Juniper Networks and IPv6

Tim LeMaster

Ipv6.juniper.net

www.juniper.net

IPv6 Leadership

IPv6 supported in Junos since 2001

IPv6 supported in ScreenOS since 2004

First router to be IPv6 Certified by DoD/ JITC in 2006

First firewall to be IPv6 Certified by DoD/ JITC in 2008

Extensive Additional IPv6 testing as part of DoD UC APL Program

Participated in many IPv6 test events including IPv6 Logo, Moonv6, and others

Juniper Networks currently deployed in many IPv6 Networks including DREN and ESNET

Juniper Networks plays a leadership role in the IETF including IPv6 development issues

Juniper USGv6 Router and Switch Status

Juniper M/MX/T Routers finished

- JUNOS 10.4 or above

Juniper EX switches testing in progress

- EX 3200, 4200, 8200
- JUNOS 10.4 or above

- http://www.iol.unh.edu/services/testing/ipv6/usgv6tested.php?company=873&type=#eqplist

USGv6 Firewall Status

Branch SRX (SRX100 – SRX650)

- Router tests and FW test have begun with Junos 11.1 software
- Expect completion in 4-6 months

ScreenOS

- Testing to begin this month
- UNH Lab uses an IPv6 enabled Juniper Networks ISG to protect the lab

High End SRX (SRX1400- SRX5800)

- Plan to start testing late summer/early fall 2011 time frame
- Limitation is test slots at lab

IPv6 Support by Release

ScreenOS 6.1- Adds IPv6 Support for:

- SSG140, SSG320M/350M, SSG520/520M, and SSG 550/550M
- ISG1000 and 2000 both support IPv6 with 512K sessions on devices with 1GB memory
- SYN-Proxy & SYN-Cookie mechanisms are supported for v6
- IPv6 is supported on E1/T1, E3/T3, and 2M-serial interfaces on SSG platforms
- IPv6 Support added for Sun and MS RPC ALGs, SIP, and RTSP ALGs
- Following screen features for v6 supported on SSG and ISG platforms:
    - Source IP limit
    - UDP flood Prevention
    - Per policy session limit
    - DNS-ALG

IPv6 Support added in 6.2

ISG1000-IDP and ISG 2000-IDP support IPv6 traffic

BGP for IPv6 Supported

Transparent Mode for IPv6

Support for IPv4 over IPv6 IPSec, IPv6 over IPv4 Ipsec, and IPv6 over IPv6 Ipsec.

NSRP for IPv6 Support

DHCPv6 Relay support

MLDv1

IPv6 Support Added in ScreenOS 6.3

OSPFv3

Ability to Inhibit AAAA Requests over IPv4

IPv6 Prefix and DNS Information Update

IPv6 Full Support on ISG-IDP

- Packet capture and packet logs for IPv6 traffic
- Configure header match info for v6 traffic and ICMPv6 messages
- IPv6 tracerout anomaly
- IPv6 log messages in the NSM log viewer

NSA IPv6 Testing of ScreenOS Firewalls

Excerpt of a test of ISG 2000 Firewall with ScreenOS 6.0

“The Juniper Networks ISG 2000 Firewall is a very stable platform with strong internal functionality.

Its strengths are in the security triad of Confidentiality, Integrity, and Availability.

The IPv6 developers at Juniper have produced a network protection device that was able to pass 100% of the IPv6-oriented test procedures.

It is built for speed on its interfaces, with any delay caused by longer Access Control Lists and signatures for its deep packet inspection being negligible.

It did well defending itself and the test network from common attacks. “

NSM and ScreenOS

In order to completely manage IPv6 configuration from NSM, the minimum version requirements are as follows:

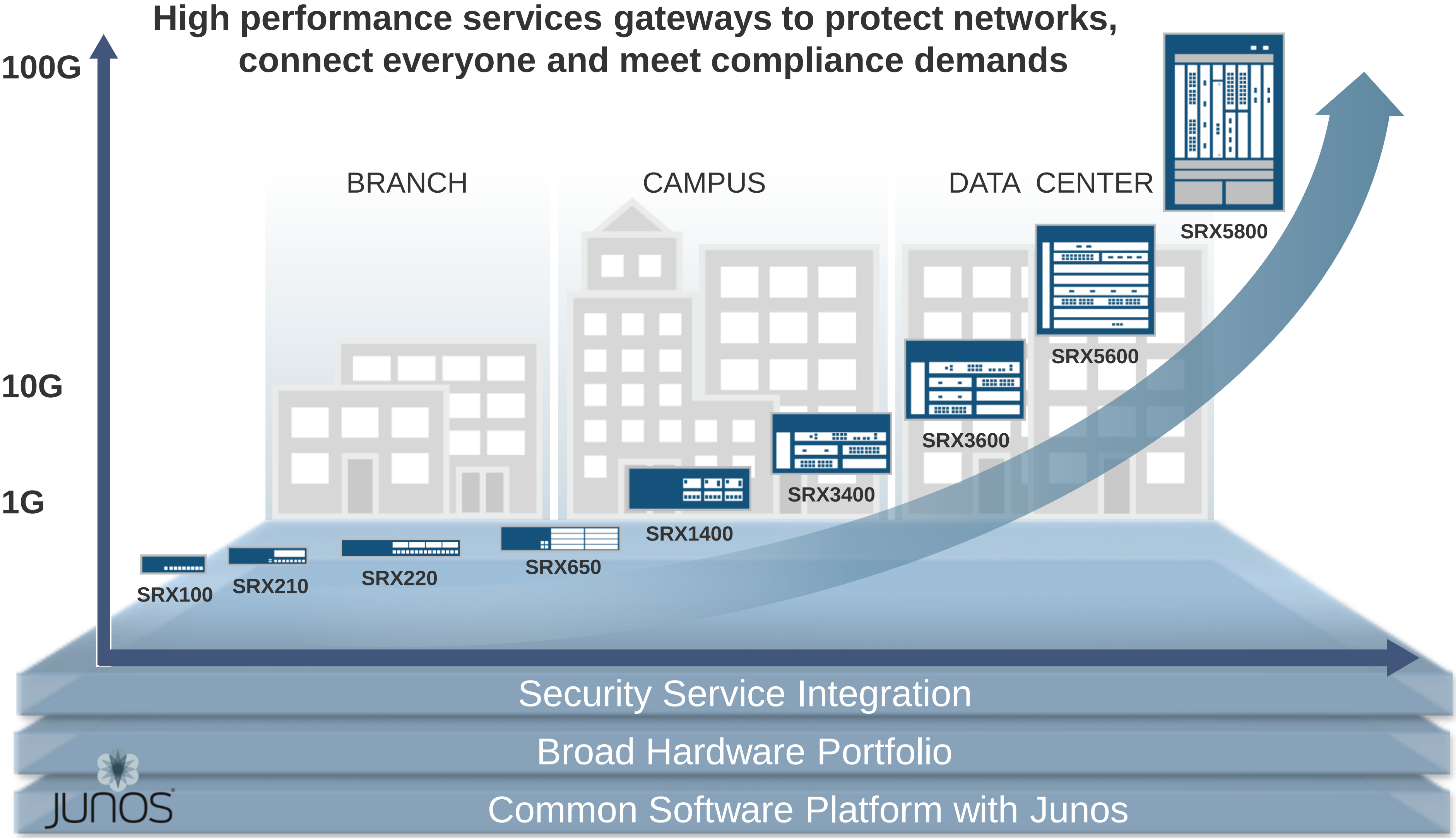
- NSM 2009.1r1 and later
- ScreenOS 6.3 and later

Even though ScreenOS 6.1 version supports IPv6, it actually does not send IPv6 configuration as part of the configuration data file to NSM.

Due to this behavior, NSM will not be able to understand that the device has IPv6 enabled.

Only in 6.3.x version onwards does ScreenOS devices send IPv6 configuration information to NSM as part of config data file.

Security Foundation with SRX


High performance services gateways to protect networks,
connect everyone and meet compliance demands
100G
10G
1G
BRANCH
CAMPUS
DATA CENTER
SRX100
SRX210
SRX220
SRX650
SRX1400
SRX3400
SRX3600
SRX5600
SRX5800
Security Service Integration
Broad Hardware Portfolio
Common Software Platform with Junos
JUNOS

IPv6: Operational support

Features

- Link/Global Address Configuration
- ICMPv6
- Active/Passive HA
- SSH
- Telnet
- Syslog
- J-Web
- SNMP
  - IPv6 MIBs
  - Transport

Futures

- LSYS (Logical System)
- USGv6 certification
- Active/Active HA

IPv6: Firewall Support

Features

- Policy Controls
  - Support for zone based firewall policies
  - Allow and deny policies
- Threat Mitigation
  - Screens
  - IDP
  - ALG (FTP/TFTP, DNS)

IPv6: Transport

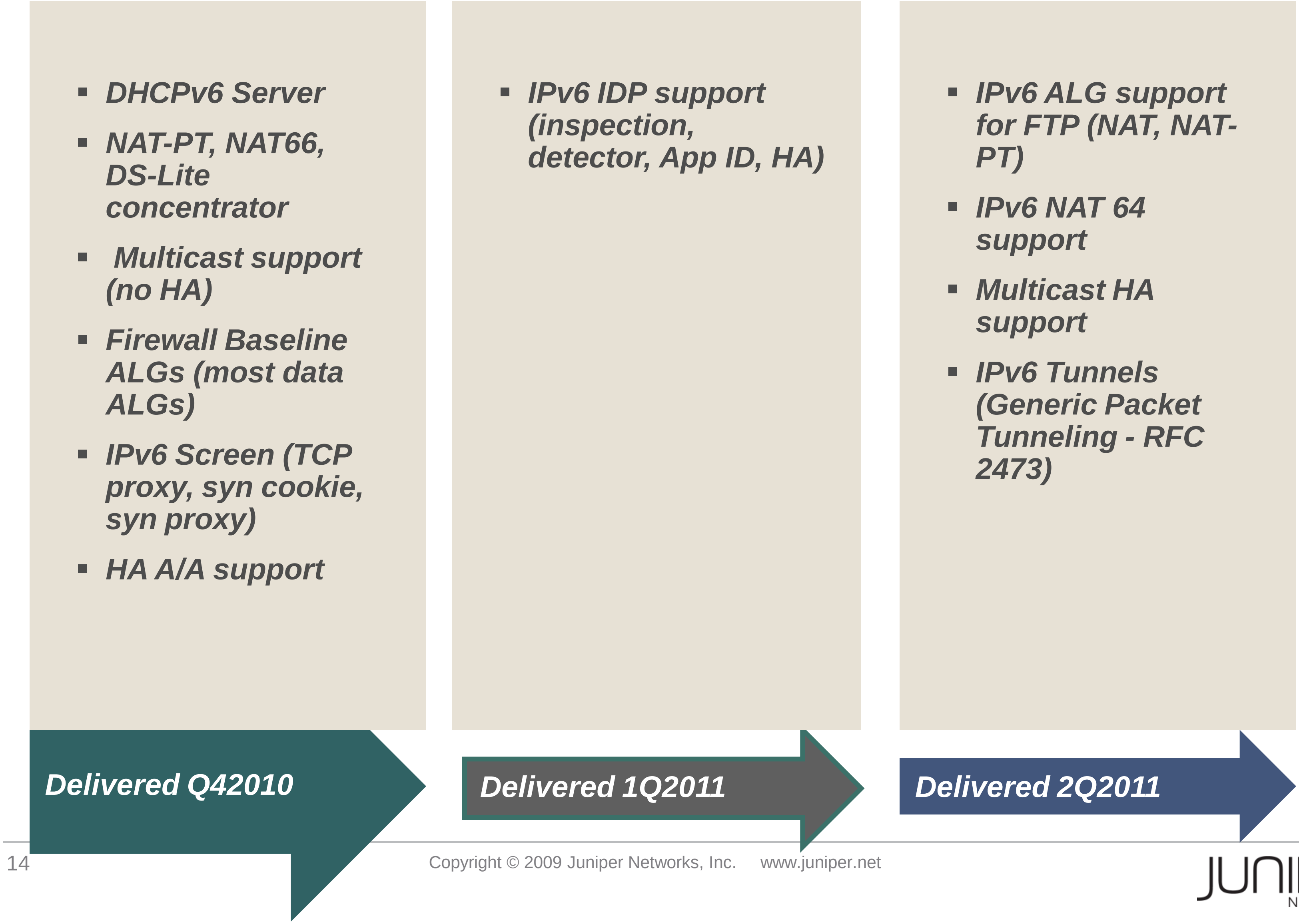
Features

- IPSec (branch 6in6)
- GRE/IP-IP Tunnel (HE 6in4)
- NAT
  - CG-NAT
  - NAT-PT
  - NAT 64
- DHCPv6 Server
- Routing Protocol (Static, RIP, BGP, OSFP and IS-IS on High End)
- IPv6 over PPP (Branch)

Futures

- IS-IS support (branch)
- DS-Lite initiator
- 6RD
- 4in6 Tunnel support
- Transparent mode
- IPSec for IKEv2/v1 High End
- DHCPv6 Client
- DHCPv6 Relay

JUNOS IPv6 Delivered Roadmap



- *DHCPv6 Server*
- *NAT-PT, NAT66, DS-Lite concentrator*
- *Multicast support (no HA)*
- *Firewall Baseline ALGs (most data ALGs)*
- *IPv6 Screen (TCP proxy, syn cookie, syn proxy)*
- *HA A/A support*

Delivered Q42010

- *IPv6 IDP support (inspection, detector, App ID, HA)*

Delivered 1Q2011

- *IPv6 ALG support for FTP (NAT, NAT-PT)*
- *IPv6 NAT 64 support*
- *Multicast HA support*
- *IPv6 Tunnels (Generic Packet Tunneling - RFC 2473)*

Delivered 2Q2011

JUNOS IPv6 Committed Roadmap (continued)

- *Firewall Auth, Web Auth IPv6 support*
- *IS-IS IPv6*

2H2011

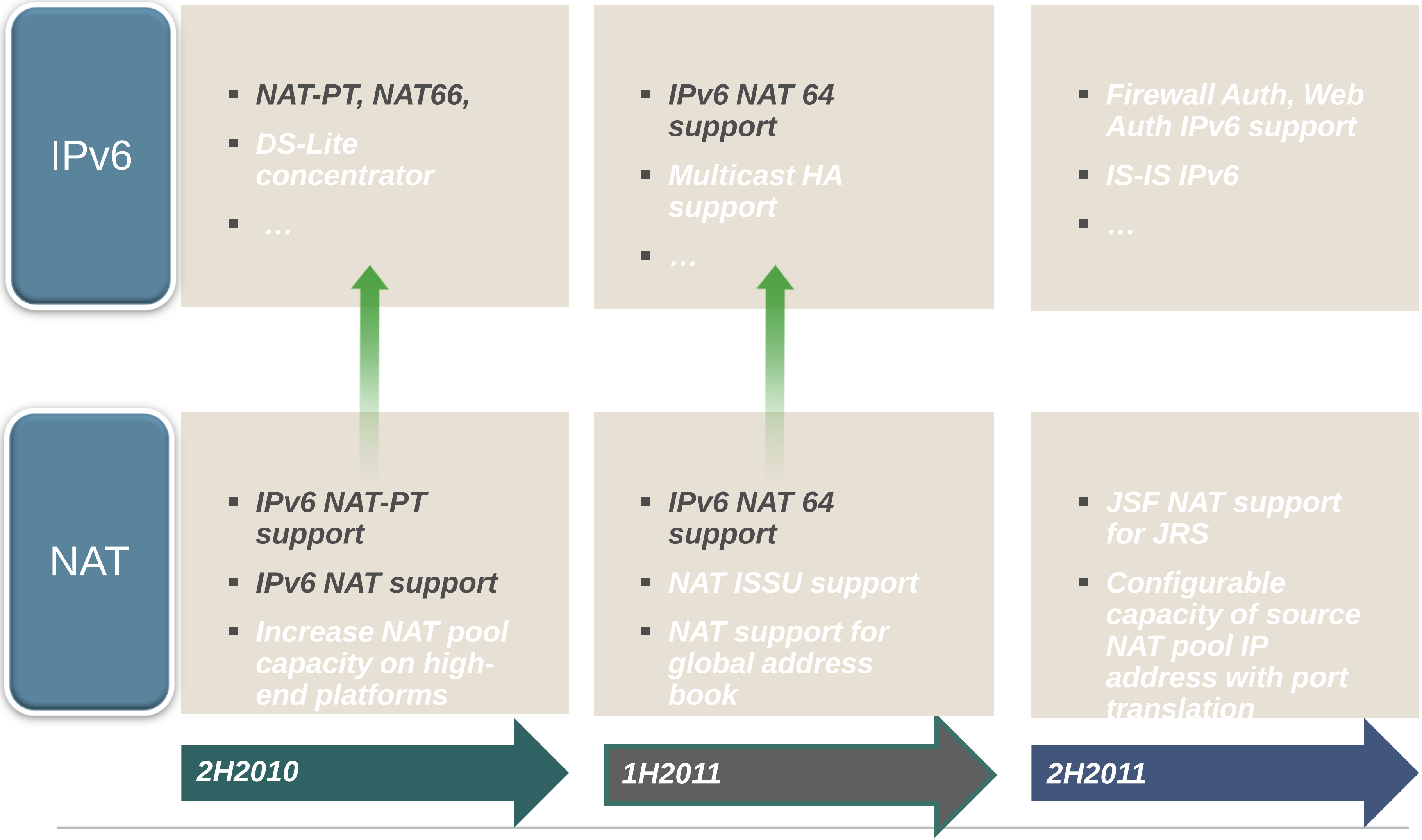
- *Logical System -- IPv6 support: DS-lite concentrator support*
- *USGv6*

1H2012

- *TBD*

2H2012

IPv6/CGN TRANSITION



IPv6

2H2010

- NAT-PT, NAT66,
- DS-Lite concentrator
- …

1H2011

- IPv6 NAT 64 support
- Multicast HA support
- …

2H2011

- Firewall Auth, Web Auth IPv6 support
- IS-IS IPv6
- …

NAT

2H2010

- IPv6 NAT-PT support
- IPv6 NAT support
- Increase NAT pool capacity on high-end platforms

1H2011

- IPv6 NAT 64 support
- NAT ISSU support
- NAT support for global address book

2H2011

- JSF NAT support for JRS
- Configurable capacity of source NAT pool IP address with port translation

NSM Features and Configuration – ScreenOS & JUNOS

Management of

- Firewall/VPN: Netscreen Firewalls
- Integrated Firewall / IDP: SRX, ISG, SSG
- J-Series Routers

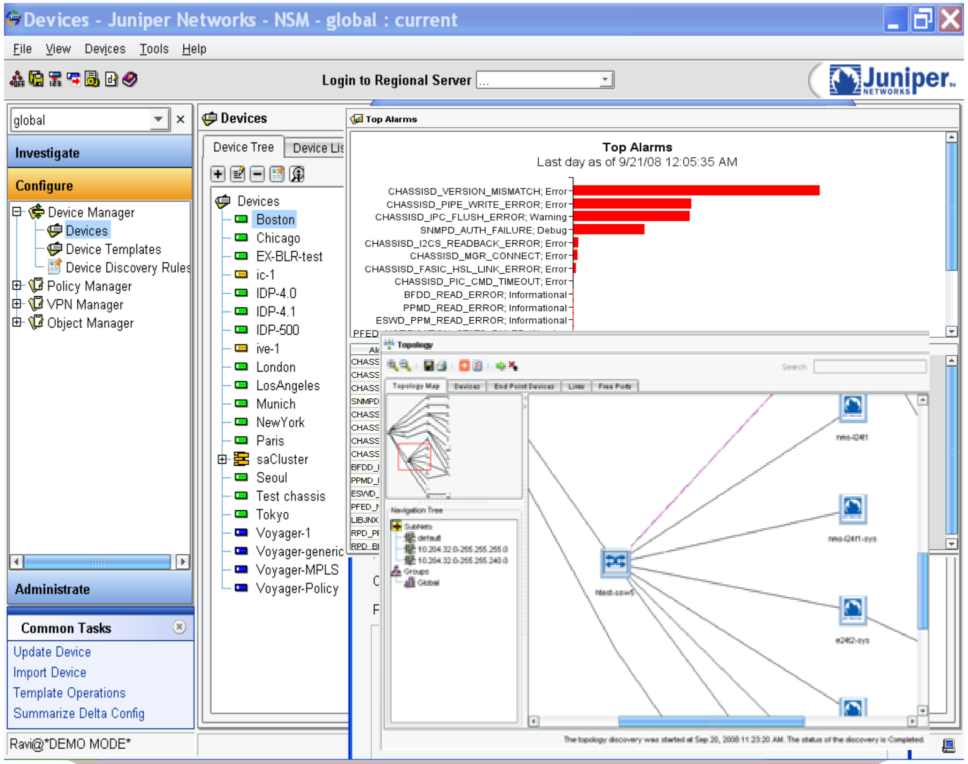
Configuration support for all device features

Improve Operational Efficiency

- VPN Manager
- Policy Manager
- Templates
- Topology Discovery
- Configuration Change Management and version control

Simplify IT Maintenance and Monitoring

- Software Management
- Hardware Inventory Monitoring
- Security Updates
- Event Visibility Management
- Real-time Monitoring status of Device, VPN



The topology discovery was started at Sep 20, 2008 11:23:20 AM. The status of the discovery is Completed.

NSM IPv6 Support

Support in 2009.1 for Netscreen

- ScreenOS 6.3

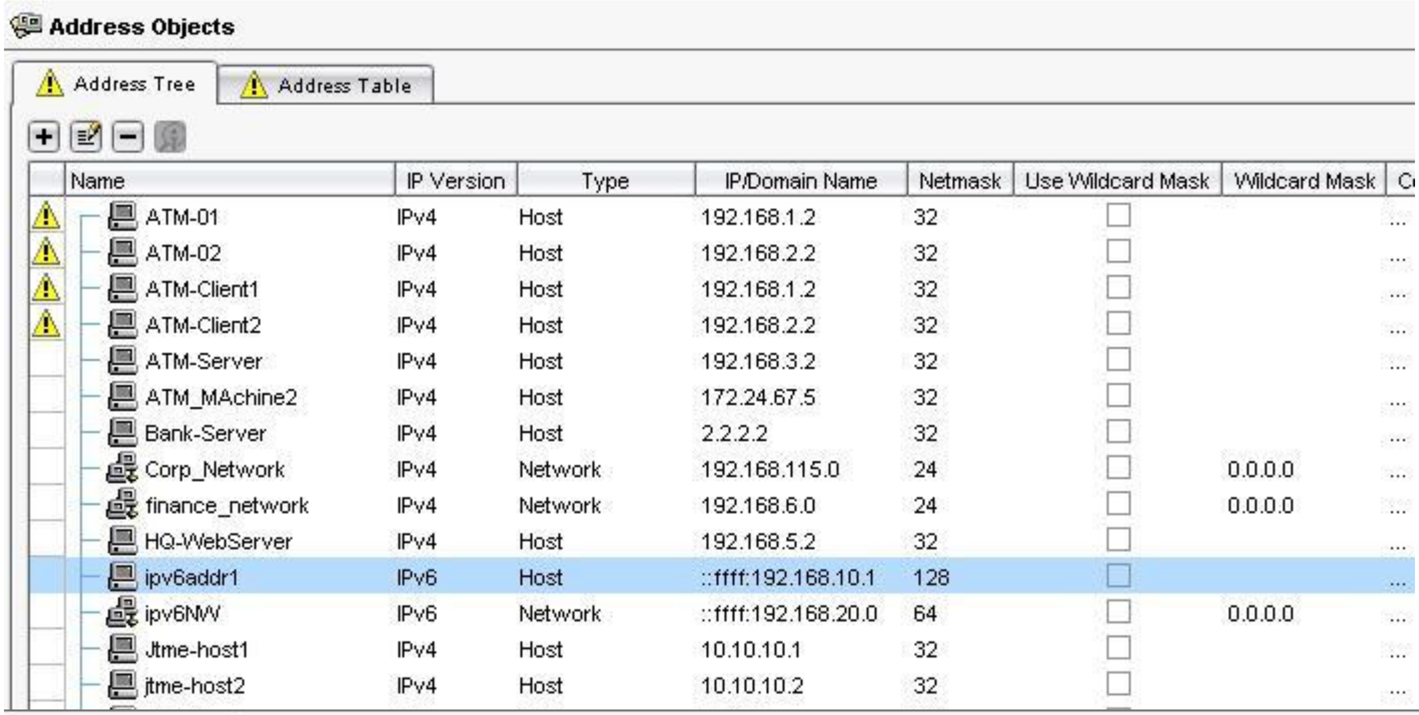
Support in 2010.1 for JUNOS

- JUNOS 10.2 (and above)

Support for IPv6 configuration in

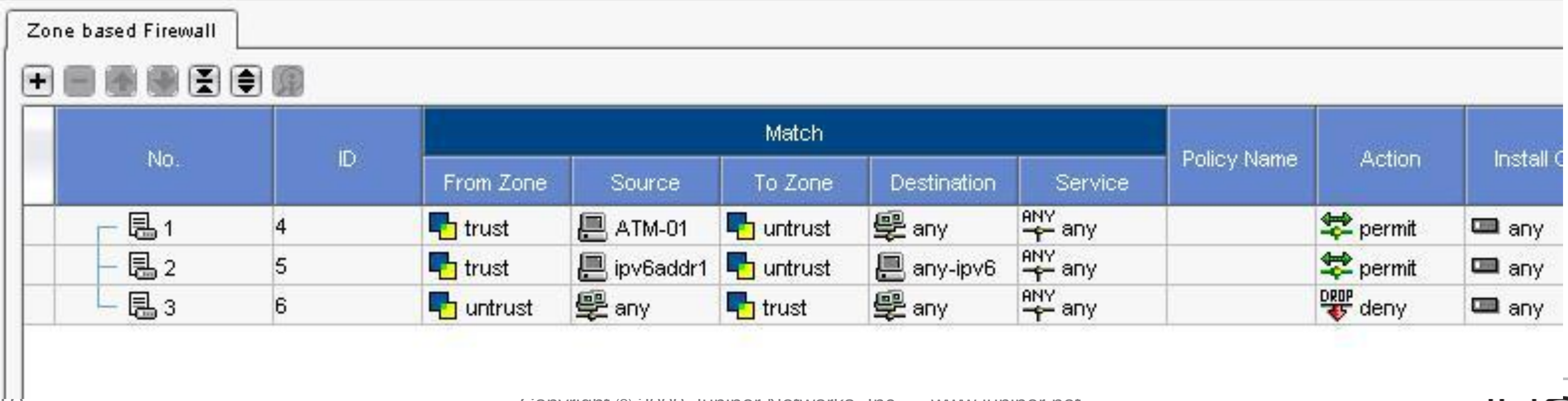
- Device Configuration Editor
- Templates
- Policy Manager
- Object Manager
- Display of logs with IPV6 Address

IPv6 addresses and Policies



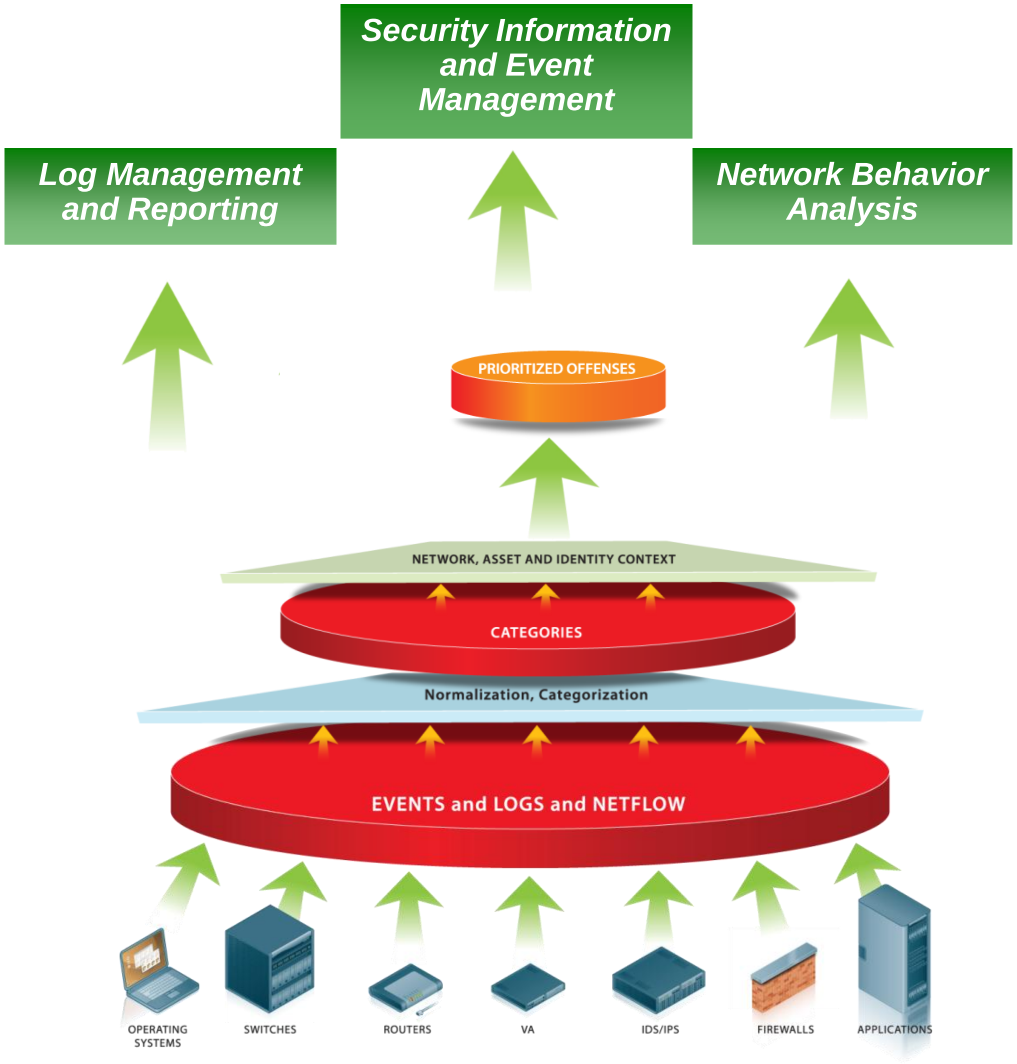
Address Objects

	Name	IP Version	Type	IP/Domain Name	Netmask	Use Wildcard Mask	Wildcard Mask	C
⚠	ATM-01	IPv4	Host	192.168.1.2	32	□		...
⚠	ATM-02	IPv4	Host	192.168.2.2	32	□		...
⚠	ATM-Client1	IPv4	Host	192.168.1.2	32	□		...
⚠	ATM-Client2	IPv4	Host	192.168.2.2	32	□		...
	ATM-Server	IPv4	Host	192.168.3.2	32	□		...
	ATM_MAchine2	IPv4	Host	172.24.67.5	32	□		...
	Bank-Server	IPv4	Host	2.2.2.2	32	□		...
	Corp_Network	IPv4	Network	192.168.115.0	24	□	0.0.0.0	...
	finance_network	IPv4	Network	192.168.6.0	24	□	0.0.0.0	...
	HQ-WebServer	IPv4	Host	192.168.5.2	32	□		...
	ipv6addr1	IPv6	Host	::ffff:192.168.10.1	128	□		...
	ipv6NW	IPv6	Network	::ffff:192.168.20.0	64	□	0.0.0.0	...
	Jtme-host1	IPv4	Host	10.10.10.1	32	□		...
	jtme-host2	IPv4	Host	10.10.10.2	32	□		...



No.	ID	Match					Policy Name	Action	Install C
		From Zone	Source	To Zone	Destination	Service			
1	4	trust	ATM-01	untrust	any	any		permit	any
2	5	trust	ipv6addr1	untrust	any-ipv6	any		permit	any
3	6	untrust	any	trust	any	any		deny	any

Security Threat Response Manager (STRM) Architecture



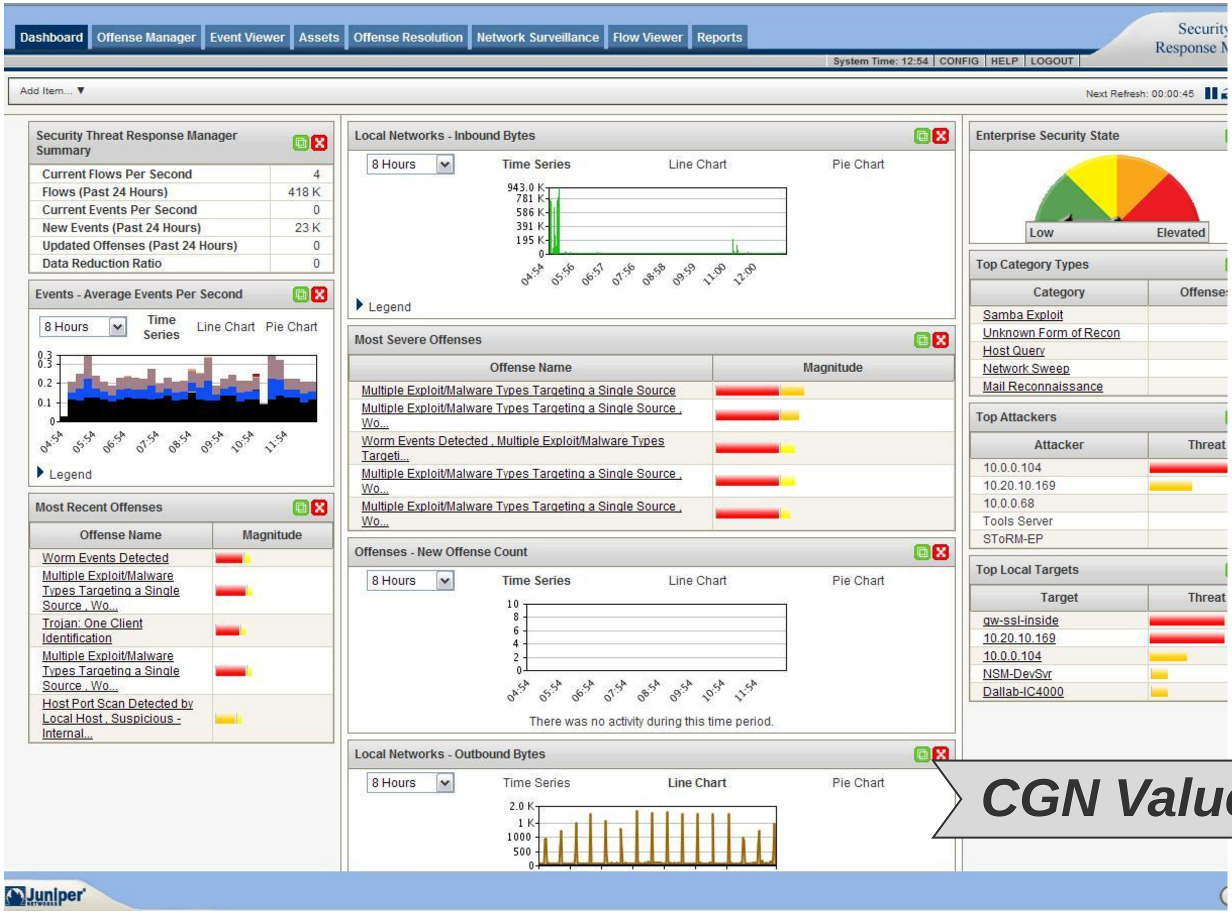
Security Information and Event Management

Log Management and Reporting

Network Behavior Analysis

- *Real time network & security visibility with layer 7 analysis*
- *Data collection provides network, security, application, and identity awareness*
- *Embedded intelligence & analytics simplifies security operations*
- *Prioritized correlated “offenses” separates the wheat from the chaff*
- *Solution enables effective Threat, Compliance, Log Management & Reporting*

STRM’s Key Value Proposition



Security Threat Response Manager Summary

Current Flows Per Second	4
Flows (Past 24 Hours)	418 K
Current Events Per Second	0
New Events (Past 24 Hours)	23 K
Updated Offenses (Past 24 Hours)	0
Data Reduction Ratio	0

Events - Average Events Per Second

Most Recent Offenses

Offense Name	Magnitude
Worm Events Detected	🟥
Multiple Exploit/Malware Types Targeting a Single Source , Wo...	🟥
Trojan: One Client Identification	🟥
Multiple Exploit/Malware Types Targeting a Single Source , Wo...	🟥
Host Port Scan Detected by Local Host , Suspicious - Internal...	🟨

Local Networks - Inbound Bytes

Most Severe Offenses

Offense Name	Magnitude
Multiple Exploit/Malware Types Targeting a Single Source	🟥
Multiple Exploit/Malware Types Targeting a Single Source , Wo...	🟥
Worm Events Detected , Multiple Exploit/Malware Types Targeti...	🟥
Multiple Exploit/Malware Types Targeting a Single Source , Wo...	🟥
Multiple Exploit/Malware Types Targeting a Single Source , Wo...	🟥

Offenses - New Offense Count

There was no activity during this time period.

Local Networks - Outbound Bytes

Enterprise Security State

Top Category Types

Category	Offense
Samba Exploit	
Unknown Form of Recon	
Host Query	
Network Sweep	
Mail Reconnaissance	

Top Attackers

Attacker	Threat
10.0.0.104	🟥
10.20.10.169	🟨
10.0.0.68	
Tools Server	
SToRM-EP	

Top Local Targets

Target	Threat
gw-ssl-inside	🟥
10.20.10.169	🟥
10.0.0.104	🟨
NSM-DevSvr	🟨
Dallab-IC4000	🟨

Dashboard:

Detect New Trends in real time

Log Archival:

Logs Compressions

Scalable solution

Report/Query:

1500+ Out of the box report templates

Security warning

Fully customizable

CGN Value

Subscriber Aware:

Radius (SBR), IC, DHCP, …

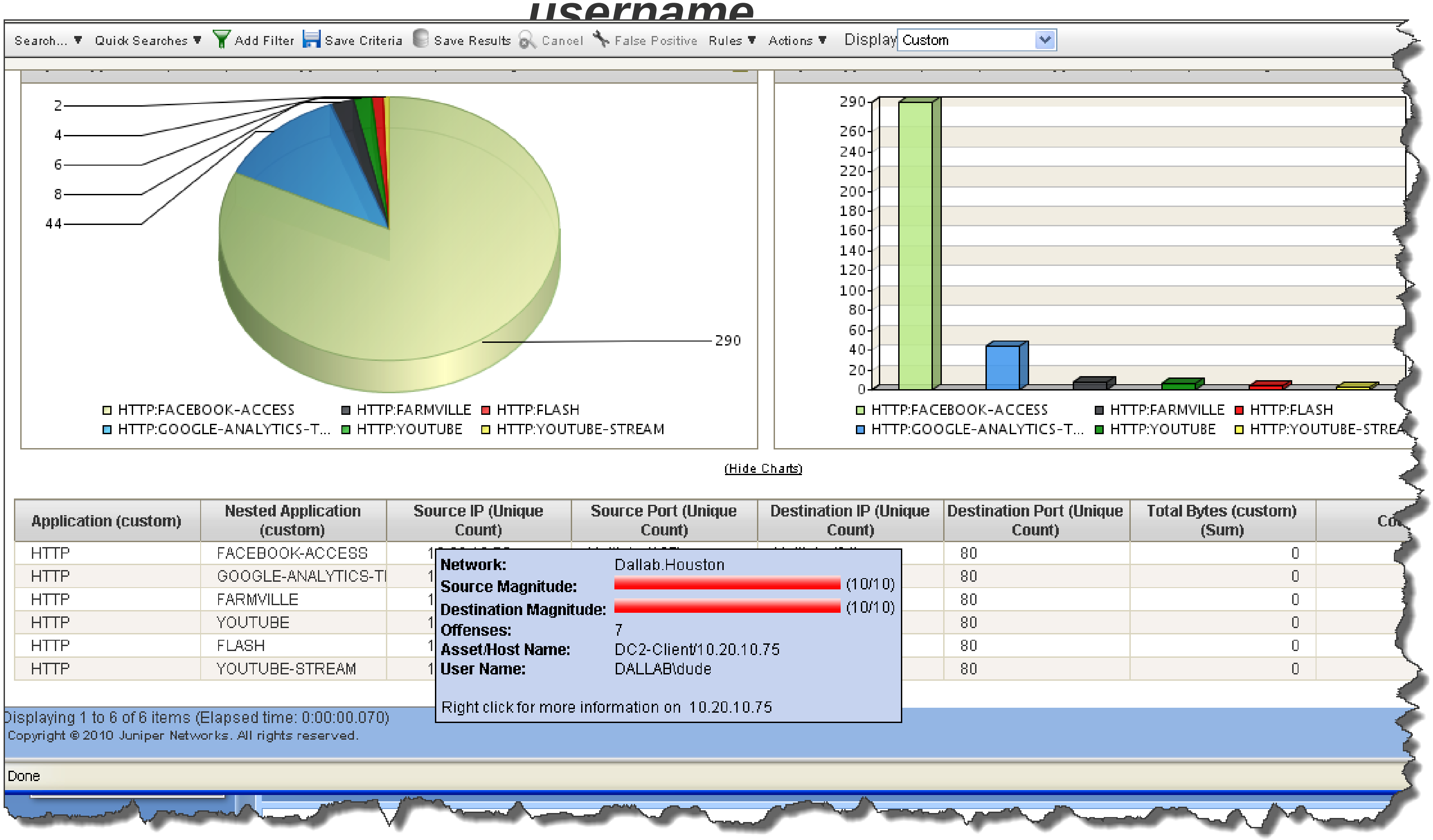
Security Threat Response Manager (STRM)

Includes support for AppTrack Reporting and includes the following predefined search templates and reports

- Top Applications by Bytes from server
- Top Applications by Packets from Server
- Top Talker Per Source IP
- Top Talkers by Zone
- Top Talkers by Destination IP
- Top Web Applications by Bytes from Server
- Top Web Applications by Packets from server

User Correlation in strm

SRX AppTrack records provide detail of application usage by username



Application (custom)	Nested Application (custom)	Source IP (Unique Count)	Source Port (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Total Bytes (custom) (Sum)	Co
HTTP	FACEBOOK-ACCESS	1			80	0	
HTTP	GOOGLE-ANALYTICS-TI	1			80	0	
HTTP	FARMVILLE	1			80	0	
HTTP	YOUTUBE	1			80	0	
HTTP	FLASH	1			80	0	
HTTP	YOUTUBE-STREAM	1			80	0	

Network:	Dallab.Houston
Source Magnitude:	(10/10)
Destination Magnitude:	(10/10)
Offenses:	7
Asset/Host Name:	DC2-Client/10.20.10.75
User Name:	DALLAB\dude

Right click for more information on 10.20.10.75

Displaying 1 to 6 of 6 items (Elapsed time: 0:00:00.070)

Copyright © 2010 Juniper Networks. All rights reserved.

Done

Security Threat Response Manager (STRM) IPv6 Integration

The following STRM components support IPv6:

- Flows Interface
- Events Interface
- Searching, Grouping, and Reporting on IPv6 Fields
- Custom Rules
- Deployment Editor

IPv6 Integration with STRM

Source IPv6/Destination IPv6

If the Offense Type is Source IPv6 or Destination IPv6, the following information is displayed in the Offense Source table:

Parameter	Description
IPv6	Specifies the IPv6 address associated with the event or flow that created this offense.
Offenses	Specifies the number of offenses associated with this IPv6 address. Click the link to view more details.
Events/Flows	Specifies the number of events or flows associated with this IPv6 address. Click the link to view more details.

IPv6 Integration with STRM: Flows Interface

Depending on your deployment, the Flows interface can display four IP address fields:

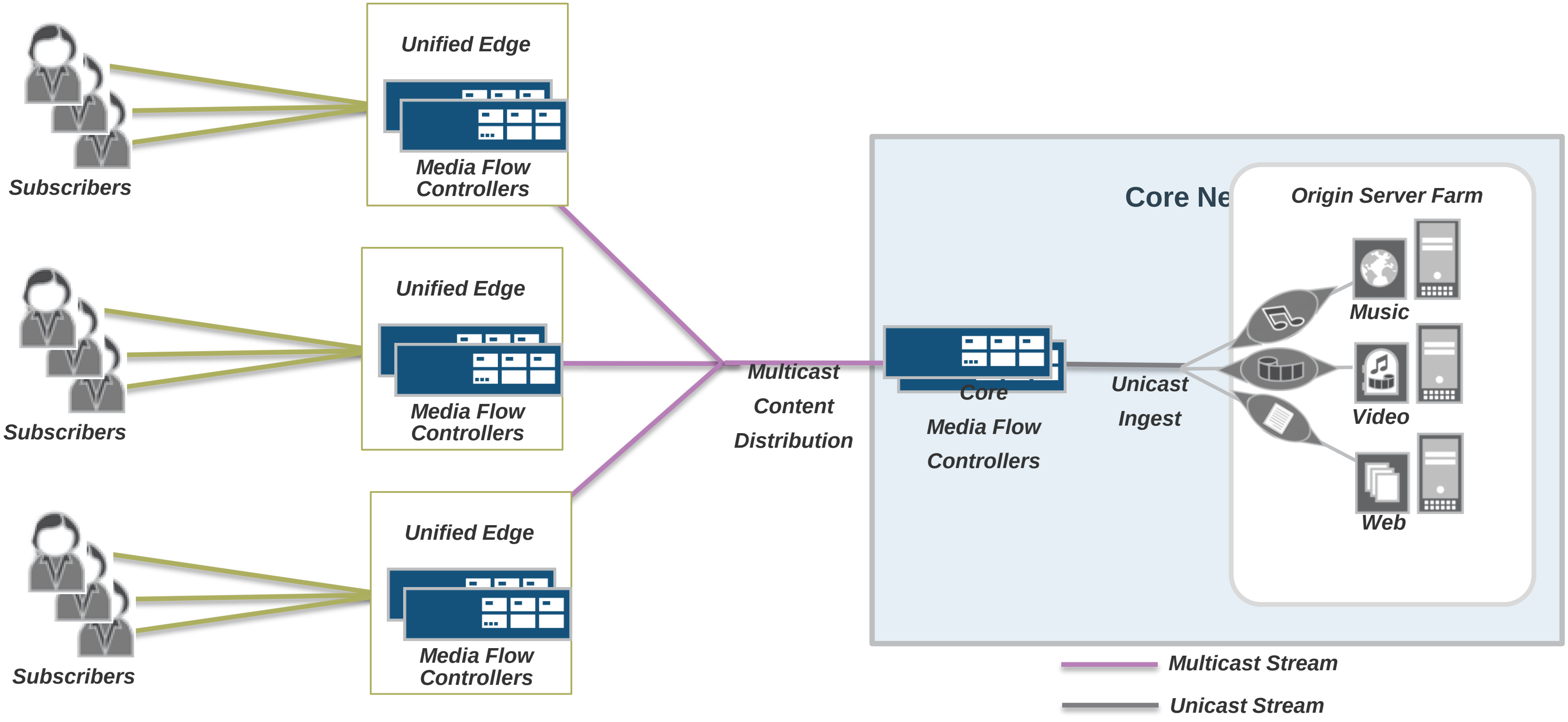
- Source IP Address
- Destination IP Address
- IPv6 Source Address
- IPv6 Destination Address

IPv6 addresses are supported for both packet data, including sFlow, and NetFlow V9 data. However, older versions of NetFlow may not support IPv6.

Media Flow Content Distribution

Media Flow deployed in a data center can push content via multicast to the edge of the network.

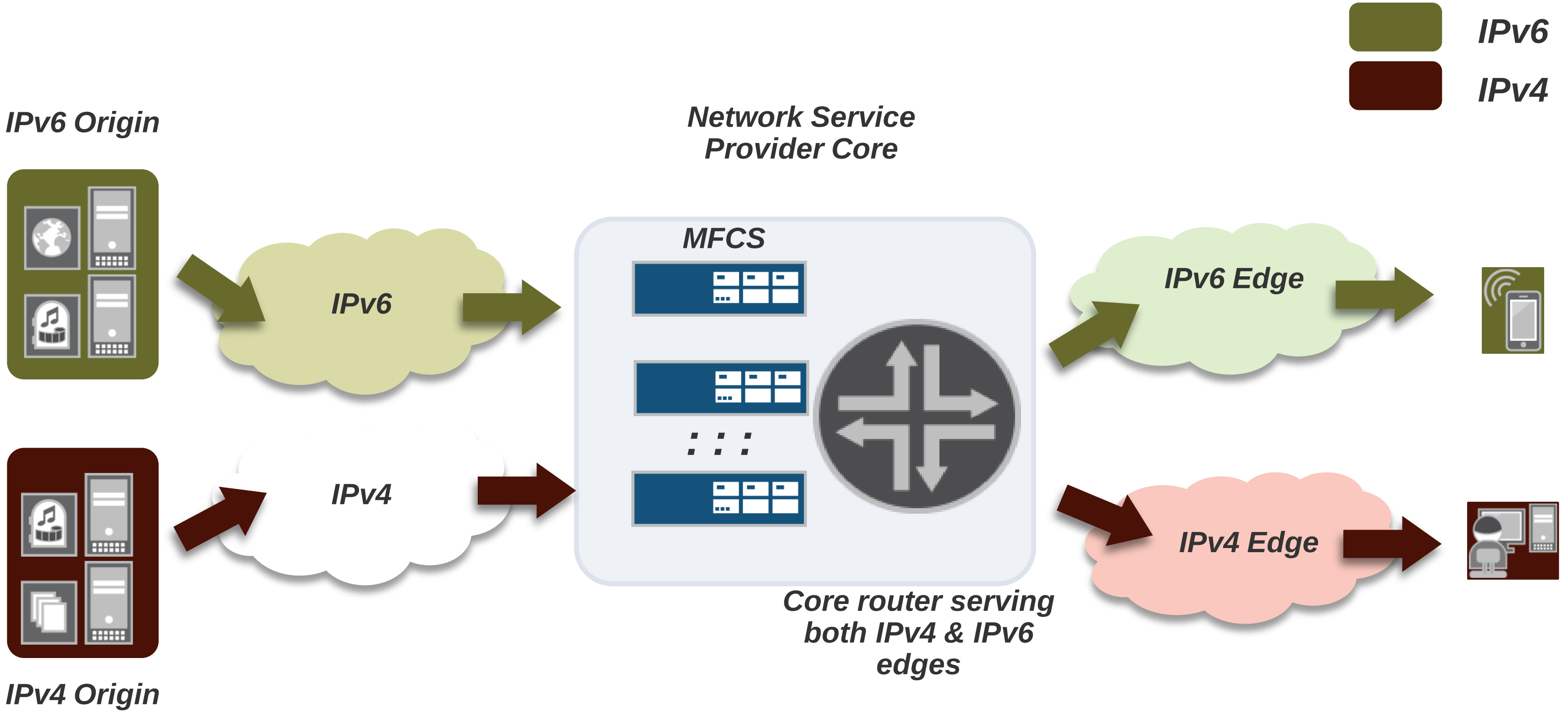
Multicast Content Distribution combines UDP multicast for content and TCP unicast for control and retransmission



www.juniper.net

JUNIPER NETWORKS

NETWORK SERVICE PROVIDER CORE


IPv6
IPv4
IPv6 Origin
Network Service Provider Core
MFCS
IPv6
IPv6 Edge
IPv4
IPv4 Edge
Core router serving both IPv4 & IPv6 edges
IPv4 Origin

- IPv4 users accessing content from IPv4 origins
- IPv6 users accessing content from IPv6 origins
- MFC able to fetch content from both IPv4/v6 origins and serve to IPv4/v6 clients, respectively
- Dedicated IPv4 and IPv6 interfaces in MFC

THANK YOU

everywhere