Traffic Management: The NetScreen Way

An overview of the need for traffic management and how NetScreen implements it

A White Paper By

NetScreen Technologies Inc.

http://www.clm.com.br/netscreen

TABLE OF CONTENTS

Traffic Management with NetScreen

Today, e-businesses, enterprises, and service providers face ever-increasing security and performance challenges. Securing web sites, corporate networks, and on-line applications is absolutely essential. At the same time, security measures must not impede performance -- in fact, these measures must work in tandem with traffic management solutions that ensure effective use of bandwidth. Controlling access to the network while maximizing performance of mission-critical traffic is one of the most complex, challenging issues that security and network administrators face.

NetScreen Technologies delivers a line of purpose-built security products that integrate firewall, VPN, and traffic management functions within one comprehensive, high-performance platform. Using NetScreen, administrators can define and enforce multi-function policies at the network edge, gaining a high degree of control over both security and performance.

This white paper describes how shared bandwidth challenges can be met through traffic management with NetScreen-5, NetScreen-10, and NetScreen-100 security appliances. It describes the business requirements that drive traffic management, the characteristics of Internet traffic, and impact of uncontrolled traffic on available bandwidth. NetScreen has created a unique, patent-pending algorithm capable of handling traffic bursts that defeat alternatives like TCP rate control and class-based queuing. This paper illustrates how NetScreen's policy-based approach enables security and performance requirements to be addressed together, within one comprehensive, scalable, ASIC-based solution.

Introduction

Over the past few years, LAN bandwidth has increased from Ethernet to Fast Ethernet to Gigabit Ethernet, but WAN bandwidth remains at a premium in most corporate networks. Many interoffice links operate at T1 or better rates, but some "last mile" links connect remote and home offices at 128 Kbps or less. Inequity between WAN and LAN bandwidths creates a traffic bottleneck that can lead to network congestion. The end result: Poor response time and broken connections reduce worker productivity and discourage on-line customers. Even when plentiful, WAN bandwidth can be expensive. Left unchecked, escalating consumption can adversely impact a company's bottom line.

Whenever traffic exceeds available bandwidth, just one greedy application can saturate the WAN link. High-volume traffic can easily starve other applications, preventing mission-critical tasks from being completed. Even at low volume, bursty traffic can adversely affect latency-sensitive applications. And non-business traffic can drive up WAN bandwidth demand, increasing cost.

Traffic management solutions deployed at the LAN-WAN junction can allocate WAN bandwidth in accordance with business priorities. By enforcing guaranteed bandwidths, mission-critical applications can be ensured a fair share of bandwidth and are never starved. By establishing priorities, the most essential or latency-sensitive traffic can always go first. By allowing unreserved bandwidth to be shared, expensive WAN resources can be more fully utilized. Finally, by ensuring business-appropriate use, return-on-investment for WAN bandwidth can be maximized.

The goal of this white paper is to help security and network administrators learn how to manage shared bandwidth using NetScreen traffic management. This paper starts by describing the characteristics of common Internet traffic, the consequences of uncontrolled WAN access, and common alternatives used to allocate bandwidth and "shape" traffic. It explains how NetScreen's patent-pending solution addresses traffic management challenges more effectively and efficiently. Finally, this paper identifies the configuration and monitoring steps involved in successful deployment.

Problems Caused By Uncontrolled Internet Traffic

Uncontrolled traffic consumes bandwidth in many different ways. To implement effective traffic management, one must first understand the behavior and bandwidth impact associated with common Internet traffic types, and how applying controls can affect application performance.

Bursty Traffic

FTP is perhaps the best-known example of bursty Internet traffic. FTP downloads usually involve a large volume of data, generated at a rate that exceeds WAN capacity. The server generates a large surge of data, then pauses for acknowledgement before generating another surge of data. Without traffic management, each surge can saturate the WAN. FTP sessions can starve other applications -- including other FTP sessions.

FTP and other bursty traffic, like multi-media (.wm, .swf, .mov) and graphic (.gif, .jpg) objects within HTTP, can be "smoothed" by limiting this traffic's share of available bandwidth. When objects are consumed by an interactive application, eliminating burstiness results in better end user experience (e.g., no more hung sessions or frozen web pages). Bursty traffic can also be granted low priority to reduce its impact on more essential or time-sensitive traffic.

Interactive Traffic

HTML files, SSL transactions, and Telnet sessions are all examples of interactive traffic -- sessions that consist of comparatively short request/response pairs. Interactive traffic typically supports applications that involve real-time interaction with an end user: for example, web browsing and on-line purchasing. Individually, interactive sessions may not consume much bandwidth. But, when there is competition for bandwidth, interactive sessions can be plagued by poor or unpredictable response time. Interactive sessions often support mission-critical applications; for example, an administrator using Telnet to diagnose and correct network congestion can be impeded by the very problem that he is trying to resolve.

Interactive traffic can clearly benefit from prioritization, ensuring precedence over non-real-time traffic and traffic that is less essential. For example, by assigning HTML and SSL higher priority than SMTP or FTP, an on-line business can ensure that website visitors consistently receive fast service. For mission-critical interactive traffic, bandwidth reservation may also be appropriate -- preferably in a manner that allows unused bandwidth to be shared by others.

Latency-Sensitive Traffic

Even traffic that is not interactive can be strongly impacted by end-to-end network delays. Examples of latency-sensitive traffic include real-time streaming (RTSP) and voice-over-IP (VoIP, H.323). Unlike interactive traffic, latency-sensitive traffic can consume considerable bandwidth on a regular basis. But these applications are not bursty: they generate a steady stream of traffic. Without traffic management, streams can easily saturate the WAN and starve other applications. Furthermore, competition for bandwidth can adversely impact service delivery, causing choppy video or poor quality audio, rendering the application unreliable or even unusable.

Latency-sensitive traffic can be ensured constant bit-rate delivery by applying bandwidth guarantees. Business priority should be used to set traffic priority. For example, VoIP might be

assigned top priority; recreational streaming audio might be permitted to consume only unreserved bandwidth at low priority.

Non-Real-Time Traffic

Some Internet protocols like news (NNTP) and sendmail (SMTP) are considered non-real-time traffic. For these applications, timely delivery usually does not matter (within reason). News bandwidth consumption is so high that some companies actually offload this traffic with satellite delivery. Traffic management is another way to prevent non-real-time traffic from adversely affecting your network, while fully utilizing the WAN resources you already have. Non-real-time traffic can be assigned scheduled bandwidth, shifting the bulk of the traffic to off-hours. During the daytime, a maximum bandwidth and low priority can be applied to limit impact on other applications.

Recreational Traffic

When classifying Internet traffic, one must consider business priority. That brings us to non-business traffic -- recreational traffic like on-line gaming and Napster. In some cases, recreational traffic is completely prohibited for security and performance reasons. In other cases, corporate policies may permit otherwise unused bandwidth to be tapped by employees.

For example, a growing number of companies provide teleworkers with residential DSL for enterprise remote access, protected by a NetScreen-5. Many acknowledge that employees are likely to use this always-on DSL connection for recreational traffic. At the same time, these companies want ensure that adequate bandwidth remains available for business use. They also want to measure business bandwidth use, without having these metrics obscured by recreational traffic. Bandwidth reservation, priority, and per-policy metering can be used to accomplish these goals.

Bringing Traffic Under Control

Once current and desired traffic behavior is understood, and business priorities have been determined, traffic "classes" can be defined. Classes can be used to implement traffic management policies that prioritize, guarantee, and meter bandwidth use, bringing enterprise traffic under control.

Traffic Management Alternatives

Traffic management has been a challenge since the early days of the Internet; over the years, many alternative solutions have been developed. To fully appreciate NetScreen's patent-pending approach, one must consider the pros and cons associated with other alternatives.

Priority Queuing

This method is very easy to understand and implement. Outbound packets are funneled into queues for each priority. When transmitting, higher priority traffic is always given precedence over lower priority traffic. Unfortunately, simplicity has its price: Low-priority traffic is easily starved by bursty high-priority traffic, and the administrator has no control over bandwidth allocation. Finally, priority queuing offers little granularity.

Class-based Queuing (CBQ)

CBQ is a methodology for classifying packets and queuing them according to administrator-defined criteria. Unlike priority queuing, CBQ is designed to prevent any one application from monopolizing the WAN -- for example, by allocating specified bandwidth for each class. One common variation of CBQ is called Weighted Fair Queuing (WFQ). In WFQ, greater weight is given by assigning larger queues to higher priority classes. CBQ and WFQ are both static methods that often do not maximize bandwidth utilization. If any class does not consume its fixed allocation, that bandwidth is wasted.

TCP Rate Control

Another alternative is known as TCP rate control. TCP rate control uses a complex algorithm to regulate the introduction of traffic into the network. This "shaping" algorithm calculates the round-trip time (RTT) for each TCP session. To "smooth" traffic -- that is, eliminate burstiness without increasing packet retransmission -- rate control delays TCP acknowledgements and modifies the advertised window size in TCP headers.

For example, consider a bursty FTP server that sends four TCP packets, pauses for acknowledgement (ACK), then sends four more packets. If each burst exceeds WAN capacity, packets will be lost or delayed, resulting in retransmission. To avoid this, a "packet shaper" intercepts ACKs from the receiver. The shaper forwards one ACK to the sender, but with a smaller window size. Upon receiving the ACK, the sender determines it has window to generate just one more packet. After a brief wait, the shaper forwards another ACK; the sender

generates another packet. In effect, the shaper "spoon feeds" the server with incremental ACKs, causing packets to be sent more evenly over time.

When implemented correctly, TCP rate control can do a good job of smoothing bursty TCP traffic, allocating bandwidth to each class of traffic. But rate control can be difficult to implement with precision. It requires accurate real-time measurement of speed and RTT -- a challenge that increases with class granularity and traffic volume. Furthermore, TCP rate control does not address UDP traffic. Vendors that implement TCP rate control must implement another method, like CBQ, in order to provide a complete traffic management solution.

ATM Generic Cell Rate Algorithm (GCRA)

Another conventional technique is used to control cell flow in ATM networks. The *ATM Forum Traffic Management Specification*[1] defines the Generic Cell Rate Algorithm (GCRA) as a continuous state "Leaky Bucket" algorithm. In GCRA, a "bucket" acts like a single server queue with a finite queue length. The bucket admits a fixed amount of traffic to the network "drip by drip", a constant rate referred to as the Sustained Information Rate (SIR). Excess data -- bursts that exceed bucket size, or burst length (BL) -- are discarded (overflow the bucket). This algorithm is illustrated in Figure 1.

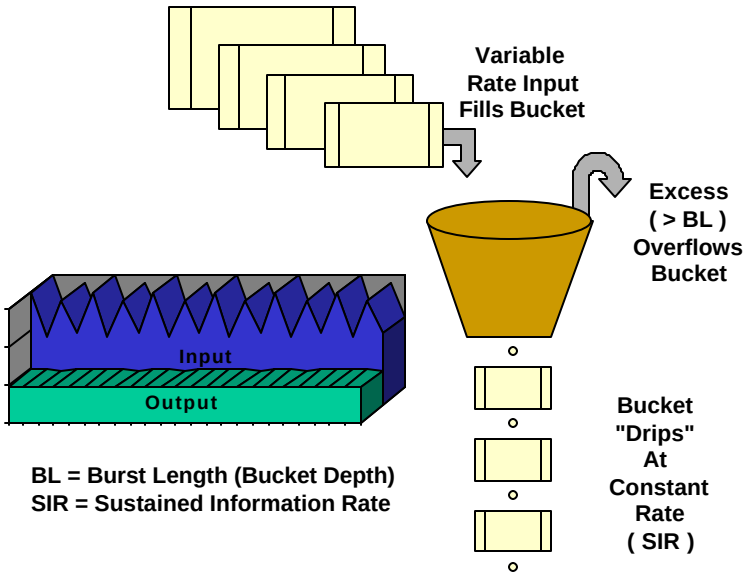

Figure 1: Leaky Bucket Algorithm

[1] ATM Forum Traffic Management Specification, Version 4.1, AF-TM-0121.000.

In ATM networks, GCRA has been proven to be highly efficient, capable of handling very high traffic volumes. When the arriving flow is relatively constant, a leaky bucket enforces SIR by discarding excess data. However, when input is very bursty, a leaky bucket can artificially restrict the flow and cause unnecessary data loss.

NetScreen's Patent-Pending Approach

NetScreen has gone beyond these common alternatives, creating a unique, patent-pending algorithm that can be implemented efficiently in hardware and is capable of handling bursty traffic. NetScreen's algorithm allocates bandwidth dynamically rather than statically. It ensures that each class of traffic receives guaranteed bandwidth, while allowing all classes to share remaining bandwidth, based on priority.

Token Bucket

NetScreen's algorithm is based on a variant of the leaky bucket convention called a "token bucket", illustrated in Figure 2. With this technique, arriving data is placed in a "wait" queue. A bucket is filled with tokens at constant rate, corresponding to bandwidth allocation (SIR). Each packet must grab and destroy a token to leave the queue (be transmitted). Packets are transmitted until they exhaust their supply of tokens. When token supply is exhausted, packets are held until the bucket has accumulated enough tokens to be replenished. Bursts are allowed, limited by the number of tokens in the bucket.

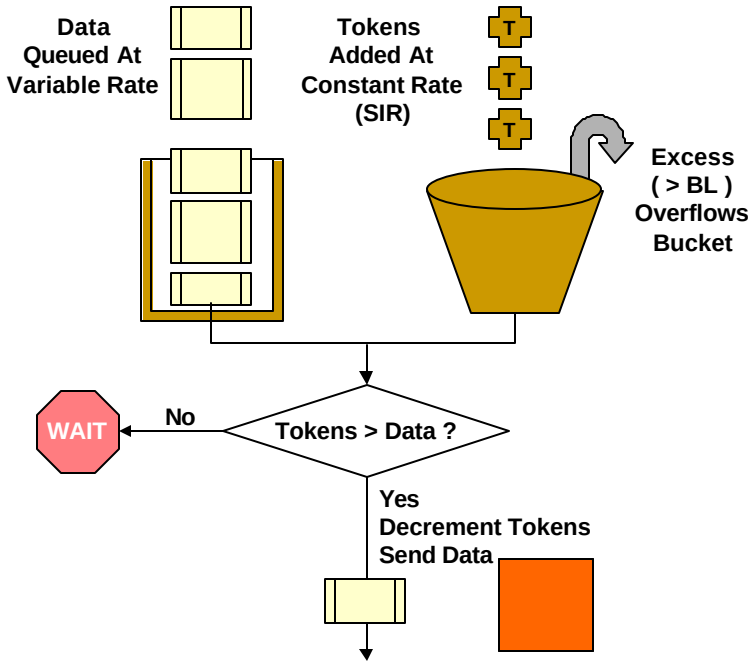

Figure 2: Token Bucket

Token bucket is a good start for accommodating bursty data while guaranteeing bandwidth. However, when tokens overflow the bucket, they are wasted. In other words, any WAN bandwidth that is not reserved goes unused.

Double Token Bucket

To share unreserved bandwidth, NetScreen implements a double token bucket as shown in Figure 3. One bucket is used to control sustained information rate (guaranteed bandwidth), while excess tokens go to a shared bucket. If the token supply is exhausted in the first bucket, the packet may be forwarded by borrowing additional tokens from the shared bucket. A low priority class receives shared bandwidth only when higher priority classes do not consume it.

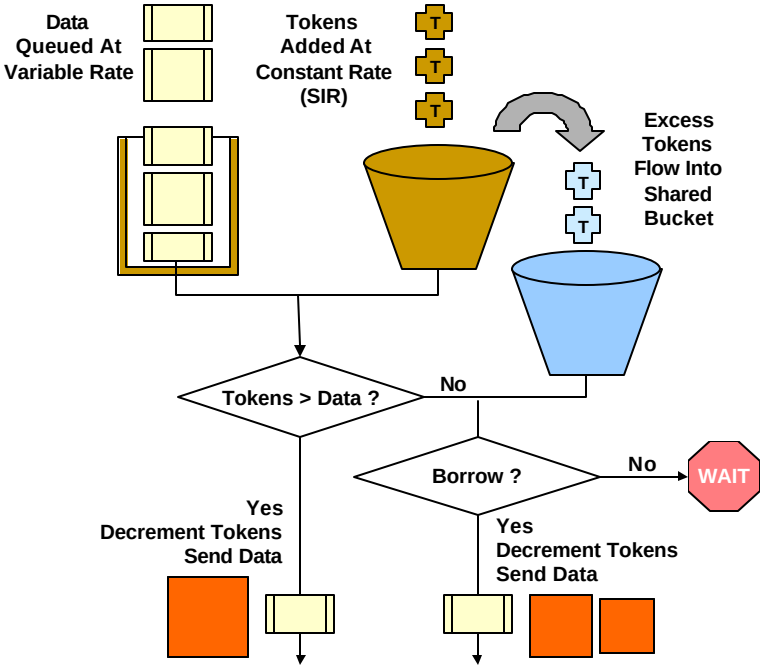

Figure 3: Double Token Bucket

Patent-Pending Approach

NetScreen's approach uses a double token bucket, controlled by the triple:

- guaranteed bandwidth (GBW),
- maximum bandwidth (MBW), and
- priority.

A double token bucket enforces guaranteed bandwidth and priority. To enforce maximum bandwidth, each class is associated with a bucket system (Figure 4).

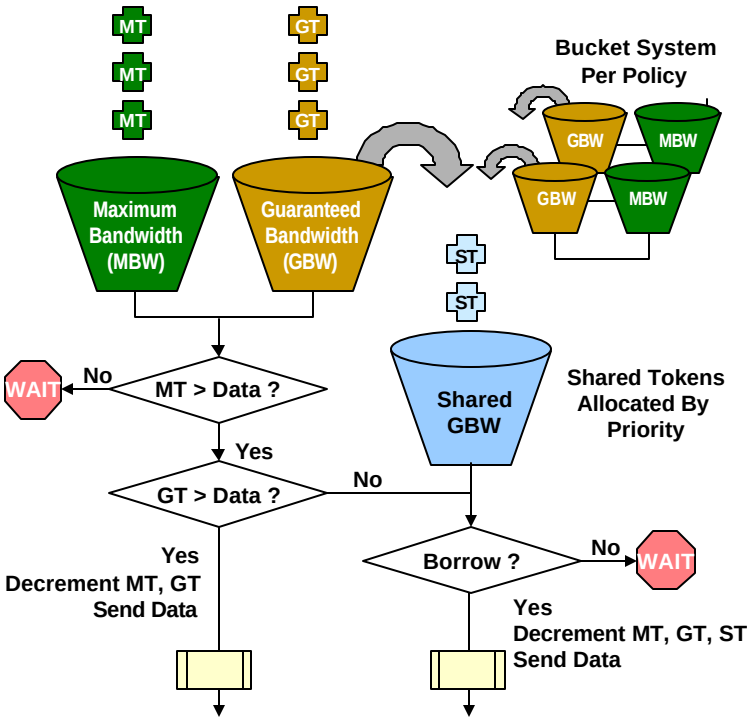

Figure 4: NetScreen's Patent Pending Approach

"MT" tokens are allocated to the maximum bandwidth bucket at the configured rate MBW. "GT" tokens are allocated to the guaranteed bandwidth bucket at the configured rate GBW. If the MT token supply is exhausted, no further traffic can be transmitted (i.e., the maximum has been reached). If MT tokens exist, but the GT token supply is exhausted (i.e., the guarantee has been reached), tokens may be borrowed from the shared bucket as previously described. Using this approach, NetScreen appliances enforce the maximum bandwidth, guaranteed bandwidth, and priority configured for each class of traffic.

When traffic management is enabled, a capacity is configured for each interface. By default, all traffic has unlimited low-priority access to shared bandwidth. Incoming or outgoing policies associated with each interface may reserve a portion of that interface's capacity by specifying a guaranteed bandwidth. For example, a WAN interface rated at 128 Kbps can be shared across three classes of traffic, illustrated in Figure 5. In this example, high-priority "B" traffic is guaranteed 20 Kbps, borrowing up to 20 Kbps from shared bandwidth. Low-priority "A" traffic is guaranteed 30 Kbps, but can use an additional 98 Kbps when no "B" or "C" traffic is competing for shared bandwidth. Any other classes that are not traffic-managed will compete with "A" for shared bandwidth at low priority.

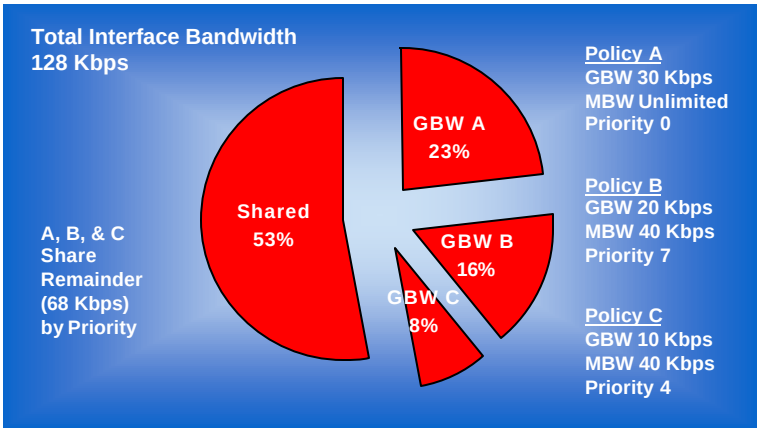

Figure 5: Interface Bandwidth Allocation

Proven, Effective Results

This patent-pending algorithm has been proven effective by third party evaluation. In head-to-head tests conducted by Network Computing, the NetScreen-5 took top honors in rate-control tests (see Figure 6). Asked to shape 1.5 Mbps of bursty HTTP into a T1 payload (490 Kbps), NetScreen toed the line at 479 Kbps. In mixed-class tests, NetScreen came within 0.1% of first-place Cisco, shaping three classes of traffic at 4 Mbps into a 2.9:2.1:1 (target 3:2:1) ratio. Overall, the NetScreen-5 took home an A- rating and second place -- at a price tag that put the competition to shame.

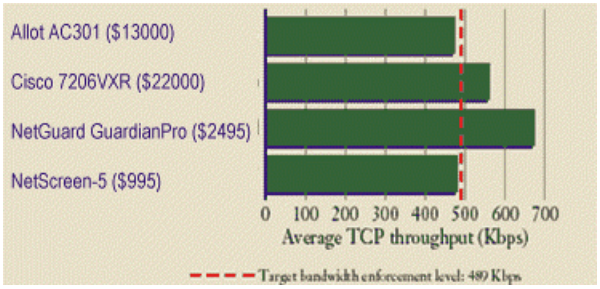

Figure 6 : Network Computing's Rate Enforcement Results[2]

Integrated Policy Management

NetScreen's policy-based management enables security and performance requirements to be addressed together, within one comprehensive, scalable, ASIC-based solution. Policies for each appliance can be administered through an easy-to-use, Java-enabled graphical user

[2] *Internet Traffic Management: From Chaos, Order*, David Newman, Network Computing Magazine, June 12, 2000 (http://www.networkcomputing.com/1111/1111f2.html)

interface, or a sophisticated command line interface. Centralized administration for up to one thousand NetScreen devices can also be accomplished using NetScreen Global Manager. In all cases, administering NetScreen traffic management features involves four basic steps.

Step 1: Define Interface Capacity

Traffic management can be enabled or disabled for the entire appliance. When traffic management is enabled, allocations are based on capacities configured for each interface. For example, consider a NetScreen-10 operating transparently between a small office LAN and a DSL router. The trusted interface can be left at its default, 10 Mbps. The untrusted interface should be configured to match DSL bandwidth, controlling traffic transmitted (over Ethernet) from the NetScreen-10 to the DSL router. In this way, LAN traffic can be prevented from "over-running" the router, improving Internet access stability.

Step 2: Classify Traffic By Defining Policies

Traffic can be classified by source/destination IP address, protocol or source/destination port (service), and time-of-day/week. For example, an "administrative" class might permit Telnet, SSH, and SNMP anywhere. A "news" class might carry NNTP to a designated server at each site. A "backup" class might let one server initiate FTP sessions at night. NetScreen's built-in list of well-known services can be extended to manage custom protocols.

Step 3: Manage Traffic For Each Policy

Next, selectively apply traffic management parameters to desired policies. (Other policies share unreserved bandwidth at low priority.) Guaranteed bandwidth reserves capacity from the interface. Maximum bandwidth enables sharing (by default, unlimited). Eight priority levels are available, ranging from 0 (low) to 7 (high). For each policy that is traffic-managed, the appliance will create a bucket system to enforce these metrics.

Step 4: Monitor and Tune Performance

Once traffic management has been configured, it must be monitored and tuned. NetScreen enables this with real-time, per-policy traffic metering. For each policy, actual bandwidth consumption is plotted against a graph describing configured parameters: source and destination address, service, direction, priority, guaranteed/maximum bandwidth, and whether traffic is actively being controlled by the policy (see Figure 7).

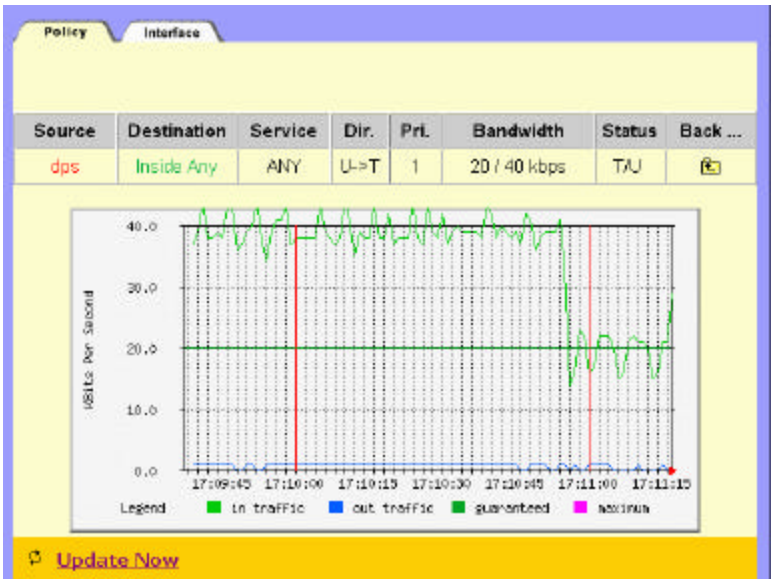

Figure 7: Real-Time Traffic Monitoring

Any policy, traffic-managed or not, can be configured to count traffic. Traffic counters can be plotted at various granularities (second, minute, hour, day, month). Graphed results can be saved to create a historical performance archive, useful for long-term traffic analysis.

In addition, traffic alerts can be configured to signal excessive bandwidth use. Use alerts to identify new, unexpected traffic that should be managed by creating more-specific policies or refining existing policies. Traffic alerts can be viewed from the GUI or forwarded to an upstream NMS as SNMP traps.

DiffServ Influences End-to-End QoS

NetScreen traffic management controls bandwidth use at the network edge, but goes one step further by influencing end-to-end quality of service (QoS). Differentiated Services[3] (DiffServ) is an IETF QoS standard that uses the Type of Service (TOS) byte in an IP packet's header to indicate priority. DiffServ support varies by carrier. For example, some carriers use a two-rate, three-color marker to meter a IP stream and mark packets red, yellow, or green, based on peak information rate and committed information rate. While interpretation may differ, DiffServ markings allow priority to be propagated from an end system or edge device into a carrier's

[3] RFC 2474, Definition of the Differentiated Services Field in the IPv4 and IPv6 Headers, K. Nichols et al, December 1998.

network. At the administrator's discretion, NetScreen appliances can set the priority field in the TOS byte to reflect traffic class priority.

Summary

Traffic management is essential for cost-effective use of WAN bandwidth. NetScreen's patent-pending approach offers flexible, high performance traffic management that guarantees bandwidth in accordance with business priority. NetScreen's algorithm maximizes utilization by sharing excess bandwidth, and it works well for any kind of TCP or UDP traffic, including bursty, interactive, and real-time applications. Because NetScreen's algorithm is implemented in custom ASICs, there is no compromise of performance for large, high-volume links.

By offering a scalable family of products, NetScreen provides cost-effective solutions for networks of any size, with a clearly-defined upgrade path. The same traffic management features are implemented by the NetScreen-5, NetScreen-10, and NetScreen-100. This consistent approach means that traffic management policies can be administered and applied uniformly across small/remote offices and central sites. In fact, NetScreen's class-based policy-driven approach enables single-point definition and enforcement of firewall, VPN, and traffic management functions.

Glossary

Asynchronous Transfer Mode (ATM) — An ITU standard for cell relay wherein multiple types of services (voice, video, data) are conveyed in small, fixed-length cells.

Burst Length (BL) — The largest data surge (burst) that can be accommodated by a token bucket; bursts that exceed BL are discarded (overflow the bucket).

Bursty — Refers to data generated in uneven spurts (e.g., FTP, multi-media, and graphic data transfers). Characterized by large surges of data, followed by pauses for acknowledgement.

Class-based Queuing (CBQ) — A traffic management methodology for classifying packets and queuing them according to administrator-defined criteria.

Constant Bit Rate (CBR) — Quality of service class defined for ATM networks, used for traffic that depends on precise clocking to ensure even, undistorted delivery.

Differentiated Services (DiffServ) — An IETF quality of service standard that uses the Type of Service (TOS) byte in an IP packet's header to indicate priority, end-to-end.

File Transfer Protocol (FTP) — An IETF standard application protocol for transferring files between network nodes.

Generic Cell Rate Algorithm (GCRA) — An ATM-standard continuous state "Leaky Bucket" algorithm that admits a fixed amount of traffic to the network at a constant rate.

Guaranteed Bandwidth (GBW) — The interface capacity reserved for use by one class of traffic. This parameter configured guaranteed throughput in kilobits per second. Traffic below this threshold will be passed without constraint by traffic management.

H.323 — An ITU standard that defines how multi-media conferencing data is transmitted across packet-based networks.

Interactive — Refers to traffic that enables real-time interaction with an end user (e.g., web browsing, Telnet sessions). Characterized by comparatively short request/response pairs.

Latency-Sensitive — Refers to traffic strongly impacted by end-to-end network delays (e.g., real-time streaming, voice-over-IP). Characterized by steady stream of data, often at generated at high volume.

Leaky Bucket — A traffic management convention that admits a fixed amount of traffic into the network "drip by drip". GCRA is one example of a leaky bucket algorithm.

Maximum Bandwidth (MBW) — Upper bound on the interface capacity that can be consumed by a single class of traffic. This parameter enables controlled sharing of unreserved bandwidth. Traffic beyond this threshold will be discarded.

Priority — In traffic management, higher priority traffic is always given precedence over lower priority traffic. Lower priority traffic is given shared bandwidth only if there is no higher priority traffic to consume it. This parameter has eight levels, ranging from 0 (low) to 7 (high).

Priority Queuing — A simple-but-limited traffic management algorithm that funnels outbound packets into queues for each priority.

Quality of Service (QoS) — A measure of performance that represents end-to-end transmission quality and service availability. Traffic management at the network edge influences QoS.

Real-Time Streaming Protocol (RTSP) — IETF standard that controls streams delivered from media servers to clients over real-time transport protocols like RTP and RDT.

Sustained Information Rate — In ATM networks, the constant cell admission rate configured for a GCRA leaky bucket.

TCP Rate Control — A complex algorithm that "shapes" traffic by calculating round-trip time for each TCP session, delaying acknowledgements, and modifying the TCP window size to "smooth" packet flow.

Token Bucket — A variant of the leaky bucket convention. Arriving data is placed in a "wait" queue and a bucket is filled with tokens at constant rate. Each packet must grab and destroy a token to leave the queue (be transmitted). NetScreen's patent-pending algorithm uses a double token bucket.

Traffic Classification — Traffic can be classified by source/destination IP address, protocol or source/destination port (service), and time-of-day/week. Traffic management policies that prioritize, guarantee, and meter bandwidth can then be applied to each class of traffic.

Voice-over-IP (VoIP) — Developing standards for transmitting voice signals over IP networks.

Weighted Fair Queuing (WFQ) — A variation of CBQ where larger queues are assigned to higher priority classes.