SANS ANALYST PROGRAM

Sponsored by NIKSUN

Monitoring Security and Performance on Converged Traffic Networks

A SANS Whitepaper – April 2008

Written by Dave Shackleford

Introduction

Today's networks are congested. In addition to carrying traditional business application data (e.g., email and file transfer), internal networks are now also carrying voice traffic and on-demand video. Coupled with additional alerting and control traffic like NetBIOS and SNMP, this is creating a perfect storm of monitoring and security problems for information security and network engineering professionals.

"The new initiatives of the 21st century are based on the business process transformation within a service-oriented architecture," says Frank Dzubeck in a Feb. 2008 *NetworkWorld* article about the growing threat of network latency. "Add organizational and supply-chain transformation through VoIP, video-based collaboration, and innovative real-time, industry-specific applications, and we have a major festering problem."[1]

Performance and security monitoring are growing closer together than ever as these new and traditional forms of traffic clog our networks. Although the presence of a performance or security issue does not necessarily indicate the existence of the other, many analysts are realizing the benefits of behavioral baselines and how a more holistic approach can alleviate the problems of both congestion and security. For example, large data transfers that are causing congestion issues could potentially indicate an attacker retrieving database records.

Another major concern for today's analysts is the fine-tuning of technologies that communicate over the network. Every SNMP-capable device can be configured to send alerts only for very specific events and conditions. With proper tuning, intrusion detection systems can have false positives identified and removed, and other devices and applications can be similarly configured to prioritize alert data.

As we add more and more to our networks, we must seek a unified way to correlate different alerts from performance and security monitoring systems. Today, many applications have their own formats for alerts that do not include enough data to adequately diagnose problems. Neither do they address the performance impacts that may be resulting from security or other problems. As more applications and systems are added to our networks, the number of alarms will continue to grow and the security analyst's visibility into the root cause of problems will likely decrease. For security teams to be effective within today's converged networks, network performance and security monitoring need to converge as well.

[1] http://edge.networkworld.com/columnists/2008/022808dzubeck.html?page=1

Network Monitoring Today

What exactly constitutes a converged network? To most people, any network that unifies voice, data, and video into a high-speed infrastructure is labeled "converged." As voice and data networks were designed for fundamentally different purposes, there have been significant challenges in creating networks that carry both types of traffic simultaneously. Voice traffic has traditionally been comprised of circuit-switched connections in which the connection parameters remain static throughout a call's duration. This allows for real-time communications to take place because a defined data path is established and doesn't change. In contrast, data networks are packet-switched, meaning that individual packets of data may take numerous paths from source to destination, making real-time communications more of a challenge. Modern converged networks attempt to unify these into a single packet-switched environment. But the Internet Protocol (IP) was never intended to handle different traffic types running over a single packet switch, nor was it intended to support the additional protocols related to other types of traffic, as discussed below:

Voice over IP (VoIP)

One of the most common applications in use on converged networks today is Voice over Internet Protocol, or VoIP. One of the major problems with traditional circuit-switched telephone networks is the issue of scalability. In order to keep adding connections and calls, more circuits must be added because each connection is allocated a fixed amount of bandwidth. VoIP allows for much more flexibility in handling multiple calls simultaneously and also helps companies save money by providing additional telephony services like three-way calling and call-forwarding without the company having to pay for them individually. VoIP also enables integration with other IP-enabled services, such as video and multimedia, file sharing, and wireless communications.

VoIP makes use of a number of new protocols. The two that are most commonly used are H.323 and the Session Initiation Protocol (SIP). There are also several others that are commonly encountered on converged networks, some of which are proprietary, for example Cisco's Skinny Client Control Protocol (SCCP). The H.323 and SIP protocols are used to initiate and manage connections, while the VoIP payloads are carried in another protocol, the Real-time Transport Protocol (RTP). Because these protocols are often used in conjunction with the connectionless User Datagram Protocol (UDP), ensuring reliability and security can be difficult due to the dynamic nature of communication channel initiation and teardown. In addition, security researchers have revealed vulnerabilities in both the SIP and H.323 protocols in recent years. In 2003 a series of SIP issues were discovered that could lead to unauthorized privileged access to systems.[2] In 2004, H.323 issues were uncovered that could lead to code execution and Denial of Service (DoS).[3]

For VoIP to operate correctly, additional devices and infrastructure must be in place. Systems like IP Private Branch Exchanges (PBXs) and VoIP gateways are commonly found on converged networks to allow proper session and protocol control handling, as well as compression/decompression and other monitoring and management functions. VoIP communication between devices is often not encrypted by default. Detection of eavesdropping and data interception is very difficult in most cases, especially in an environment with numerous endpoints. VoIP calls are in scope for PCI DSS compliance rules if people take credit card numbers over the phone. If an eavesdropper can intercept and record the calls, credit card and identity theft becomes a very real possibility.

Video

Because video is increasingly being used for training and other corporate purposes, many networks are now carrying video over IP in addition to voice and traditional data. The Real-time Transport Protocol (RTP) is often used for transmission of video data within IP, as are other protocols like Real-Time Streaming Protocol (RTSP) and RealNetworks' Real Data Transport (RDT). Video conferencing can often be coupled with VoIP solutions that employ the SIP protocol, as well. Much like VoIP protocols, video-related protocols were not designed with security in mind and will require additional inspection and attention. RTP, in particular, is susceptible to Denial of Service attacks and uses weak hashing algorithms. As a result, system passwords are easier to crack with password cracking tools.[4]

Additional Converged Applications

In addition to voice and video, other applications that have traditionally used circuit-switched or cable networks are moving into the converged IP network. These include fire alarm and building security systems, surveillance cameras, and fax applications. Some of these may be implemented using standard protocols like RTP, while others may be more proprietary in nature. In many cases, availability is a critical issue for these services. For example, a DoS attack that disables building security sensors or fire alarms could endanger people working in the facility.

[2] http://www.cert.org/advisories/CA-2003-06.html
[3] http://www.cert.org/advisories/CA-2004-01.html
[4] http://kotiweb.kotiportti.fi/vhallivu/files/rtp_security.pdf

Security and Performance Impacts on Converged Networks

With the addition of many new services and systems on IP-based networks, a number of new issues arise. Performance impacts become more numerous and considerably more complex to mitigate. For example, the addition of VoIP telephones into a network adds a significant number of new IP endpoints to a network segment. If the VoIP infrastructure is poorly configured, excessive traffic may be generated by each phone seeking updates and communication with VoIP servers, leading to network congestion and possible loss of telephony services. In addition to application and data availability concerns, new security issues are present due to the continually changing patterns of network behavior.

Performance

Circuit-switched networks have also traditionally been known for stability and reliability, with industry standards of 99.999% uptime considered normal. Packet-switched networks were not designed to have this level of reliability, and so extensive monitoring features and methods have been developed to attempt to rapidly detect and repair any problems. Many of these technologies are vendor-specific and don't natively interact with other tools like security monitoring and management systems. Frequently, one or several groups within an organization will use one set of tools to analyze certain aspects of the network, such as Network Operations Center teams using SNMP tools to monitor network performance and events. Meanwhile, other groups will use entirely different tools to analyze the same network traffic for security analysis and application troubleshooting.

Traditional network analyzers can be used to good effect on network teams in assessing common converged network performance issues such as latency, jitter (signal fluctuation), and packet loss. With the influx of new and more complex protocols, as well as large numbers of distinct endpoints for which available bandwidth must be managed for critical services such as customer-facing applications and daily business traffic, performance monitoring on converged networks is of paramount importance. For services like VoIP, the use of Quality-of-Service (QoS) mechanisms is common for dynamically monitoring and detecting common issues like latency and jitter. In most cases, high-end network equipment can be tuned to self-adjust for many issues. However, the need to continuously monitor critical services is even more pronounced in converged environments. A viable threat to VoIP is Denial of Service (DoS) attacks, which could cripple all telephone service without proper monitoring.

Security

The lack of coordination with tools and techniques for examining converged network traffic is a real problem because each group is only getting some of the information but not enough to see the entire picture. For example, the network engineering team may be monitoring SNMP traps and QoS on several network segments — and may have a fair idea of what the bandwidth patterns should look like in the context of a normal behavioral baseline. However, the information security team may have completely different views of the bandwidth usage patterns due to network forensics and event monitoring that they are performing. Without collaborating or correlating the data, significant security issues may be missed.

Security teams must also keep pace with new attacks on protocols, such as SIP, which include registration hijacking and eavesdropping. Increased visibility into network traffic and behavioral baselines is critical to detect and prevent such attacks.

Another major concern for security teams is the increased storage needs required in converged environments. With new critical applications and data types, the need for considerable enhancements to logging infrastructures is quickly becoming a reality. Security and audit teams are also tasked with implementing controls for regulatory and industry-specific compliance mandates, which bolsters the need for logging, forensics, encryption or other access controls.

Leveraging Network Data for In-Depth Security

How can network policies be adequately enforced in converged networks? The types of enforcement might include the following:

- **Access controls**, with which certain users or systems are either allowed to or prevented from communicating depending on numerous factors including IP address, configuration details, type of traffic, etc.
- **Bandwidth control**, with which tools like QoS and rate limiting are configured to detect particular traffic conditions that trigger policy enforcement events
- **Security detection and prevention controls**, with which signatures or behaviors in application or other traffic cause events to be generated or access to be denied
- **Threshold alerting**, with which tools like SNMP traps are generated due to specific conditions on systems or in traffic patterns

Aside from access controls, most other types of security and performance monitoring can be leveraged for enforcing policy. The need has never been greater for tools that provide proactive monitoring, alerting and forensic analysis capabilities. In converged networks, with many types of application traffic traversing the network simultaneously at high speeds, monitoring tools must be capable of accurately identifying specific application traffic, differentiating normal traffic flow between known endpoints from unknown or malicious traffic based on known patterns for those traffic types, and establishing distinct thresholds from which alerts can be generated and disseminated appropriately.

TCP Traffic Analysis

From a purely logical perspective, traffic is traffic — it's what we see in it and do with it that differentiates intrusion detection and forensics from performance monitoring and troubleshooting. With tools that can capture large volumes of traffic and allow accurate reconstruction of scenarios and conversations, security teams are much better armed to analyze potential attacks and events. For example:

- **Full application data:** For many of today's more complex attacks, as well as the majority of sophisticated malware, analysts will need to inspect the full content of packets on the network. For applications like VoIP, analysts will need to decode content within RTP packets with additional tools or inspect specific SIP packets. In October 2007, Proof of Concept code (see Figure 1) was released that demonstrates how malware could be launched on a user's system via Cross-Site Scripting (XSS) attacks via VoIP[5] :

[5] http://packetstormsecurity.org/0710-exploits/sip-pwn.txt

```
INVITE sip:h@192.168.1.3 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.9:5060;rport
To: sip:h@192.168.1.3
From: "<script>alert('hack')</script>""natraj"
<sip:natraj@loria.fr>;tag=002f000c
Call-ID: 401010907@192.168.1.9
CSeq: 4857 INVITE
Content-Type: application/sdp
Subject: sip: natraj@loria.fr
Contact: "natraj" <sip:192.168.1.9:5060;transport=udp>
Content-Length: 214


v=0
o=root 47650 47650 IN IP4 192.168.1.9
s=session
c=IN IP4 192.168.1.9
t=0 0
m=audio 5070 RTP/AVP 3 0 110 5
a=rtpmap:3 GSM/8000/1
a=rtpmap:0 PCMU/8000/1
a=rtpmap:110 speex/8000/1
a=rtpmap:5 DVI4/8000/1
```

Figure 1: Proof of Concept code for XSS attack via the SIP protocol

- **Session data:** Session data consists of source IP and port, destination IP and port, timestamps, and quantity of data exchanged.[6] Although many applications, such as VoIP and streaming video, use connectionless protocols such as UDP for transport, approximations of sessions can be construed from observing patterns of communication, which can be useful for establishing traffic patterns and communication behavior on network segments. Cisco's NetFlow and sFlow are two common standards used for session data analysis.

[6] Bejtlich, Richard. "The Tao of Network Security Monitoring."

- **Performance and behavior statistics:** Analysts looking into performance or security issues can benefit from monitoring performance and behavior statistics. Some of these might include the amount of traffic seen on device interfaces, the types of protocols seen in use, how much of each type of traffic is currently on the network, and packet quantities at different times. For example, a significant increase in UDP packets may be indicative of a malware outbreak. Below are some screenshots of open-source and commercial tools that can actively watch traffic or take traffic captures from other systems to analyze.

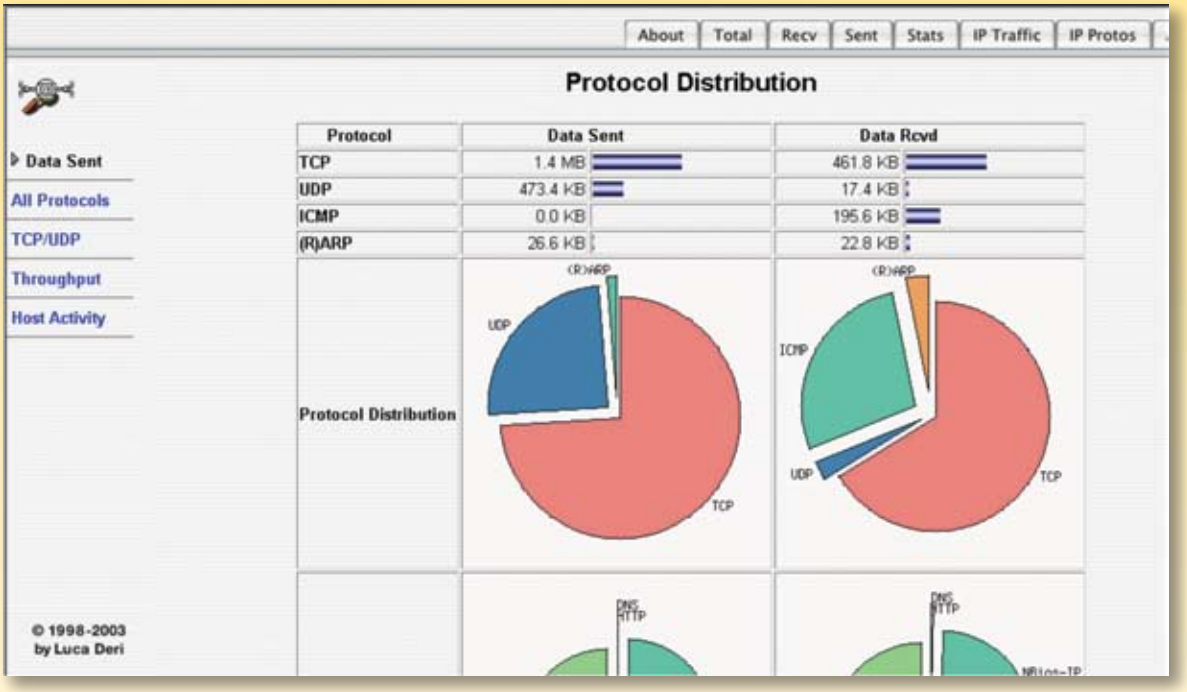
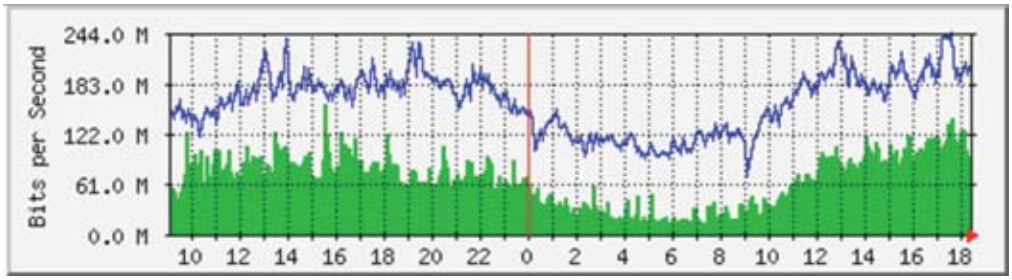


Figure 2: Analysis of top applications showing protocol information



	Max	Average	Current
In	158.2 Mb/s (15.8%)	64.8 Mb/s (6.5%)	79.7 Mb/s (8.0%)
Out	242.1 Mb/s (24.2%)	159.5 Mb/s (15.9%)	193.7 Mb/s (19.4%)

Figure 3: Daily traffic load

Figure 4: Hourly VoIP traffic load showing MOS, jitter, packet delay and packet loss

Behavior Analysis

Using monitoring tools, analysts can develop a baseline of normal network activity within the converged environment. The different aspects of network usage that can be gathered are almost infinite; but several key measurements that may be useful include:

- Load statistics on specific network segments (bits/second)
- Protocols in use on specific network segments
- "Top talkers" on network segments — and who they frequently talk to
- Services in use (source and destination ports)

Both network and security staff can make use of this information. However, monitoring the frequency and types of communication becomes more difficult in a true converged environment for three major reasons:

1. Most converged networks are running at Gigabit and greater speeds by necessity. This makes capturing traffic more difficult and requires tools capable of handling this volume.
2. The number of endpoints to monitor goes up tremendously due to new IP-enabled devices like VoIP phones and mobile devices. Tracking flow statistics and session data can be very hard to manage when the number of devices increases.
3. The complexity of the traffic itself is a factor. Many engineers do not fully understand all the new protocols and applications in use. For the SIP protocol alone, the paper "SIP-based VoIP Traffic Behavior Profiling and Its Applications" describes a behavioral profiling method that involves: identifying SIP users and registrars by inspecting SIP REGISTER and INVITE messages, analyzing user and server behavior patterns, and assessing expected ratios of SIP requests and responses.[7]

[7] http://www.ece.rice.edu/~sranjan/publications/minet-sip.pdf

Enterprise Correlation

Full traffic captures are the primary data source for assessing network-based performance and security issues. However, the ability to correlate this data with other sources is also valuable for incident response and forensics efforts. Tools that offer enterprise dashboard capabilities for monitoring and analyzing network behavior, inspecting and prioritizing alerts from SNMP traps and network-based detection devices, and correlating this data with other sources, such as log data and device configurations, will be invaluable for network and security teams.

Today, security teams may use Security Information and Event Management (SIEM) systems and Intrusion Detection and Prevention systems to assess network events and behaviors. At the same time, network teams may use network analyzers, network and systems management tools, and protocol analyzers to maintain networks. Even more specialized tools may be used for monitoring in Network Operations Centers and Security Operations Centers (NOCs/SOCs). A June 2007 Gartner report sees operations and security markets converging in 2008 with one product set providing a common network monitoring infrastructure for the NOC and the SOC.[8] "With the added complexity and traffic volume present in converged networks, more effective collaborative capabilities will be needed," the report stated.

[8] Gartner, Inc. "Select the Right Monitoring and Fraud Detection Technology," Mark Nicolett et. al., June 28, 2007

An Outline for Monitoring Converged Networks

As the network grows in complexity, organizations will need to develop and adhere to processes for assessing the risks to their environments. Any process should likely include the following steps:

- **Establish Baselines:** Understand how your network normally functions, which devices talk to whom, what kinds of traffic are normally seen (and in what quantities), and what times are peak load times. Decide on a reasonable period of time (usually between 30-90 days is appropriate) and capture traffic from critical network segments. Observe the patterns of usage each day, being careful to investigate any spikes or strange traffic patterns. Note why the spikes or abnormal patterns occurred. Also take any unique events into consideration, such as holidays or business promotions that could cause short-term fluctuations. In the article, "10 Best Practices for Managing a Converged Network," Leslie T. O'Neill's first three recommendations include defining organizational goals, testing the network with assessment tools, and establishing and configuring QoS metrics[9]. Taking these steps is an excellent approach for beginning your baseline establishment process.
- **Apply Monitoring Rules:** Configure a number of different types of monitoring once you have established traffic baselines. These include:
  - *Security monitoring.* Monitoring should include vulnerability signatures and other types of known attacks for specific applications. Access control monitoring should also be in place to look for failed attempts to log in to critical systems. An example of such monitoring in a converged environment would be finding multiple failed attempts to access the IP PBX in a VoIP network.
  - *Behavioral monitoring.* Such monitoring can be handled by creating rules for session-related data, such as NetFlow or sFlow, as well as general network performance monitoring using probes that leverage SNMP MIBs like Remote Network Monitoring (RMON). An example of Internet2 NetFlow statistics for voice and video is shown in Table 1[10]:

[9] http://www.itmanagement.com/features/10-practices-converged-network-082807
[10] http://netflow.internet2.edu/weekly/20080310

Traffic type	Octets		Packets	
Audio/Video	---	---	---	---
Any-Source Multicast	1.50%	11.950T	0.94%	10.560G
Real Player	0.38%	3.051T	0.62%	6.932G
Windows Mediaa	0.03%	231.100G	0.03%	368.600M
H.323 Signaling	0.02%	133.400G	0.01%	168.400M
Backbone Radio	0.01%	73.250G	0.01%	90.250M
StreamWorks	0.00%	16.670G	0.00%	25.820M
Subset of VoIP	0.00%	6.425G	0.00%	11.420M
Camarades Webcams	0.00%	1.710G	0.00%	4.486M
Single-Source Multicast	0.00%	0.000	0.00%	0.00

Table 1: Audio/Video NetFlow Statistics on Internet2

- *Traffic threshold and network device monitoring.* This is commonly measured using tools like QoS and SNMP traps. QoS alerts can indicate that traffic in particular segments is exceeding anticipated bandwidth, which can indicate a need for additional infrastructure changes to accommodate new converged services. SNMP commonly makes use of local device traps that alert when thresholds are met. You can configure other alerts to detect possible Denial of Service (DoS) conditions or fast-spreading malicious code activity.
- *Other types of monitoring* might include protocol frequency and general error monitoring; for example, looking for the presence of malformed SIP packets or misconfigured applications that are sending out broadcasts. Other anomalies can be detected by unique packet signatures that may indicate the presence of softphones or other specific vendor equipment that is not permitted by policy, etc.

• **Develop Custom Reports:** Too much information can be just as bad as too little information; thus, it's important to determine what should be reported and how often. If enterprise dashboard tools are available — and can integrate and correlate the information from both performance monitoring rules and security-focused rules for behavior and attacks — it is much easier to generate unified reports that present a holistic view of a converged network's health. If separate reports are generated for unique monitoring statistics and events, the information may need to be correlated manually. For most converged networks, whenever possible, the three major categories of reports should include voice traffic reports, network and application performance reports, and consolidated security events.

• **Pay Attention to Storage:** Network traffic and other logs will require significant storage on converged networks. This should be carefully planned ahead of time, and a Storage Area Network (SAN) or other similar technology should be employed if possible. Over time, packet and log data stores should be carefully monitored to ensure critical data isn't lost or overwritten.

Conclusion

Today, many organizations that run voice, video, and data application on the same infrastructure are implementing or moving toward converged networks. Although this often makes excellent business sense, the increase in new protocols, diverse endpoints, and overall traffic volume make network performance and security monitoring more difficult — and also more critical than ever before. Performance issues can cripple the ability to perform normal business functions, while security problems are more difficult to identify inside all these new types and patterns of traffic. New tools must address these issues by converging themselves. Having distinct monitoring applications for the network team, security group, and help desk just doesn't make sense. Each group is looking at the same information from their different silos. As networks converge, so too will the monitoring tools used to maintain and manage those networks. With adequate planning and preparation, organizations can develop enterprise-wide monitoring capabilities that improve performance and security, and even retain packet data for more in-depth forensics and analysis.

About the Author

Dave Shackleford, Director of Configuresoft's Center for Policy & Compliance, is a course and exam author for the SANS Institute, where he also serves as a GIAC Technical Director. He is the co-author of ***Hands-On Information Security*** from Course Technology, as well as the "Managing Incident Response" chapter in the Course Technology book, ***Readings and Cases in the Management of Information Security***.

Previously, he worked as CTO for the Center for Internet Security, as well as for a security consulting firm in Atlanta. He has also worked as a security architect, analyst, and manager for several Fortune 500 companies. He has consulted with hundreds of organizations in the areas of regulatory compliance, security and network architecture and engineering. His specialties include incident handling and response, intrusion detection and traffic analysis, and vulnerability assessment and penetration testing.

SANS would like to thank its sponsor: