

# Management of Network Security Applications

## **Philip C. Hyland**

Ph.D. Candidate, George Mason University

TASC, Inc.

4801 Stonecroft Blvd.

Chantilly, VA 20151

Phone: (703) 633-8300 (W)

Fax: (703) 449-1080

E-Mail: [pchyland@tasc.com](mailto:pchyland@tasc.com)

<http://mason.gmu.edu/~phyland>

## **Ravi Sandhu**

Professor, Department of Information and Software Engineering

George Mason University

Fairfax, VA 22030-4444

Phone: (703) 993-1659 (W)

Fax: (703) 993-1638

E-Mail: [sandhu@gmu.edu](mailto:sandhu@gmu.edu)

<http://www.list.gmu.edu/~sandhu>

## **ABSTRACT:**

Security policy and security techniques have been major research topics for a long time, but relatively little work has been reported on management of distributed security applications. This paper reviews several security management projects and related security research to date. We present a core set of security managed objects for use with the Simple Network Management Protocol (SNMP). Security applications are assessed for value of management via SNMP. A scenario of corporate firewalls illustrates concepts of security management correctness, sufficiency, and completeness. Ongoing investigations, case studies, and implementation issues are discussed. Introduction of a Packet-Filter Information Protocol (PFIP) suggests propagation of security information in a manner used by routing protocols. We conclude with recommendations for further work to advance SNMP-based management of security applications.

## **KEYWORDS:**

Firewalls, Management Information Base (MIB), Network Management, Packet-Filter Information Protocol (PFIP), Security Application Management, Security Management, SNMP

## I. Introduction

General security solutions try to establish perimeters or layers of protection to filter what data passes in or out. Multiple layers and access points make robust network security systems a natural example of distributed operations in both implementation and management aspects. The level of threat to the resources and data within a system makes active management of security capabilities an important distributed operations mission.

Computer security has been of interest since the first multi-user systems. Only recently, since vital data and critical business functions moved onto networked systems, have network security mechanisms proliferated. User expectations of system quality, privacy, performance, and reliability are growing. The rapid deployment of new security technology needs flexible, efficient management to help system operators from being overwhelmed by configuration and monitoring overhead. The complexity and interdependent nature of network security demands an up-to-date system view and the capability to gather and correlate underlying event details.

A security program depends on the correctness, completeness, and reliability of three related components – *security policy*, *implementation mechanisms*, and *assurance measures*. **Figure 1** shows the relationships between these components and end users. Security policies set the guidelines for opera-

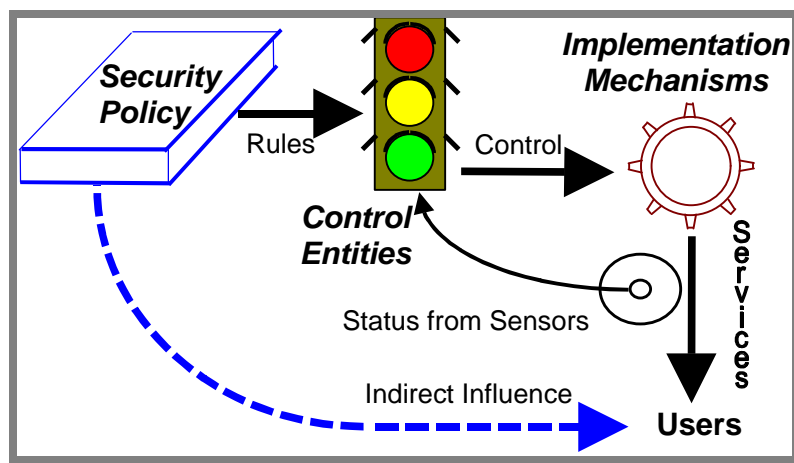
tional procedures and security techniques that counter security risks with controls and protective measures. Security policy has a direct impact on the rules and policing actions that ensure proper operation of the implementation mechanisms. Policy has an indirect influence on users; they see security applications and access services, not policies. The security policies of the organization determine the balance between users' ease of use and level of responsibility versus the amount of controls and countermeasures.

The goal of the security manager is to apply and enforce consistent security policies across system boundaries and throughout the organization. The challenges in achieving a functional security system are twofold. First, a consistent and complete specification of the desired security policy must be defined, independent of the implementation. The second need is a unified scheme to enforce the applicable security policies using available tools, procedures, and mechanisms. The difficult task in achieving a "state of security" is not obtaining the necessary tools, but choosing and integrating the right ones to provide a comprehensive and trustworthy chain of security.

Security policy and security techniques have been major research topics for many years. However, study and experience with operational network security management are lacking. We believe that the need for security management will multiply, much as the

growth of LANs created a demand for better network management solutions. As the active part of the assurance component, operational security management deserves and requires additional research to harness the full potential of many evolving security systems.

The quantity, variety, and complexity of security applications represent so many different functions and security states that integrated management would be



**Figure 1. Security Components**

impossible without mapping attributes to a common management model. In this paper, we present a structure for a common security Management Information Base (MIB) and discuss its application to representative security mechanisms. A new Packet-Filter Information Protocol (PFIP) is introduced for propagation of security information.

Our goal is to promote a better understanding of the issues and approaches to integrated, consistent security management. Section 2 provides background in the related topics of network management and a review of security and system management work to date. Section 3 develops the foundation for a security management concept using common security attributes, extension of the network management infrastructure to encompass security management, and core challenges to a more robust security management environment. It also identifies ongoing work being done at GMU's Laboratory for Information Security Technology to implement security management prototypes. Section 4 draws conclusions on the state of development of security management and needs for further work.

## II. Background and Related Work

Security management has long been considered a sub-function of network management. It is one of the five functional areas defined in the OSI management framework [5]. International standards for security functions like audit trails, security alarms and notifications, key management, authentication, and access control have generally progressed much farther than similar work in the IETF community. Between 1992 and 1994, a European security management prototype called Project SAMSON [7] identified an integration architecture that included both CMIP and SNMP interfaces for management of security mechanisms. Another project called WILMA [13] produced some SNMP development tools in 1995 for security management.

### A. Terminology

We define security management as the “*real-time monitoring and control of active security applications that implement one or more security services.*” The purpose of security management is to ensure that the security measures are operational, in balance with current conditions, and compliant with the security policy. Not only must the services function correctly and in a timely fashion, they must counteract existing threats to generate *justifiable* confidence in the system trustworthiness. One of the largest security pitfalls is to focus on certain security products or technologies without defining a balanced security policy and thereby gaining a false sense of security. Protection is only as strong as the weakest link.

Assurance is the conventional term for methods that are applied to assess and ensure a security system enforces and complies with intended security policies. One may use assurance tools before, during, or after security mechanism operations. Post-processing of security events typically includes audit trail analysis and related off-line intrusion detection and trend analysis methods. Many Intrusion Detection System (IDS) applications began as post-processing functions due to limited processing and software capabilities, but most are migrating toward interactive, real-time operations [12].

Pre-operational analysis of security may involve extensive testing and the use of rigorous logical analysis referred to as *formal methods*. This approach is widely applied in critical aviation, nuclear power and medical systems, as well as security kernels, to enhance reliability [9]. The need for highly reliable security systems cannot be satisfied only through design and testing, especially since protection from malicious parties is a fundamental need<sup>1</sup>. Developers for critical

---

<sup>1</sup> Critical systems depend somewhat on the low likelihood of random conditions to cause error states, but

systems have found that reliable systems must address:

- Fault prevention during design and development,
- Fault detection during operations and
- Fault recovery during abnormal or error states.

Network security management applications concentrate on the latter two areas as they relate to networks. Like security kernels, security mechanisms must properly implement security, but the assurance role typically occurs in a separate application rather than internally. Security management tools are active assurance methods that function to monitor operational security services, allowing observation and reaction to key fault, configuration, and performance status. While security kernels and security mechanisms are like automobile drivers who are ultimately responsible for safe operations, security management is like the traffic cop who reinforces the rules and assists in trouble spots.

Security management has two roles—monitoring and control. The first involves data collection that provides insight for system stakeholders<sup>2</sup> on whether security operations achieve the security policies intended by the system design. Status presentation may be in the form of real-time graphical displays or periodic printed reports of data trends or exceptions. The frequency and granularity of data gathering are necessarily tradeoffs with the network traffic volume and processing load of monitoring components. The second role of security management is to provide a means to adjust the level of security monitoring and operational safeguards if the current level

---

computer hackers purposely search for the weak points that exist in any complex system.

<sup>2</sup> Stakeholders is a term meant to imply all responsible persons, beyond just the system operators and users. It may include data or business application owners or equivalent security accreditors in government organizations.

rent level does not match security policy or the desired level of risk.

Traditionally, security management has been viewed as a special case of network management. Security and management are interdependent by their nature, so each needs the services of the other. Thus, *management of security* and *security of management* are different facets of the same issue. Security of management is a prerequisite of many high reliability and secure applications, particularly management of security. This is the so-called security of management *before* management of security requirement. To date, much more work has been done to define security mechanisms than to extend management capabilities to security applications.

### **B. Network Security**

Network security management is by nature a distributed function. Applications that may utilize security management include firewalls, databases, Email, teleconferencing, electronic commerce, intrusion detection, and access control applications. Security management faces the same security threats as other distributed applications. Coordinated management of security is not feasible without a secure management infrastructure that protects in transit messages from modification, spoofing, and replay. Although end system security is beyond the scope of this discussion, it is clear that key management, access control, and reliable implementation of management software are critical also.

In its crudest form, security management could require human presence at every security device and manual evaluation of all significant events. On the other hand, we believe that remote monitoring with computer assisted correlation and management of system events is just as viable for security management as it is for network management. In fact, it may be argued that detection of sophisticated attacks need the help of computer-assisted correlation tools even more than network management systems.

Some network management systems use remote trend analysis and pattern recognition of management data to initiate automated or recommended operator responses. Similar possibilities for security are more a matter of market demand and investment than technology limitation. We also believe the lack of standard definitions for managed security objects have limited more widespread, interoperable implementations.

Even a small network with modest security needs will soon face significant administrative overhead to configure and monitor firewalls, authentication servers, secure Email servers, etc. Organizations are now coming to expect both privacy mechanisms and firewall protection, but competitive pressures are driving administrators to reduce labor costs of network and system management through automation and consolidation of management activities. The rapid deployment of security services in corporate and public networks reinforces the need for security management.

Like other distributed applications, security management modules must speak a common language. Two standards-based management protocols have addressed security management somewhat. SNMPv2 proposed many security enhancements over the existing SNMPv1, however the standards process collapsed under its own weight. SNMPv3 is emerging to combine the best aspects of SNMPv2 (RFC 1445-1452) with SNMPv2c (RFC1901-1907). Since SNMP is more pervasive than the ISO's Common Management Information Protocol (CMIP) standard, SNMPv3 is expected to be an important security management protocol. Some research efforts such as the SAMSON project have looked at integration aspects of the security management problem, but more sustained research needs to establish a real vision and plan so as to bring order and synergy to the topic. With that thought in

mind, we seek to offer some common security management rules, views and tools, and a roadmap for additional research needs.

### C. Security Management Research

The literature and available products related to management of security applications is quite sparse. Despite vendor hype, management tools for secure applications are limited in capabilities and generality. Although a few firewall vendors have used SNMP Traps to identify security alarms to a network management station, most security research has focused on techniques and data analysis. Intrusion detection, multicast conferencing, and web (HTTP) security have received some attention, but no security MIBs exist nor are integrated security management functions in wide use.

Most readers will be familiar with the basic concepts of common SNMP and the CMIP network management protocols as covered by authors such as Rose [8] and Stallings [11]. Distributed Management Environment (DME), an important alternative, began as a part of the Open Software Foundation's (OSF) broader Distributed Computing Environment (DCE) initiative. DME aimed to address management of large, heterogeneous networks by defining a common high-level interface for network devices and applications using a single API to access common functions of the SNMP and CMIP protocols (see **Figure 2**). As a first step, the OSF announced the Network Management Option (NMO) 1.0 specification in May

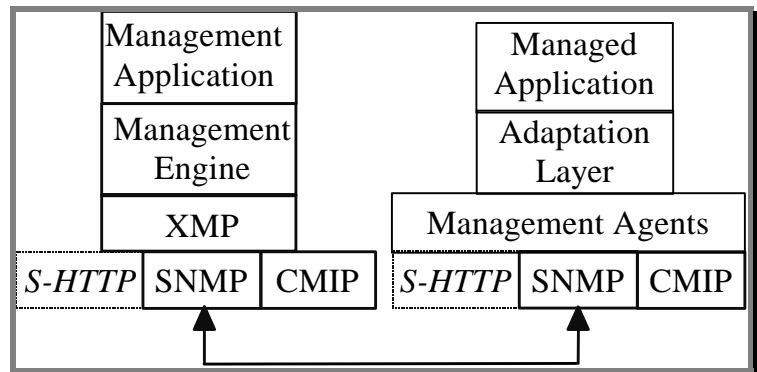


Figure 2. XMP Management Infrastructure

1994. The independent SAMSON project studied and developed a working prototype using XMP with SNMP and CMIP stacks. **Figure 2** also shows another management interface alternative using Secure HTTP (S-HTTP). Although use of S-HTTP is not proposed by existing working groups, the use of HTTP for GUI front-ends for non-secure management has been gaining momentum.

The Network Management Forum has also attempted to reconcile the SNMP and CMIP environments. Its OMNIPoint 1 document was a roadmap for compatible specifications. As part of this effort, the ISO/CCITT Internet Management Coexistence (IIMC) working group defined MIB translation rules and proxy definitions toward this end. Its review of management security issues is in [6].

Much of the security management work published to date relates to IDS applications. Early IDS work related to off-line analysis methods for detecting anomalies or attack patterns in audit data from standalone systems. As analysis techniques and distributed processing capabilities have improved, recent IDS work is becoming more real-time and cooperative, similar to other event-driven network management functions. Recently, Crosbie [3] proposed using “autonomous agents” for redundancy and simplicity. White, Fisch and Pooch are working on “cooperative, peer-based” IDS [12]. Both efforts are intent on the functionality of the IDS application, but intercommunication and management functions are clearly needed and identified. This suggests that the future of IDS may consist of independent, but communicating detection tools. Coordination and management of distributed IDS agents are distributed management functions specialized for IDS. If the IDS protocol and management capabilities were to be aligned with SNMP, then linkage to other management applications may be the next logical progression.

Multicast management issues have been an active research topic due to the growing interest in Internet conferencing. As business use of multicast becomes common, the demand for multicast privacy solutions will grow. Authentication, encryption key management and access control are big concerns as participation increases. Late joins and early departures from secure sessions complicate key management due to the need to dynamically refresh the keys of active participants. Gong [4] has raised many of these issues specific to group-oriented multicast security, but many are also general security management issues. Some issues from multicast security also relate to network management scenarios in which a central site needs to communicate with many distributed devices. Key management is usually handled outside the network management standards arena, but using secure management to monitor and control a key management application is very conceivable.

Control of access to network transmission resources has been a research concern because multicast can consume a large amount of bandwidth when broadcasting to a large population of receivers. Ballardie in [2] has identified problems of limiting access to multicast trees and suggested a method for controlling abuses by users who may inadvertently or maliciously consume major chunks of network resources. Later, we apply some similar concepts in our proposed Packet-Filter Information Protocol (PFIP) to monitor and control restrictive firewall filters.

A direct application of security management was discussed by Banning in [1]. Banning built a distributed audit system to collect data from heterogeneous systems using network management protocols. Although only a simple prototype, it demonstrated the steps to integrate other security applications using similar MIB definition, agent development, and value-added processing of collected data. Not every security management application

should have to apply this process. We believe a core set of attributes and procedures would greatly promote extension of management functions to other security applications and support synergy between those applications.

### III. Integrated Security Management

Deployment of effective security management requires three basic management components – applications, infrastructure, and agents. We focus on the issues of adapting the predominant management status and control mechanisms (management infrastructure and agents) to accommodate security management needs. Processing and display applications are beyond the scope of this discussion.

The basic management infrastructure must provide suitable mechanisms for the following factors to maintain secure management of applications:

- confidentiality and integrity
- data transport
- common data encoding
- liveness<sup>3</sup>

These capabilities may or may not be available from existing network management systems. The use of standard protocols such as SNMPv3 along with proven security mechanisms for authentication, access control, integrity and confidentiality ensures no weak security links<sup>4</sup>. In addition, the management platform itself needs protection through good system and physical security.

<sup>3</sup> Liveness, a term from security research, may also be called freshness to indicate that the value of the data is not merely in its quantity, but also in its quality (timeliness).

<sup>4</sup> In a chain, each link is important, while some other models represent security as being layered like an onion whereby one layer covers the weakness of another.

### A. Management of Security Applications

It is widely agreed that consolidation and integration of management functions is necessary to keep costs down and allow small network operations staffs to extend their scope of control. It is also clear that moves toward centralized management can lead to single points of failure and performance problems. A recent trend within the network management industry is the deployment of distributed management systems that can cooperatively share information and implement control functions. Many security applications may benefit from consolidated, cooperative management, especially those that are dynamic and widely duplicated across multiple sites.

Several security applications are potential candidates for integrated management using standard protocols. **Table 1** below shows our assessment of the relative suitability of some possible applications. We used three subjective factors to assess each application for integration with a security management system. *Proliferation* rates how widespread the application is, *research value* assesses the importance of the application technology, and *real-time management* indicates the usefulness of interactive management in the application domain. For example, due to the

Application	Proliferation	Research Value	Real-Time Management	Total
Security Firewalls*	H	H	H	9*
S- HTTP	L	H	H	7
Secure DNS	L	M	M	5
Secure Email	M	H	M	7
Kerberos	M	M	M	6
Intrusion Detection System*	M	H	H	8*
Secure Audit Trail	M	M	L	5
Secure Multicast	L	M	M	7
System Security	H	H	L	7

\* Candidate for Case Study

L = Low (1), M = Medium (2), H = High (3)

**Table 1. Security Applications**

rapid deployment and variety of vendor offerings, network security firewalls show great promise for management by standard protocols. Likewise, the substantial research interest in IDS applications makes it another good subject for study.

### B. MIB Security

Of the three core security principles (confidentiality, integrity and availability), integrity is the most critical to management operations. The authentication of users and the reliable delivery of the correct data are constant imperatives. While confidentiality of some data may be desired (such as transfer of new keys or passwords during login), it is not a constant driver. Availability of security management applications is also a lesser concern since many applications can continue to operate and maintain status information during gaps in communications.

It may seem that a security management system that manages a trusted application should go through the same rigorous testing and analysis as the primary security application. Rushby [10] indicates a security kernel must have access to and control over the vital security features of a system and must maintain secure attributes in spite of any possible sequence of operations. If the security management application enforces security, it and all related infrastructure would have to meet all security requirements of the core application (*e.g.*, *security kernel*). We conclude that the purpose of security management is not to enforce security, but to manage security *risk* by sensing and displaying status of important parameters. It is a means to gather status information and tune performance parameters to meet current data safety needs.

### C. Security MIB Template

A basic security MIB should include common attributes from all applications with security roles. A sound security model is crucial in extending the network management paradigm to encompass security. The major challenge is to define a common set of managed objects that are useful to security managers in detecting and reacting to security events. After the core set of MIB attributes has been defined, each security application may extend the security MIB to specify items that support unique features in their domain. Also important to effective, active management is definition of trap events. Traps generate real-time alerts for critical events at a node such as exceeding absolute or rate thresholds.

A good first step in defining a core security MIB is to apply the standard Fault, Configuration, Accounting, Performance and Security (FCAPS) network management factors in the security context. Although a single security MIB definition cannot cover every need, there are advantages in a common standard that all compliant systems must support and may extend as necessary. **Table 2** shows some core elements from the general system and packet-filter sections of our draft Firewall MIB.

▪ fwSysObjectID	▪ pfIn/Out_Flag	▪ pfStart_Time
▪ fwSysSecAdmin	▪ pfProtocol	▪ pfEnd_Time
▪ fwSysServices	▪ pfSourceAddress	▪ pfPollInterval
▪ fwSysForwarding	▪ pfSource_PortLB	▪ pfDroppedSinceLastPoll
▪ fwSysNonIPAction	▪ pfSource_PortUB	▪ pfTop10SrCsSinceLastPoll
▪ pfTabUpdate	▪ pfDestAddress	
▪ pfTable	▪ pfDest_PortLB	
▪ pfEntry	▪ pfDest_PortUB	

**Table 2. Potential Firewall MIB Attributes**

Although the MIB variables in **Table 2** require detailed explanations to apply them precisely, it should be evident that a MIB could implement the packet-filter access rule table of a firewall. Management operations (SET/GET) on the packet-filter table entries, for example, would enable configuration of a



specific filter rule. Rules for an application level "proxy server" firewall are also being developed as a separate MIB section. To build a complete security MIB, additional MIB modules can be defined for other security mechanisms such as security audit trails, security guards, authentication servers, and IDS. In addition, trap events should be defined for real-time alerts for key events.

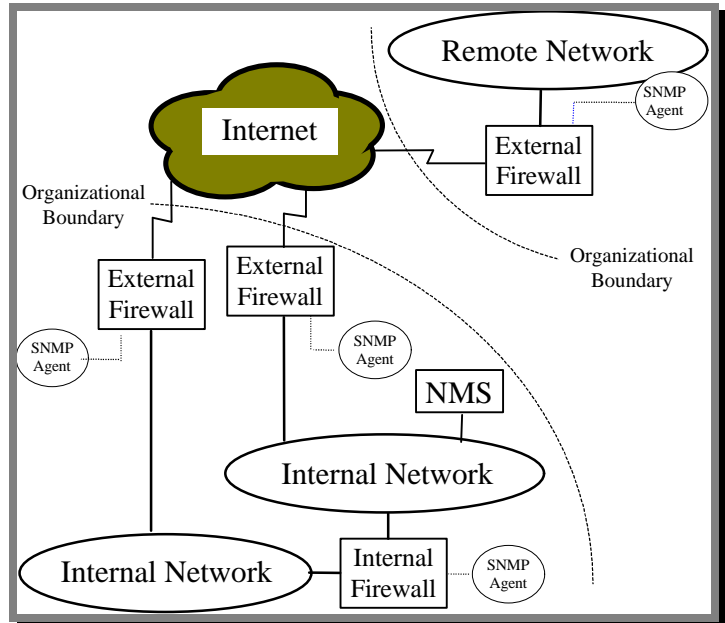
Ongoing research is testing the viability and utility of preliminary MIB definitions. Usefulness for both configuration operations and status gathering is important. Validation will consist partly of assessing whether a particular configuration is effective in detecting one or more attacks described CERT advisories. Development systems include a simple packet-filtering firewall using the Texas A&M University's Drawbridge package on a PC platform. Instrumentation of the security application with an SNMP agent will allow implementation and enhancement of the security MIB. The testing against known scenarios will give implementation and experimental experience. Our implementations of consolidated security management will also involve other widely available security tools, such as `tcp_wrappers` and the TIS firewall toolkit.

#### D. Management Application Scenario

When several similar manageable devices or applications are in a common management domain<sup>5</sup>, a common management application may be considered. Below we present an example application with one Network Management Station (NMS) to manage a group of network security firewalls.

ACME Enterprises has several externally connected LANs that require new firewalls and some that need firewalls between de-

partments. ACME has remote offices that connect via the Internet as in **Figure 3**. Although most firewalls would be managed from an NMS inside the firewall, external management of firewalls is necessary for organizations that want central administration. This can be problematic, since SNMP uses the UDP service and management capabilities would be hindered if UDP access through the firewall is restricted.



**Figure 3. Management of Internal vs. External Firewalls**

ACME managers want to use an existing network management platform to monitor the new firewalls. To do so, an upgrade from SNMPv1 to SNMPv3 will support data integrity and confidentiality. Typically, the events of interest for a firewall will be the number of incoming packets that are dropped due to packet-filter restrictions. If a large number of drops occur in rapid sequence, a significant security event *may* be occurring. Alternatively, if a high percentage of packets in an interval (say 50% in a 30-second interval) are rejected, there may be cause for concern. Both of these events could trigger a trap event to the NMS to alert an operator for further assessment.

The NMS may raise or lower the security monitoring posture based on the recent pat-

<sup>5</sup> A single management domain exists when management entities can be accessed from a single location and they are the administrative responsibility of one organization.

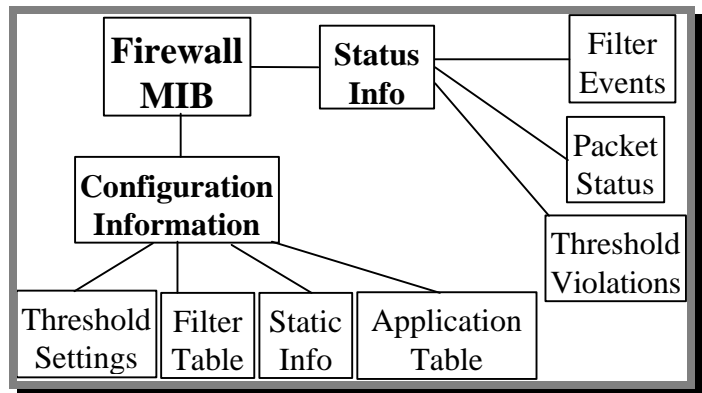
tern of alerts, external information, or system security policy. If a reoccurring security alert is being generated from the same source, the manager may want to set the filtering action as “log packet” or “log header” for later review rather than just dropping it. Such a management response may provide needed evidence to trace intruders. Care is needed to keep flooding attacks from overflowing storage areas, however. Recording packet drops requires the NMS operator to SET the packet-filtering rule that is associated with the alert. This may be done by doing a GET and searching through the packet-filter table for the rule, or the original alert may indicate the associated rule in the trap message. To change the configuration of the packet-filtering table, the “action” column must allow read/write access.

Another approach to assess the configuration and efficiency of a packet-filtering firewall is through summary variables such as the TopTenRuleHits, TopTenSrcIPAddr and TopTenDroppedPktSrcIPAddr similar to the Remote Monitoring (RMON) MIB (RFC1757/ 2021). In this way, the most important rules and problems can be closely assessed and the effect of changes can be seen. Specific rules may be changed and turned on or off as conditions dictate. Possibly, better performance can be attained if rules that are fired most are rearranged in the filtering table.

Packet-filter tables and application proxies only allow approved traffic to pass through. Changes to the firewall configuration may result from reaction to status information or from external needs. New applications may be opened for use on a proxy server, or a security trigger could shut-down dangerous applications or locations. Thus, application and packet-filtering tables may function like a router that permits traffic to flow onward toward its destination.

**Figure 4** shows high-level firewall MIB definition groups that might be accessed from

a standard NMS platform. The procedures to make an update are as follows. If a firewall is operational and a new proxy application is to be added, the management station would update the application table by initiating a SET operation on the appropriate row values. Certain columns such as source and destination addresses would be mandatory parts of the table information. If a need for application access is temporary (i.e. user needs access while on travel), the management application could set a timed trigger to remove the access automatically.



**Figure 4. Firewall MIB**

**E. Packet-Filter Information Protocol (PFIP)**

While defining the packet-filter MIB, we noted some similarities with the MIB-2 implementation of an IP routing table. We questioned whether packet-filter information could be propagated amongst routers and compatible hosts in the same manner that routing tables are updated by the Routing Information Protocol. Instead of *establishing* routes, a packet-filter *blocks* known and potential routes to and from particular destinations. The PFIP described below is the result. Further investigation to assess extensions for sharing application gateway, audit event, and IDS "tip-off" information is ongoing.

The PFIP is intended to allow propagation of packet-filter information among hosts and routers in an IP-based network. Whereas routing protocols deal with information about available paths between networks and hosts,

the PFIP is a restrictive mechanism to conveniently limit the flow of data packets from sources that are considered bothersome or untrustworthy. The PFIP can only propagate *deny* rules between known entities. If a means of strong trust is established between entities through authentication, encryption, digital signatures, etc., then full packet-filter table administration may occur. PFIP works in concert with existing routing protocols to control network access as close as possible to traffic sources.

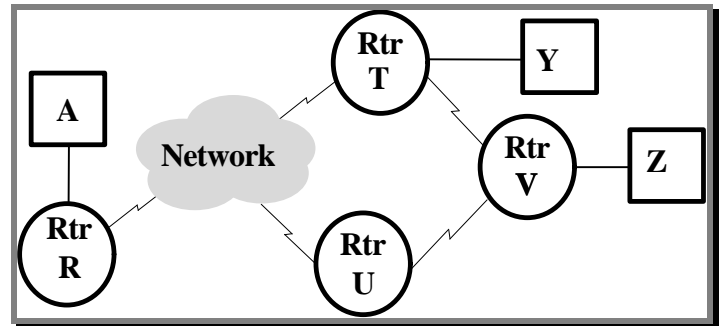
PFIP is a means to distribute the responsibility for screening out data that is undesirable to the recipient. Its intent is to drop unwanted packets as close as possible to their source, rather than leaving the responsibility strictly with the recipient. The obvious benefit is a reduction in wasted network bandwidth since packets are discarded nearer the source rather than at the destination. The capability also offers potential as a means to implement service blocking for households or businesses that want to ensure undesirable data is blocked from certain sites and/or during certain hours.

Each packet-filtering host is assumed to have a packet-filter table. This table has an entry for every filtering rule that has been defined for its interfaces. Rules may be defined locally by the network administrator or may be the result of requests from remote sites whose own rules call for limitations on traffic from the local hosts. Each packet-filter table entry will be defined according to the Firewall MIB.

Lack of trust between organizations creates a major obstacle to implementation, since source squelching requires that the source implement externally defined filters. Without some form of trust mechanism, the threat of denial of service by a third party is significant. If the required trust level is not satisfied for packet-filter updates or a node does not support PFIP, routing information is

used to attempt a filter update at another node next closest to the source.

**Figure 5** will illustrate the preceding concepts. It shows one instance of how the PFIP may work to update packet-filter tables in a mixed network of compliant and non-compliant hosts.



**Figure 5. PFIP Update Scenario**

**Step 1:** Host A creates new packet-filter rule that denies traffic from Host Z.

**Step 2:** Host A, after a configurable number of hits on the new rule, sends a PFIP packet to Z requesting suppression of traffic.

**Step 3:** Host Z accepts or rejects the PFIP update according to its authentication and/or validation requirements. Either acceptance or rejection causes a reply from Z to A so that future updates are not attempted.

**Step 4:** An acceptance message from Z causes A to mark the PF rule as remotely activated. If Host A receives a rejection message, it immediately sends a PFIP update message to node V, the node next closest to the source.

**Step 5:** If no response is received after a PF update attempt, a timer at Host A expires and A assumes that either the update or response was lost. If three consecutive update attempts fail, the distant node is assumed incapable of PFIP updates. In that case, Host A acts as if a reject message arrived and tries further updates with the next closest node(s).

**Step 6:** Steps 2-5 are repeated until an acceptance message confirms the new update, or there are no more nodes to try.

## IV. Conclusions

The expansion of the Internet and the number of sensitive applications that require strong security foreshadow a growth in demand for security management capabilities. As electronic commerce, secure messaging and firewall applications proliferate, management applications will be needed to limit administrative burdens while also allowing greater flexibility and control of security operations.

Before an effective security management capability can be developed and demonstrated, there are a few prerequisites. First, a secure management infrastructure must be in place. SNMPv3 is poised as the secure successor to SNMPv1. Next, a security MIB must be defined to allow SET/GET operations on essential values for the security application to be managed. This is a contentious and difficult step because of the need to map terms and status parameters from many different vendor applications and features to a small set of commonly defined values. In this paper, we have suggested a core security MIB with some general parameters applicable to all security applications. The core MIB can be extended to define configuration and status parameters for security applications and vendor features in the same manner as other MIBs.

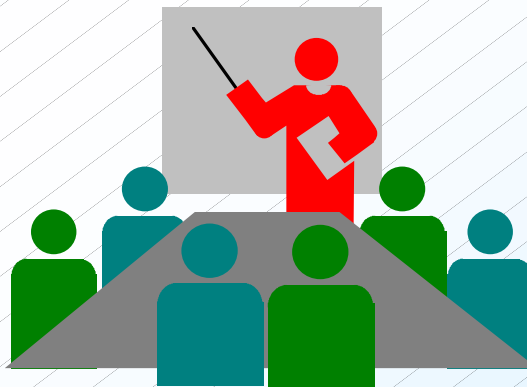
The foundational work of defining a common core of security management infrastructure, attributes and MIB definitions will allow progression to the next phase of capability development, that is, better correlation of management events with security problems. The modification of agent modules and security management applications to effectively access a common set of security values will open new management features. Then, innovative use of security management views and synergy with other management and security information across the network can unleash new power for security management.

## References

- [1] Debra Lynn Banning, "A Distributed Audit System Using Network Management Protocols", Master's Thesis, California State University, Long Beach, 1992.
- [2] Anthony J. Ballardie, "A New Approach to Multicast Communication in a Datagram Internet", Ph.D. Dissertation, University of London, May 1995.
- [3] Mark Crosbie, "Active Defense of a Computer System Using Autonomous Agents", Purdue Univ., <http://www.purdue.cs.edu/homes/spaf/tech-reps/9508.ps>.
- [4] Li Gong and Mencham Shocham, "Elements of Trusted Multicasting", In *Proceedings 1994 International Conference on Network Protocols*, p. 23-30, IEEE Computer Society, Los Alamitos, CA, 1994.
- [5] ISO/IEC 7498-4, ISO Open Systems Interconnection, Basic Ref. Model, Pt. 4: Management Framework, 1989.
- [6] Lee LaBarre, ISO/CCITT to Internet Management Coexistence (IIMC): ISO/CCITT to Internet Management Security (IIMCSEC), Internet draft, MITRE, Feb 1994.
- [7] S. Lechner, "SAMSON: Management of Security in Open Systems", *Computer Communications*, Sep 1994.
- [8] Marshall T. Rose, *The Simple Book: An Introduction to Management of TCP/IP-based Internets*, Prentice Hall Series in Innovative Technology, Prentice-Hall, Englewood Cliffs, New Jersey, 1991.
- [9] John Rushby, "Critical System Properties: Survey and Taxonomy", *Reliability Engineering and System Safety*, 43(2): 189-219, 1994.
- [10] John Rushby, "Kernels for Safety?", *Safe and Secure Computing Systems*, pp. 210-220, Blackwell Scientific Publications, 1989.
- [11] William Stallings, *SNMP, SNMPv2 and CMIP: the Practical Guide to Network Management Standards*, Addison-Wesley, 1993.
- [12] Gregory B. White, Eric A. Fisch and Udo W. Pooch, "Cooperating Security Managers: A Peer-Based Intrusion Detection System", *IEEE Network*, pp. 20-23, January/February 1996.
- [13] WILMA: [ftp://ftp.ldv.e-technik.tu-muenchen.de/dist/WILMA/WHAT\\_IS\\_WILMA.html](ftp://ftp.ldv.e-technik.tu-muenchen.de/dist/WILMA/WHAT_IS_WILMA.html)

# *Management of Network Security Applications*

**Authors: Philip C. Hyland, TASC, Inc.  
Dr. Ravi Sandhu, GMU**



# Outline

- **Introduction**
- **Background**
  - *Terminology*
  - *Network Security*
  - *SM Research*
- **Integrated Security Management**
  - *Management of Security Applications*
  - *Security MIB*
  - *Firewall MIB Template*
  - *Packet Filter Information Protocol (PFIP)*
- **Conclusions**

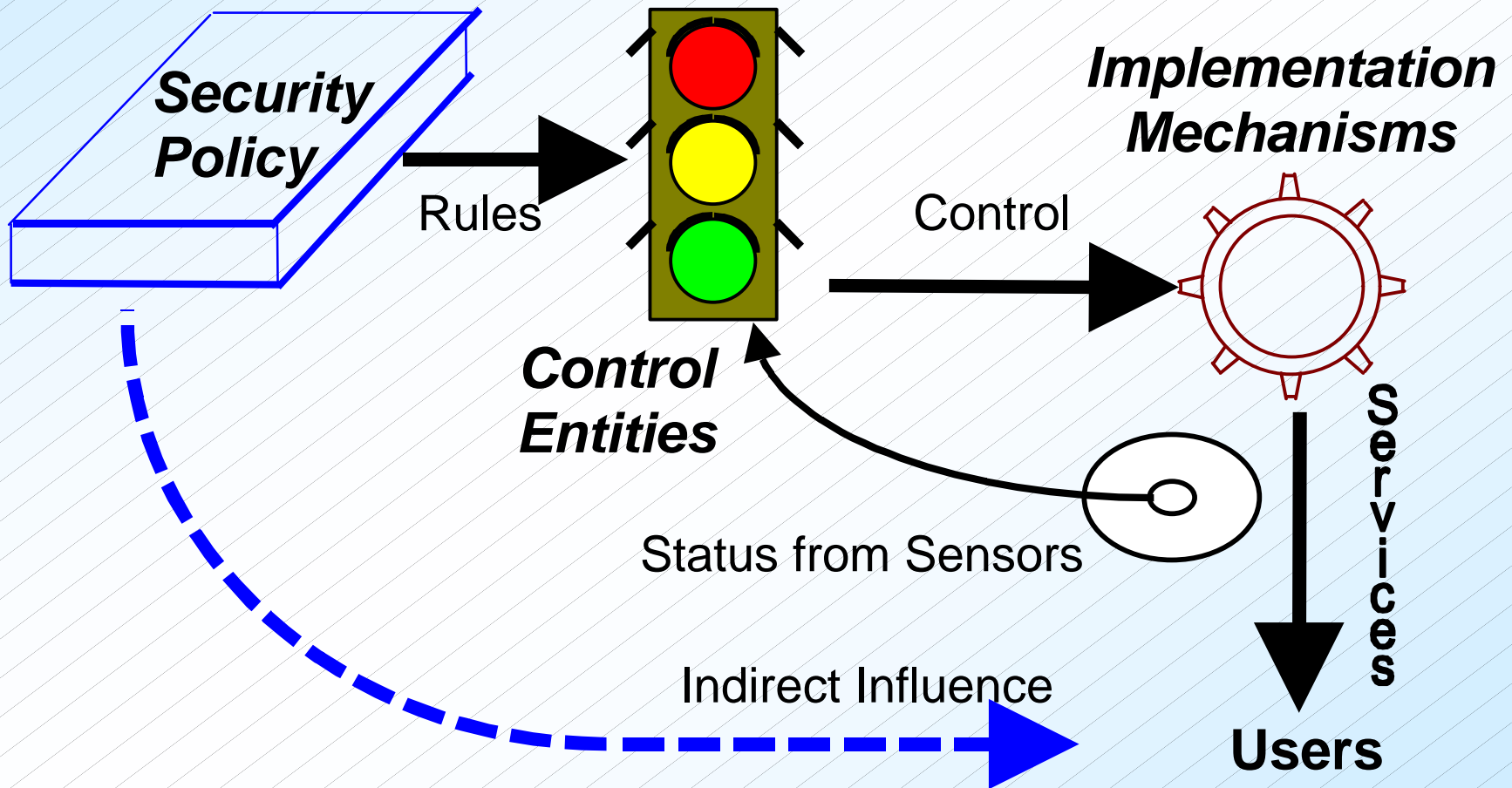
# *Introduction*

- **General Security Management Components**
  - *Security Policy*
  - *Security Mechanisms*
  - *Security Assurance*

**Goal:** Trust that “state of security” matches current policy

**Problem:** Secure Management infrastructure needs improvement to handle complexity, variety and quantity of new security applications

# Security Components





# Background

- OSI Management Framework has several SM-oriented standards, IETF has none
- At least two European projects have developed SM tools
  - SAMSON (CMIP/SNMPv2)
  - WILMA (SNMP)

Problem: *Few, if any, public SM research efforts ongoing*

Lesson from Network Management experience:

*Standards generally benefit all players, even if relatively simple*

# ***TERMINOLOGY***

- **Security Management**
  - Real-time monitoring and control of active security applications implementing one or more security services
- **Assurance**
  - *Prevention*
  - *Detection*
  - *Recovery*
- **Security of Management versus Management of Security**


# ***Network Security***

- **Benefits from a layered approach**
- **Requires a secure infrastructure**
- **System view permits coordinated management**
- **Efficient administration is key factor**
- **Emergence of SNMPv3 is important**

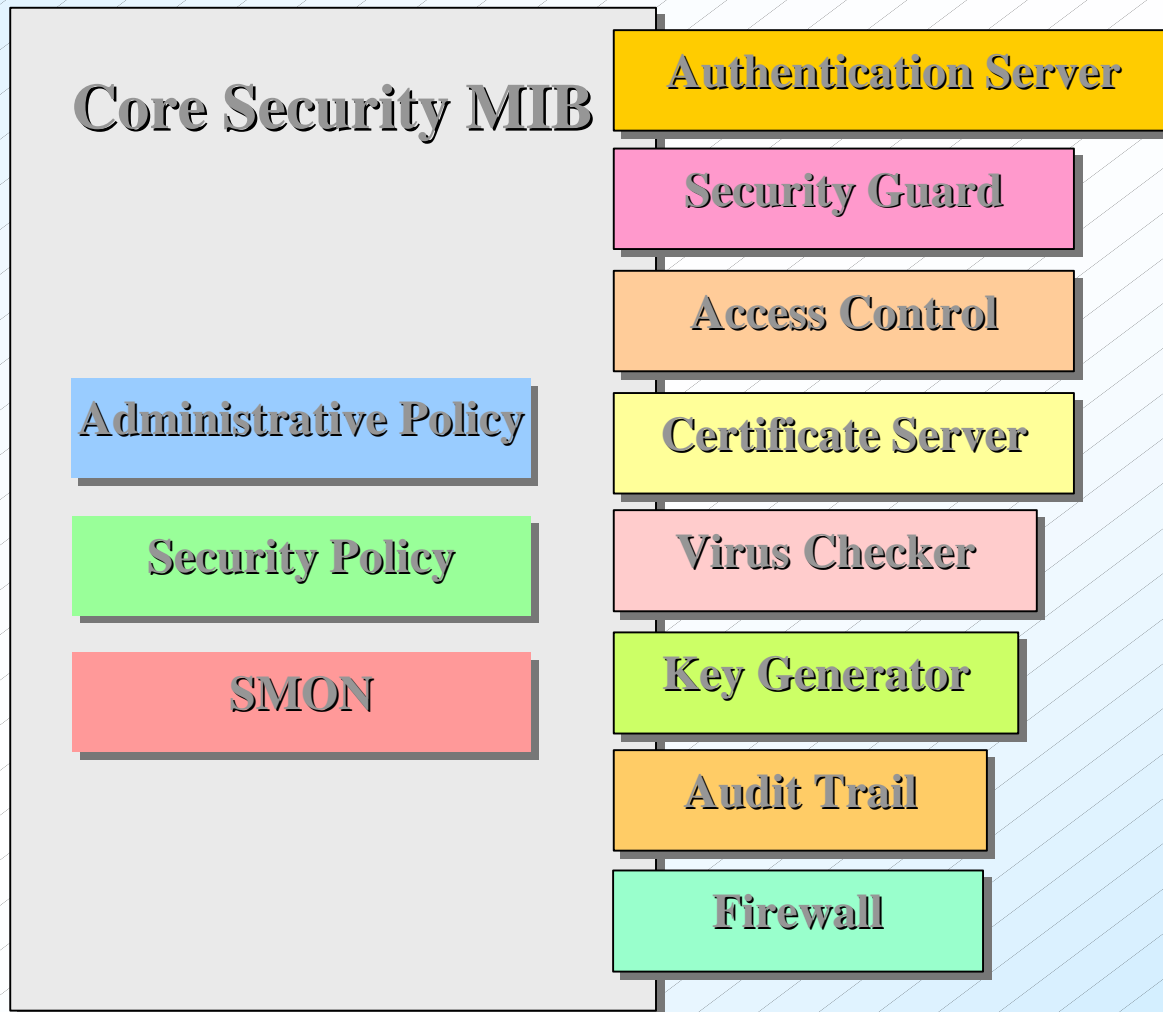
## ***SM Research: Example Component Efforts***

- **DCE Security**
- **Intrusion Detection Systems**
- **Key Management for Multicast**
- **Distributed Audit System**
- **SNMPv2/v3, etc.**

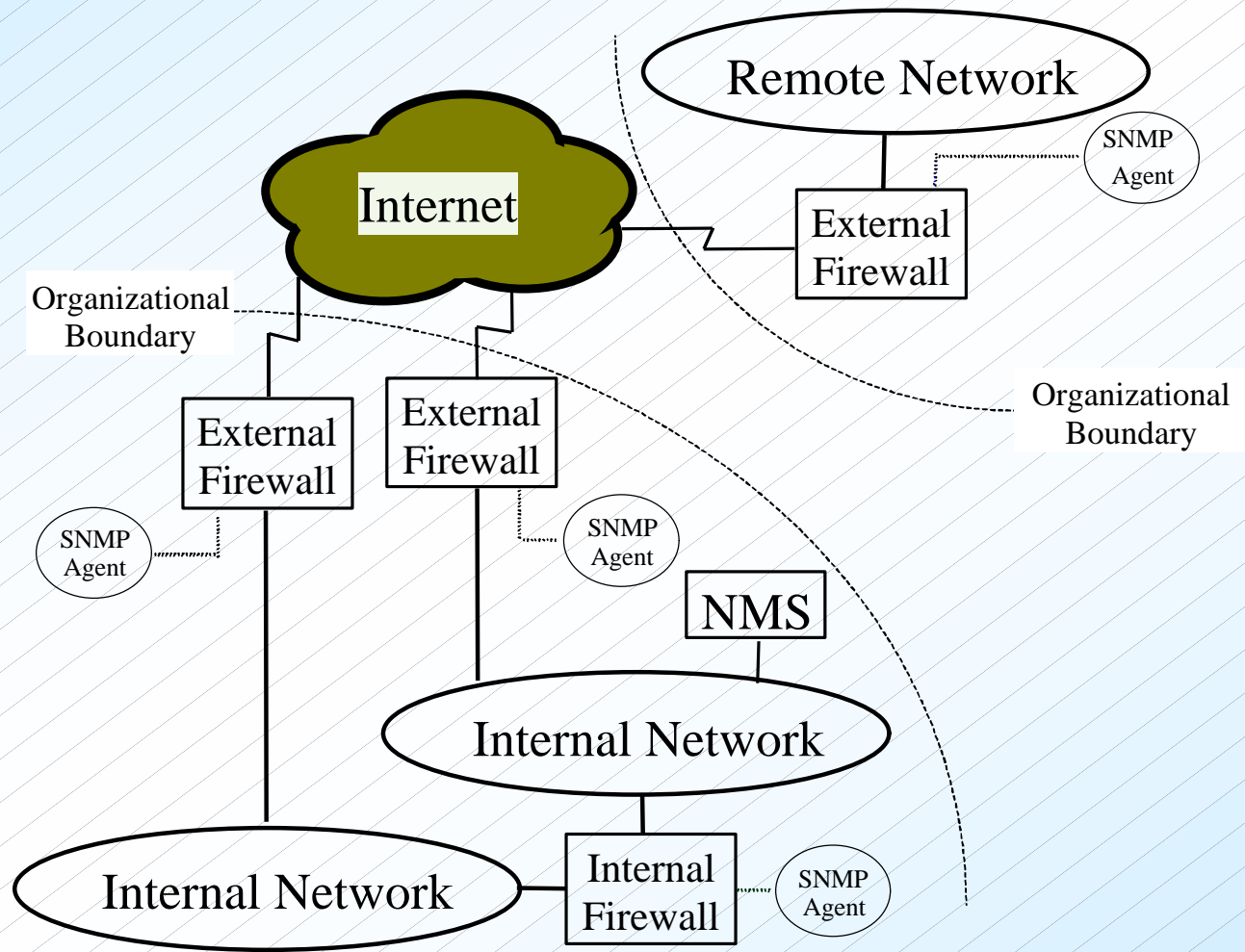
# ***Integrated SM Framework***

- **Confidentiality**
- **Data Integrity**
- **Liveness**
- **Encoding** 
- **Core Security MIB**
- **Security Application MIBs**

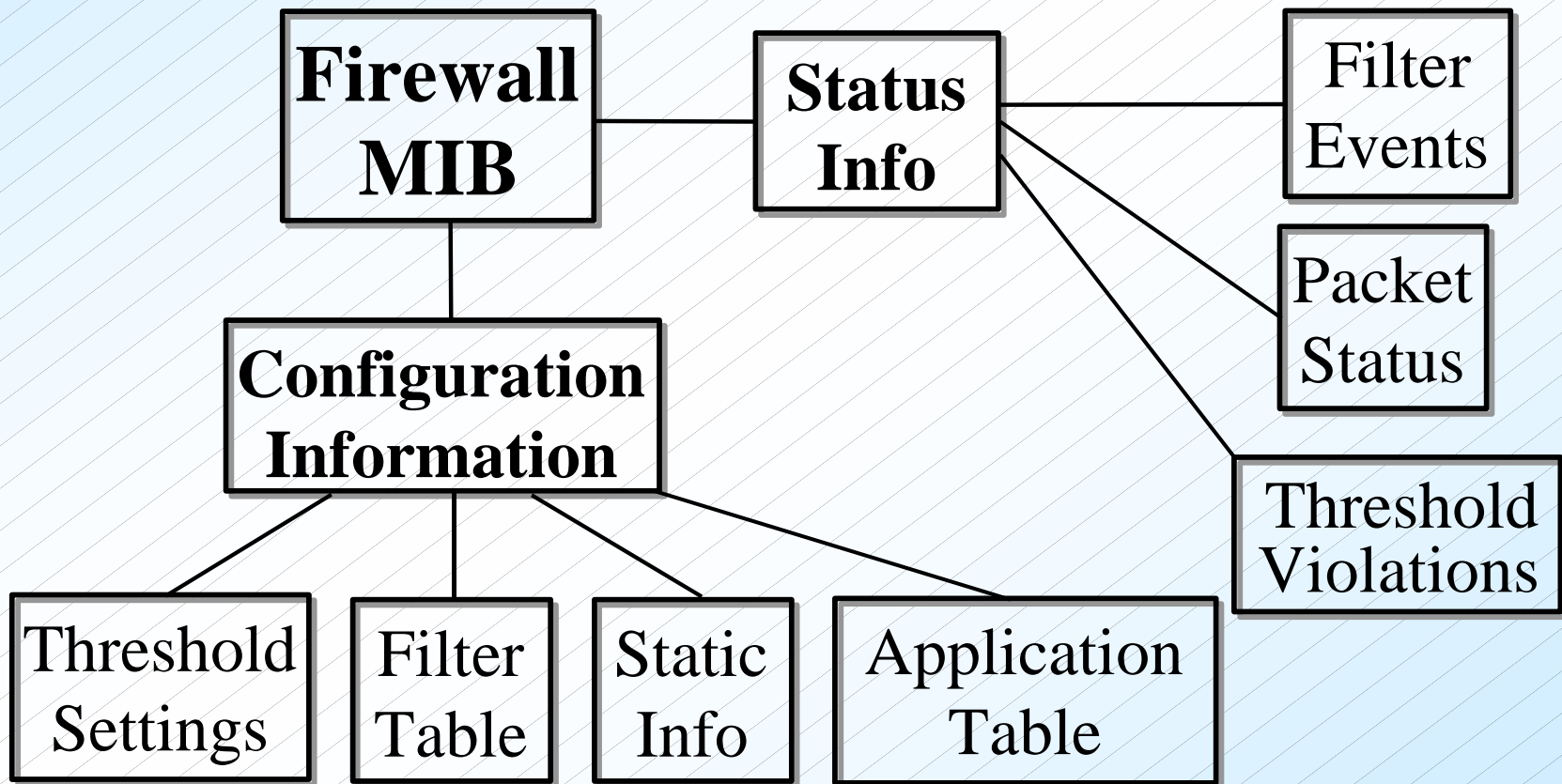
# *Extensible Concepts - Core Security MIB with Plug-ins*



# Example Objective: Firewall Management

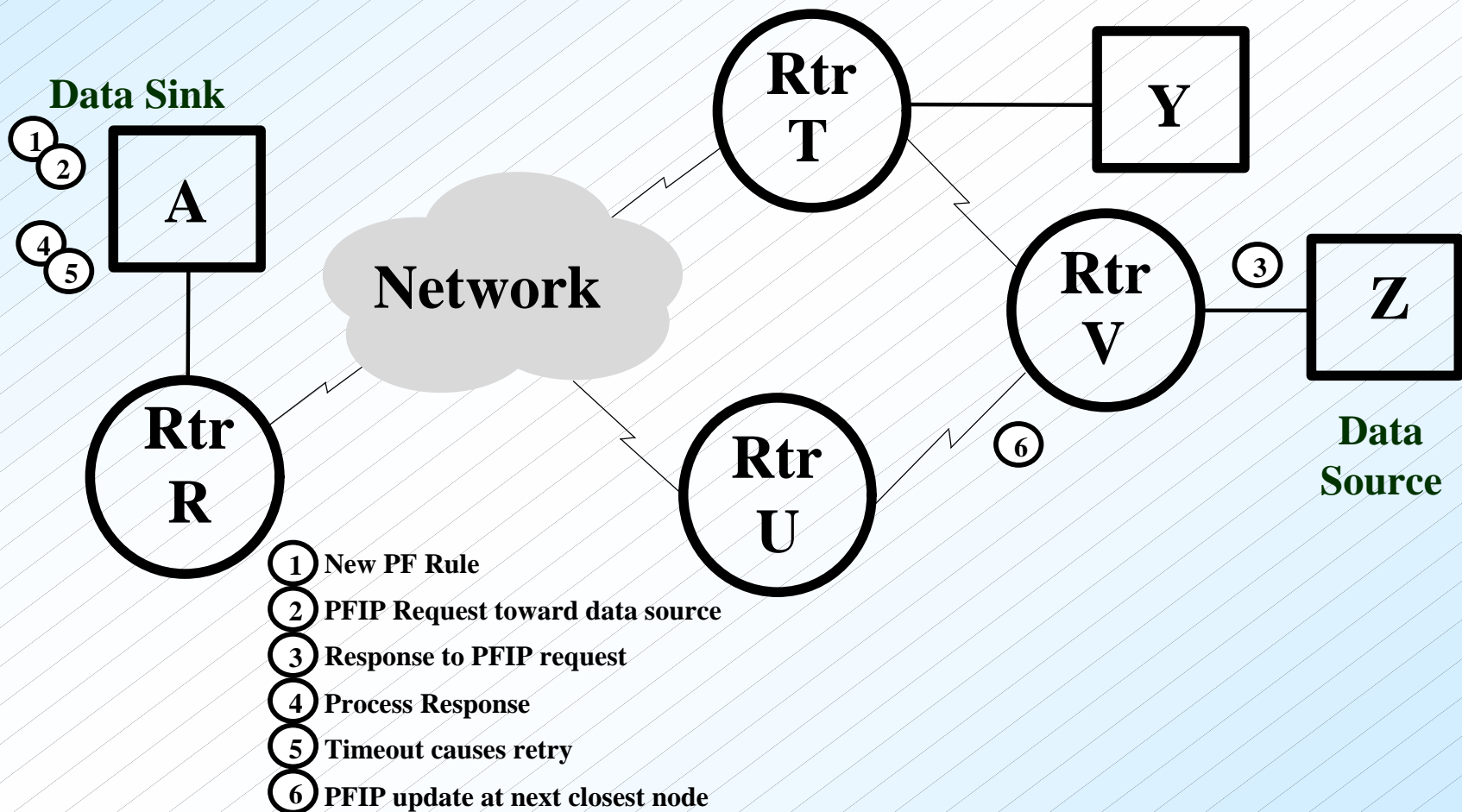


# *Firewall MIB*





# PFIP Update Scenario



# Conclusions

- **Need for security management solutions is growing**
  - *More complexity and variety*
  - *Tighter budgets*
  - *More pervasive applications*
- **Secure management infrastructure is evolving, but need is for more emphasis on common security management objects**
- **Time to develop consensus on core Security MIB is now**
  - *Promotes interoperability*
  - *Large potential for synergies from “big picture”*
  - *Common foundation while permitting extensions*