Implementation Guide

Branch Office UTM Implementation Guide

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408.745.2000
1.888 JUNIPER
www.juniper.net

Part Number: 801011-001 Oct 2008

Table of Contents

List of Figures

Introduction

Wide-spread adoption of new applications operating over the Internet has created new types of security threats for today's distributed enterprise. This trend has sparked growth in the IT security space, where hundreds of vendors have emerged offering point solutions to protect against most threats. The modern enterprise uses many different products to protect against several "vectors of attack" and to mitigate risks. Anti-X technologies such as URL filtering, network antivirus and intrusion protection have been selectively deployed throughout enterprise networks. These anti-x technologies are predominately deployed in larger campus and data center networks for protecting the most critical resources.

Deploying this type of security technology across entire distributed enterprises at hundreds of small branch offices, often with minimal onsite IT support, has been until recently impractical and simply cost-prohibitive. Security at the branch has always been a compromise between the cost of managing a large number of branch security devices and the security benefits provided. As a result, large distributed enterprises have typically backhauled all Internet traffic through the head-end, which incurs large recurring costs because far larger head-end bandwidth is required. Also, enterprises simply ignored branch security altogether, giving up defense-in-depth, exposing branch users and the entire enterprise network to a myriad of threats on the Internet.

Juniper Networks has integrated these latest security technologies into its entire line of branch office firewalls, consolidating key security functions into a single device. Juniper Networks Secure Services Gateways (SSG) offer on-board URL filtering, antivirus/worm and intrusion prevention features, in addition to proven firewall, VPN, and routing functionalities. These features are managed seamlessly at scale using Juniper Networks Network and Security Manager (NSM).

Scope

This guide explains how to implement and manage Juniper Networks Unified Threat Management (UTM) features. In this paper, we address typical security threats that face today's distributed enterprise, and discuss how an appropriate security policy enforced by Juniper Networks family of SSG devices can help mitigate these threats. We then address, in detail, how to deploy and manage these features efficiently and uniformly throughout a distributed enterprise, across hundreds of remote branch offices, each protected by Juniper Networks proven security gateways.

Target Audience

- Security and IT engineers
- Network architects

Design Considerations

Understanding the Threats—Why Enterprises Need UTM Protection

Distributed enterprise networks face ever-increasing security threats such as viruses, trojans, and worms that infect users constantly through Web sites, email, Webmail, Instant Messaging (IM), and peer-to-peer applications. As a result, these threats require additional IT staff attention and efforts.

More and more users access inappropriate Web sites or download illegal files, thereby consuming precious bandwidth and creating business liability issues. Users and guests can attack servers using well-known vulnerabilities and can create serious information leaks or security breaches.

Rogue Internet sites that target users through server-to-client attacks create backdoors into your network or infect other users. A denial of service (DoS) attack is another type of threat against your own network consuming bandwidth and resources that can cause downtime and lost productivity. The source of these threats (attack vectors) includes the Internet, infected or malicious users, servers or guests, and unauthorized users. Their targets are your users and guests, servers and storage systems, VoIP infrastructure, and most importantly, the enterprise network itself. According to Dark Reading (8/13/08), on the average during the second quarter of this year, more than 10 million zombie computers (systems infected by "bot" and controlled remotely by cyber criminals) were sending spam and emails with malware every day.

Today's enterprise is even faced with protecting the Internet itself (other sites) from malicious or infected users on your network. This has become increasingly important as enterprises strive to create a barrier of liability by blocking attacks, viruses, and worms originating from inside the corporate network. This barrier has expanded recently to include blocking or logging illegal Web sites, peer-to-peer file sharing, and IM conversations.

For the security or IT administrator, protecting against all attack vectors might seem like an impossible task. However, network administrators and IT professionals can avoid spending countless hours designing and configuring security policies. Juniper Networks SSGs, combined with the examples and best practices outlined in this document, will steer you in the right direction as you work to improve security, optimize bandwidth usage, and reduce liability for your distributed enterprise.

Juniper Networks UTM Solutions for Branch Office Security

The Juniper Networks UTM approach takes other vendors' unified threat management to another level, offering more than just point products. Juniper Networks offers a full line of branch and regional office SSG devices with onboard UTM functionality, in addition to high-end Integrated Security Gateways (ISG) for the data center or larger regional offices. All devices run ScreenOS, an operating system designed from the ground up to deliver high-performance, policy-based stateful firewall and IPsec VPN connectivity. Additionally, all devices are managed seamlessly using NSM to enable centralized policy provisioning, log consolidation, and reporting.

The UTM security features include:

- Stateful inspection firewall to perform access control and stop network-level attacks
- Intrusion Prevention System (Deep Inspection firewall) to stop application-level attacks
- Best-in-class anti-malware protection based on Kaspersky Lab's scanning engine that includes antivirus, anti-phishing, anti-spyware, anti-adware protection to stop viruses, trojans, and other malware before they damage the network
- Anti-spam through a partnership with Symantec to block spammers and phishers
- Web filtering using Websense to block access to known malicious Web sites and Web content that is inappropriate for your business
- Site-to-site IPSec VPN to establish secure communications between offices
- DoS mitigation capabilities
- Application Layer Gateways (ALGs) for H.323, Session Initiation Protocol (SIP), Skinny Client Control Protocol (SCCP), and Media Gateway Control Protocol (MGCP) to inspect and protect voice over IP (VoIP) traffic.

For further details, refer to Concepts & Examples ScreenOS Reference Guide Vol. 6, Voice-over-Internet Protocol. This reference guide describes the supported VoIP ALGs and specifically covers the H.323 protocol. It provides examples for configuring the H.323 ALG on the Juniper Networks security device and SIP ALG, and it presents an overview of the MGCP ALG, listing the firewall security features of the implementation. Examples of typical scenarios follow a summary of the MGCP architecture.

Hardware Components

The Juniper Networks hardware components relevant to UTM include SSG and ISG firewalls and the SRX-series services gateways.

SSG

Juniper Networks industry-leading SSG family of products running ScreenOS consists of comprehensive and cutting-edge attack prevention features continuously developed and fine tuned over time. Each product release continues to further evolve UTM capabilities, as well as enable further customization to meet the needs of any organization's security policies. Today, ScreenOS offers best-in-class UTM features which run on board SSG devices. These features include DoS protection, deep packet inspection, URL logging and filtering, complete anti-x protection, including network antivirus and anti-spam protection.

ISG

The Juniper Networks ISG devices are purpose-built, security solutions that leverage a fourth-generation security application-specific integrated circuit (ASIC), the GigaScreen3, along with high-speed microprocessors to deliver unmatched firewall and VPN performance. The ISG family of products also offers integrated hardware-based Intrusion Detection and Prevention (IDP) that allows enterprises to deploy a high-performance single box solution to secure branch office connectivity to the data center or VPN head-end.

SRX

Juniper Networks SRX-series products are next-generation services gateways based on a revolutionary architecture that provides market-leading scalability and service integration.

Advanced SRX-series security features automatically detect and mitigate threats, while routing features intelligently to prioritize and accelerate traffic. These features protect and distribute advanced services and applications to support millions of subscribers or multiple enterprise departments across the network.

The SRX-series includes the following integrated components:

- Firewall
- Intrusion Prevention System (IPS)
- DoS
- Quality of Service (QoS)
- Network Address Translation (NAT)
- Routing and switching

The SRX-series services gateways scale in performance, including shared cards and power supplies.

Central Management

Juniper Networks centralized management technologies primarily consist of the Juniper Networks Network and Security Manager (NSM) and its appliance version, NSMXpress.

NSM

Central management is critical to managing geographically distributed security devices. Juniper Networks NSM offers centralized policy management, log consolidation and reporting. NSM manages SSG devices, NetScreen firewalls, IDP appliances, EX-series Ethernet switches, J-series routers, Secure Access SSL VPN, and the Unified Access Control (UAC) Infranet Controller.

Additional Juniper Networks devices are often being added to the NSM support list. To find the latest support list, visit Products & Services. NSM also contains key features designed specifically for the distributed enterprise such as device provisioning, licensing, and automatic "roll-back" during a failed configuration update.

NSMXpress

NSMXpress is an appliance version of NSM. It simplifies the complexity of security device administration by providing a single integrated management interface that controls every device parameter. This robust hardware management system installs in minutes with full high availability (HA) support, making it easy to scale and deploy.

Larger distributed enterprises should consider using at minimum a four box NSM configuration as outlined in the *Network and Security Manager Administration Guide* at http://www.juniper.net/techpubs/software/management/security-manager/nsm2008_1/nsm2008.1_admin_guide.pdf

The four box approach divides the primary graphical user interface (GUI) server and device server into separate boxes, each located across separate geographic data centers. This enables physical site, independent HA for device management, and logging.

STRM

Juniper Networks Security Threat Response Manager (STRM) offers integrated log management and threat correlation capabilities, security information and event management (SIEM), and network behavior analysis in a single console that reduces security management solution acquisition costs and improves IT efficiency.

Juniper Networks recommends using a centralized SEIM solution to get a comprehensive view of the enterprise security state and be able to respond to threats in real time.

All mission-critical devices in the branch office should be configured to send logs to the STRM. There are plenty of built-in correlation rules that can be used to detect virus and worm activity inside the network. STRM can isolate the source and identify corrective measures for dangers hiding in daily network activity. STRM flow and event processors provide distributed scalability for the processing of network and security events, and network and application flow data. Typically, STRM 500/2500 can be deployed at the branch office to enhance the scalability of an enterprise SIEM solution.

STRM can efficiently correlate UTM log information from various branch offices, and it can alert the security operations center/network operations center (SOC/NOC) administrators about an impending worm or virus outbreak that may sprawl across the network from the branch office to the data center.

Implementation—Best Practices when Deploying UTM Capabilities

The following sections describe recommended best practices when deploying UTM.

Deep Inspection

Juniper Networks recommends using Deep Inspection (DI) for any service where one of the endpoints might contain malicious code that can exploit vulnerabilities at either of the endpoints, for example any inward/outward bound network traffic from/to the untrust zone of the network. Your network uses the untrust zone interface to connect to the Internet. The untrust zone connects the networks that are *not* fully controlled by the overall enterprise to the security gateway of the branch office.

DI allows you to inspect traffic at the application layer, relying on regular expressions (Regex) to determine malicious content in a packet. For example, if a worm spreading over the Internet attempts to exploit your Internet Information Server (IIS) Web vulnerabilities by sending a harmful string of characters to your Web server, a custom signature can identify that attack string and stop it. By applying the custom signature to a policy, the traffic in that policy is inspected for that specific string.

Therefore, it is important to use only signatures that are relevant to inbound or outbound traffic. For example, for outbound HTTP traffic originating from an employee's computer to the Internet (*trust to untrust*), it is extremely important to secure the server-to-client vulnerability vector for mitigating risk to employee computers.

Additionally, Juniper Networks recommends that you secure the client-to-server interactions to limit enterprise liability in case of attacks originating from their IP address space. It is critical to ensure that all attack blocking and identifications are logged and monitored regularly.

Antivirus

Juniper Networks recommends that enterprises scan all peer-to-peer and email traffic for worms, viruses, trojans, and other malware to ensure that branch office devices do not receive any contaminated content. Some customers might choose to block out peer-to-peer traffic completely.

In addition, Juniper Networks recommends applying scanning to all external file transfers/sharing, more specifically to three different traffic types:

- Webmail
- User point of presence (POP3) mail retrieval
- Mail server Simple Mail Transfer Protocol (SMTP) inbound email.

Further, it is important to centrally collect all logs originating from the antivirus engine. This allows an audit trail for liability purposes and allows for easy reporting of infected users.

NOTE: Malware often infects machines that are not on the corporate network, for example when users take their laptops for home or travel use. Also, malware infections can come from within the branch network or spread through USB adapters, MP3 players, and CD-ROMs. To ensure maximum protection against viruses, Juniper Networks always recommends an in-depth defense approach. IT managers should augment network-level antivirus with traditional host-based antivirus and security software that scans the users hard drive, decodes compressed files or scripts, and evaluates the entire contents of the user's PC for potential threats.

Anti-spam

Juniper Networks recommends installing the anti-spam engine on the UTM device if the mail server is located at the branch office. However, this is often not the case in a distributed enterprise, as the anti-spam engine is located in the data center or at headquarters.

Web Filtering

Juniper Networks recommends filtering all HTTP/FTP traffic for threats using Web filtering. This helps ensure that branch users do not send or receive any contaminated content on your network, and allows the enterprise to customize, detect abuse, and enforce an acceptable-use policy for Internet access. The Web filtering profile should comply with the enterprise's top level security policy and acceptable use policy. It is important to centrally collect all logs from Web filtering engines across all branches so that they can be viewed alongside other security logs.

Redirected Web Filtering

In large-scale branch VPN deployments where logging and reporting are key Web concerns, Juniper Networks suggests using the *Redirect* method where HTTP URLs are redirected to a centralized Websense server for logging and classification. In this case, filtering, reporting, and daily management and updates are all performed on the centralized Websense servers maintained at the head-end. As a management advantage, when a change is made to the Web filtering policies, *only* the central server requires updating as opposed to updating all branch devices. If high availability is a concern, a pair of Websense servers can be used, with one located at each data center and accessed through separate VPNs to provide extra resiliency. ScreenOS firewalls can also be configured to "fail-open" if the Web filtering server cannot be contacted.

Design and Implementation Background

Branch Types, Access, and Connectivity Background

Juniper Networks reference architecture builds a model that addresses the security and availability needs of the enterprise, as well as the number of users at particular branch office locations. Juniper Networks classifies branch office architectures into three branch office profiles: Branch Office Type A – Basic, Type B – Optimized, and Type C – Critical. Each of these three profiles can vary in size from supporting as few as 5 users to hundreds of users.

Branch Office Type A – Basic: This branch office profile typically consists of a single integrated security and routing device and one or more Ethernet switches to address the number of devices that are connected. WAN connectivity to the data center is implemented with single or dual Internet connections. This profile is designed for small branch office locations where cost effectiveness is paramount (for example, retail facilities and small offices), and supports a basic feature set with standard availability. Typically, these locations consist of a simple LAN infrastructure to provide employee access. Very small branch office locations can simply utilize the switching capabilities of the integrated security and routing device.

Branch Office Type B – Optimized: This branch profile consists of two integrated security and routing devices and two or more Ethernet switches, all deployed in a fully meshed configuration. WAN connectivity to the data center utilizes both private WAN and Internet connections. This profile supports small to medium-size branch office locations and offers high availability. Typically, these are larger offices and might require support for network segmentation or separate networks like employee networks and guest networks that typically require identity-based access control.

Branch Office Type C – Critical: This branch profile consists of two edge routers, two security gateways, and two or more Ethernet switches, all interconnected using full mesh. WAN connections to the data center use both Internet and private WAN connectivity. This profile provides the highest level of performance and availability, and it is designed to support diverse requirements for services such as VoIP and video. Also, some of these types of branch offices might be directly on the MPLS network as well. In addition to network segmentation and/or separate networks, these branch offices can host some local servers and services that typically require a separate server LAN network.

Use Cases

In this section, we examine four use cases relevant to branch office security and distributed enterprises.

- Secure against Internet threats (inbound)
- Secure the Internet against threats in the branch (outbound)
- Secure the enterprise WAN/VPN from the branch (outbound and inbound)
- Provide guest users restricted Internet access while blocking branch/VPN access

Secure Against Internet Threats (Inbound)

This design uses UTM to protect branch office employees from the vulnerabilities of the Internet. UTM's goal here is to protect the branch office itself from security threats, increase employee productivity, and reduce IT's burden in detecting viruses, trojan, or worm infections. For this purpose, we use UTM to protect branch office employees from malicious Web sites associated with server-to-client attacks by using DI, URL filtering, and network-level antivirus. This implementation also conserves bandwidth at the branch office for legitimate business purposes using outbound QoS.

Secure the Internet Against Threats in the Branch (Outbound)

In this design, UTM helps protect the Internet from branch office employees and guests. UTM's goal here is to increase worker productivity by enforcing Internet usage policy using strict firewall rules and URL filtering. We also create a "Barrier of Liability" blocking outbound attacks, file sharing, and illegal sites by using DI and application enforcement. We also conserve bandwidth at the branch office for legitimate business purposes using inbound (QoS).

Secure the Enterprise WAN/VPN from the Branch (Outbound and Inbound)

This design uses UTM to protect the distributed enterprise from the branch office and vice versa. Here we must reduce the spread of worms/trojans/spyware beyond any branch office using network-level antivirus. We must also block attacks and floods at the source (the branch office) using DI and flood protection. And we must conserve VPN bandwidth at the data center and branch office for legitimate business purposes using inbound and outbound QoS.

Provide Users Restricted Internet Access and Block/Log All Other Guest Access

In this design, we must first isolate guest users into a separate subnet and firewall zone. UTM provides guests with limited Internet access, preventing guest users from spreading attacks and limiting the enterprise's liability. Separate *guest zones* and policies are used to isolate the branch office and enterprise VPN from guests. These policies block and log these types of access attempts.

Implementing a Security Policy

In the first section, we discussed branch office threats and the role SSG plays in protecting branch offices against these threats. Using SSG's capabilities, we can develop an appropriate security policy for your distributed enterprise. While the network security policy that we define might not match your organization's exact needs, it is at least a starting point which can be extended or customized to further meet the needs of the enterprise.

When developing the security policy for a distributed branch network, it is important to clearly define the goals, from a business and technical perspective. Often the ideal and most "locked down" security policies are *not* effective in a more "open" enterprise such as retail. In these environments, taking a drastic approach like blocking Web access, Instant Messaging, or email entirely, or requiring every user to authenticate with SecureID for network access, might be too burdensome for your organization to handle. Finally, when defining your security policies, consider your average user's computer skill-set. Requiring your users to advance through a steep learning curve or install or update software might *not* be feasible for your specific corporate environment.

Developing the Security Policy—Begin with a Simple Firewall Rule Set

As branch firewalls in large organizations become more numerous, their scale can make them the most difficult and costly to manage. To ease management, keep branch office Layer 3/4 firewall security policies as generic as possible, while still enforcing necessary source, destination IP, and protocol usage. The goal is to minimize changes to branch office security policies. (You do *not* want to update 1,000 device policies every week.) One major advantage to the hub and spoke design used in our implementation is that host-specific and dynamic firewall security policies can be managed and enforced at the VPN hub—the other end of the tunnel from the branch—thus keeping the branch policies fairly simple and generic. When additional servers or resources are added to existing subnets, only the hub VPN policies require updates, typically only two to four devices.

The branch firewall polices should be created and tested first, prior to applying additional UTM enforcement, and (if possible) prior to applying strict security policies to the VPN hub device. This approach simplifies testing or troubleshooting, and hopefully eliminates re-engineering policies later. The branch firewall policies for the three types of branch offices are as follows:

- Type A – Basic: User zone (firewall uses onboard traffic shaping)
- Type B – Optimized: User zone, guest zone (firewall uses onboard traffic shaping)
- Type C – Critical: User zone, guest zone, demilitarized zone (DMZ) ((firewall uses Differentiated Services (DiffServ) marking on policies; a separate router performs actual traffic shaping))

In our implementation, the IP addressing schema is clearly defined because the network was designed from the ground up. In this case, your security policies can use similar supernet-based network addresses. However, most networks built and extended over time might not benefit from such a simple and consistent IP addressing schema. For these types of networks, simple policies can be developed using address groups containing multiple networks.

Supernet-based source and destination address objects are used on all branches, creating an initial template for Layer 3/4 access control.

Careful consideration and effort should be taken when developing your branch firewall policies, such as:

- Consider future growth plans, new networks, or IP ranges that can be added in the coming month or year.
- Extend the extra time into developing a generic firewall policy for different branch types that scale with your data center, DMZ, voice, or other triple-play networks, or with a newly acquired company that must be integrated into your existing network.
- If another engineer or department handles IP routing and address allocation in your organization, consult with them when designing your branch security policies.

Implementation Guidelines

This section presents implementation guidelines concerning the following types of security policies:

- Internet security
- Guest zone
- VPN outbound and inbound
- Complementary VPN hub/data center

NOTE: Before we discuss the policies and their associated zones, it is important to consider the role of centralized policy management and selectively enable UTM on a per-policy basis.

Centralized Policy Management

Simple firewall policies are first created using NSM Security Policy Editor.

Because NSM allows common addresses for objects, groups, and protocol groups, objects only need to be created once inside NSM. One security policy (template) can be used for each branch type by simplifying Branch Type A – Basic policies which were first developed then cloned using Save As to create Type B – Optimized, and then again for Type C – Critical policies.

Once created, these policies are applied to each SSG device tested and then "pushed" out to *all* branch SSG devices.

Adding UTM to Security Policies

Juniper Networks policy-based architecture allows UTM security features to be enabled selectively on a per-policy basis, giving you granular control over the enforcement of UTM. As a result, firewall policies can be created and tested first, before UTM features are enabled.

Internet Security Policies (Trust to Internet Zone)

The following policies will help us protect the local branch users from threats on the Internet, as well as protect the Internet from threats posed by branch users. Refer to Figure 1 when reviewing these policies.

Policy 100 allows all branch users access to mail servers on the Internet. The mail services service group used includes SMTP, POP3, and Internet Message Access Protocol (IMAP). Antivirus is enabled on this policy to scan all attachments and block any that contain malicious content. DI is enabled using the **MAIL-Profile**, as described in *Appendix B—NSM Services and Attack Group*, to prevent attacks on Internet mail servers.

Policy 9 allows all branch users access to Web services on **Port 80 or 8080** (http-ext). Antivirus is enabled on this policy to scan all HTTP-based file uploads or downloads and blocks malicious content. Web filtering is enabled on this rule to redirect all URL requests to a Websense server for validation and reporting. DI is enabled using the **HTTP/FTP Profile**, as described in *Appendix—B NSM Services and Attack Group*. This prevents both outbound attacks against mail servers and server-to-client (inbound) attacks from malicious Web sites from infecting branch users.

Policy 20 allows all branch users FTP-server access on the Internet. Antivirus is enabled on this policy to scan all FTP file uploads or downloads and blocks malicious content. DI is enabled using the **HTTP/FTP Profile,** as described in *Appendix B NSM Services and Attack Groups*. This prevents branch users from launching outbound attacks against Internet FTP servers.

Policy 14 allows all branch users access to other Internet services, such as Domain Name System (DNS) and Lightweight Directory Access Protocol (LDAP) using the service group created in A*ppendix B NSM Services and Attack Groups.* Antivirus is enabled on this policy to scan all FTP file uploads or downloads and block any that contain malicious content. DI is enabled using the **Inet Apps Profile**, as described in *Appendix B NSM Services and Attack Groups*. This prevents branch users from launching outbound attacks against the Internet.

Policy 16 allows all branch users to access Internet Messaging such as MSN or Yahoo Messenger using the service group created in *Appendix B NSM Services and Attack Groups*. Antivirus is enabled on this policy to scan all file uploads or downloads and block any that contain malicious content. DI is enabled using the **Messaging-Profile**, as described in *Appendix B NSM Services and Attack Groups*. This prevents branch users from launching outbound attacks against the Internet.

Policy 8 blocks all other traffic that originates from inside the *trust* zone from accessing any *untrust* subnets, including the Internet. This policy blocks all other non-approved protocols. Logging and counting are enabled to record any blocked Internet connection attempts.

Note on Traffic Shaping: Traffic shaping is enabled on all trust-to-Internet policies, and configured with second-lowest priority and no guaranteed bandwidth. This ensures enterprise VPN traffic priority over branch Internet access.

100	trust	All Branches	untrust	any	MAIL-Services	permit	Branch Type A	NAT Traffic Shaping Log/Count Antivirus MAIL-Profile
9	trust	All Branches	untrust	any	HTTP HTTP-EXT	permit	Branch Type A	NAT Traffic Shaping Log/Count Antivirus Web Filtering HTTP Profile Miscellaneous
20	trust	All Branches	untrust	any	FTP	permit	Branch Type A	NAT Traffic Shaping Log/Count Antivirus FTP Profile Miscellaneous
14	trust	All Branches	untrust	any	INET Misc Services	permit	Branch Type A	NAT Traffic Shaping Log/Count Antivirus Web Filtering Inet Apps
16	trust	All Branches	untrust	any	INET-IM-Services	permit	Branch Type A	NAT Traffic Shaping Log/Count Antivirus IMessaging-Profile
8	trust	any	untrust	any	any	deny	Branch Type A	Log/Count

Figure 1. Network and Security Manager (NSM) Trust to Untrust Policies

Guest Zone Policies

The following policies are extended to those branches with *guest* zones. Refer to Figure 2 when reviewing these policies.

Policy 24 and **25** prevent any hosts that are connected to *guest* zones from accessing local users (*trust* zone) or remote offices and data center resources (VPN zone) by implementing a specific policy that denies resources and logging. Counting can be specified to log any blocked access attempts to these networks from the *guest* zone.

Policy 26 permits guests outbound access to email which reuses the "MAIL-Services" group to permit outbound SMTP, POP3, and IMAP traffic. Antivirus and DI can be enabled later under this policy to provide UTM protection for email traffic.

Policy 27 allows all branch guests access to Web services on **Port 80** or **8080** (http-ext). Antivirus is enabled on this policy to scan all HTTP-based file uploads or downloads, and to block any that contain malicious content. Web filtering is enabled on this rule to redirect all URL requests to a Websense server for validation and reporting. Deep inspection is enabled using the **HTTP/FTP Profile,** as described in *Appendix B—NSM Services and Attack Group*. This prevents both outbound attacks against mail servers and server-to-client (inbound) attacks from malicious Web sites from infecting branch guests.

Policy 30 allows all branch guests FTP-server access on the Internet. Antivirus is enabled on this policy to scan all FTP file uploads or downloads and block any that contain malicious content. DI is enabled using the **HTTP/FTP Profile** described in *Appendix B—NSM Services and Attack Group*. This prevents branch guests from launching outbound attacks against Internet FTP servers.

Policy 28 allows all branch guests access to other Internet services such as DNS and LDAP using the service group created in *Appendix A Branch SSG* Configuration. Antivirus is enabled on this policy to scan all FTP uploads or downloads and block any that contain malicious content. DI is enabled using the **Inet Apps Profile**, as described in *Appendix A Branch SSG* Configuration. This prevents branch guests from launching outbound attacks against the Internet.

Policy 20 drops all other traffic from guest to Internet that is not specifically permitted above. An implicit drop rule is used with logging and counting, as this allows for centralized logging of any unauthorized connection attempts by guest users. See Figure 1**.**

Traffic shaping is enabled on all guest-to-Internet policies and configured with lowest priority and no guaranteed bandwidth. This ensures enterprise VPN traffic and branch users priority over branch guest access. Furthermore, this helps ensure that guests cannot consume excessive bandwidth, thereby impacting legitimate VPN user traffic. Without such traffic shaping, a single guest user downloading a large file could saturate the upstream link, and as a result impact business-critical traffic.

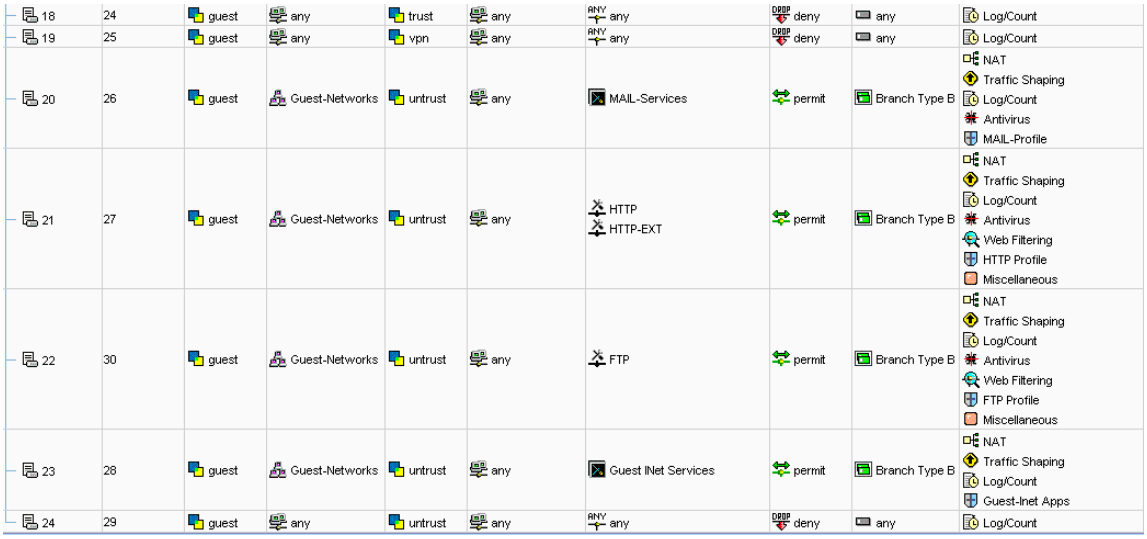

Figure 2. NetScreen Manager (Guest Zone Policies)

VPN Outbound Policies (Trust to VPN Zone)

These policies help us protect the other branches and the VPN head-end from malicious traffic originating from the branch's local user zone (*trust* zone). Refer to Figure 3. when reviewing these policies.

Policy 10 allows outbound SIP traffic from branch trust subnets to all other branches and data center subnets. Traffic matching this rule is subjected to application inspection, which validates only legitimate SIP traffic. Traffic shaping is performed making SIP traffic the highest priority and guaranteeing 300 kbps of bandwidth to outbound SIP traffic.

Policy 15 allows all branch trust subnets to access email services within any data center network. The service group "MAIL-Services" includes SMTP, POP3, and IMAP. Traffic matching this rule is subject to antivirus inspection, blocking both inbound and outbound viruses and worms. DI is also performed blocking well known attacks against the mail protocols using the **MAIL-Profile** created. Traffic shaping tags mail traffic as second priority, below SIP.

Policy 11 allows all branch trust subnets HTTP access to all data center networks. Application inspection is performed to validate that only legitimate HTTP traffic matches this rule. In addition, antivirus and URL filtering is enabled on this rule, as well as DI where the **HTTP Profile** blocks well-known HTTP outbound attacks, as well as server-to-client HTTP attacks. Traffic shaping tags this traffic as second priority, below SIP.

Policy 19 allows FTP Client access to all data center networks. Application inspection ensures that only valid FTP traffic matches this rule. Antivirus inspects and blocks all viruses and worms contained in any file uploads or downloads. DI is enabled protecting data center resources from well known FTP attacks. Traffic shaping tags this traffic as third priority, below HTTP and centralized applications.

Policy 12 allows all branch trust subnets access to centralized applications behind any data center networks. URL filtering is enabled for the HTTPS traffic, and DI blocks well known attacks using the **Enterprise-Apps** profile created earlier.

Policy 6 blocks all other traffic originating inside the *trust* zone from crossing any VPNs in the VPN zone. Again, logging and counting (**LogCount**) are enabled to record any blocked connection attempts.

10	trust	All Branches	vpn	All Branches&DC	SIP	permit	Branch Type A	Traffic Shaping Log/Count Miscellaneous
15	trust	All Branches	vpn	All-DC-Networks	MAIL-Services	permit	Branch Type A	Traffic Shaping Log/Count Antivirus MAIL-Profile
11	trust	All Branches	vpn	All-DC-Networks	HTTP HTTP-EXT	permit	Branch Type A	Traffic Shaping Log/Count Antivirus Web Filtering HTTP Profile Miscellaneous
19	trust	All Branches	vpn	All-DC-Networks	FTP	permit	Branch Type A	Traffic Shaping Log/Count Antivirus FTP Profile Miscellaneous
12	trust	All Branches	vpn	All-DC-Networks	Centralized Applications	permit	Branch Type A	Traffic Shaping Log/Count Antivirus Web Filtering Enterprise-Apps
6	trust	any	vpn	any	any	deny	Branch Type A	Log/Count

Figure 3. NetScreen Manager (Trust to VPN Policies)

VPN Inbound Policies (VPN to Trust Zone)

The following policies help us protect the branch users from malicious traffic originating from other branches or from the VPN head-end. Refer to Figure 5 when reviewing these policies.

ID	Match					Action	Install On	Rule Options
	From Zone	Source	To Zone	Destination	Service			
1	vpn	All Branches&DC	trust	All Branches	SIP	permit	Branch Type A	Traffic Shaping Log/Count Miscellaneous
18	vpn	NOC Admins	trust	All Branches	HTTP HTTP-EXT	permit	Branch Type A	Traffic Shaping Log/Count Antivirus HTTP Profile Miscellaneous
2	vpn	NOC Admins	trust	All Branches	FTP	permit	Branch Type A	Traffic Shaping Log/Count Antivirus FTP Profile Miscellaneous
3	vpn	NOC Admins	trust	All Branches	Remote Administration	permit	Branch Type A	Traffic Shaping Log/Count Remote Administration Profile
5	vpn	any	trust	any	any	deny	Branch Type A	Log/Count

Figure 4. NetScreen Manager (Trust to VPN Policies)

Policy 1 allows inbound access from the VPN zone to all branch *trust* zones, and subnet using SIP to support the organization's VoIP infrastructure. Because voice traffic is sensitive to latency and bandwidth constraints, traffic shaping is performed on this policy, setting inbound SIP traffic as the highest priority, with a guaranteed bandwidth of 300 kbps. Application inspection uses DI to verify that only valid SIP traffic (**port 5060**) matches this rule.

Policy 18 allows inbound access from NOC administrators in the VPN zone to the branch's *trust* zone and subnet using HTTP on **port 80** and **8080/8000** (http-ext). Application inspection uses DI to verify that only valid HTTP traffic is processed. A custom Attack Profile (**HTTP Profile**) is applied to this policy to drop critical and high HTTP attacks, including server-to-client attacks. Antivirus is applied to this policy; however, URL filtering is *not* needed on this policy, as it is performed on the egress point for the NOC administrator, if desired. Traffic shaping sets this traffic to second priority.

Policy 2 allows inbound access from NOC administrator in the VPN zone to the branch's *trust* zone and subnet using FTP. Application inspection uses DI to verify that only valid FTP traffic is processed. A custom Attack Profile (**FTP Profile**) is applied to this policy to drop critical and high FTP attacks, including server-to-client attacks. Antivirus is enabled on this policy; however, URL filtering is not enabled because it is performed on the egress point for the NOC administrator, if desired. Traffic shaping sets this traffic to third priority.

Policy 3 allows other remote administration services inbound from the NOC Administrator. The service group "Remote Administration" permits NOC administrators to access branch users using Internet Control Message Protocol (ICMP), Telnet, Reliable Data Protocol (RDP), Virtual Network Computing (VNC), and SSH. A matching Attack Profile (**Remote Administration Profile**) applies further DI to these remote administration services. Traffic shaping treats this traffic as second priority.

Policy 5 blocks all other traffic originating from the VPN zone from terminating inside the branch's *trust* zone. Logging and counting is enabled to record any blocked connection attempts.

ID	Match					Action	Install On	Rule Options
	From Zone	Source	To Zone	Destination	Service			
1	vpn	All Branches&DC	trust	All Branches	SIP	permit	Branch Type A	Traffic Shaping Log/Count Miscellaneous
18	vpn	NOC Admins	trust	All Branches	HTTP HTTP-EXT	permit	Branch Type A	Traffic Shaping Log/Count Antivirus HTTP Profile Miscellaneous
2	vpn	NOC Admins	trust	All Branches	FTP	permit	Branch Type A	Traffic Shaping Log/Count Antivirus FTP Profile Miscellaneous
3	vpn	NOC Admins	trust	All Branches	Remote Administration	permit	Branch Type A	Traffic Shaping Log/Count Remote Administration Profile
5	vpn	any	trust	any	any	deny	Branch Type A	Log/Count

Figure 5. NetScreen Manager (Trust to VPN Policies)

Developing Complementary VPN Hub/Data Center Policies

The VPN hub device plays an important but secondary role by further enforcing access control on the other side of the tunnel. Here, where only a few high-end devices are used, more specific rules and changes can be managed more easily on a daily basis. Additional inspection can be done at this point, such as IDP or Redirect URL filtering, without deploying such devices across *all* branches. In our implementation, ISG firewalls with on-board IDP functionality provide full IDP inspection for all inbound, outbound, and backhauled Internet traffic.

The data center address objects and policies also can be more specific at the head-end. This can include segregating server types (tier 1, 2, 3, as examples), DNS servers, and mail servers. This is often needed in existing data centers as it might not be possible to segregate with subnets. Instead, use address objects and groups to combine common application services into common policies.

Consequently, most policy changes can be made to the central data center devices which often require only two to four firewalls. This approach is much more efficient than redeploying policies to hundreds or thousands of branch devices. Furthermore, it makes troubleshooting much easier to implement a generic policy across branches, and it permits additional and specific filtering on the VPN concentrators or data center firewalls. This implementation also allows network administrators authority for delegating data center teams to manage access to their devices without impacting branch/VPN groups.

Summary

Overall, UTM features and capabilities are best suited for mid-to-large sized enterprises and government agencies that have remote branch offices and require access to more security features than just the traditional firewall. For specific compliance requirements such as Sarbanes-Oxley (SOX), Healthcare Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry (PCI), implementing UTM helps easily meet these types of stringent security and performance requirements.

Implementing and managing UTM provides a significant advantage to securing the branch office from constant, ever-changing threats. Because UTM can be implemented efficiently and uniformly throughout a distributed enterprise across hundreds of remote branch offices, network administrators and IT professionals can both experience the ease in centrally managing security devices, as well as the reduced efforts required to identify and mitigate security attacks. With Juniper Networks policy-based architecture, UTM security features can be enabled selectively on a per-policy basis. This gives network administrators granular control over the enforcement of UTM. Furthermore, by consolidating UTM capabilities into a common platform at the branch, network administrators gain significant cost savings and ease of management benefits.

Using Juniper Networks products and practicing the recommended implementation guidelines provides a basis for developing strict security across the distributed enterprise, allowing network administrators to meet their enterprise security goals. The policy configuration statements in this implementation guide provide best practices in using UTM to secure business networks in common scenarios.

Appendix A Branch SSG Configuration

The following major steps explain how to configure the branch SSG.

Obtain Required Licenses

Licensed UTM features are resident in all SSG devices. Juniper Networks offers antivirus, DI, and URL filtering on a yearly subscription basis tied to the serial number of your SSG device. The features implemented in this guide require both antivirus and DI (base package). To quickly find the serial number of your device, enter the following:

```
SSG5-D-> get system | include serial
Serial Number: 0168102006001518, Control Number: 00000000
```

To determine which licenses are currently installed, enter the following:

```
SSG5-D-> get license
...
Sessions:           16064 sessions
Capacity:           unlimited number of users
NSRP:               ActiveActive
VPN tunnels:        40 tunnels
Vsys:               None
Vrouters:           4 virtual routers
Zones:              10 zones
VLANs:              50 vlans
Drp:                Enable
Deep Inspection:    Enable
Deep Inspection Database Expire Date: 2009/4/23
Signature pack:     Standard Deep Inspection Pack
IDP:                Disable
AV:                 Enable(1)
Antispam:          Enable(1)
Url Filtering:      Expire Date: 2009/4/23
```

You can always trigger a manual license update by using the following command. Make sure that your device can access the Internet and that DNS is configured properly before triggering a license update.

```
SSG5-D-> exec license-key update
```

Update the Deep Inspection Database

```
SSG5-D-> exec attack-db update   (ensure working Internet Default Gateway and DNS)
  or
SSG5-D-> save attack-db from tftp 1.2.3.4 attack.db to flash   (Manual download from
TFTP)
```

Update Antivirus Database

```
SSG5-D-> exec av scan-mgr pattern-update
```

AV: pattern update will start shortly. URL http://update.juniper-updates.net/AV/5GT/

Configure URL Filtering (Websense Redirect Used)

```
set url protocol websense
set config enable
set server 192.168.4.39 15858 10
set server src-interface bgroup0

exit
```

Add SSG Device to NSM

Refer to the NSM Administrator Guide to add the device; using the "reachable" method is recommended. See http://www.juniper.net/techpubs/software/management/security-manager/nsm2008_1/nsm2008.1_admin_guide.pdf.

Import the SSG Device Configuration into NSM

This import device method is recommended when you have existing SSG devices in use, and they are already configured for adding to NSM.

Apply the Security Policy, then Update the Device

Once the device has been imported successfully, apply the security policy to the device with NSM, then update the device.

Appendix B NSM Services and Attack Groups

The following figures show the NSM Deep Inspection attack groups and services used for the security policies in this document. These groups must be created first. Then they can be applied to the security policies as outlined in this document.

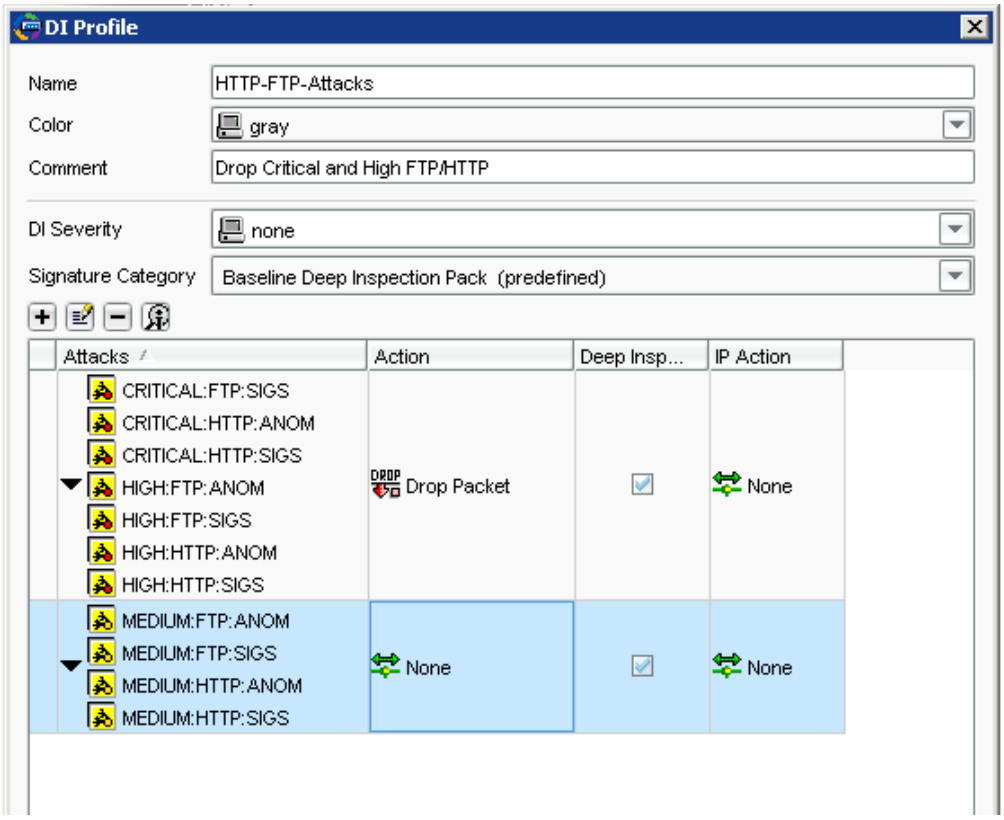

Figure 6. Deep Inspection Profile for Outbound HTTP/FTP Traffic (Outbound VPN and Outbound Internet)

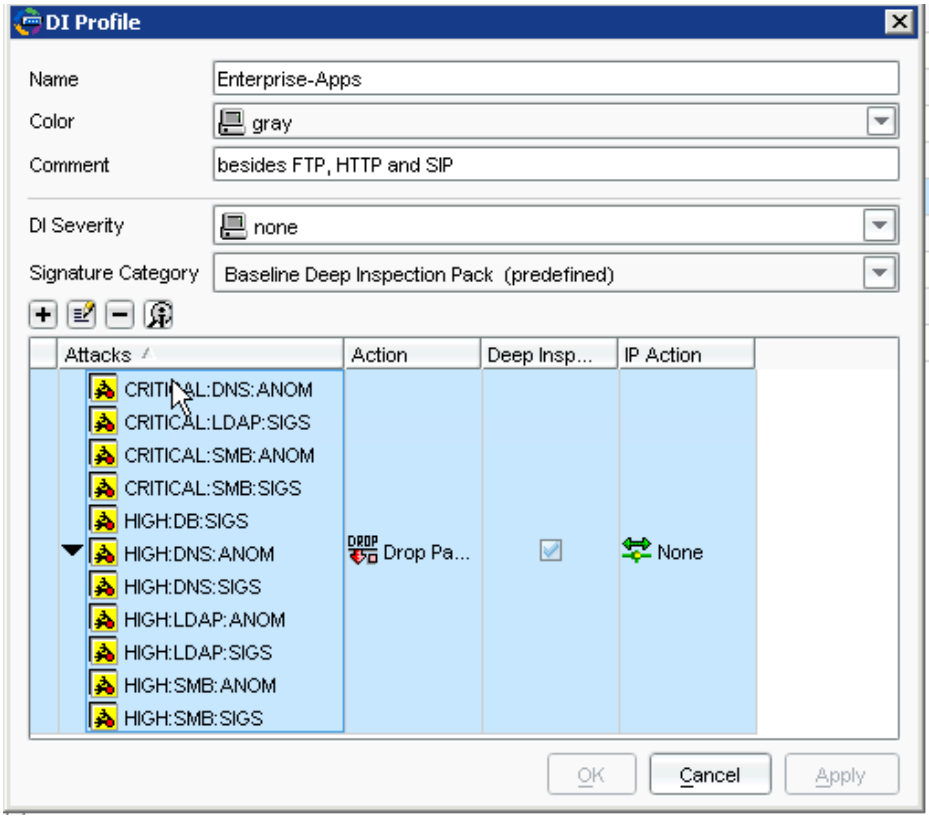

Figure 7. Deep Inspection Profile for Other Common Internet Services (Outbound VPN and Internet)

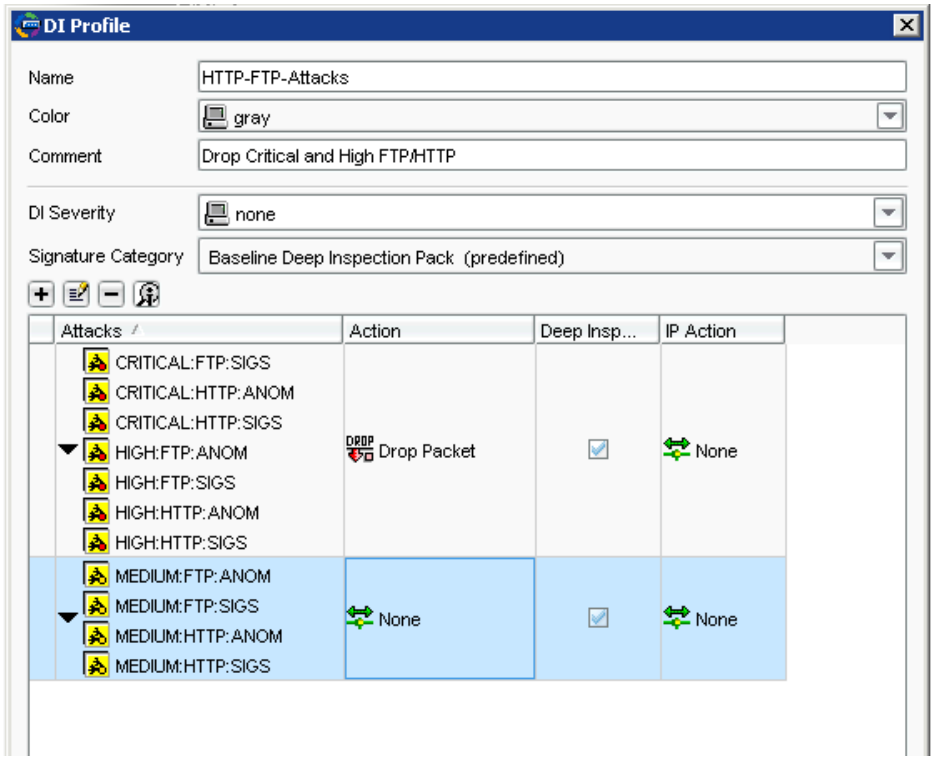

Figure 8. Deep Inspection Profile for Internet and Enterprise Email Inspection (Outbound VPN & Internet)

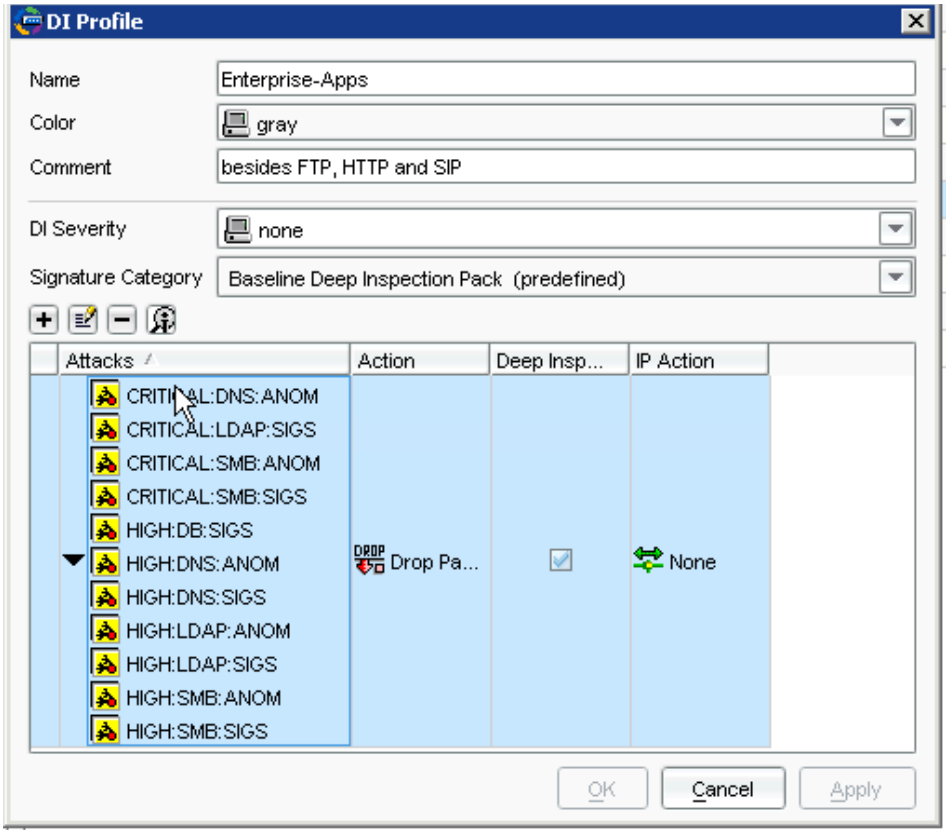

Figure 9. Deep Inspection Profile for Common Enterprise Applications (Inbound and Outbound VPN)

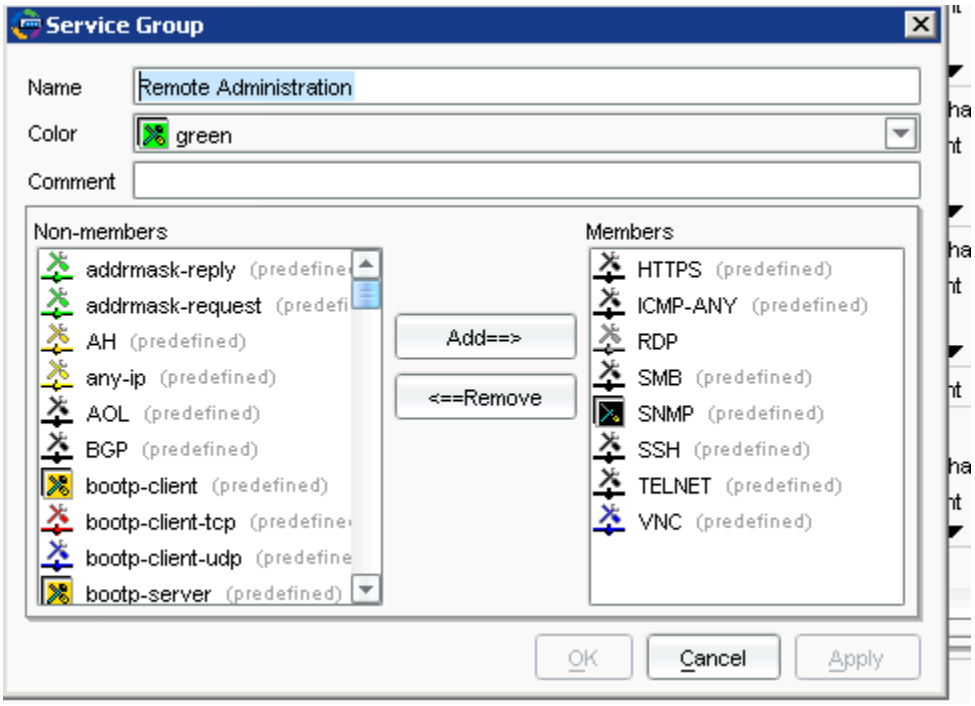

Figure 10. NSM Services Object for Remote Administration Services (Inbound VPN)

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. 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
Fax: 35.31.8903.601

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