 707 pe-02 HTTPRULD_MITHCD_UMME Home 91770221,115168/ M bali-dalla Dalla-Hittack 10.9141,110 12.911	lime	Device Name	Site	Source Address	Source Port	Source Interface	Destination Address	Destination Port	Destination Interface	Attack Name	Threat Severity
D3170221,115.847AM balt-datas Dials-Hitask. 10.9147/100 S542 ge-01 S5182.1151.114 S54 ge-02 HTTP/NULD_MENDO_IMAGE Mong 9170221,115.8477AM balt-datas Datas-Hitask. 10.9147/100 S5182.1151.114 S54 ge-02 HTTP/NULD_MENDO_IMAGE Mong 9170221,115.8477AM balt-datas Datas-Hitask. 10.9147/100 S5182.1151.114 S54 ge-02 HTTP/NULD_MENDO_IMAGE Mong 9170221,115.8477AM balt-datas Datas-Hitask. 10.9147/100 S5182.1151.114 S54 ge-02 HTTP/NULD_MENDO_IMAGE Mong 9170221,115.8477AM balt-datas Datas-Hitask. 10.9147/100 S5182.1151.114 S70 ge-02 HTTP/NULD_MENDO_IMAGE Mong 9170221,115.8477AM balta-datas Datas-Hitask. 10.9041/100 S722 ge-01 S5182.1151.114 770 ge-02 HTTP/NULD_MENDO_IMAGE Mong 9170221,115.8477AM balta-datas Datas-Hitask. 10.9041/170 S226 ge-01 S5182.1151.114 770 ge-02 HTTP/N	1/17/2023, 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://WALID:MSNG-HTTP-VER	 Major
39/72021,1158/744 beh-dellas Dalles-Hilback 10.00,171/00 554 ge-01 25.112.115.114 554 ge-02 HTTPSVULU_METHOD_UMME below 39/72021,1158/744 beh-dellas Dalles-Hilback 10.00,171/00 3520 ge-01 25.112.115.114 554 ge-02 HTTPSVULU_METHOD_UMME below 39/72021,1158/74 beh-dellas Dalles-Hilback 10.00,171/00 2744 ge-01 25.112.115.114 554 ge-02 HTTPSVULU_METHOD_UMME below 39/72021,1158/74 beh-dellas Dalles-Hilback 10.00,171/00 2744 ge-01 25.112.115.114 7070 ge-02 HTTPSVULU_METHOD_UMME below 39/72021,1158/74 beh-dellas Dalles-Hilback 10.00,171/00 4722 ge-01 25.112.115.114 7070 ge-02 HTTPSVULU_METHOD_UMME below 39/72021,1158/74 beh-dellas Dalles-Hilback 10.00,171/00 4724 ge-01 25.112.115.114 7070 ge-02 HTTPSVULU_METHOD_UMME below 39/72021,1156556 beh-dellas D	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_NAME	Minor
D2172021,1158,47A4 bab-datas Date-MBask 1005147.100 5429 ge-1 5512,1151,114 554 ge-0 HTTP:WULD:MSHeiTT-WB Mage D2172021,1158,47A4 bab-datas Date-MBask 1005,117,100 12829 ge-01 55112,1151,114 554 ge-02 HTTP:WULD:MSHeiTT-WB Mage D2172021,1156,07A4 bab-datas Date-MBask 1005,117,100 12829 ge-01 55112,1151,114 554 ge-02 HTTP:WULD:MSHEID:WULD:WHITE Mage D2172021,1156,07A4 bab-datas Date-MBask 1005,117,100 12822 ge-01 55112,1151,114 777 ge-02 HTTP:WULD:MSHEID:WWLD:WHITE Mage D1720221,1156,05A4 bab-datas Date-MBask 1005,117,100 12822 ge-01 55112,1151,114 777 ge-02 HTTP:WULD:WHITE:WULD:	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://WALID:MSNG-HTTP-VER	Major
DV770521,1158,47A4 bab-datas Date-MBask 1000,117,100 5455 ge-61 55182,1151,114 554 ge-62 HTTPANULD_MTHOD_LVMM Filter DV770521,1158,104 /K bab-datas Date-MBask 1000,117,100 2444 ge-61 35182,1151,114 7770 ge-62 TTGPANGCONTCEIDDSCONTECT Segan DV770521,1158,104 /K bab-datas Date-MBask 1000,117,100 2722 ge-61 35182,1151,114 7770 ge-62 HTTPANULD_MTHOD_LVMM More DV770521,1156,104 /K bab-datas Date-MBask 1000,117,100 2722 ge-61 35182,1151,114 7770 ge-62 HTTPANULD_MTHOD_LVMM More DV770521,1156,104 /K bab-datas Date-MBask 1000,117,100 2724 ge-61 35182,1151,114 7770 ge-62 HTTPANULD_MTHOD_LVMM More DV770221,1156,104 /K bab-datas Date-MBask 1000,117,100 2846 ge-61 35182,1151,114 754 ge-62 HTTPANULD_MTHOD_LVMM More DV770221,11555,104 /K bab-datas Date-MBask	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_NAME	Minor
Physical 158104M Mail-Addisa Dallac-Mitsuk 10.914-7100 27.44 ge-01 35.112.113.131 27.07 ge-02 PHICHNELDCORNECTED02KCONNECT Mappin V172022, 1158.04 M Mail-Addisa Dallac-Mitsuk 10.914.7100 2022 ge-01 35.112.113.131 54 ge-02 PHTTPANULD_MICLO_LINKE Marce V172022, 1158.04 M Mail-Addisa Dallac-Mitsuk 10.914.7100 27.22 ge-01 35.112.113.131 27.07 ge-02 PHTTPANULD_MICLO_LINKE Marce	8/17/2023, 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://WALID:MSNG-HTTP-VER	 Major
Dyr.2022, 1156,393.44 beh-dafks Dafks-Mitsuck 189,147,100 5222 ge-01 53,182,113,134 554 ge-02 HTTPS/NULD_MITHCD_UMME Enters V172022, 1156,397.44 beh-dafks Dafks-Mitsuck 189,417,100 5222 ge-01 53,182,115,134 777 ge-02 HTTPS/NULD_MITHCD_UMME Marce V172022, 1156,397.44 beh-dafks Dafks-Mitsuck 199,417,100 2722 ge-01 53,182,115,134 777 ge-02 HTTPS/NULD_MITHCD_UMME Marce Marce <t< td=""><td>v/17/2023, 11:58:47 AM</td><td>lab1-dallas</td><td>Dallas-FullStack</td><td>10.90.147.100</td><td>58250</td><td>ge-0-1</td><td>35.182.119.134</td><td>554</td><td>ge-0-2</td><td>HTTP://WALID_METHOD_NAME</td><td>Minor</td></t<>	v/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://WALID_METHOD_NAME	Minor
17172021,1156.39 AM bab databa Databa Palibaak 1955,147,110 4722 ge-01 53,182,115,134 7070 ge-02 HTTP:NULD_METHICD_LIMME Bataba 17172022,1156,053 AM bab databa Databa Palibaak 1955,147,110 47224 ge-01 53,182,115,134 7070 ge-02 HTTP:NULD_METHICD_LIMME Bataba 17172022,1156,053 AM bab databa Databa Palibaak 1955,147,100 47224 ge-01 53,182,115,1134 7070 ge-02 HTTP:NULD_METHICD_LIMME Bataba 17172022,1156,053 AM bab databa Databa Palibaak 1955,147,100 4724 ge-01 53,182,115,1134 7070 ge-02 HTTP:NULD_METHICD_LIMME Bataba 1717202,1156,053 AM bab databa Databa Palibaak 1950,147,100 2844 ge-01 53,182,115,1134 554 ge-02 HTTP:NULD_METHICD_LIMME Bataba 1717202,1155,054 AM bab databa Databa Palibaak 1950,147,100 2844 ge-01 53,182,115,1134 54 ge-02 HTTP:NULD_METHICD_LIMME Bataba 1717202,1155,	/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	TROJAN:BACKORIFICE:B02K-CONNECT	Major
17172021,1156.25 AM bali-datas Datas-Adfisuo, 10.95.47.10 422.4 ge-0.1 53.182.115.134 2010 ge-0.2 HTTP:NNULDMSHG-HTT-VR5 Edage 17172022,1156.25 AM bali-datas Datas-Adfisuo, 10.95.47.100 20214 ge-0.1 53.182.115.134 54 ge-0.2 HTTP:NNULDMSHG-HTT-VR5 Edage 17172022,1156.25 AM bali-datas Datas-Adfisuo, 10.95.47.100 52214 ge-0.1 53.182.115.134 54 ge-0.2 HTTP:NNULDMSHG-HTT-VR5 Edage 17172022,1156.25 AM bali-datas Datas-Adfisuo, 10.95.47.100 5221 ge-0.1 53.182.115.134 54 ge-0.2 HTTP:NNULDMSHG-HTT-VR5 Edage 17172022,1156.25 AM bali-datas Datas-Adfisuo, 10.95.47.100 524 ge-0.1 53.182.115.134 54 ge-0.2 HTTP:NNULDMSHG-HTT-VR5 Edage 17172022,1156.25 AM bali-datas Datas-Adfisuo, 10.95.47.100 364 ge-0.1 53.182.115.134 54 ge-0.2 HTTP:NNULDMSHG-HTT-VR5 Edage 17172022,1155.05 AM <t< td=""><td>/17/2023, 11:56:39 AM</td><td>lab1-dallas</td><td>Dallas-FullStack</td><td>10.90.147.100</td><td>50232</td><td>ge-0-1</td><td>35.182.119.134</td><td>554</td><td>ge-0-2</td><td>HTTP://WALID_METHOD_NAME</td><td>Minor</td></t<>	/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://WALID_METHOD_NAME	Minor
University Solution	/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://WALID_METHOD_NAME	Minor
1772022,1156.35 AM babi-dallas Dallas-Millsack. 19.95.47.100 4724 ge-01 35.182.115.134 7070 ge-02 HTTP:NNULD_MTHCD_LMMIL € More 7772022,1156.35 AM babi-dallas Dallas-Millsack. 19.95.47.100 2026 ge-01 35.182.115.134 554 ge-02 HTTP:NNULD_MTHCD_LMMIL € More 7772022,1155.05 AM babi-dallas Dallas-Millsack. 19.05.47.100 2046 ge-01 35.182.115.134 554 ge-02 HTTP:NNULD_MTHCD_LMMIL € More 7772022,1155.05 AM babi-dallas Dallas-Millsack. 19.05.47.100 3844 ge-01 35.182.115.134 554 ge-02 HTTP:NNULD_MTHCD_LMMIL € More 7772022,1155.05 AM babi-dallas Dallas-Millsack. 19.05.47.100 3864 ge-01 35.182.115.134 554 ge-02 HTTP:NNULD_MTHCD_LMMIL € More 7772022,1155.05 AM babi-dallas Dallas-Millsack. 19.05.47.100 3864 ge-01 35.182.115.134 554 ge-02 HTTP:NNULD_MTHCD_LMMIL € More 7772022,1105.05 AM	/17/2023, 11:56:35 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	47224	ge-0-1	35.182.119.134	7070	ge-0-2	HTTP://WALID:MSNG-HTTP-VER	Major
3/17/2021, 15563/AM bali-dallar Daller-Mittakk 1000, 147,100 5021 ge-01 35.182,115,114 554 ge-02 HTTPRVDLD_MITHOD_MARE More 3/17/2021, 15563/AM bali-dallar Daller-Mittakk 1000, 147,100 3684 ge-01 35.182,115,114 554 ge-02 HTTPRVDLD_MITHOD_MARE Mare 3/17/2021, 15563/AM bali-dallar Daller-Mittakk 1000, 147,100 3684 ge-01 35.182,115,114 554 ge-02 HTTPRVDLD_MITHOD_MARE Mare 3/17/2021, 15563/AM bali-dallar Daller-Mittakk 1000, 147,100 3684 ge-01 35.182,115,114 554 ge-02 HTTPRVDLD_MITHOD_MARE Mare 3/17/2021, 15563/AM bali-dallar Daller-Mittakk 1000, 147,100 3654 ge-01 35.182,115,114 554 ge-02 HTTPRVDLD_MITHOD_MARE Mare 3/17/2021, 15563/AM bali-dallar Daller-Mittakk 1000, 147,100 3656 ge-01 35.182,115,114 54 ge-02 HTTPRVDLD_MITHOD_MARE Mare 3/17/2021, 15563/AM bali-dallar Daller-Mittakk 1000, 147,100 3656 ge-01 35.182,115,114 54 ge-02 HTTPRVDLD_MITHOD_MARE Mare 3/17/2021, 15563/AM bali-dallar <td< td=""><td>3/17/2023, 11:56:35 AM</td><td>lab1-dallas</td><td>Dallas-FullStack</td><td>10.90.147.100</td><td>50216</td><td>ge-0-1</td><td>35.182.119.134</td><td>554</td><td>ge-0-2</td><td>HTTP://WAUD:MSNG-HTTP-VER</td><td> Major </td></td<>	3/17/2023, 11:56:35 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	50216	ge-0-1	35.182.119.134	554	ge-0-2	HTTP://WAUD:MSNG-HTTP-VER	 Major
Unit 2021, 1055.90 AM beh -dalka: Dalke - Mittaski, 10.90, 47,100 3854 ge-01 35.182, 119,134 554 ge-02 HTTP/NULD/MING-HTT-VHT Major V170222, 1056.90 AM beh -dalka: Dalke - Mittaski, 10.90, 47,100 3864 ge-01 35.182, 119,134 554 ge-02 HTTP/NULD/MING-HTT-VHT Major V170222, 1056.90 AM beh -dalka: Dalke - Mittaski, 10.90, 47,100 3864 ge-01 35.182, 119,114 554 ge-02 HTTP/NULD/MING-HTT-VHT Major V170222, 1056.90 AM beh -dalka: Dalke - Mittaski, 10.90, 47,100 3864 ge-01 35.182, 119,114 554 ge-02 HTTP/NULD/MING-UMME Monor V170222, 10.556.90 AM beh -dalka: Dalke - Mittaski, 10.90, 47,100 3864 ge-01 35.182, 119,114 554 ge-02 HTTP/NULD/MING-UMME Monor V170222, 10.556.91 AM beh -dalka: Dalke - Mittaski, 10.90, 47,100 3864 ge-01 35.182,119,114 554 ge-02 HTTP/NULD/MING-UMME Monor V170222, 10	v17/2023, 11:56:35 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	47224	ge-0-1	35.182.119.134	7070	ge-0-2	HTTP://WALID_METHOD_NAME	Minor
D172022,105580.M ball-datas Datas-Mitsuki 110.05.17.100 3864 ge-01 35.182.191.134 554 ge-02 HTTPINUULDMENGHTTVER Major D172022,105580.M ball-datas Datas-Mitsuki 100.51.7.100 3864 ge-01 35.182.191.134 554 ge-02 HTTPINUULDMENGHTTVER Major D172022,105580.M ball-datas Datas-Mitsuki 100.51.7.100 3864 ge-01 35.182.191.134 554 ge-02 HTTPINUULDMENGO_UMME Mitor D172022,105580.M ball-datas Datas-Mitsuki 100.51.7.100 3866 ge-01 35.182.1191.144 554 ge-02 HTTPINUULDMENGO_UMME Mitor D172022,105580.M ball-datas Datas-Mitsuki 100.51.7.100 3856 ge-01 35.182.1191.144 554 ge-02 HTTPINUULDMENGO_UMME Mitor D172022,105580.M ball-datas Datas-Mitsuki 100.51.7.100 3856 ge-01 35.182.1191.144 554 ge-02 HTTPINUULDMENGOUNCHT Major D172022,105580.M ball-datas Datas-Mitoski 100.51.7.100 3856 ge-01 35.182.1191.144	3/17/2023, 11:56:35 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	50216	ge-0-1	35.182.119.134	554	ge-0-2	HTTP://WALID_METHOD_NAME	Minor
Dir.2022, 105520 AM ball-dallas Dallas-Mitsack 10.00 ± 47.100 3864 ge-01 35.182.119.134 554 ge-02 HTTPSVDLD_METHOD_MAKE Behory V172022, 105520 AM ball-dallas Diale-Mitsack 10.00 ± 47.100 3864 ge-01 53.182.119.134 554 ge-02 HTTPSVDLD_METHOD_MAKE More V172022, 105520 AM ball-dallas Diale-Mitsack 10.00 ± 47.100 3864 ge-01 53.182.119.134 54 ge-02 HTTPSVDLD_METHOD_MAKE More V172022, 105520 AM ball-dallas Diale-Mitsack 10.00 ± 47.100 3869 ge-01 53.182.119.134 54 ge-02 HTTPSVDLD_METHOD_MAKE More V172022, 105520 AM ball-dallas Diale-Mitsack 10.00 ± 47.100 3806 ge-01 53.182.119.134 54 ge-02 HTTPSVDLD_MENGLOMENG Mager V172022, 105530 AM ball-dallas Diale-Mitsack 10.00 ± 47.100 3804 ge-01 53.182.119.134 779 ge-02 HTTPSVDLD_MENGLOMENGLOMENG Mager V172022, 105543 AM ball-d	3/17/2023, 10:58:50 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	38654	ge-0-1	35.182.119.134	554	ge-0-2	HTTP://WALID:MSNG-HTTP-VER	Major
U1720221,105830 AM babi-datas Datas-Attissack 10.90.147.100 3164 ge-01 35.182.119.114 554 ge-02 HTTPINVLID_METHICO_LAMME Mmore U1720221, 105830 AM babi-datas Datas-Attissack 10.90.147.100 3660 ge-01 35.182.119.114 554 ge-02 HTTPINVLID_METHICO_LAMME Mmore U1720221, 105830 AM babi-datas Datas-Attissack 10.90.147.100 3680 ge-01 35.182.119.114 554 ge-02 HTTPINVLID_METHICO_LAMME Mmore U1720221, 105840 AM babi-datas Datas-Attissack 10.90.147.100 3680 ge-01 35.182.119.114 554 ge-02 HTTPINVLID_MERACOBINECEDOSCONDECCT Magore U1720221, 105840 AM babi-datas Datas-Attissack 10.90.147.100 3690 ge-01 35.182.119.114 7070 ge-02 HTTPINVLID_MERACOBINECEDOSCONDECCT Magore U1720221, 10544 AM babi-datas Datas-Attissack 10.90.147.100 69059 ge-01 35.182.119.114 7070 ge-02 HTTPINVLID_METHICO_LAMME Manore	8/17/2023, 10:58:50 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	38648	ge-0-1	35.182.119.134	554	ge-0-2	HTTP://WALID:MSNG-HTTP-VER	Major
DV72022, 105580 AM balt-dafiles Dafile-Millskek 10.00 x17,100 3865 ge-01 35.182.119.114 554 ge-02 HTTPINVLID_MITHOD_VLMME Memor DV72022, 105580 AM balt-dafiles Dafile-Millskek 10.00 x17,100 3865 ge-01 35.182.119.114 554 ge-02 HTTPINVLID_MITHOD_VLMME Memor DV72022, 105580 AM balt-dafiles Dafile-Millskek 10.00 x17,100 3865 ge-01 35.182.119.114 554 ge-02 HTTPINVLID_MITHOD_VLMME Memor DV72022, 105580 AM balt-dafiles Dafile-Millskek 10.00 x17,100 3265 ge-01 35.182.119.114 554 ge-02 HTTPINVLID_MITHOD_VLMME Major DV72022, 105580 AM balt-dafiles Dafile-Millskek 10.00 x17,100 2690 ge-01 35.182.119.114 7070 ge-02 HTTPINVLID_MITHOD_VLMME Memor DV72022, 105560 AM balt-dafiles Dafile-Millskek 10.30 x17,100 2690 ge-01 35.182.119.114 7070 ge-02 HTTPINVLID_MITHOD_VLMME Memor	3/17/2023, 10:58:50 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	38654	ge-0-1	35.182.119.134	554	ge-0-2	HTTP://WALID_METHOD_NAME	Minor
University Disker-Mitsuck Disker-Mits	8/17/2023, 10:58:50 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	38648	ge-0-1	35.182.119.134	554	ge-0-2	HTTP://WAUD_METHOD_NAME	Minor
9/17/2023, 1058/14 M bb1-dallas Dallas-Aulfsack 10.90.147.100 42044 ge-01 35.182.119.134 7079 ge-02 TRG/MESACCORNECE 0.94ger 9/17/2023, 1056/43 M bb1-dallas Dallas-Aulfsack 10.90.147.100 50592 ge-01 35.182.119.134 554 ge-02 HTTP://WULD.METHOD_UMME ● Minor 9/17/2023, 1056/43 AM bb1-dallas Dallas-Aulfsack 10.90.147.100 60599 ge-01 35.182.119.134 7079 ge-02 HTTP://WULD.METHOD_UMME ● Minor	J/17/2023, 10:58:50 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	38636	ge-0-1	35.182.119.134	554	ge-0-2	HTTP://WALID_METHOD_NAME	Minor
1/17/2021, 105643 AM lab1-dallas Dallas-Aultisack 10.90.147.100 50592 ge-01 25.112.119.134 554 ge-02 HTTP://WULD.METHOD.WAME ● Minor 9/17/2023, 105643 AM lab1-dallas Dallas-Aultisack 10.90.147.100 60550 ge-01 25.112.119.134 7070 ge-02 HTTP://WULD.METHOD.WAME ● Minor	J/17/2023, 10:58:50 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	38636	ge-0-1	35.182.119.134	554	ge-0-2	HTTP://WALID:MSNG-HTTP-VER	Major
2/17/2023, 10:55:43 AM lab1-dallas Dallas-FulStack 10:90.147.100 60950 ge-0-1 35.182.119.134 7070 ge-0-2 HTTP:NVAUD_METHOD_NAME Minor	3/17/2023, 10:58:14 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	42084	ge-0-1	35.182.119.134	7070	ge-0-2	TROJAN:BACKORIFICE:B02K-CONNECT	Major
	3/17/2023, 10:56:43 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	50592	ge-0-1	35.182.119.134	554	ge-0-2	HTTP://WALID_METHOD_NAME	Minor
N17/2023, 10:56:38 AM lab1-dallas Dallas-FullStack 10:90:147.100 37028 ge-0-1 35:182.119.134 554 ge-0-2 HTTP:INVALID:MSNG-HTTP:VER • Major	3/17/2023, 10:56:43 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	60950	ge-0-1	35.182.119.134	7070	ge-0-2	HTTP://WALID_METHOD_NAME	Minor
	3/17/2023, 10:56:38 AM	lab1-dallas	Dallas-FullStack	10.90.147.100	37028	ge-0-1	35.182.119.134	554	ge-0-2	HTTP://WALID:MSNG-HTTP-VER	Major

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.

						United	l States 🗸	Contact U	Log Ir	
	Why Juniper?	Products & Solutions	Support	Training		Search .	luniper.ne	t	۹	
ome / Security / Threat	t Labs / IPS Signatures									
Signature Det	ail							f	У	\geq
TROJAN: Back Orifice	e 2000 Client Conn	ection				Short Name	TROM	AN:BACKORIFI	CE-BO2K	CONNE
		Back Orifice 2000 (BO2K) essful connection to a server				Severity	Major	an.brickonan	CLIDOEN	CONINE
standard BO2K port. It a	llows a remote attack	er to take control of the infe	ected host.			Recommended	False			
Extended Description						Recommended	Drop			
Voyager will follow relati	ve paths passed to it	er demo disk contains sever in requests. This includes/	style paths, wh	nich will allow		False Positive	Unkno	own		
Voyager to serve pages outside of the "document root". Another vulnerability is that the web server does not have sufficient security restrictions - this means that the web server can access any file,				Category	TROJ	AN				
including protected files and special /dev entries. As well, due to the integration of the web browser and web server, information used by the Photon GUI is easily exposed by requesting files under				Standard Ports	TCP/6	000-10000,31	337			
/ photon/. Additionally. html files generated by the web browser (error messages, for example) and the QNX configuration interface share the same directory as published html files. While the Voyager web server is not intended to be used in a production environment, and is in fact intended only to be a demo of the ONX oS, users should be aware of these design errors.				Keywords		Back CVE-199 e bid:1648	9-0660 Cli	ent Conr		
demo of the QNX OS, us	sers should be aware	of these design errors.				Release Date	10/16	/2003		
Affected Products						Sigpack Version	3336			
Qssl voyager References Bugfraq: 1648 CVE: CVE: 1299-0666 URL: http://secunia.cc rifice2000.trojan.html	om/virus_information	/4619 http://www.sarc.com	n/avcenter/ven	c/data/back.o		Supported Platforms	srx-br srx-br vmx-1 vmx-1 vsrx-1 vsrx-1 vsrx-1	1.3 1.4 1.3 1.3 1.4 1.4 1.4 1.4 1.4 1.5 1.5 1.5 1.5 1.5 1.5 1.5 1.5 1.5 1.5		

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® <u>SRX Series</u> <u>Firewall</u> at your branch or data center.

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

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



Driven by Experience

Copyright 2023 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.