Learn About Application Visibility and Control

This Learn About explains how application visibility and control functionality plays an important role in protecting critical high-speed networks against the penetration and proliferation of existing and emerging application-level threats by identifying the applications traversing the network using application identification.

It introduces you to the basics of Juniper Networks AppSecure security suite, reviews each of the core AppSecure services, and explains why those services are becoming increasingly necessary for successful businesses.

The Application Landscape

The rapidly evolving world of contemporary business has benefited from many technologies that were unheard of just 10 years ago. But every new technology brings new security challenges, and with the huge numbers of users, devices, and data being deployed to take advantage of the latest technologies, enterprises are becoming increasingly vulnerable to data loss, malicious attacks, and network instability. Let's begin by discussing some security challenges related to the evolution of applications.

Web-based applications have changed the dynamics of security. In the past, specific applications were associated with specific protocols and ports, and setting and enforcing policies at the host level was relatively straightforward. Now, given the reliance on Web applications, virtually all traffic is HTTP-based (ports 80/443) as shown in Figure 1.

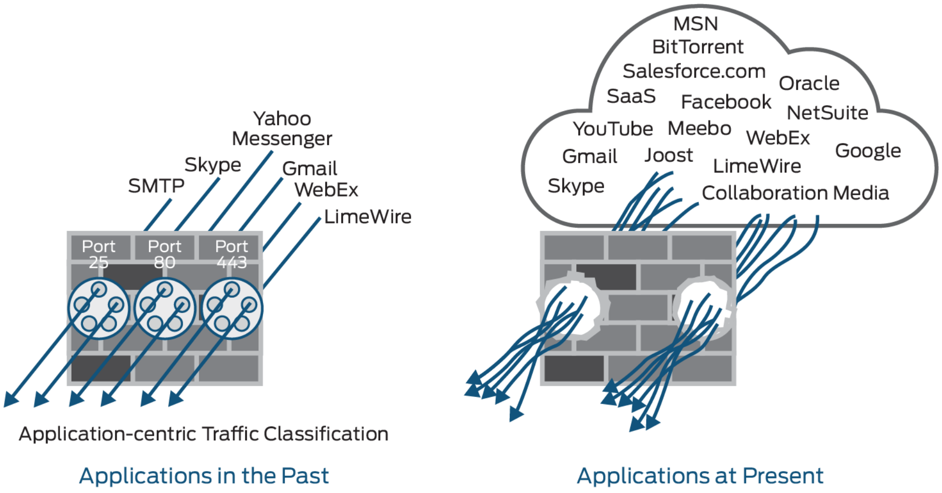


Figure 1 *Applications Landscape – Past and Present*

Use of nonstandard ports and encryption are two of the means by which applications have become more accessible, but cyberattackers implement the same technology to create cyberthreats or hide those threats within the application traffic itself.

Consequently, network security solutions operating solely on basic Internet Protocol (IP) layer information are unable to distinguish between permitted and malicious activity. Further, the very advantage of Web applications—the fact that they can be accessed from anywhere by employees, contractors, partners, and service providers through the firewall—creates its own set of access control challenges.

User-centric applications designed primarily for personal communications, such as instant messaging, peer-to-peer file sharing, Webmail, social networking, and IP voice/video collaboration, present a specific set of challenges as many of these applications evade traditional security mechanisms by dynamically changing their communications ports and protocols, or by tunneling within other commonly used services (for example, HTTP or HTTPS).

The concept that any application can be used on any port is one of the fundamental changes in the application landscape, driving the migration from port-based firewalls to next-generation firewalls.

Yet another challenge is maintaining core business applications, as they are heavily targeted by cyberattackers using multifaceted attacks. Organizations need more control over the applications and traffic on their networks to simultaneously protect their assets against attacks and manage bandwidth use. An effective security solution needs to deliver the right security services in order to provide administrators with visibility and control over the applications traversing their networks.

Requirement for Application Visibility and Control

In response to major industry trends such as mobility and virtualization, applications are increasingly appearing in a dynamic environment that includes mobile devices, mobile apps, hosted virtual desktops, and hybrid clouds. Since users coming in from a variety of media must be accounted for, achieving effective application visibility becomes a challenge.

Businesses are often left vulnerable to threats, or rendered unable to respond to threats, by the complexity caused by voice, data, video, and applications running on the same network. So it is essential that the network be aware of each application traffic type and provide the appropriate priority, routing, and bandwidth required to ensure the maximum user quality of experience. Factors adding to these complexities include the following:

- Applications are often highly extensible, and often include features that may introduce unwarranted risk. Such applications represent both business and security risks and your challenge will be to determine how to strike an appropriate balance between blocking some and securely enabling others.
- Converged solutions, such as peer-to-peer applications, are also driving new traffic patterns that are foreign to the way today's networks were provisioned. Ensuring that networks are application-aware enables them to flexibly adapt to new applications and traffic patterns as they emerge. In addition to the highly publicized legal concerns surrounding peer-to-peer file sharing applications, these applications can rob network bandwidth and leave the majority of users with a poor network and application experience.

- Use of nonstandard ports, for example when a Web server is running on a port other than those commonly associated with HTTP (that is, 80 and 443), applications can set up sessions at nearly 5000 other ports. Many applications that use SSL never use port 443, nor do they use SSL-defined ports.

Application visibility and control is necessary in order to:

- Identify applications, and allow, block, or limit applications – regardless of the port, protocol, decryption, or any other evasive tactic.
- Identify users, regardless of device or IP address, by using granular control of applications by specific users, groups of users, and machines that the users are operating. This helps organizations control not only the types of traffic allowed to enter and exit the network, but also what a specific user is permitted to send and receive.
- Support all inbound and outbound SSL decryption capabilities. This includes recognition and decryption of SSL on any port, inbound and outbound, policy control over decryption, and the necessary features to perform SSL decryption across tens of thousands of simultaneous SSL connections. This helps an organization identify and prevent threats and malware in encrypted network streams.
- Integrate with IPS so that it applies appropriate attack objects to applications running on nonstandard ports. Application identification improves intrusion detection and prevention (IDP) performance by narrowing the scope of attack signatures for applications without decoders. It can be activated and deactivated as required.
- Support the exact same firewall functions in both a hardware and virtualized form factor.
- Scan all applications on all ports in real time for viruses and malware to protect against known and unknown threats embedded across applications.

How Does Application Visibility and Control Work?

A growing number of applications running over HTTP, including video and even hosted applications, are causing strain on the network, leading to higher infrastructure costs and making the network more difficult to manage. Also, the increase in complexity of applications is making it more difficult for network administrators to optimize the performance of these applications running on thier network.

It is no longer effective to block or allow TCP and/or UDP ports, since most applications do not map to individual ports. For example, controlling traffic on an HTTP or HTTPS port is ineffective against complex social networking sites and cloud applications.

To overcome this problem, you need to use application identification (App ID) as the primary classification engine and then add an application signature pattern-matching engine that operates at Layer 7 and inspects the actual content of the payload for identifying applications.

App ID performs a deep packet inspection (DPI) of traffic on the network and on every packet in the flow that passes through the application identification engine until the application is identified. Application findings such as IP addresses, hostnames, and port ranges are saved in the application system cache (ASC) to expedite future identification.

Let's review the different mechanisms used by App ID to identify traffic.

Application Signatures

Context-based signatures are used to first look for unique application properties and related transaction characteristics to correctly identify the application regardless of the protocol and port being used. Application signature mapping, or signature mapping, is a precise method of identifying the application that generated traffic on the network. Signature mapping operates at Layer 7 and inspects the actual content of the payload. The payload of the first few packets is compared to the content of the database. If the payload contains the same patterns as an entry in the database, the application related to the traffic is identified as the application mapped to that pattern in the database entry.

Heuristic Detection

Evasive applications such as peer-to-peer applications do not provide any obvious patterns for matching. Heuristics detection looks at the behavior of the traffic in an analytical fashion to detect what application is running; it can examine the byte stream to determine if it is encrypted by measuring the randomness of the payload bytes. Any application stream that is encrypted (or compressed) will exhibit a highly randomized byte stream.

Alternate Mapping Techniques

In some cases, an alternative method of identifying an application might be required. For example, if traffic on a network is generated by an internal proprietary application, a predefined application signature will not exist. Application identification will identify the application of the traffic as unknown. To keep this traffic from being handled as unknown, Layer 3 or Layer 4 information specific to this application can be mapped to the application name, overriding the application identification process.

Custom Signatures

User-defined custom application signatures can also be used. Custom application signatures are unique to your environment and are not part of the predefined application package. You can create custom signatures using hostnames, IP address ranges, and ports, which allows you to track traffic to specific destinations.

SSL Inspection

Application identification detects encrypted applications based on the patterns in HTTP contexts. However, some HTTP sessions are encrypted in Transport Layer Security (TLS) and Secure Sockets Layer (SSL). The SSL inspection feature is used for identifying applications that use HTTP over SSL/TLS or HTTP. If App ID determines that SSL encryption is in use, the traffic is decrypted and then passed to other identification mechanisms as needed. An SSL proxy must be enabled for application identification of HTTPS traffic to take place.

Application Protocol Decoding

Once the application is identified, it is further decoded at protocol level, if necessary. Protocol decoders are used to check protocol integrity and protocol contextual information by looking for anomalies and ensuring that RFC standards are met. An anomaly can be any part of a protocol, such as the header, message body, or other individual fields that deviate from RFC standards for that protocol.

When protocol contextual information is available, protocol decoders check for attacks within those contexts. By using protocol contextual data, rather than the entire packet, for attack detection, protocol decoders improve overall performance and accuracy.

About Juniper Networks AppSecure

The Juniper Networks AppSecure (AppSecure) suite of application-aware security services for the SRX Series, which was born from App ID technology, classifies traffic flows, while bringing greater visibility, enforcement, control, and protection to your network security.

App ID enables you to see the applications on your network and learn how they work, their behavioral characteristics, and their relative risk. Using several different identification mechanisms, App ID detects the applications on your network regardless of the port, protocol, and encryption (TLS/SSL or SSH) or other evasive tactics used. The number and order of identification mechanisms used to identify the application will vary, depending on the application.

AppSecure uses a sophisticated classification engine to accurately identify applications regardless of port or protocol, including applications known for using evasive techniques to avoid identification. It gives you the context to regain control of your network traffic, set and enforce policies based on accurate information, and deliver the performance and scale required to address your business needs.

The Onbox Application Identification Statistics feature adds application-level statistics to the AppSecure suite. Application statistics allow an administrator to access cumulative statistics as well as statistics accumulated over user-defined intervals.

Figure 2 shows the different AppSecure service modules.

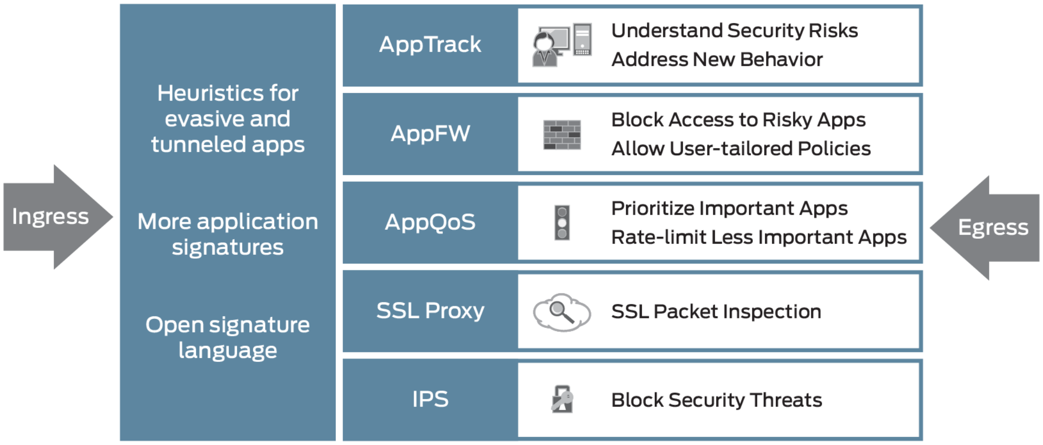

Ingress
Heuristics for evasive and tunneled apps
More application signatures
Open signature language
AppTrack
Understand Security Risks
Address New Behavior
AppFW
Block Access to Risky Apps
Allow User-tailored Policies
AppQoS
Prioritize Important Apps
Rate-limit Less Important Apps
SSL Proxy
SSL Packet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

Figure 2 *AppSecure Service Modules*

The services enabled by AppSecure include AppTrack for detailed visibility of application traffic, AppFW for granular policy enforcement of application traffic, and AppQoS for prioritization and metering of application traffic. SSL proxy provides visibility of encrypted traffic to allow deep packet inspection (DPI). These modules perform various tasks on the traffic based on the result of the App ID.

AppSecure works with additional content security through integrated unified threat management (UTM), intrusion prevention systems (IPS), and Juniper Networks Sky Advanced Threat Prevention (Sky ATP) on the SRX Series for deeper protection against malware, spam, phishing, and application exploits.

Essential Capabilities for a Complete Solution

AppSecure service modules are capable of addressing the application visibility challenges faced by many organizations by monitoring and controlling traffic for tracking, prioritization, access control, detection, and prevention, based on the application ID of the traffic.

Here are some examples of situations in which App ID is used along with AppSecure in order to solve common problems with application visibility and control.

Application Awareness and Control

Requirement (1): Increased use of cloud-based services, mobile devices, and media-rich applications puts more strain on a network, leads to higher infrastructure costs, and makes a network more difficult, and critical, to manage. The performance of your applications and business services depends on the performance of your network, so enhanced visibility into the nature and behavior of applications running on your network is a must. Administrators need to ensure their network delivers optimal performance for the applications that matter most to their business.

Requirement (2): Internet and social media applications are a common source of vulnerabilities and attacks. Organizations have the challenge of managing or controlling a vast array of Web applications without hindering productivity. More and more, applications such as instant messaging applications, peer-to-peer file sharing, or Voice over Internet Protocol (VoIP) are capable of operating on nonstandard ports or can hop ports.

In order to enforce application-specific firewall policies, organizations need to detect all applications, regardless of the port on which they occur, by inspecting traffic to establish the true identity of applications.

Solution: App ID provides granular control over applications, including video streaming, peer-to-peer communication, social networking, and messaging, as well as identifying services, port usage, underlying technology, and behavioral characteristics within applications. The App ID module matches applications for both client-to-server and server-to-client sessions.

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

Devices enabled with AppSecure provide your network team with enhanced visibility into application behavior. As a result, administrators can gain improved control over the prioritization, routing, load balancing, and optimization of application traffic in order to improve user experience and reduce costs.

Application Control with AppQoS

Requirement: Organizations need to control access to applications not only because of the vast number of vulnerabilities they introduce to a network, but also because they consume an excessive amount of bandwidth, resulting in a considerable loss of productivity.

Sometimes simply permitting or denying traffic is not a granular enough response. For instance, you might have traffic that you do not want to explicitly block, but at the same time, you do not want to give it free rein on your network. Examples are applications that impact productivity, such as online games, or consume large amounts of bandwidth, such as peer-to-peer apps or streaming video. You might also have business-critical applications that need to be prioritized over other applications so they are not forced to deal with insufficient bandwidth, resulting in poor application control and frustrated users.

Solution: Identify and control access to specific applications so as to achieve optimal bandwidth utilization for business-critical applications.

AppQoS allows you to do this by providing the ability to invoke it on top of your firewall rule base. AppQoS provides the ability to prioritize, rate-limit, perform DSCP rewrite on, set loss priority for, and queue traffic. It provides the granularity of the stateful firewall rule base (including User Role Firewall and Dynamic Application identified by App ID) to match and enforce quality of service (QoS) at the application layer. This results in prioritizing business-critical applications, queuing up noncritical applications, and selectively allowing business-critical applications while blocking undesirable or malware-infected applications based on network policy, user, and time.

Application Enforcement with AppFW

Requirement: Traditionally, applications like HTTP, SMTP, and DNS use well-known standard ports and are easily controlled by a stateful firewall. However, it is possible to run these applications on any port, as long as the client and server are using the same protocol as the well-known ports.

Additionally, with the growing popularity of Web applications and the shift from traditional, full client-based applications to the Web, more and more traffic is being transmitted over HTTP. Network administrators must be able to detect evasive applications and enforce protocol and policy control at Layer 7. An application firewall must be able to identify not only HTTP, but also any application running on top of it, allowing you to properly enforce your organization’s policies. For example, an application firewall rule could block HTTP traffic from Facebook, but allow Web access to HTTP traffic from Microsoft Outlook.

Solution: Application Firewall (AppFW) refers to the ability to take the results from the App ID engine and leverage them to make an informed decision to permit, deny/ reject, or redirect the traffic. AppFW sits on top of the existing stateful firewall engine that makes decisions based on the standard seven-tuple (from-/to-zone, source/ destination IP address, source/destination port, and protocol). This still allows you to enforce traditional firewall controls on the traffic while layering AppFW to ensure that the application conforms not only to the well-known port information, but to what is actually being transmitted between the client and the server. AppFW provides an auxiliary rule base that is tied to each firewall rule for maximum granularity with the ability to leverage the standard match criteria of the firewall rule, plus the application identity. You can permit, deny, or reject applications, and also use a special redirect feature for HTTP and HTTPS. The redirect action provides a better user experience; instead of explicitly blocking the application, the user can be redirected to a custom Webpage or an externally hosted URL.

Application Visibility with AppTrack

Requirement: Administrators need visibility and control of applications and Websites (including related sub-Websites) resident in all parts of their networks, from the wired or wireless edge all the way through the core and the data center, as well as of application traffic from the enterprise to the private cloud, public cloud, or any service on the Internet. Administrators need to optimize the network for each and every application, enhance security for those applications, and provide data for business analytics. Administrators require that they can log/report, as well as enforce actions on sessions based on the result of App ID. Administrators must be able to send the results of App ID via syslog so that these results can be leveraged both on box and on an external device such as Juniper Secure Analytics (JSA Series) appliance which can provide a rich logging and reporting experience based on the data in these logs.

Solution: AppTrack is essentially a logging and reporting tool that can be used to share information for application visibility. After App ID identifies an application, AppTrack not only keeps statistics on the box for application usage, but also sends log messages via syslog providing application activity update messages. Because these log messages are sent by syslog, they can be consumed by Juniper products like the JSA Series appliances as well as third-party devices.

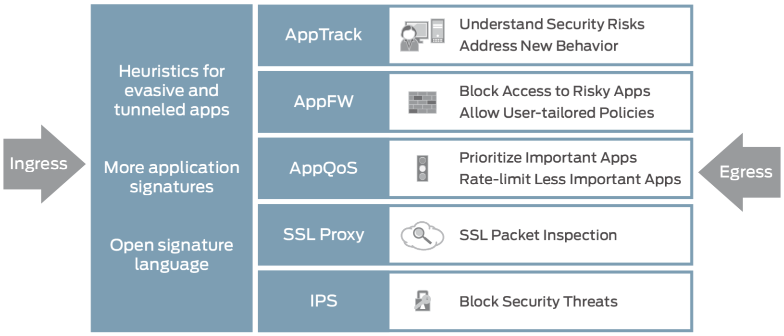
References and Resources

- The Juniper TechLibrary includes everything you need to understand and configure all aspects of AppSecure. See http://www.juniper.net/techpubs/en_US/junos15.1x49-d40/information-products/pathway-pages/security/security-application-identification.html.
- Resources for the AppSecure including datasheets, white papers, and solution briefs. See http://www.juniper.net/us/en/products-services/security/appsecure/, and, http://www.juniper.net/assets/us/en/local/pdf/solutionbriefs/3510505-en.pdf.
- *The Juniper SRX Series*, published in 2013 by O'Reilly Media. See http://www.juniper.net/us/en/training/jnbooks/oreilly-juniper-library/srx-series/.

Learn About Application Visibility and Control

by Madhavi Katti

Every new technology is accompanied by new security challenges. With the number of users and devices, and the data created by them steadily on the rise, your network is increasingly vulnerable to instability and malicious attacks. Learn about the security challenges engendered by the evolution of applications, how susceptible applications and data are to attack, and how you can use technologies such as the Juniper Networks suite of AppSecure security services to secure your network.


Ingress
Heuristics for evasive and tunneled apps
More application signatures
Open signature language
AppTrack
Understand Security Risks
Address New Behavior
AppFW
Block Access 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

About the Author:
Madhavi Katti is an Information Development Engineer at Juniper Networks with over 10 years of experience in writing and developing documentation for networking and telecommunications.

Version History: First Edition, September 2016   2 3 4 5 6 7 8 9

For more information go to the TechLibrary at:
www.juniper.net/documentation