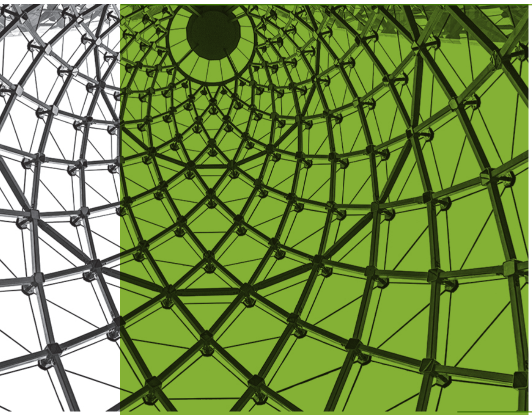

APPSECURE: APPLICATION VISIBILITY AND CONTROL

Protect Against Cyber Attacks with Comprehensive Security

Challenge

Modern technologies have evolved rapidly, introducing a host of new security challenges such as packet loss, unstable networks, malicious attacks, and others.

Solution

AppSecure software provides the visibility into and control over applications needed to identify, allow, block, or limit application access, regardless of port, protocol, or decryption method. The solution protects network investments while reducing TCO by enabling application-aware networks.

Benefits

- *Identifies users, regardless of device or IP address, through granular control of applications, improving customer confidence and awareness*
- *Supports all inbound and outbound SSL decryption techniques to identify and block threats and malware in encrypted network streams*
- *Prioritizes mission-critical applications with built-in QoS*
- *Improves network capacity planning with detailed reporting*

In the recent past, setting and enforcing policies at the host level for applications associated with specific protocols and ports was a relatively straightforward process.

Now, with web-based applications, virtually all traffic is HTTP-based, using ports 80/443. While these nonstandard ports make applications more accessible, intruders use the same technology to launch cyber attacks or hide threats within the application traffic itself. Additionally, IP-based security solutions cannot distinguish between permitted and malicious activity.

The Challenge

As mobility and virtualization grow exponentially, new user-centric applications are emerging for mobile devices, virtual desktops, hybrid clouds, and other dynamic environments. Since users access the network from a variety of sources, effective application visibility is critical.

The complexity created by voice, data, video, and application traffic all running on the same network leaves businesses vulnerable to threats. Network admins need to know every application type entering the network, as well as where the traffic originated, in order to prioritize and route the traffic appropriately and provide the necessary bandwidth and security to ensure the best possible user experience.

The following factors contribute greatly to the complexity network admins are experiencing:

1. Applications are often highly extensible and include features that introduce both business and security risks. Admins must strike the appropriate balance, blocking some applications while securely enabling others.
2. Converged solutions are driving new traffic patterns that are inconsistent with the way today's networks are provisioned. Only application-aware networks can flexibly adapt to new applications and traffic patterns.
3. Peer-to-peer file sharing applications consume an inordinate amount of bandwidth, leaving users with a poor network and application experience.

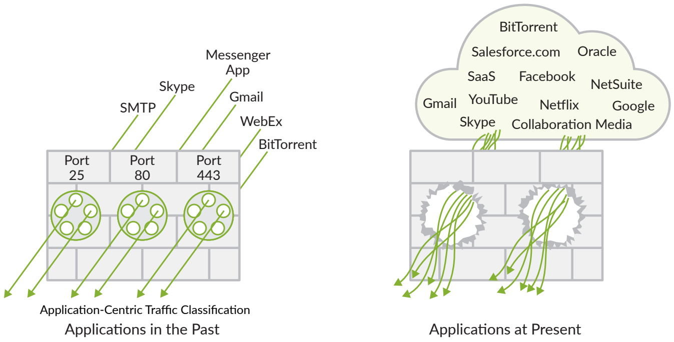

Figure1: The applications landscape, past and present

The Juniper Networks AppSecure Solution

The Juniper Networks® AppSecure suite of application-aware security services for Juniper Networks SRX Series Services Gateways classifies traffic flows while bringing greater visibility, enforcement, control, and protection to customer network security. AppSecure uses a sophisticated classification engine, AppID—available as part of the Juniper Networks Junos® operating system—to identify applications regardless of port or protocol, including those known for using evasive techniques to avoid identification.

Every packet in the flow passes through the AppID engine for processing. Applications are identified through the use of a protocol bundle containing application signatures and parsing information. Application bindings are saved in the application system cache (ASC) to expedite the identification process in the future.

Once the application is identified, AppSecure service modules can be configured to monitor and control traffic for tracking, prioritization, access control, detection, and prevention based on the traffic's application ID.

The following features enable AppSecure to provide the context users need to regain control of their network traffic, set and enforce policies based on accurate information, and deliver the performance and scale required to address their business needs.

- AppTrack: Tracks and reports applications passing through the device.
- Intrusion Detection and Prevention (IDP): Applies appropriate attack objects to applications running on nonstandard ports. Application identification improves IDP performance by narrowing the scope of attack signatures for applications without decoders.
- AppFW: Implements an application firewall using application-based rules.
- AppQoS: Provides quality-of-service (QoS) prioritization based on application awareness.

Use Cases

The following use cases show how AppSecure, used in conjunction with the AppID engine, solves common problems with application visibility and control.

Application Awareness and Control with AppID

Requirement: Increased use of cloud-based services, mobile devices, and media-rich applications puts tremendous strain on a network. This leads to higher infrastructure costs and

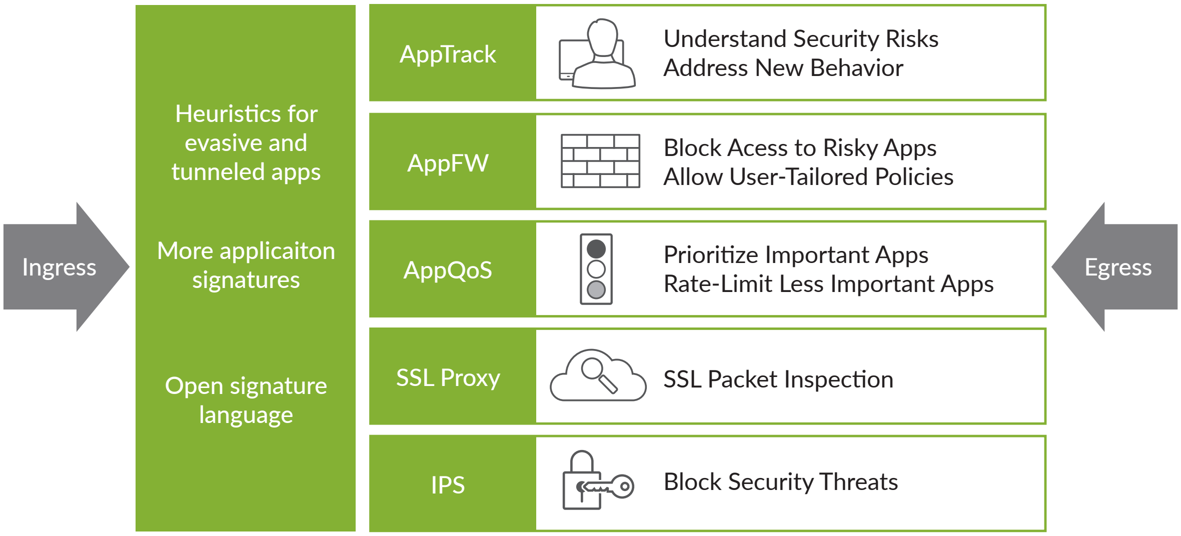
Ingress
Heuristics for evasive and tunneled apps
More applicaiton signatures
Open signature language
AppTrack
Understand Security Risks
Address New Behavior
AppFW
Block Acess to Risky Apps
Allow User-Tailored Policies
AppQoS
Prioritize Important Apps
Rate-Limit Less Important Apps
SSL Proxy
SSL Packet Inspection
IPS
Block Security Threats
Egress

Figure 2: AppSecure service modules

makes the network more difficult—and critical—to manage. Internet and social media applications are a common source of vulnerabilities and attacks. Organizations must be able to manage or control a vast array of web-based applications without hindering productivity.

Solution: The AppID engine lets users exert granular control over applications, including video streaming, peer-to-peer communication, social networking, and messaging. It also helps users identify services, port usage, underlying technology, and behavioral characteristics within applications. The AppID module matches applications for both client-to-server and server-to-client sessions.

Application Control with AppQoS

Requirement: To achieve optimal bandwidth utilization for business-critical applications, it is necessary to identify and control access to specific applications.

Solution: The AppSecure AppQoS service module allows users to invoke identification and control capabilities on top of the existing firewall rule base. With AppQoS, users can prioritize, rate-limit, and queue traffic, not to mention perform DiffServ code point (DSCP) rewrites and set loss priorities—all with the granularity of the stateful firewall rule base (including user role firewall and dynamic application identified by AppID) to match and enforce QoS at the application layer.

Application Enforcement with AppFW

Requirement: Traditionally, applications such as HTTP, SMTP, and Domain Name System (DNS) use well-known standard ports and are easily controlled by a stateful firewall. However, these applications can run on any port, provided the client and server are using the same protocol as the well-known ports. Also, an application firewall not only has to identify HTTP, but any application running on top of it, allowing you to properly enforce your organization’s policies.

Solution: The AppSecure Application Firewall (AppFW) service module leverages information from the AppID module to make informed decisions about permitting, denying, or redirecting traffic. The AppFW module provides an auxiliary rule base tied to each firewall rule for maximum granularity, providing the ability to leverage the standard match criteria of the firewall rule and application identity.

Application Visibility with AppTrack

Requirement: Administrators need to optimize the network for every application, enhancing security for those applications and providing data for business analytics. Administrators must also be able to log and report, as well as enforce actions on sessions based on the result of the App ID module.

Solution: The AppSecure AppTrack service module is a logging and reporting tool used to share information about application visibility. Once AppID identifies an application, AppTrack not only monitors and records its usage, it also sends regular application activity update messages. Since these messages are sent by syslog, they can be read by any compatible third-party device, including Juniper Networks JSA Series Secure Analytics Appliances and Contrail Service Orchestration.

Features and Benefits

- The AppSecure AppID module uses a variety of mechanisms, including application signatures, heuristic detection, alternate mapping techniques, custom signatures, SSL inspection, and application protocol decoding to identify network traffic.
- AppSecure service modules include AppTrack, which provides detailed visibility into application traffic; AppFW, for granular policy enforcement of application traffic; and AppQoS, which prioritizes and meters application traffic.
- AppSecure supports all SSL decryption capabilities. This includes recognizing and decrypting SSL on any port, inbound and outbound, policy control over decryption, and the necessary features required to perform SSL decryption across tens of thousands of simultaneous SSL connections, helping organizations identify and prevent threats and malware in encrypted network streams.

Summary: AppSecure Provides Full Application Visibility and Control

The fact that any application can be used on any port means today’s firewalls must evolve from port-based solutions to a next-generation structure that can protect core business applications from multifaceted cyber attacks. An effective solution needs to deliver the required security services while providing administrators with visibility into and control over the applications traversing their networks.

The AppID engine, available as part of Junos OS, recognizes traffic at different network layers using characteristics other than port number. Once AppID identifies the application, the Juniper Networks AppSecure service modules monitor and control traffic for tracking, prioritization, access control, and attack detection and prevention purposes based on the traffic application ID:

- The AppTrack module tracks and reports applications passing through the device.
- AppFW implements an application firewall using application-based rules.
- AppQoS provides quality-of-service prioritization based on application awareness.

- Intrusion Detection and Prevention applies the appropriate attack objects to applications running on nonstandard ports, improving IDP performance by narrowing the scope of attack signatures for applications without using decoders.

Next Steps

For more information on Juniper Networks AppSecure, please visit us at www.juniper.net/us/en/products-services/security/next-generation-firewall-services/ or contact your Juniper Networks representative.

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
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

Engineering
Simplicity