

ADAPTIVE THREAT MANAGEMENT SOLUTIONS REFERENCE ARCHITECTURE

Table of Contents

Introduction	3
Scope	3
Open Systems Approach—Juniper Networks Enterprise Framework	4
Locations in the Network	5
Solution Profile Overview	6
Protecting the Perimeter—Inbound and Outbound Traffic	6
Protecting Critical Resources	7
Securely Enabling Remote Access	7
Enabling Centralized Security Management/Provide Enterprise-Wide Visibility and Control	7
Solution Requirements Summary	8
Reference Architecture	10
Design Considerations	14
Protecting the Perimeter	14
Recommendations for Protecting the Perimeter	16
NOC/SOC View of Perimeter Protection	17
Example of Perimeter Attack	17
Protecting Critical Resources	17
Recommendations for Protecting Critical Resources	19
NOC/SOC View of Protection of Critical Resources	20
Example of an Attack on a Critical Resource	20
Protecting Remote Access	20
Recommendations for Protecting Remote Users	22
NOC/SOC View of Protecting Remote Access	23
Example of Remote Access Attack	23
Protecting from Insider Threats	24
Recommendations for Protecting Against Insider Attacks	25
Example of an Insider Attack	25
Conclusion	26
Appendix A: Products and Features	26
Appendix B: Threats and Definitions	27
About Juniper Networks	27

Table of Figures

Figure 1: Juniper Networks Enterprise Framework	4
Figure 2: Juniper Networks Adaptive Threat Management Solutions protect all locations in the network.	5
Figure 3: Protecting the perimeter, critical resources, and remote access of users and devices	8
Figure 4: Juniper Networks Adaptive Threat Management Solutions logical architecture	10
Figure 5: Juniper Networks Adaptive Threat Management Solutions reference network	12
Figure 6: Protecting the perimeter (internal network)	14
Figure 7: STRM Series showing flows and firewall events representing a DoS attack	17
Figure 8: Protecting critical resources	18
Figure 9: STRM Series showing firewall and IDP Series events representing an attack on a critical resource	20
Figure 10: Protecting remote access	21
Figure 11: STRM Series showing events and logs from SA Series and IDP Series for protection of remote access	23
Figure 12: Protecting remote access	24

Introduction

For most organizations today, the network is a strategic asset and zero downtime is the goal. Some key challenges to achieving this goal are in the areas of security, scalability, performance, usability, and manageability.

From a security perspective, many current security solutions lack the ability to adapt and respond proactively in real time to constantly evolving threats like hacking, scanning, denial-of-service (DoS) attacks, new exploits in applications, worms and viruses, to name a few. Further, the lack of tight integration between security products such as firewalls and intrusion prevention systems (IPS), in combination with disparate features specific to network location such as different protection mechanisms for small branch offices to large campus locations to data centers, creates a challenge to the job of adequately addressing security breaches.

Security and IT administrators are also faced with the challenge of making sure that the products they deploy scale to support ever increasing network traffic and a diverse user population, while at the same time maintaining fast, reliable, and secure access to applications and network resources. Most often this results in a compromise, where adding extra security degrades performance of the service or vice versa. Performance and scalability are also an issue, especially when service is required under heavy traffic load such as seasonal retail transactions or end of financial quarters.

Finally, because existing solutions consist of a mix of different products and technologies that are not tightly integrated, administrators are faced with the challenge of understanding and managing multiple security products and management systems. This challenge grows exponentially when one tries to identify the root cause of an attack, where reports and logs need to be viewed from multiple systems and several hundred devices that are spread over many locations. This makes forensic analysis difficult at best, and leaves the network extremely vulnerable to emerging threats that take advantage of gaps between disparate devices to cause disruption and downtime.

Juniper Networks® Adaptive Threat Management Solutions consist of high-performance security platforms that leverage a dynamic cooperative system and provide network-wide visibility and control, in order to adapt to changing risks. Juniper Networks Adaptive Threat Management Solutions provide a responsive and trusted security environment for your high-performance network. By leveraging a cooperative system of tightly integrated security products that include firewall, Juniper Networks SA Series SSL VPN Appliances, IC Series Unified Access Control Appliances (UAC), IDP Series Intrusion Detection and Prevention Appliances, WXC Series Application Acceleration Platforms, STRM Series Security Threat Response Managers, and Juniper Networks Network and Security Manager (NSM), this cooperative set of solutions adapts and secures the network against the threats that constantly evolve in today's network environment. The key characteristics of these adaptive threat management solutions are the following:

- Includes a system of tightly integrated security products that adapt and proactively respond in real time to address emerging threats,
- Supports growth in network requirements, traffic, and applications while maintaining fast, reliable, and secure access to applications and network resources, thereby eliminating trade-offs between security and performance,
- Provides a single network-wide view for identification, mitigation, and reporting on complex attacks, which eliminates false positives by using a highly advanced correlation system that enables IT and security staff to concentrate on actual security incidents,
- To effectively secure your network, these solutions deliver centralized management capabilities to help you adaptively protect your perimeter, proactively protect critical resources, mitigate insider threats, and provide secure remote access with confidence.

Scope

This paper presents Juniper Networks Adaptive Threat Management Solutions reference architecture for securing the enterprise, and includes associated information related to data centers, campuses, branch offices, remote users, and network operations centers (NOCs).

Open Systems Approach—Juniper Networks Enterprise Framework

The Juniper Networks Enterprise Framework (as illustrated in Figure 1) encourages a best-in-class, heterogeneous network environment by using open, standards-based, and industry accepted interfaces to communicate between applications, services, and infrastructure. This framework enforces policy across various elements and simplifies management. For details concerning Juniper Networks Enterprise Framework, refer to the *Enterprise Data Center Network Reference Architecture*.

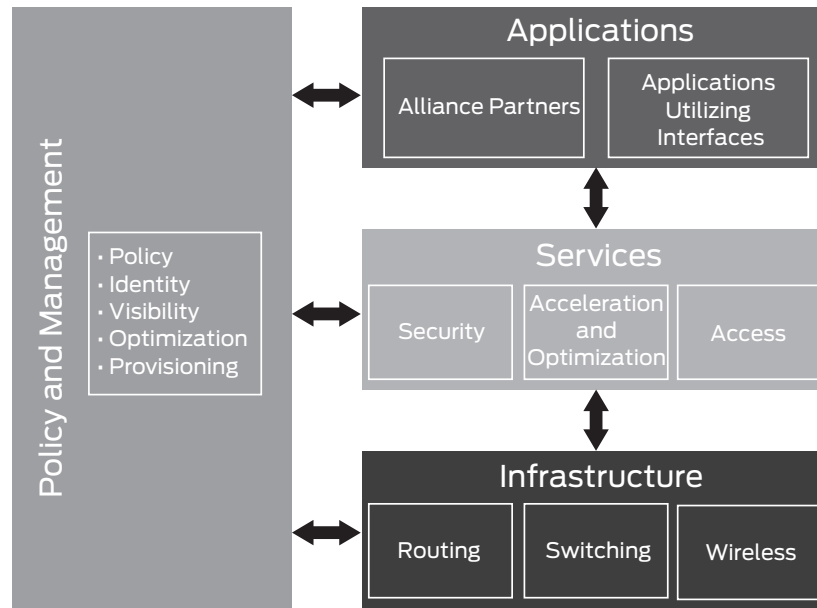


Figure 1: Juniper Networks Enterprise Framework

Juniper Networks Enterprise Framework simplifies the Open Systems Interconnection (OSI) model by creating three functional layers that are controlled by a policy and management domain. In this logical model, the applications layer provides support to the various software applications that are required to support the business. This framework provides the environment that allows applications to run and interoperate. The services layer combines the traditional presentation, session, and transport layers and provides support to users and applications. This layer includes security services, applications interfaces, and acceleration and optimization services. The infrastructure layer combines the network, data link, and physical layers, and consists of routing and switching features that manage the network including LAN and wireless local area network (WLAN) switching, connection management, data flow, application quality of service (QoS), and transmission behavior. The policy and management domain integrates with the customer's centralized policy and management functions to help reduce operational costs while simultaneously enabling compliance with security requirements. Juniper Networks Adaptive Threat Management Solutions fit seamlessly into this framework.

Like the Enterprise Framework, Juniper Networks Adaptive Threat Management Solutions are also multilayered, providing adaptability, scalability, accessibility, and visibility with single enterprise-wide view and control. Juniper Networks Adaptive Threat Management Solutions are based on an open, standards-based architecture and thus integrate easily into multivendor environments. An additional advantage is that these solutions can be deployed in stages on your existing network infrastructure, depending on your corporate business needs and growth.

Locations in the Network

Juniper Networks Adaptive Threat Management Solutions are designed for an enterprise-wide environment. This implies hundreds and possibly thousands of users requiring access to centralized applications and servers hosted in one or more data centers. In addition, on campus (off campus) and remote sites make up a significant part of the enterprise, all requiring access to a variety of applications hosted in the data center.

As shown in Figure 2, Juniper Networks Adaptive Threat Management Solutions provide a set of highly scalable capabilities that can consistently protect any location, from the small branch office to the large data center, while at the same time providing a set of highly powerful visibility tools that enable network managers to manage all aspects of enterprise security from a centralized network operations center (NOC) or security operations center (SOC).

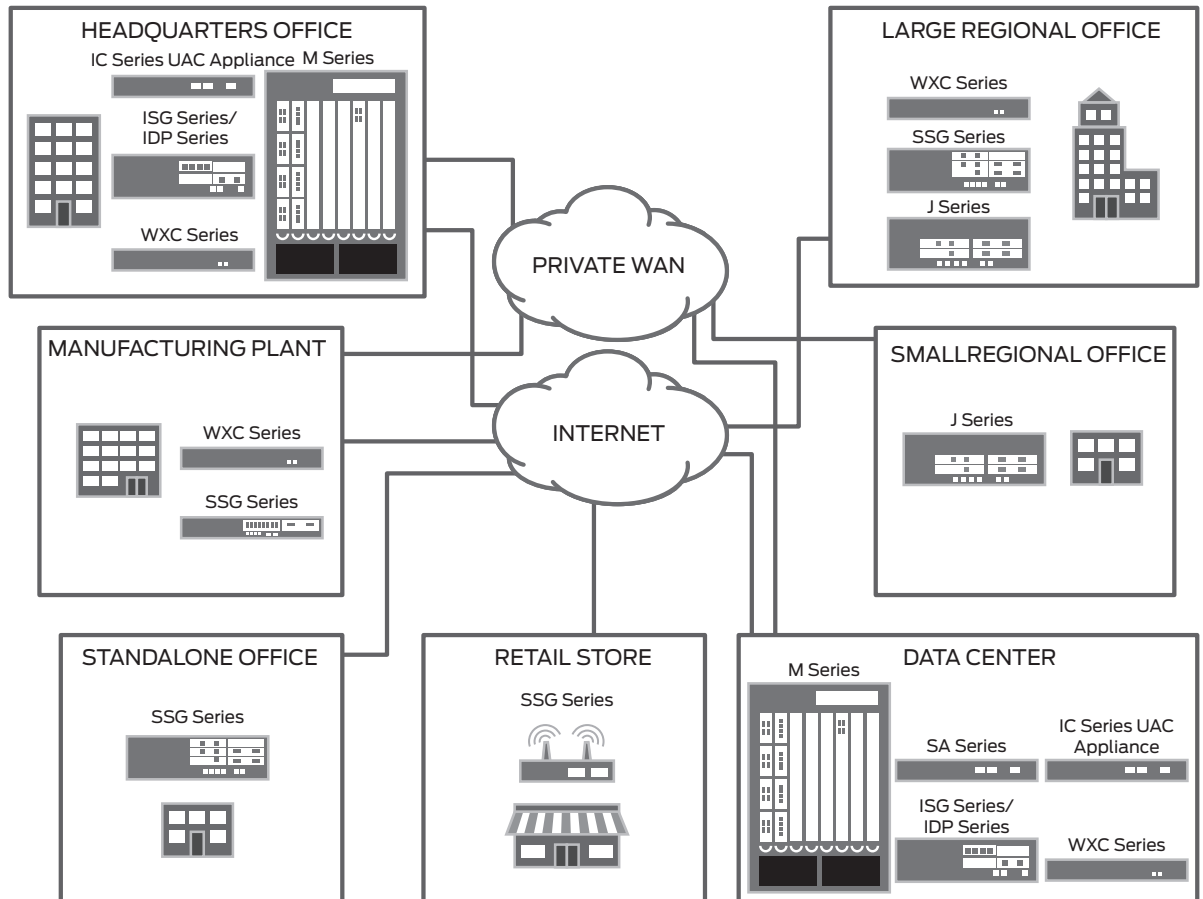


Figure 2: Juniper Networks Adaptive Threat Management Solutions protect all locations in the network.

Table 1: Terms and Definitions

TERMS	DEFINITION
Events	Reporting mechanisms that are generated by various devices (routers, firewalls, IPS, switches, etc.).
Triggers	Messages created when correlation of traffic, events, and flow data exceeds policy thresholds. IT originated or recommended policy can be created on security devices or in Security Information and Event Managers (SIEMs). For example, when a combination of traffic, events, and flow data from across the network shows network traffic behavior that is out of policy, a trigger message is created.
Threats	Attempts to exploit computer vulnerabilities, usually in the form of software that is directed against network security devices, servers, computers, and other devices, with the intent to disrupt, destroy, annoy, steal data, escalate server privileges, or halt data communications. Types of threats include hacking, flooding, brute force, identification (ID) spoofing, unauthorized access, DoS, etc.
Perimeter	Any point where two different networks that don't fully trust each other meet. Examples are the border between the intranet and Internet, or the connection point where two or more different organizations' networks meet.
Secure access/remote access	Applies to any employee and/or partner who accesses the corporate intranet and applications from remote locations (home, hotel, airport, etc.).
Critical resources	Computer servers, appliances, devices, and stored data that need to be protected from external elements in order to maintain confidentiality and protect intellectual property.
Coordinated Threat Control (CTC)	SA Series and IDP Series appliances cooperate with each other to offer a unified view of user, application, and traffic flow. IC Series and IDP Series appliances can also cooperate with each other in a similar fashion. CTC is a Juniper Networks innovation that takes dynamic actions against an attack. This gives IT more detailed information when examining remote access reports and reduces manual correlation of IP address logs to users. It also allows application control on remote access users, for example, point-to-point without file transfer may be allowed for some users while other users may have full point-to-point capabilities.

Solution Profile Overview

Now that we have reviewed the different locations in the enterprise that need to be addressed, this section covers the key solution requirements revolving around Juniper Networks Adaptive Threat Management Solutions. To effectively secure the enterprise, one must take into account the following requirements:

- Protect the perimeter (inbound and outbound traffic)
- Protect critical resources
- Enable secure remote access
- Mitigate insider threats
- Enable centralized security management and provide enterprise-wide visibility and control

Knowing and understanding the importance of these key requirements is critical to ensuring complete security coverage throughout the entire enterprise. Let us now look at these requirements in greater detail.

Protecting the Perimeter—Inbound and Outbound Traffic

Inbound traffic is all traffic coming into the particular location (data center, branch, campus). Inbound traffic typically experiences such threats as malicious hackers, floods, scanning, and brute force attacks.

- Hacking refers to multi-stage attacks where the attacker tries to gain information about vulnerabilities and execute a targeted attack to gain control or manipulate data.
- Scanning (also known as reconnaissance) refers to systems scanning open ports for the purposes of connection or DoS attacks.
- Brute force attack is a method of defeating a cryptographic scheme by trying a large number of possibilities; for example, exhaustively working through all possible keys in order to decrypt a message.
- Flooding attack is one where the attacker sends many packets or application-level requests to a system, from one or multiple sources in an attempt to overwhelm the processing power of the target machine, thereby impeding or denying the actual service delivered by that machine.

Outbound traffic is all traffic that leaves a particular location (data center, branch, campus). Outbound traffic threats typically include intellectual property leakage, resource abuse, phishing, etc.

- Intellectual property leakage can occur when an employee either knowingly or unknowingly sends out sensitive material to sites/computers outside the corporate network.
- Resource abuse involves an employee who abuses a privilege of his or her computer or computer facilities in the company (such as unauthorized access to or alteration of data). Other examples of resource abuse are downloading content and using valuable bandwidth or browsing websites not appropriate in a corporate environment.
- Phishing occurs when a user browses for what seems to be a legitimate Internet site URL that actually translates into a site that breaches corporate security.

Protecting Critical Resources

In addition to protecting the perimeter, enterprises need to protect critical applications and servers from both internal and external attacks that focus on activities, such as exploiting application vulnerabilities, unauthorized access, and application/service DoS.

- Vulnerability exploitation is associated with a hacker taking advantage of software vulnerabilities in an attempt to stop the service and take control of the system.
- Unauthorized access is an attempt to access a resource without having the right permissions/privileges, either through using a guest or anonymous account, using another's credentials, or through vulnerability exploitation.
- Application/service DoS means targeting a specific service on a server such as HTTP, Simple Mail Transfer Protocol (SMTP), or other services, and deliberately overwhelming the device by sending harmful traffic which prevents system accessibility for end users.

Securely Enabling Remote Access

Enabling remote access allows an employee or partner to access corporate applications. Typical threats at this juncture are identity spoofing, unauthorized access to resources, and possibly infecting critical resources.

- Identity spoofing is where a rogue person will try to use a real employee's credentials and gain access to systems.
- Unauthorized access involves one legitimate remote user trying to access internal resources using someone else's credentials.

Infecting critical resources can occur when a remote user accesses corporate applications through an unmanaged endpoint (personal PC) and unknowingly inserts worms or other harmful traffic into the corporate network.

Enabling Centralized Security Management/Provide Enterprise-Wide Visibility and Control

A critical requirement of any security solution that spans the entire enterprise is its ability to provide a network-wide view of all security events occurring across all locations at any given time. All aspects of the solution need to be managed centrally. Events/logs from multiple devices in the path of traffic (switches, routers, firewalls, intrusion prevention systems), must be managed and correlated to gain a realistic perspective of the ever-increasing security attacks and overall health of the network. Saving and storing the events/logs for forensic analysis should be a critical requirement for any network administrator. Administrators cannot control what they cannot view.

Figure 3 illustrates the perimeter, critical resources, and remote access of users and devices that comprise the enterprise infrastructure.

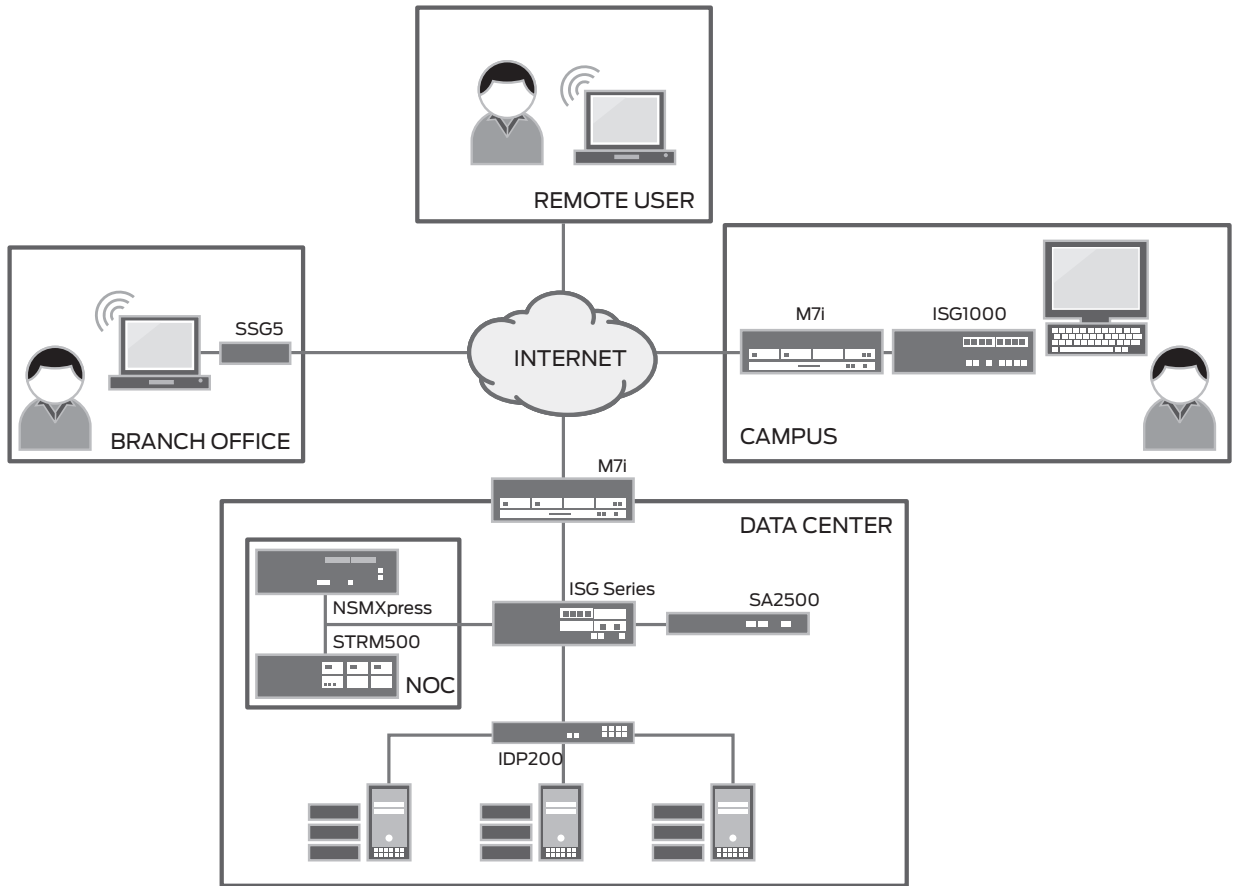


Figure 3: Protecting the perimeter, critical resources, and remote access of users and devices

Solution Requirements Summary

Table 2 summarizes the different types of threats and the solution requirements that need to be addressed for each, to combat the kinds of threats that can cause serious damage to the enterprise’s revenue, reputation, and intellectual property by infecting its major elements—perimeter, critical resources, and remote access for users and their devices.

Table 2: Solution Requirements

PROTECTION	THREATS	SOLUTION REQUIREMENTS
Perimeter protection	<ul style="list-style-type: none"> Hacking, scanning, brute force attacks, and flooding IP leakage, resource abuse, phishing 	<ul style="list-style-type: none"> A consistent, highly scalable and adaptive solution that protects the perimeter of small branch offices up through large data centers from internal and external attacks. Protect corporate liability and intellectual property by ensuring that only valid traffic leaves the particular location. Provide visibility via a centrally managed NOC/ SOC whereby all aspects of security policies and their management are controlled centrally and implemented locally. A high-performance flexible solution that quickly adapts to rapidly evolving security threats.

PROTECTION	THREATS	SOLUTION REQUIREMENTS
Critical resources protection	<ul style="list-style-type: none"> Unauthorized access, service level DoS, vulnerability exploitation 	<ul style="list-style-type: none"> Provide a high-performance security solution to protect critical resources from both network and application-level attacks. A highly scalable and adaptive solution that is able to quickly address known and unknown attacks and exploitation of vulnerabilities. Provide visibility via a centrally managed NOC/SOC whereby all aspects of security policies and their management are controlled centrally and implemented locally. Implement application-specific session limits. Deploy access control using stateful firewalls.
Remote access protection	<ul style="list-style-type: none"> Identity spoofing, unauthorized access to resources, website enumeration, evasion, infection of critical resources and IPsec VPN piggy backing. 	<ul style="list-style-type: none"> Provide a high-performance, secure remote access solution that works across a wide variety of platforms (PCs, MACs, mobile devices, PDAs, and others) and seamlessly integrates and operates with all types of existing vendor products. Provide end-to-end security by ensuring that the remote client meets the security posture (antivirus software, patch levels, etc). Dynamically change user access privileges if a threat condition is detected to prevent abuse/infection of internal resources. Seamlessly integrate and operate with all types of existing vendor products. Support remote users and their accessibility via clientless connection that works on any Internet connection. Dynamically change user access privileges if a threat condition is detected. Encrypt traffic to prevent theft of data in transit. Authenticate transported data to prevent and prove data authenticity. Provide user-friendly enterprise-wide reports that are correlated together to minimize manual analysis of security events and to expedite corrective action.

PROTECTION	THREATS	SOLUTION REQUIREMENTS
Securing LAN access (insider threat mitigation)	<ul style="list-style-type: none"> Identity spoofing, unauthorized access to resources, website enumeration, privilege escalation, infection of critical resources. 	<ul style="list-style-type: none"> Identify and mitigate fraudulent activities originating from the trusted users on the corporate LAN in the distributed enterprise environment, in real time. Provide end-to-end security by ensuring that the endpoint meets the recommended security posture (antivirus software, patch levels, etc). Dynamically change user access privileges if a threat condition is detected to prevent abuse/infection of internal resources. Seamlessly integrate and operate with all types of existing 802.1X-enabled vendor products including wireless access points, switches, etc. Encrypt traffic to prevent theft of data in transit, typically through the use of a VPN connection to the gateway/resource. Authenticate transported data to prevent and prove data authenticity. Provide user-friendly enterprise-wide reports that are correlated together to minimize manual analysis of security events and to expedite corrective action.

In addition to the critical requirements listed above, it is extremely important that threat management solutions address the key role of policy, visibility, and control from the IT manager’s perspective. IT managers have to check logs and events coming from multiple systems frequently, to trouble shoot and find the root cause of problems/attacks that may occur on their high-performance networks. Moreover, because a variety of devices need to be tracked across geographically diverse locations, it becomes even more important to collect these events and logs centrally and analyze them rapidly to address threats and attacks. As such, solutions that provide a centralized view of network and security events, combined with rapid correlation tools, are also a key requirement. See the three related NOC/SOC View sections for viewing events from a central location discussed later in this document.

Reference Architecture

Following the descriptions of the enterprise locations and the overall set of requirements, we describe how this reference architecture addresses the requirements in all enterprise locations.

Administrators running the NOC/SOC must have crucial information at their fingertips. This includes security events/triggers that are generated by a variety of Juniper Networks and other vendor networking devices (switches, routers, firewalls, intrusion prevention systems, SSL VPN) across a wide number of environments (branch offices, data centers, campuses). Juniper Networks Adaptive Threat Management Solutions enable administrators to be proactive. Administrators can centrally view these triggered events and be quickly warned with succinct information about any and all suspect data/traffic, so that they can quickly complete an analysis and make appropriate business security decisions. Also, eliminating false positives enables IT and its security staff to concentrate on the actual security threats affecting their environment.

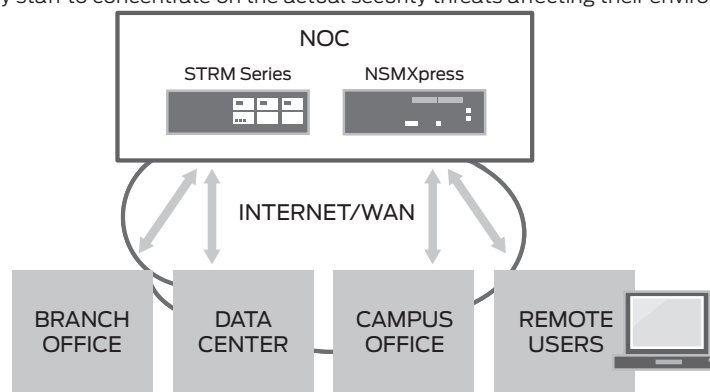


Figure 4: Juniper Networks Adaptive Threat Management Solutions logical architecture

Juniper Networks Adaptive Threat Management Solutions enforce security at Layers 3 through 7 based on network characteristics, for example, IP address, TCP port, and user information such as role and access privilege and client machine threat levels.

A single set of management systems defines unified security policy. This policy is enforced globally in a distributed way across all enterprise locations to create a single comprehensive security policy applicable to the entire enterprise. The relevant security policy rules will be enforced at different devices in different locations to create an overall policy that applies the appropriate level of protection to the applicable systems throughout the enterprise.

For instance, in the data center and branch offices, security policies specify allowed application usage, and security enforcement points enforce the same policies. Policies will be applied close to the source and close to the destination to enforce the tightest security. All access event information logged by enforcement points in both the data center and branch offices will be sent to the NOC/SOC. At this point, network administrators can receive detailed reports of network and application usage to support educated decisions and modify policies or optimize settings as needed. For example, traffic that is blocked at the data center but is permitted at the branch office may easily be identified and the relevant security policies will be applied to the branch office.

With Juniper Networks Adaptive Threat Management Solutions, the network and security enforcement points collaboratively control two key functions:

- Collecting data about network usage and application transactions, and presenting this data to the central NOC/SOC where the information will be correlated and reports showing the network state are generated
- Enforcing policies that are managed and defined in the NOC/SOC in a unified way so that all enterprise locations enforce the same policy or in other cases, the policies may be dynamic and based on a response to a specific threat

Figure 4, represents the logical architectural view (overall set of elements that can jointly and adaptively manage and mitigate threats) in our customer's enterprise. It is important to note that bidirectional communications enforcement points such as firewalls, switches, and IPS send event information to NOC systems presenting data about security events. Additionally, the same devices receive directives from the NOC systems as to changes needed to the security protections and policies. In this way, there is a closed loop mechanism by which security changes are made according to security events.

Let us now look at the way this design fits into existing network architecture, as represented in Figure 5. This figure illustrates a high level view of the enterprise (branch office, campus, data center, headquarters, mobile or home or remote office, and required devices).

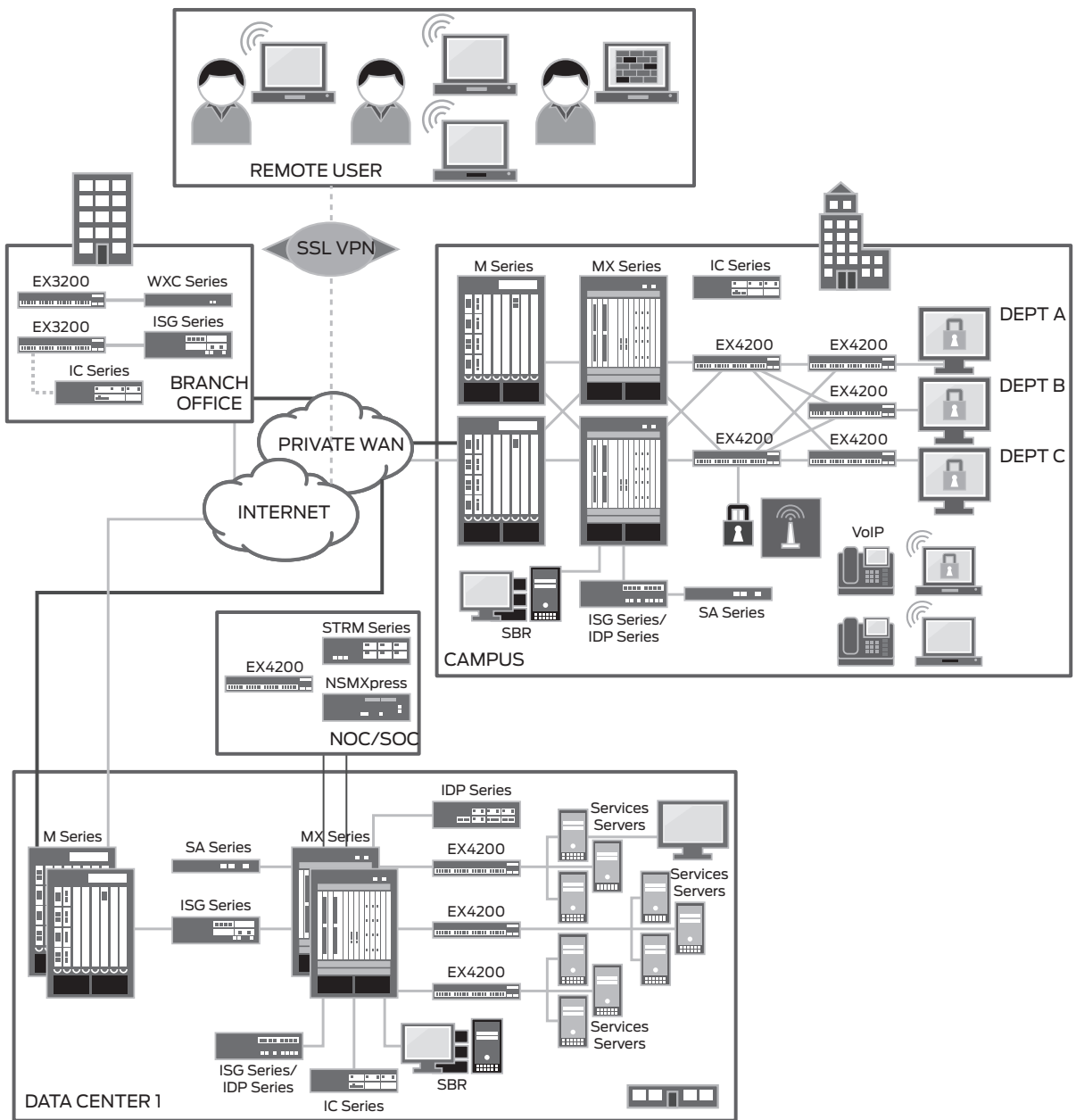


Figure 5: Juniper Networks Adaptive Threat Management Solutions reference network

Table 3 describes each of the network locations and identifies the solution requirements and devices deployed.

Table 3: Locations, Solutions Requirements, and Recommended Devices

LOCATION	SOLUTIONS REQUIREMENTS	RECOMMENDED DEVICES
Data center	<ul style="list-style-type: none"> High performance/high throughput Highly scalable and adaptable solution Separate security and networking infrastructure (separate firewalls and routers) Application layer security 	<ul style="list-style-type: none"> Juniper Networks ISG1000 Integrated Security Gateway, Juniper Networks ISG2000 Integrated Security Gateway (optional integrated intrusion detection processor) Juniper Networks NetScreen-5200, Juniper Networks NetScreen-5400 Juniper Networks SRX5600 Services Gateway, Juniper Networks SRX5800 Services Gateway Juniper Networks IDP8200 Intrusion Detection and Prevention Appliance Juniper Networks IC6500 Unified Access Control Appliance Juniper Networks SA6500 SSL VPN Appliance Juniper Networks STRM Series Security Threat Response Managers Juniper Networks Network and Security Manager (NSM)
Campus	<ul style="list-style-type: none"> High performance/high throughput Highly scalable and adaptable solution Separate security and networking infrastructure (separate firewalls and routers) Application layer security Supports campus mobility of employees Supports various policies for conference rooms, guests, contractors, partners, employees, executives 	<ul style="list-style-type: none"> ISG1000, ISG2000 IDP8200 Juniper Networks SRX650 Services Gateway NetScreen-5200, NetScreen-5400 NSM STRM Series SA6500
Branch office	<ul style="list-style-type: none"> Requires fewer devices, an integrated solution Provides the same level of security as available at data centers and other large enterprise locations 	<ul style="list-style-type: none"> Juniper Networks SSG Series Secure Services Gateways Juniper Networks IDP200 Intrusion Detection and Prevention Appliance Juniper Networks SRX Series Services Gateways
Remote office	<ul style="list-style-type: none"> Provides a high-performance remote access solution that works across a wide variety of platforms (PCs, MACs, mobile devices, PDAs). Seamlessly integrates and operates with all types of existing vendor products Supports remote users and their accessibility via clientless connection that works on any Internet connection Provides end-to-end security by ensuring that remote clients meet the security posture (antivirus software, patch levels, etc.) Provides dynamic access privilege management Encrypts traffic to prevent theft of data in transit 	<ul style="list-style-type: none"> SA6500 or other models hosted in the data center Secure clientless access via SSL VPN (no proactive deployment to the remote user)
NOC/SOC	<ul style="list-style-type: none"> Provides visibility via a centrally managed NOC/SOC whereby all aspects of security policies and their management are controlled centrally and implemented locally Provides user-friendly enterprise-wide reports that are correlated together to minimize manual analysis of security events and to expedite corrective action 	<ul style="list-style-type: none"> STRM Series Juniper Networks NSMXpress

For more details on Juniper Networks Adaptive Threat Management Solutions, see *Appendix A: Products and Features*.

Design Considerations

Now that we've seen the solution requirements, let's take a look at the design recommendations for implementing Juniper Networks Adaptive Threat Management Solutions throughout the entire enterprise.

Design recommendations encompass three major considerations to enable the network administrator to:

- Identify and protect the primary elements (perimeter, critical resources, and remotely accessible resources)
- Deploy security technologies (firewall, IPS, UAC, SSL VPN) that are best suited for the enterprise locations (data center, branch office, campus)
- Centrally manage all aspects of security—policy, visibility, and control—so that IT managers can leverage automated tools to identify the root cause of issues, correlate events (generated from multiple devices and locations), and take corrective action, both immediate and ongoing

Protecting the Perimeter

Figure 6 highlights the locations (branch office, data center, campus, remote office) that represent the enterprise locations, some of their respective required devices, the perimeter, and the flow of inbound traffic. For further details on Juniper Networks security products, see Appendix A which lists and describes applicable Juniper Networks Adaptive Threat Management Solutions and their benefits.

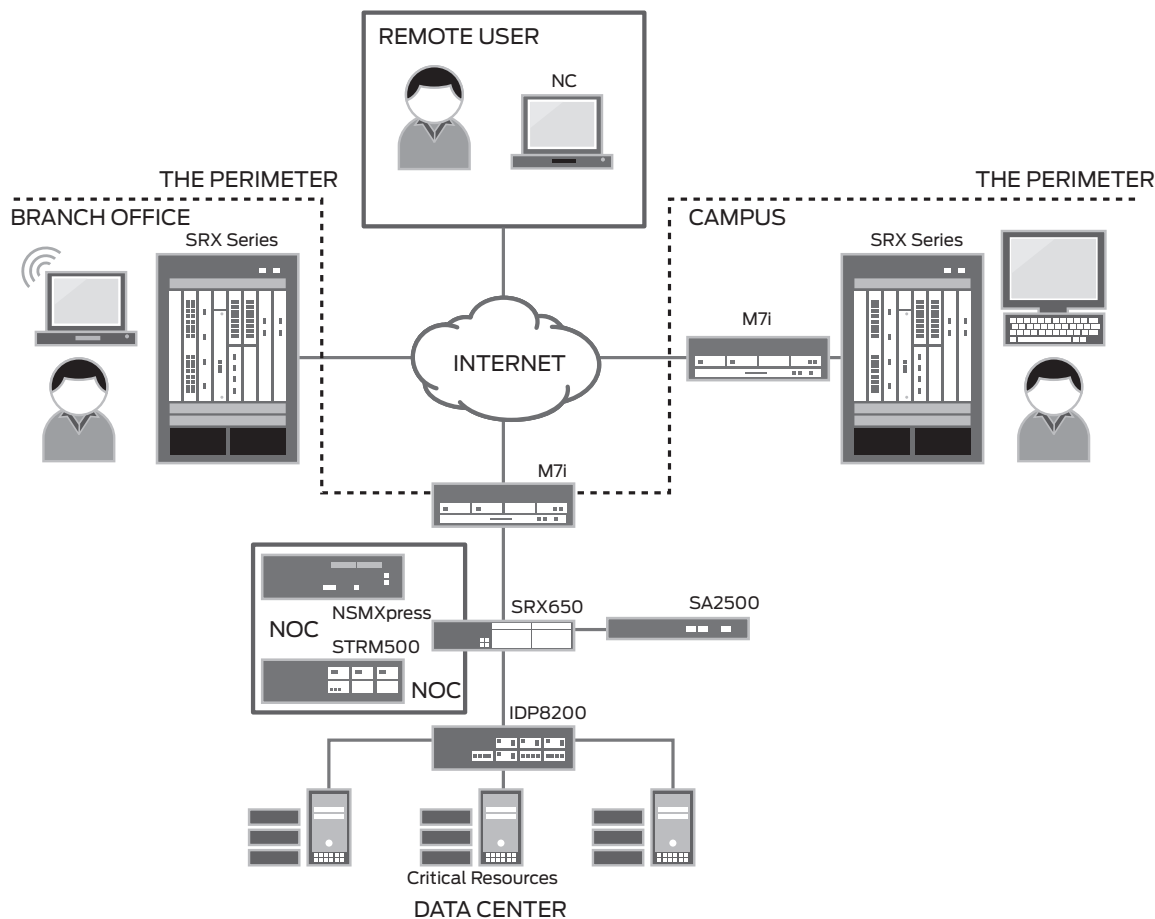


Figure 6: Protecting the perimeter (internal network)

Because there is no control over the originating traffic that attempts to reach the internal network, a security solution must be adaptable and prepared to respond to a changing risk landscape. By providing network-wide visibility and control, this solution is extremely adaptable in addressing constantly evolving threats by dynamically sharing critical risk information among IT staff. The perimeter spans across all enterprise locations, as shown in the example in Figure 6, identifying four perimeters—one for each location of branch office, data center, campus, and the remote user. It is best practice for the same security protection to apply at the different Internet edge points available for the enterprise, irrespective of the location (branch, data center, campus, or remote).

Table 4 summarizes the different types of threats typically associated with the perimeter, events that occur from the result of a threat, and recommended actions that can mitigate these threats. The threats trigger actions such as generated events and logs from more than one Juniper Networks security device. These events and logs are sent to Juniper Networks STRM Series Security Threat Response Managers, a centralized adaptive engine for further analysis and correlation. Some actions may be taken directly by the access control security device, such as when the SA Series appliance drops traffic from a rogue remote user trying to gain entry into the corporate network.

Table 4: Perimeter Threats, Events, and Recommended Actions Summary

PROTECTION	EVENTS AND LOGS USED FOR DETECTION	RECOMMENDED ACTIONS
Flooding	<ul style="list-style-type: none"> Flow information generated by Juniper Networks Junos® operating system routers and analyzed by STRM Series can indicate a pattern of flooding (flow specification RFC 1363). Router policer events indicating traffic exceeding certain thresholds. Firewall events indicating zone level screen violations. 	<ul style="list-style-type: none"> Block source IP on firewall or router using access control lists (ACLs) or policy changes. Perimeter routers sending upstream BGP flow-spec, RFC 1363 signaling messages to block a source of a DoS attack. Implement rate-limiting policies on Junos OS routers to limit the amount of DoS traffic.
Scanning	<ul style="list-style-type: none"> J-Flow information may show multiple short sessions indicating a scan. Router policer events indicating that certain traffic has exceeded the threshold level may indicate a scan. Firewall events originating from screen settings can indicate a scan. IDP Series/deep inspection events indicating application-level scans or application scans are also useful information to be processed by the STRM Series to form a unified view into the scan attempt. 	<ul style="list-style-type: none"> Firewall policy to block the source of the scan. Honey pot (entices attacker to access pretentious services first, drawing attention away from valid, critical systems) may be used to determine if the scanner is malicious. Rate limiting to limit amount of traffic coming from that specific source. Create reports and capture history showing statistics of network scanning.
Brute force	<ul style="list-style-type: none"> IPS/deep inspection events may specifically indicate a brute force attack. Resource events displaying multiple login attempts or recurring application requests can help in the overall formation of the offense by STRM Series. 	<ul style="list-style-type: none"> Time-based firewall policies that block access from clients to servers at certain times or for a specific amount of time. Create reports and capture history showing statistics of brute force attacks.
Access control	<ul style="list-style-type: none"> Router ACL events indicating attempts to make unauthorized connections. Firewall events indicating attempts to make unauthorized connections. 	<ul style="list-style-type: none"> A possible action against an access control violation suspicion is likely to move the firewall policy to a higher layer in the network.
Malicious attacks	<ul style="list-style-type: none"> J-Flow records showing abnormal traffic patterns may indicate malicious attacks. Router policer events indicating a threshold that has been exceeded can help form the overall picture of the attack. IPS/deep inspection events indicate a specific targeted attack that occurred can help specifically identify the root cause of the attack. 	<ul style="list-style-type: none"> Adaptive firewall policies to block all of the malicious attack sources. Automatic dropping of specific sessions by the IDP Series system. Reports on compromised assets that may lead to investigation so that action can be taken against the source.

Following are the design recommendations for protecting your perimeter from external attacks/threats described in the solution requirements section of this document.

Recommendations for Protecting the Perimeter

- Deploy an adaptive engine like the STRM Series along with an appropriate process so that STRM Series is configured to receive and analyze events and then trigger an educated manual security policy change.
- Use a closed loop adaptive mechanism to create an enforcement point that provides automatic adaptive logic (without requiring additional systems), such as a coordinated threat control available on SA Series devices.

Protocols signaling access controls:

- If under sustained heavy attack, it may be necessary to take action upstream, closer to the source of the attack, to free bandwidth for good traffic.
- A feedback loop between the enterprises Internet router(s) and service provider router(s) is necessary in this case; routers upstream in the Internet service provider (ISP) core can block or rate-limit blacklisted IP addresses.
- Juniper Networks routers implement BGP Flow Specification notification messages that can be used to dynamically change rate limits or blacklist IPs. Alternatively, you may report blacklisted IP addresses to your ISP or other peering routers.
- BGP Flow Specification implementation enables actions to be taken upstream, leaving your network unaffected by attacks.
- Use NSM-driven remote scripts that are executed upon detection of perimeter attacks.
- Deploy a high-performance security solution that is scalable so that the system can accommodate ever-increasing growth in network traffic and can maintain functionality during distributed DoS attacks. Juniper Networks products such as SRX series, SSG Series and ISG Series.
- Use NetScreen Series Security Systems to provide predictable CPU utilization while under load and with security service features enabled.
- Enforce a multi-tier protection plan by first having a consistent security policy and applying it to routers, firewalls, and IPS systems that are inline with the traffic.
- Routers should include rate limiters based on IP header information and TCP UDP header information to allow a next tier of defense to operate at optimal performance.
- Firewalls should screen as much information as possible prior to forwarding the traffic to the backend applications.
- Security policies should be defined in detail on the firewalls to limit traffic to only authorized communications.
- IPS and DI should be defined optimally to allow for relevant data to be reported and for optimal security.
- Reports should present easily actionable information.
- Attack source should be easy to identify and enable easy remediation.
- Devices like routers, switches, firewalls, and IPS should be administered in a way that provides important triggers and events giving meaningful data from a security perspective.
- J-Flow records should be used to provide bidirectional flow records in real time to identify traffic patterns in sessions that help administrators understand application usage of overall bandwidth. J-Flow information is sent by Junos OS.
- Flow information from the routers and switches can be collected by the flow collector to the STRM Series appliance and this information can be correlated and analyzed by the STRM Series and shown in reports.
- Compliance reports and offenses determined by event correlation use firewall logs extensively. Juniper Networks firewalls provide extensive information about traffic that has been permitted and blocked along with overall session counts for various applications.
- IDP Series profiler reports can help categorize machines on the network passively and add information about the operating system and version of applications that are running on servers when investigating infected systems or machines suspected of running malware.
- End-to-end tracking of branch office or remote users through a comprehensive collection of information by NSM and STRM Series from firewalls and routers across the enterprise enables a unified perimeter picture to be viewed.

NOC/SOC View of Perimeter Protection

The following diagram shows an STRM Series display of flows and firewall events representing a DoS attack.

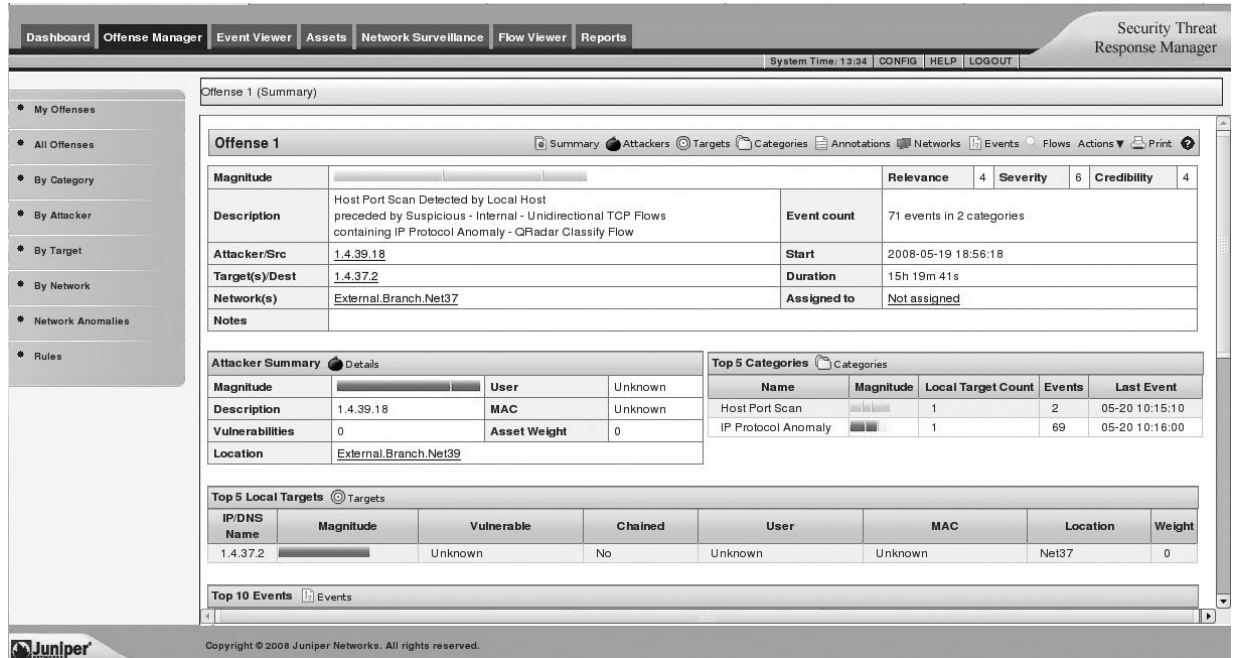


Figure 7: STRM Series showing flows and firewall events representing a DoS attack

Example of Perimeter Attack

Remote user initiates a network scan to the range of IP addresses owned by the enterprise. The scan shows that a few devices are accessible via the Internet. STRM Series picks up the network scan through the router flow events and the firewall screen events logs.

Remote user performs a port scan to the IP addresses that were found accessible in the enterprise network and identifies a few services accessible over the Internet. Following this action, the remote user tries to enumerate the service versions of the accessible services. STRM Series picks up firewall and IDP Series event logs indicating the port scan with direct correlation to the network scan previously performed.

Based on the enumeration of the services, the remote attacker attempts to exploit a known vulnerability in one of the enterprise resources. The vulnerability exploit is picked up by the IDP Series and an adaptive protection message is sent to the STRM Series appliance.

Network operator receives an email and pager alert from the STRM Series system indicating that there is a suspicious access attempt into the network that needs immediate attention. The network security operator directly logs into the STRM Series system, and through the Offense Manager decides to take action and instantly blocks access from the source IP address that is suspicious at the router level. The network processing capacity is not affected by the attacker's attempt. Additionally, an immediate remediation action is taken to verify that the protected systems have not been negatively affected.

Protecting Critical Resources

To adequately protect critical information resources, whether centrally located in the data center or distributed across multiple branch offices, Juniper Networks Adaptive Threat Management Solutions offer a multi-tier capability that combines inline Layer 3 through Layer 7 protection. These capabilities are available using stateful firewalls with high performance, in conjunction with deep inspection available on branch office devices such as SSG Series or standalone intrusion prevention appliances such as the IDP Series, or an integrated firewall and IDP Series appliance such as the ISG Series of devices implemented at the campus or data center.

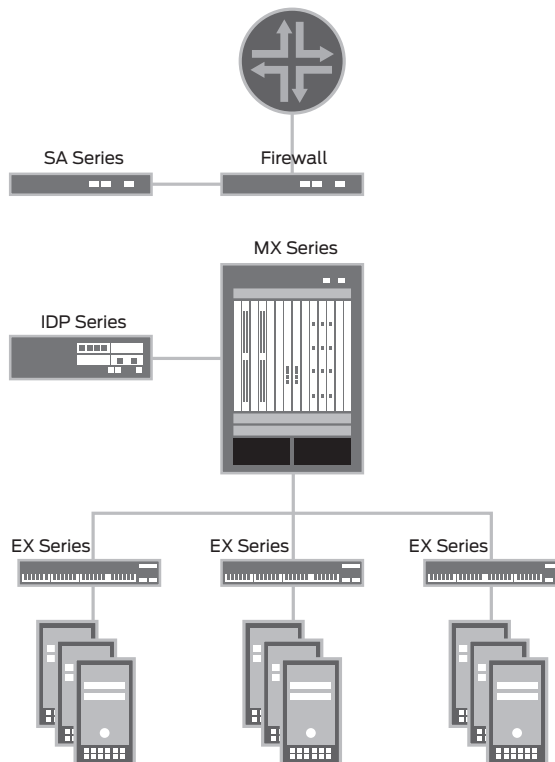


Figure 8: Protecting critical resources

Security enforcement is managed centrally from a single security management console such as NSM, which deploys a single policy to protect all critical resources throughout the information systems infrastructure. Table 5 summarizes the different types of threats, events that occur from the result of each type of threat, and the actions that can be used to mitigate these threats.

Table 5: Critical Resource Threats, Events, and Recommended Actions Summary

THREATS	EVENTS	RECOMMENDED ACTIONS
Unauthorized access	<ul style="list-style-type: none"> IPS events indicating invalid access attempts to applications. Resource events from servers or applications indicating users accessing applications and files. Firewall events indicating a pattern of failed access attempts. 	<ul style="list-style-type: none"> Block source IP on firewall or router. Apply a specific application-level policy on IDP Series to block unauthorized commands on applications.
Service level DoS	<ul style="list-style-type: none"> Service level DoS IPS/DI events may specifically indicate excessive application access attempts that can cause a DoS. 	<ul style="list-style-type: none"> Bring service back up on backend servers. Apply a specific application-level policy on IDP Series or firewall DI to block the illegal access.
Vulnerability exploitation	<ul style="list-style-type: none"> IPS/DI events can specifically indicate attacks based on a signature matching the access attempt or a protocol anomaly. Resource events indicating a disruption to service or overall patching level of an application that may be vulnerable to an attack identified by a different data source. 	<ul style="list-style-type: none"> Apply a specific application-level policy on IDP Series to block known signatures on the network and enforce protocol anomaly detection. Leverage STRM Series reports showing overall threat level to vulnerable systems in the infrastructure to change security policy.

Following are design recommendations for protecting critical resources from internal and external attacks and threats.

Recommendations for Protecting Critical Resources

The following bulleted list identifies Juniper's recommendations for protecting critical resources.

- Depending on the location, implement either deep packet inspection on the branch devices or IDP Series (standalone or integrated into ISG Series) at the campus or data center to protect not only from traditional attacks but application and network-level attacks as well, and to have policy-based access to critical resources.
- Provide application-specific protection:
 - IDP Series and firewall DI can protect local and central applications from unwanted use. Application contexts and commands can be defined in policies and blocked or reported. This allows applications to run safely and avoid the processing of undesired requests.
 - IDP Series and DI capabilities in conjunction with line rate stateful inspection allow an administrator to easily react to a request from server administrators to block or open specific traffic to allow for better availability of the application. Policies can be defined at the IP address layer, the service layer, or the application layer. This capability helps prevent unauthorized access to applications and data.
- Use Layer 7's hardening and patching capabilities:
 - Unknown application vulnerabilities can be protected by enforcing application-level protocol baseline behavior whereby non-conforming traffic will either be dealt with on the fly or simply reported to a central event repository like STRM Series for further investigation/action.
 - Known application vulnerabilities that are being exploited can be protected on the fly by IDP Series signatures. These signatures are quite powerful when a new vulnerability is discovered and even more so when an administrator is required to protect hundreds or thousands of servers in real time and the software patching process is lengthy.
 - Implement appropriate network segmentation to provide zone-specific network quota capabilities.
- Zone-specific network quota capabilities allow an administrator to connect applications with similar characteristics in distinct security zones, and define application behavior protections bound to the zone. By using this method, operators spend less time figuring out the policies that apply to certain devices.
- Application groups can be protected by limiting the number of source IP addresses by which each application can be accessed or the number of concurrent sessions the group can accept. This capability can help protect against service-level DoS attacks.
- Different zones can be configured to block specific application-level attacks or anomalies, thereby allowing for quick reaction times to emerging threats.
- Use firewall prevention polices made of address filters or rate limiting or both, similar router and switch access lists, and deep inspection of packets to determine if there is an attack, and then take the appropriate measures of dropping the infected packets.
 - Gain visibility into application usage by implementing a centralized adaptive engine like STRM Series
- IDP Series profiler collects application usage at a level that shows specific session durations and popularity or specific application actions. This capability can extend to enforce an application-level policy (for example, disallowing the HTTP GET command for certain files) on a given web server.
- Junos OS-based routers can complement the IDP Series profiler information with flow information and send it to the STRM Series.
- STRM Series can provide behavioral statistics about popularity of applications and potential trends in the coincidence of events.

NOC/SOC View of Protection of Critical Resources

The following diagram shows STRM Series display resource profiles and application attack events from the IDP Series and firewall traffic events representing an application attack/worm.

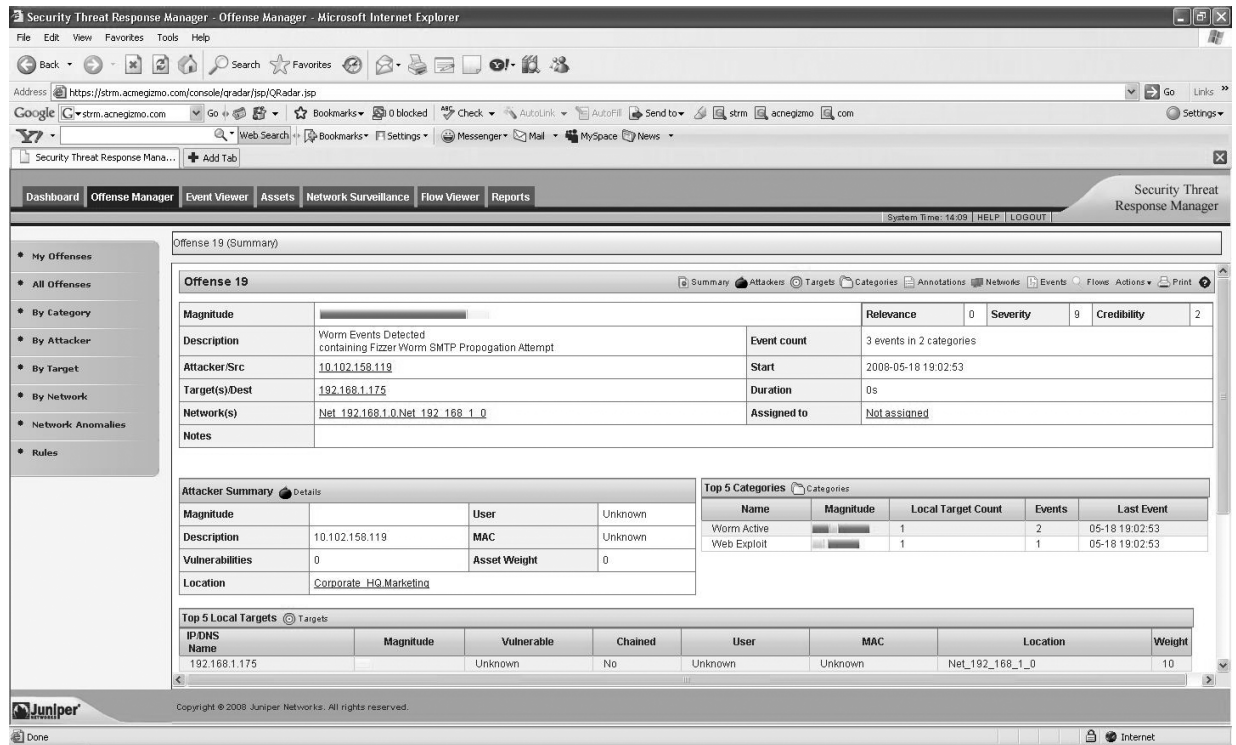


Figure 9: STRM Series showing firewall and IDP Series events representing an attack on a critical resource

Example of an Attack on a Critical Resource

A hacker identifies a vulnerable critical resource and attempts a targeted attack. The attack is unique and no signature can pick up the attack. In this scenario, the hacker attempts an unpublished exploit and gains access to the critical resource (database server). At this point, the IDP Series device reports that a protocol anomaly has been identified in the network and sends an event log to the STRM Series system.

An attacker, through controlling the compromised system, pulls tools from the Internet to execute a script on the server and extract sensitive data. The ISG Series reports that the server has connected to a known black list Internet server, thereby raising a flag for the outbound connection. Lastly, the logs are sent to the central STRM Series system, where correlation of events and logs takes place and appropriate alerts are generated. The network operator at this point limits the bandwidth from the server to any Internet target.

Once the data has been extracted, the hacker tries to open a single connection to the attacker machine and starts transferring a 3 GB database file. The router reports this prolonged flow to STRM Series, which immediately raises the flag and sends an alert to the network operator. The limited bandwidth allows the network operator sufficient time to block the connection.

Based on the alert that was sent by STRM Series, the network operator can block the connection, apply strict security policies, and learn more about the magnitude of the hacker's actions.

Protecting Remote Access

Juniper Networks Adaptive Threat Management Solutions support secure remote access into enterprise applications, while allowing for dynamic measures to control the remote user access entitlement in reaction to threats originating from the remote user. Such threats can be attempts to access resources, or information disallowed to the remote user, or the spread of a worm throughout the network. Additionally, systems making up this solution adapt automatically to changes in the access privileges as populated to the corporate name directories and user stores.

The solution's remote access protection provides detailed visibility through STRM Series by correlating all access and network usage information from the Juniper Networks firewalls, SA Series, and IDP Series devices, as well as all corporate systems such as servers and applications.

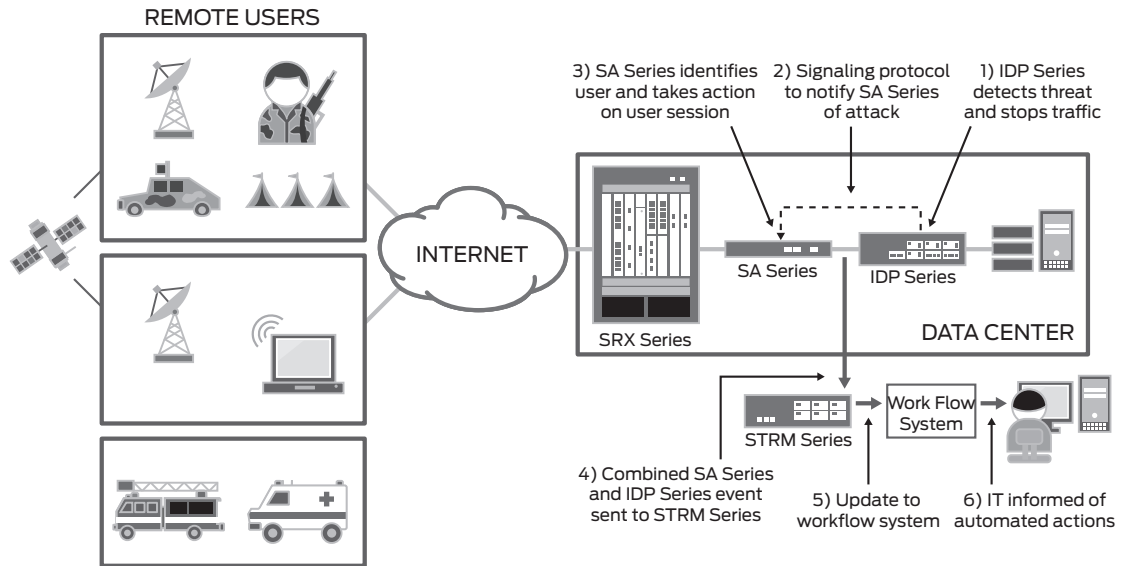


Figure 10: Protecting remote access

Table 6 summarizes the different types of threats, events that result from each kind of threat, and the actions that can mitigate these attacks.

Table 6: Remote Access Threats, Events, and Recommended Actions Summary

THREATS	EVENTS	RECOMMENDED ACTIONS
Unauthorized access	<ul style="list-style-type: none"> IPS events indicating invalid access attempts to applications. Resource events from servers or applications indicating users accessing applications and files. Firewall events indicating a pattern of failed access attempts. 	<ul style="list-style-type: none"> Block source IP on firewall or router. Apply a specific application-level policy on IDP Series to block unauthorized commands on applications.
Service level DoS	<ul style="list-style-type: none"> Service level DoS IPS/DI events may specifically indicate excessive application access attempts that can cause a DoS. 	<ul style="list-style-type: none"> Bring service back up on backend servers. Apply a specific application-level policy on IDP Series or firewall DI to block the illegal access.
Vulnerability exploitation	<ul style="list-style-type: none"> IPS/DI events can specifically indicate attacks based on a signature matching the access attempt or a protocol anomaly. Resource events indicating a disruption to service or overall patching level of an application that may be vulnerable to an attack identified by a different data source. 	<ul style="list-style-type: none"> Apply a specific application-level policy on IDP Series to block known signatures on the network and enforce protocol anomaly detection. Leverage STRM Series reports showing overall threat level to vulnerable systems in the infrastructure to change security policy.

Recommendations for Protecting Remote Users

The following list identifies our recommendations for protecting remote users.

- Deploy an integrated appliance such as an SA Series device that operates seamlessly across multiple platforms and enables easy accessibility without compromising security efforts. Juniper Networks solution provides network-wide coverage, including branch and satellite locations, thus minimizing downtime by preventing security attacks from occurring in the first place.
- Deploy IDP Series appliances at the data center in conjunction with the SA Series device so that policies can be applied to discover viruses, and can apply a specific set of rules (such as the dropping of packets) to address security breaches.
- Implement appropriate policies to protect the network and applications from the remote user.
- Using SSL VPN, an administrator can enforce access to applications throughout the enterprise and create an additional security point to control application access privileges—the remote access infrastructure is the first line of security provided to protect the remote user.
- A seamless authorization policy is created using role-based access control founded on central LDAP or Active Directory. Hence, remote users are easily granted access only to resources that the enterprise allows them to have. Access privilege changes in the directories are represented automatically in the SSL Access policy.
- Threats originating from remote users will automatically be handled in a similar manner as local threats to the network. If a remote user creates a threat, the system can automatically assign the user session to a quarantine access profile.
- Implement detailed logging and accounting for remote access protection.
- Through detailed logging and accounting usage information, the enterprise can gain visibility into compliance with different regulations.
- Logging and accounting information can include information about IP address assignment at certain time frames. The information sources can be SSL VPN, firewalls, and IDP Series appliances, and the STRM Series can correlate the user data with the TCP session information.
- Additionally, information provided by SSL VPN can show detailed Web application usage by user and access to solid state information.
- The information presented by STRM Series can easily be viewed and presented to allow for efficient policy changes in the firewall and IDP Series infrastructure.

NOC/SOC View of Protecting Remote Access

The following diagram shows an STRM Series display of remote access events, IDP Series event logs, and firewall events representing a remote access originated worm.

The screenshot displays the STRM Series interface for an offense. The main view shows a summary of the offense with the following details:

Magnitude	Relevance	Severity	Credibility
AdTM: Malicious User Activity - Quarantined containing Unwanted program moved to quarantine	4	8	4

Additional details include:

- Description:** AdTM: Malicious User Activity - Quarantined containing Unwanted program moved to quarantine
- Attacker/Src:** 172.20.1.244
- Target(s)/Dest:** Remote (1)
- Network(s):** other
- Notes:**
- Event count:** 6 events in 2 categories
- Start:** 2009-05-21 04:34:51
- Duration:** 3h 48m 7s
- Assigned to:** Not assigned

The interface also includes sections for:

- Attacker Summary:**

Magnitude	User	MAC	Asset Weight
172.20.1.244	Unknown	Unknown	0
- Top 5 Categories:**

Name	Magnitude	Local Target Count	Events	Last Event
Virus Detected	4	0	3	05-21 08:20:59
Session Denied	4	0	3	05-21 08:20:59
- Top 10 Events:**

Event Name	Magnitude	Device	Category	Destination	Time
Session Denied - Event CRE	4	Custom Rule Engine-8 : acmestrm	Session Denied	172.20.1.65	05-21 08:20:59
Session Denied - Event CRE	4	Custom Rule Engine-8 : acmestrm	Session Denied	172.20.1.65	05-21 08:19:54
Unwanted program moved to quarantine	4	JuniperSA @ 172.20.1.65	Virus Detected	172.20.1.65	05-21 08:20:59
Unwanted program moved to quarantine	4	JuniperSA @ 172.20.1.65	Virus Detected	172.20.1.65	05-21 08:19:54
- Top 5 Annotations:**

Annotation	Time	Weight
"CRE Event". CRE Rule description: [AdTM: Malicious User Activity - Quarantined] Coordinated Threat Control - Quarantined Users IDP reported malicious activity by user	05-21 04:35:28	6
"CRE Event". CRE Rule description: [AdTM: Malicious User Activity - Quarantined] Coordinated Threat Control - Quarantined Users IDP reported malicious activity by user	05-21 08:20:43	6
"[2] 'TargetEventAnalysis'. The number of events this attacker generated during this attack, was deemed worth a value of 2 on a scale of 0-10, with higher values indicating high volumes of events generated, and lower numbers indicating a smaller grade attack.	05-21 08:21:43	6
[AdTM: Malicious User Activity - Quarantined] "Offense Renamed". This offense has been renamed to "AdTM: Malicious User Activity - Quarantined" by user request, based on an Event Rule that has fired. Typically this is done because a particular sequence of recognizable and important security events has been detected, and the offense has been named accordingly."	05-21 04:35:28	1

Figure 11: STRM Series showing events and logs from SA Series and IDP Series for protection of remote access

Example of Remote Access Attack

Step 1: User connects using a browser to the enterprise portal on the SA Series device. User logs in with user-specific credentials. Thereafter, the user launches the network connect virtual adapter and is assigned an IP address of the enterprise internal network. WXC Client will also be automatically downloaded from the SA Series device which is used to accelerate traffic to the data center from the client PC. Host Checker automatically downloads and installs from the SA Series upon logging into Network Connect NC VPN; this is transparent to the end user. Based on user-specific policy setup, the user will be allowed to connect to a known server resource such as Microsoft Outlook™.

Step 2: The user's machine may inadvertently spray a worm onto the network that will reach multiple servers. The IDP Series picks up the attack based on a known signature and sends the attack information to both STRM Series and the SA Series devices.

Step 3: The SA Series device immediately associates the attack with the relevant user. Based on the threat management policy defined on the SA Series device, it will either terminate the user session or map the user to an alternative role. In the case where users are mapped to the alternative role, they are presented with remediation information that they can use to fix their machine and then log in again.

Step 4: STRM Series will report the worm as it is launched, and allow network operators and administrators to look through and identify how far the worm has propagated and what remediation actions are required in the network.

Protecting from Insider Threats

Today's networks need to effectively handle unmanaged devices and branch/guest users attempting network access, as well as address support for unmanaged devices and a session-specific access control policy for each user. Juniper Networks Adaptive Threat Management Solutions support secure LAN access through Unified Access Control and IDP Series appliances coupled with NSM and the STRM Series for management and visibility.

UAC combines user identity and device security state information with network location to create a unique, session-specific access control policy for each user that is enforced throughout the network. Unified Access Control can be enabled at Layer 2 using any vendor's 802.1X-enabled switches or wireless access points, or at Layer 3 using any of Juniper Networks firewalls, or a combination of both.

UAC solutions enable businesses to establish and enforce policies that grant users differentiated network access based on their roles. For instance, full-time employees may have unrestricted access, while partners and contractors may be able to reach designated servers, and guests may have limited-bandwidth Internet access. Individual devices can also be scrutinized to ensure compliance with security standards. For example, if a laptop does not contain the latest antivirus software, the user may be directed to a quarantine VLAN and given the option to update the computer's security software or be denied access altogether. The UAC solution delivers rich policy enforcement capabilities that extend to the network edge. Securing intranet applications and resource traffic is vital to protecting your network from insider threats. You can add levels of application security to detect internal threats generated from branch and campus users who are authenticated through the UAC Series by integrating UAC with an IDP Series sensor.

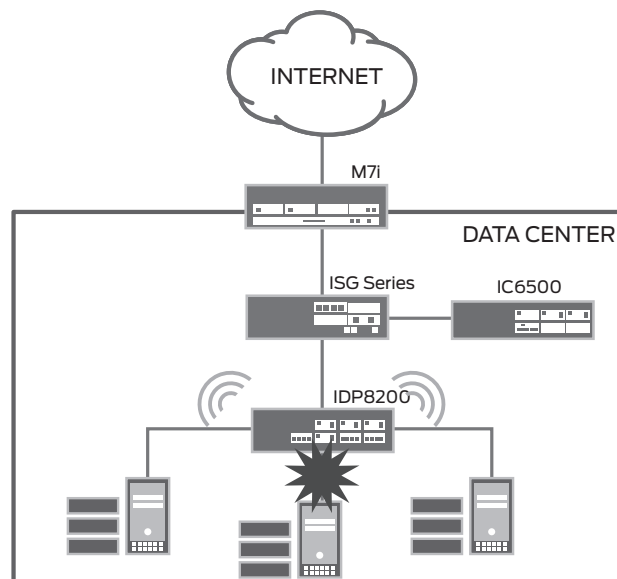


Figure 12: Protecting remote access

Recommendations for Protecting Against Insider Attacks

The following list identifies the recommendations for detecting and preventing insider attacks.

- Deploy an integrated appliance such as an IC Series device that operates seamlessly across multiple platforms and enables easy accessibility without compromising security efforts. Juniper Networks solution provides network-wide coverage, including branch and satellite locations, thus minimizing downtime by preventing security attacks from occurring in the first place.
- Deploy IDP Series at the data center in conjunction with IC Series UAC Appliances so that policies can be applied to discover viruses and can apply a specific set of rules (such as the dropping of packets) to address security breaches.
- Implement appropriate policies to protect the network and applications from the trusted user on the corporate LAN.
- Using UAC Series solutions, an administrator can enforce access to applications throughout the enterprise and create an additional security point to control application access privileges—the remote access infrastructure is the first line of security provided to protect the remote user.
- A seamless authorization policy is created using role-based access control found in central LDAP or Active Directory repositories. Hence, genuine users are easily granted access only to resources that the enterprise allows them to have. Access privilege changes in the directories are represented automatically in the UAC Series access policy.
- Threats originating from authorized LAN users will automatically be handled in an effective and efficient manner. If a user doesn't comply with Acceptable Use Policy (AUP), the system can automatically assign the user session to a quarantine access profile.
- Implement detailed logging and accounting to track and monitor all end user activity.
- Through detailed logging and accounting usage information, the enterprise can gain visibility into compliance with different regulations.
- Logging and accounting information can include information about IP address assignment at certain time frames. The information sources can be IC Series, SSL VPN, firewalls, and IDP Series appliances, and the STRM Series can correlate user data with the TCP session information.
- The information presented by STRM Series can easily be viewed and presented to allow for efficient policy changes in the firewall, switching, and IDP Series infrastructure.

Example of an Insider Attack

Step 1: User is inside the enterprise network and connects to the corporate network by using credentials via Juniper Networks Odyssey Access Client.

Step 2: The user goes to the command line and brings nmap to life against the accounting systems to perform a scan against that accounting subnet. The IDP Series picks up the attack based on a known signature and sends the attack information to both STRM Series and IC Series devices.

Step 3: The IC Series device immediately associates the attack with the relevant user. Based on the threat management policy defined on the IC Series, it will either terminate the user session or map the user to an alternative role. In the case the following can occur: the user can be mapped to the alternative role (quarantined), or the user can be taken off line until the administrator determines what specific action to take.

Step 4: STRM Series will report this activity and escalate it as a critical offense in the dashboard, allowing network operators and administrators to look for and identify the user.

Conclusion

To effectively protect today's enterprise, network administrators, IT managers, and network security specialists must have insight into the multiple types and levels of evolving threats that impact the integral elements of the enterprise, including perimeter, critical resources, and remote access. Juniper Networks Adaptive Threat Management Solutions is a dynamic and high-performance security solution that adapts to changing risks. By leveraging a cooperative system of tightly integrated security products, this solution provides network-wide visibility and control that adapts and secures the network against constantly evolving threats. By providing centralized security management and enterprise-wide visibility and control with multilayered security, this industry-leading security solution enables network administrators to protect their perimeter, critical resources, and remote access of users and devices to prevent threats from compromising their organization's revenue, reputation, and intellectual property.

Appendix A: Products and Features

Table 7 summarizes the key products and their benefits that are integral components of Juniper Networks Adaptive Threat Management Solutions.

Table 7: Products and Features Summary

PRODUCTS	FEATURES
Firewall/VPN	<ul style="list-style-type: none"> High-performance, purpose-built line of firewalls scaling from enterprise to service provider networks. Tightly integrated set of best-in-class security applications to protect against worms, trojans, viruses, and other malware.
IDP Series	<ul style="list-style-type: none"> High performance with industry-leading 10 Gbps throughput. Comprehensive easy-to-use protection to stop network and application-level attacks.
SA Series	<ul style="list-style-type: none"> Market-leading SSL VPN features, including secure virtualization, access privilege management, Host Checker, monitoring, and reporting. Scalable up to 10,000 concurrent users on a single SA6500, or up to 30,000 concurrent users in a four-unit cluster.
NSM	<ul style="list-style-type: none"> Centralized security policy management. Facilitates rapid deployment while minimizing ongoing operational costs.
STRM Series	<ul style="list-style-type: none"> Multivendor support for major network and security devices for correlation, collection, analysis, and reporting of logs. Network Behavior Anomaly Detection (NBAD) discovers aberrant activities using network flow data, and enhances the ability to identify zero-day threats by baselining network traffic patterns. Compliance support for monitoring, reporting, and auditing processes of regulatory and security standards. Provides a detailed view into the systems that are available remotely and suggests appropriate changes.
Routers	<ul style="list-style-type: none"> Granular QoS with low latency and jitter performance to support voice, video, and other real-time applications. High-performance J-Protect Network Address Translation (NAT), stateful firewall, attack detection, and IPsec via Adaptive Services PIC. Comprehensive range of interfaces supporting NxT1/E1/DS3/E3, OC-3/STM-1, fast Ethernet, and Gigabit Ethernet WAN links. Service-built architecture supports multiple services on a single platform.

Appendix B: Threats and Definitions

Table 8 lists and defines the different types of threats.

Table 8: Threats and Definitions

TYPES OF THREATS	DEFINITION
Malicious hacking	Not done for the purpose of theft, malicious hacking is an indiscriminate form of hacking; there is also theft-related hacking which can easily attack the perimeter.
Scanning	Otherwise known as reconnaissance are systems scanning open ports for the purposes of connection or DOS attacks.
Brute force	Brute force Is an attack on a website whereby the attack continues to try all sign-on and password permutations. Each attempt is an attack in its own right and keeps the system under attack replying to each failed attempt.
Flooding	Flooding comes in various forms; however, in general terms this is an attack whereby the system that is being flooded has to respond in either an active or passive manner, thereby taking up its own CPU cycles.
Unauthorized access	An attack against critical resources with an overriding load of packets meant to keep the server busy and unable to service other systems, this type of attack is used, for example, to open ports to exploit the vulnerability of the resource.
Server DoS	Server DoS targets a specific service on a server such as HTTP, SMTP, or other services and deliberately overwhelms the device by sending harmful traffic which makes the device inoperable and unavailable for end users.
Vulnerability exploitation	A remote attacker takes advantage of software vulnerabilities (software running on a server) by employing a tool that exploits the vulnerability of the software, and attempts to stop the service with the goal of taking control of the system.
Identification spoofing	Identification spoofing describes when an attacker appearing to be a trusted system finds back doors to applications and accesses them without authorization. Because virus or worm protection may not be available in remote places or on remote systems, corporate devices can be infected via remote access portals that link to the corporate systems.
Unauthorized access to resources	A user who does not have the authority or privilege to access a specified resource.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.

Corporate and Sales Headquarters

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

Copyright 2010 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS 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.

8030002-004-EN Nov 2010

 Printed on recycled paper