IBM Telecom Core Infrastructure Security Solution

The IBM Telecom Core Infrastructure Security Solution monitors and manages the health of both the network elements and the actual traffic itself from a single, integrated system.

Highlights

- ***Optimizes operational security systems investments***
- ***Reduces time to market for new security services to customers***
- ***Addresses the security in the "cloud"***
- ***Addresses end-to-end security: networks, systems, users***
- ***Addresses increasing customer demands and Service Level Agreements***
- ***Provides integrated and reusable components***

Changing dynamics in the telecom security landscape

Significant changes have occurred in the telecommunications (telecom) security landscape. From embedded worms traveling in the communication clouds and infecting scores of networks to denial of service attacks that are designed to disrupt commerce, malicious attacks over the Internet have historically been targeted at "end-points" through their telecom links. The burden of protecting against these attacks is falling more and more on the owners of these telecom networks.

In the past, there was no need for telecom service providers to provide security for the connections that end-point customers used to access the Internet. The telecom role has traditionally been that of "a purveyor of bits." End-point customers would buy bandwidth, and would pay for it by the bit—regardless of whether those bits were clean data, viruses, or worms.

The burden of responsibility between the user, enterprise, and telecom has shifted. Let's take a closer look at these changing dynamics.

Evolving relationship between user, enterprise, and telecoms

The first of these dynamics is driven primarily by the changing role of the telecom. As the average revenue per user for traditional voice service has declined, the telecom industry has re-directed its efforts into launching and delivering a full suite of IP-based services.

Some examples of IP-based services are Voice over Internet Protocol (VoIP), Internet Protocol Television (IPTV), Push to Talk, and instant messaging. This change in focus is magnified by the consolidation of wireline and wireless carriers as service providers race to deliver "any service on any device."

Now that telecoms are themselves IP service providers, they are also, by definition, end-point owners. Therefore, telecom assets are now just as vulnerable to attack as any other end-point device. In fact, an entirely new breed of attack has emerged, one that is specifically designed to cripple key IP service components such as SIP proxy servers (used for VoIP and IPTV), DNS servers, and even the network routers themselves.

As telecoms surveyed the landscape of available technology for securing their infrastructure, they found newly evolving network elements that can help secure a carrier-class network combined with enterprise-class appliances.

Shifting burden of managing the complexities of defending against attack

The second of these dynamics is driven by the dramatic acceleration of the frequency, sophistication, and malevolence of attacks. This acceleration and its substantial increase in complexity have severely taxed the ability of enterprise customers to defend their networks effectively. In addition, IT managers must now protect against threats from inside their network and not just from the outside.

Despite their investments in security technology, most customers can only hope to identify an attack after it has occurred and try to prevent the same attack from occurring more than once. To that end, enterprise customers are now expecting their telecom vendors to shoulder a significant portion of the load. They are demanding "clean pipes" from their service providers, and the service level agreements (SLAs) from the telecoms are reflecting those demands. SLAs that once triggered small penalties for passing infected traffic can now cost the telecom a month of bandwidth charges per instance or, in some cases, even more. Moreover, as bandwidth prices become a commodity, aggressive SLAs have become a much more prominent tool in the competitive arsenal of telecoms as they try to attract new customers.

To meet the diverse security demands of their enterprise customers while driving additional revenue, telecoms are beginning to offer managed security services. These services require that the technology used to secure their own core be extended to reach out to the enterprise and work with the security components already installed.

Requirements for a comprehensive security protection solution

Telecom service providers cannot wait for emerging network elements to develop because attacks are continuously experienced. Some are only being reported after the damage has been done. A comprehensive "security protection" solution therefore must meet the needs of both core telecom carrier security and downstream enterprise security effectively. To do so, it must have the following attributes:

- *A unified view of the network* with the ability to perform real-time analysis of all the traffic on the network while simultaneously understanding the underlying infrastructure through a combination of discovery and event collection

- *Both macro and granular visibility of traffic and network elements* for monitoring the behavior of the network as a single entity while also providing full-packet capture and forensics capabilities down to a single IP address

- *Full correlation that can span all traffic and network elements* with the ability to detect even the most distributed of attacks with extremely high accuracy and very low false positives or negatives

- *Flexible attack mitigation* to support both manual and automatic forms of attack mitigation, providing access control similar to a circuit-switch network for the operator

- *Superior reporting and management capabilities* with a management console that can provide a single, unified view of the health of all traffic and network elements, flexible pre-configured reports, and real-time, dashboard-style reports

- *Robust storage capability* to meet the storage requirements of historical and trend analysis

- *Scalability* to meet the demands of large, highly distributed carrier networks

- *Flexibility and customization* that includes configurable reporting, a configurable user interface that can interface with any network element, and the ability to create custom algorithms to detect any type of anomaly

IBM Telecom Core Infrastructure Security Solution

The IBM Telecom Core Infrastructure Security Solution monitors and manages the health of network elements (or the cloud) and the actual traffic itself from a single, integrated system. It features a powerful combination of technology designed to detect virtually any malicious threat or network anomaly, no matter where it originates.

From worms and viruses propagating from outside the network perimeter to insider threats emanating from within the network, this solution can detect these threats early and accurately.

In addition, the Core Infrastructure Security Solution features powerful, flexible mitigation options that network operators can use to take action and enforce policy either manually or automatically. This solution is scalable to meet the demands of large, highly distributed carrier networks.

The solution features three core components. IBM Tivoli® Security Operations Manager provides the monitoring and correlation of the elements found in the network while NarusInsight™ Secure Suite (NSS) provides similar monitoring and correlation of the network traffic itself. IBM Tivoli Netcool® then acts as the manager of the managers by providing an additional tier of correlation between Tivoli Security Operations Manager and NSS. User interfaces for reporting and portal access are provided by Netcool Impact and Webtop.

• Complete monitoring of both IP traffic and network elements

With the Tivoli Netcool Precision component, the Core Infrastructure Security Solution can provide flexible, automated discovery of all Layer 1, 2, and 3 devices in the IP network from the transport layer optical devices to routers, switches, and IP addresses. Netcool Precision generates an accurate up to date inventory of devices, systems, and applications within an infrastructure.

Tivoli Netcool Precision also provides a snapshot of the network topology and a basic mapping of applications to their underlying servers. This view is critical to monitoring the health of network elements and is the first line of defense against attacks in or originating from the network.

To monitor and detect threats from outside the network, the solution uses the NSS component, which can analyze and profile live IP traffic in real time and inspect packets from layer 2 to layer 7. The NSS Semantic Traffic Analyzer monitors traffic directly as a "smart probe" by passively tapping the network. Alternatively, using a software agent, NSS can interface with any network element such as a router (Cisco Netflow or Juniper cflowd), IDS/IPS/Firewall, RADIUS server, SNMP MIB or DBMS. NSS is typically deployed in carrier networks close to the core (between the gateway router and the backbone router) and can monitor traffic at speeds up to 10 Gb/sec (OC 192).

- **Multi-tiered correlation capability**

The Tivoli Security Operations Manager and NSS components offer correlation between network elements and IP traffic features. It also offers correlation between its software components to provide the most complete picture of network behavior. Using this multi-tiered correlation capability, the solution detects the widest possible range of attacks with significantly increased accuracy.

The NSS component correlates traffic features across multiple sophisticated security algorithms that are based on Signal Processing and Information Entropy. In this way, it can monitor even the largest network as a single entity.

In addition to detecting changes in traffic volume or known worm signatures, NSS can use the Information Entropy technology to detect minute shifts in features such as "traffic randomness" that are the precursor warning signs of malicious threats. This leads to much earlier detection of even the lowest-volume, most-distributed attacks, such as DDoS, Zero-day worms, and Polymorphic worms. NSS can also detect an entire class of attacks directed at layer 7 applications (such as VoIP, DNS, http, and SMTP) and the Border Gateway Protocol (BGP) routing infrastructure found at Layer 3.

Tivoli Security Operations Manager can also provide infrastructure feature correlation between data generated by both discovery and event collection. It offers several correlation methods, including event reduction and device-level, policy, and service correlation.

- **Unique analytics and forensics**

With the solution, users have access to a top-down, macro view and the granular, IP-address specific view of both traffic and network elements. With this "zoomable" view, operators can rapidly investigate detected anomalies and make mitigation decisions in near real time. NSS is not visible to the installed security infrastructure (for example, firewalls, IDS/IPS) and can immediately enable full-packet capture on the traffic after an anomaly is detected.

NSS provides real-time analysis of questionable traffic with powerful forensics capabilities. It can quickly identify the nature of the anomaly, its source IP address, and its propagation path and create a signature for the threat. NSS can also distinguish malicious threats (for example, worms and viruses) from benign ones (for example, a mis-configured router).

NSS analyzes packet headers and payloads for behavioral signs of malicious activity, and it can detect many classes of attack that IDS/IPS systems might not see (such as fragmented or "TearDrop" attacks, for example). Moreover, NSS can detect these traffic-based attacks as they occur, providing faster response and even mitigation.

Tivoli Security Operations Manager uses network infrastructure logs that include events that have actually occurred, so it can detect attacks outside the flow of the traffic itself. In other words, it can monitor not only device event records, but also user and file access activity. This means that it can track changes to file permissions, attempts to install new executables, or attempts to access privileged services.

- **Powerful reporting and mitigation: "the manager of managers"**

Tivoli Security Operations Manager and NSS have been integrated with IBM Tivoli Netcool®/OMNIbus and Netcool Impact so that the solution has flexible reporting and mitigation capabilities. The solution supports a wide range of reporting and mitigation options, from manual notifications that guide human decisions to fully automated device-level clearing and diagnostics to direct interfaces to 3rd party traffic shaping, blocking, or quarantine products. Tivoli Security Operations Manager and NSS both use Tivoli Netcool as the common policy management engine for manual notification and automatic mitigation. A reporting interface that can be customized displays reports and dashboard alerts. In addition, operators can access the solution using a portal that they can define.

For automatic mitigation, the solution interfaces directly with any third-party device such as IBM Tivoli Provisioning Manager and Cisco SCE for automated, real-time traffic shaping and blocking. For automatic quarantine and infected traffic cleansing, the solution interfaces with products such as Cisco Guard.

- **Integrated storage featuring significant capacity**

IBM Telecom Core Infrastructure Security Solution offers significant storage facilities for historical data analysis. The solution can archive most types of data—from finely granular information to summarized metadata—into most database management systems (such as DB2, MySQL, and Oracle) and retrieve it at the time it is needed with negligible latency.

Historical data analysis can drive a wide range of decision support systems. Now operators can access historical data to decide in real time which actions to take based on successful actions taken in the past. In addition, trend analysis can facilitate many business decisions such as capacity forecasting, bandwidth usage, and revenue forecasting.

- **Scalability**

The Core Infrastructure Security Solution offers scalability in the monitoring of network elements, network links, and sheer volume of traffic. From the network element perspective, Tivoli Security Operations Manager supports 200 different devices such as routers, IDS/IPS, and firewalls. Netcool/OMNIbus supports even more devices, which means the solution can scale to Tier-1 carrier traffic. Meanwhile, NSS offers real-time traffic monitoring and analysis at speeds up to 10 Gb/ sec. Currently monitoring Tier-1 carrier networks that pass over 2.5 petabytes of traffic each day, NSS is designed to support an unlimited number of network links on a carrier network (including high-speed peering links).

Core Infrastructure Security Solution data flow

The IBM Core Infrastructure Security Solution consists of IBM software and systems and NSS. Figure 1 illustrates the data flow of the solution. The role each of the products plays is as follows:

1. Anomalies are detected by TSOM (using network element analysis) and NarusInsight Secure Suite (using real-time traffic analysis) running on IBM BladeCenter® servers. Information about these anomalies is either passed to Tivoli Netcool in the form of security events, or into a DBMS (IBM DB2®, Oracle, MySQL, and so on) as metadata for historical trend analysis (or both).

2. IBM Tivoli Netcool adds additional correlation of the security events from TSOM and NSS and delivers these correlated events to the DBMS so that the events are available for querying and reporting.

3. The reporting engine developed in Netcool Reporter can be used to query the correlated security events and the traffic classification metadata in the DBMS .

4. Pre-configured reports and dashboard alerts are delivered to the user from a portal developed with Netcool Webtop.

5. After an anomaly is detected, the policy of the organization (either manual or automatic) is then enforced by Netcool.

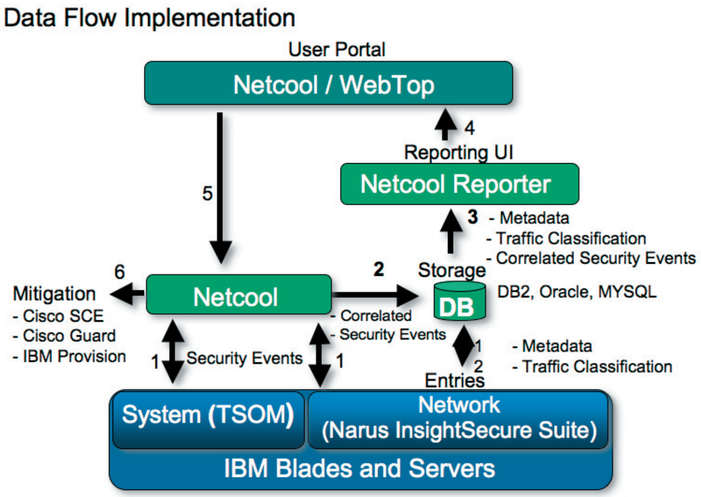

Figure 1: IBM Core Infrastructure Security Solution data flow

6. Netcool provides mitigation either directly to a given device or it can use an external mitigation system such as IBM Policy Manager, Cisco Guard, or Cisco CSE.

Sample attack scenario: NSS and TSOM in action detecting Sasser worm attack

In this section, we describe an attack scenario for a managed security service environment and the strengths of the combined solution to tackle this problem. In this scenario, one machine is infected by the Sasser worm.

The Sasser worm scans IP addresses using port 445 for vulnerable machines. As soon as this worm detects an unpatched system, it drops a script that downloads a copy of itself. This spreads the infection wide and deep through Internet without targeting a specific customer. Figure 2 shows NSS detecting the Sasser worm as soon as the first machine (192.1.1.2) is infected by registering a change in the structure and randomness of the traffic as a whole. In this case, the infected machine begins to request open

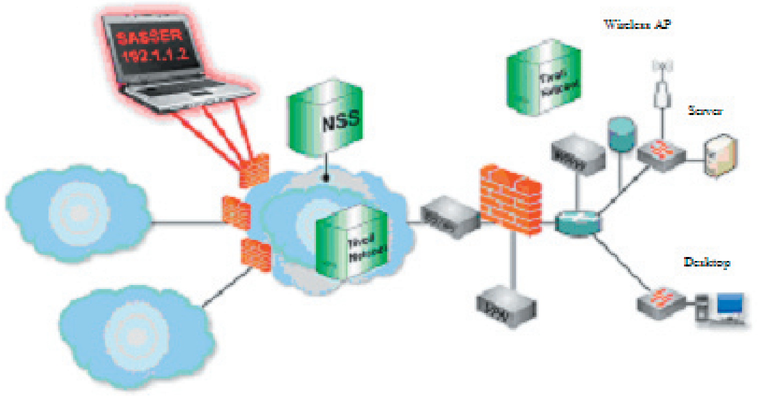

Figure 2: NSS detects the Sasser worm as soon as the first machine (192.1.1.2) is infected.

sessions from a significant number of hosts, but it always requests the same port number. This subtle change in the randomness of the traffic is detected well before any significant change in traffic volume is noticed, and well before it reaches the enterprise network running Netcool.

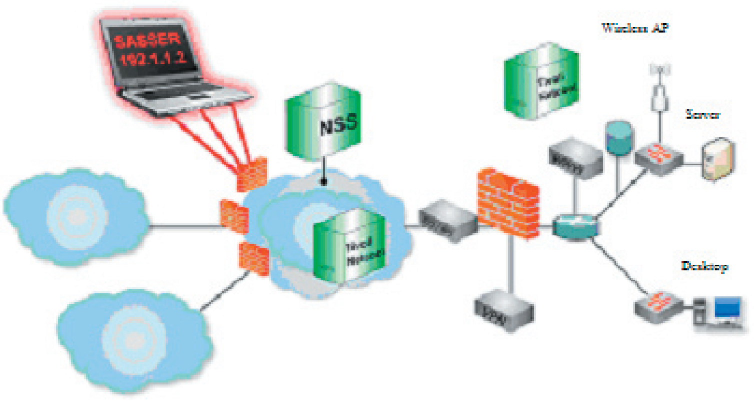

Figure 3. NSS begins to see the Sasser worm propagate across the network

Figure 3 shows NSS as it begins to see the Sasser worm propagate across the network. As soon as more machines are infected by the worm, NSS reports an anomaly to the Tivoli Netcool server inside the enterprise network. NSS provides Netcool with detail records so that it can decide whether or not to take any action.

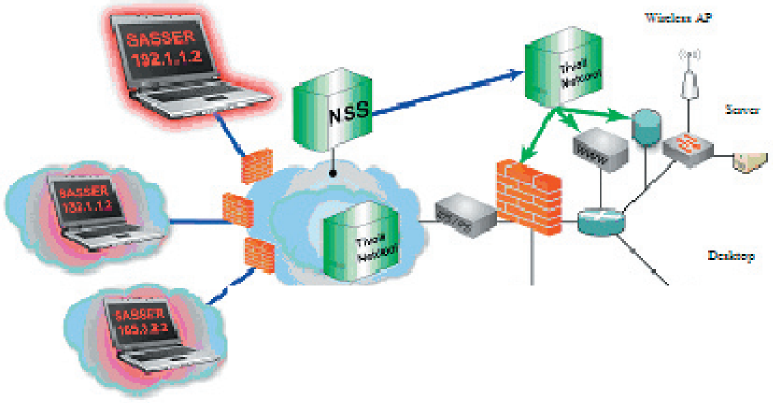

Figure 4. Tivoli Netcool contains a policy for worm enforcement designed by the customer

The customer has designed a policy for worm enforcement for Tivoli Netcool. After NSS has informed Netcool of a worm outbreak, Netcool then enforces that policy. In this case the policy calls for NSS to extract the unique fingerprint (or signature) of the worm and deliver that fingerprint back to Netcool. Figure 4 shows this process. Netcool then forwards the worm signature to all of the IDS/IPS/firewalls located on the edge of the network so that they can immediately update their databases.

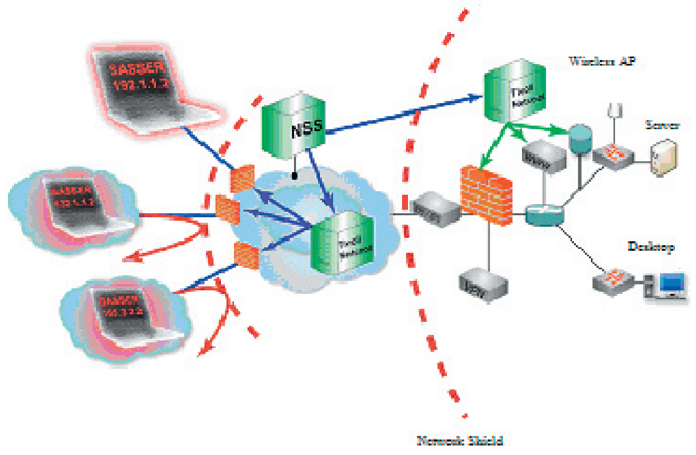

Figure 5. Worms reaching the customer perimeter are bounced at the edge of the network.

As Figure 5 demonstrates, by the time the worm reaches the customer perimeter, it is bounced at the edge of the network IDS/IPS/firewalls. Tivoli Netcool mitigates the attack using NSS anomaly records.

Core Infrastructure Security components

Key professional services:

- *Security consulting for carriers*
- *Secure solution design for telecommunications*
- *Pilot/proof-of-concept implementation*
- *Solution implementation for telecom security*

Technology platform:

- *IBM systems*
- *IBM System Storage™*
- *IBM BladeCenter*

System software:

- *IBM Tivoli Netcool*
- *IBM DB2*
- *IBM Tivoli Security Operations Manager*
- *NarusInsight Secure Suite (NSS)*

Enablers:

- *Linux®*

How IBM can help

IBM has a long history of working with telecommunications companies to make them more efficient and secure, which makes us an ideal partner for core infrastructure security. IBM is a leader in the application software, hardware, and services critical for monitoring and managing the health of networks and network traffic.

IBM helps plan and design core infrastructure security solutions for telecom carriers. We have the broad capability, industry expertise, leading-edge technology, and experience to help you build the right telecom core infrastructure security solution.

To learn more about IBM, contact your IBM representative.

Summary

- *IBM Telecom Core Infrastructure Security Solution monitors and manages the health of network elements and the actual traffic itself from a single, integrated system.*
- *Built with world-class, best-of-breed technology, the solution is able to detect a much wider range of threats early.*
- *The solution has multi-tiered correlation capability. It can provide much greater detection accuracy and better data points, so that telecoms can make faster and better decisions.*
- *Powerful analytics, forensics, and reporting capabilities help you target and mitigate threats as quickly as possible.*
- *Carriers can take advantage of integrated data storage with capacity, which supports historical analysis, faster attack detection, greater network capacity, more bandwidth, and revenue forecasting.*
- *Because the solution is designed to scale from the enterprise to the largest carrier network, carriers can now obtain a comprehensive, integrated "security protection" solution from a single vendor.*

IBM Corporation
New Orchard Road
Armonk, NY 10504
U.S.A.

Produced in the United States of America 03-07.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.