Enhancing Regulatory Compliance with IPScan

Establishing Internal Ethernet/IP Network Access Controls

ViAScope USA

Executive Summary

Organizations of all sizes and across industries are now affected by regulatory requirements to protect sensitive financial, customer, and patient information. While SOX, HIPAA and Gramm-Leach Bliley regulations differ in their focus, they all carry similarly stiff financial and even criminal penalties for non-compliant organizations. As a result, IT departments must implement much tighter control technologies and processes, and be able to document not only their deployment and operation but also their effectiveness in preventing data privacy breaches. IPScan offers a significant enhancement to regulatory compliance efforts as the leading solution for real-time, policy-based monitoring, enforcement and auditing of Ethernet/IP network access policies across the enterprise network.

The Internal Security Threat and Regulatory Compliance

One of the major holes in many organizations' network security systems is the lack of internally-oriented controls. The bulk of security tools are oriented towards external threats from Internet-based hackers, viruses, and worms. While these are certainly necessary, the fact is that internal threats remain a huge and under-managed source of security threats to private data. In fact, according to the 2004 CSI/FBI Survey on Computer Crime and Security, 68% of responding organizations reported that they had suffered at least one, if not more, insider security breaches. Furthermore, the same 2004 survey reported that the average cost of insider network abuse was over $10 million per incident, as seen in Figure 1.

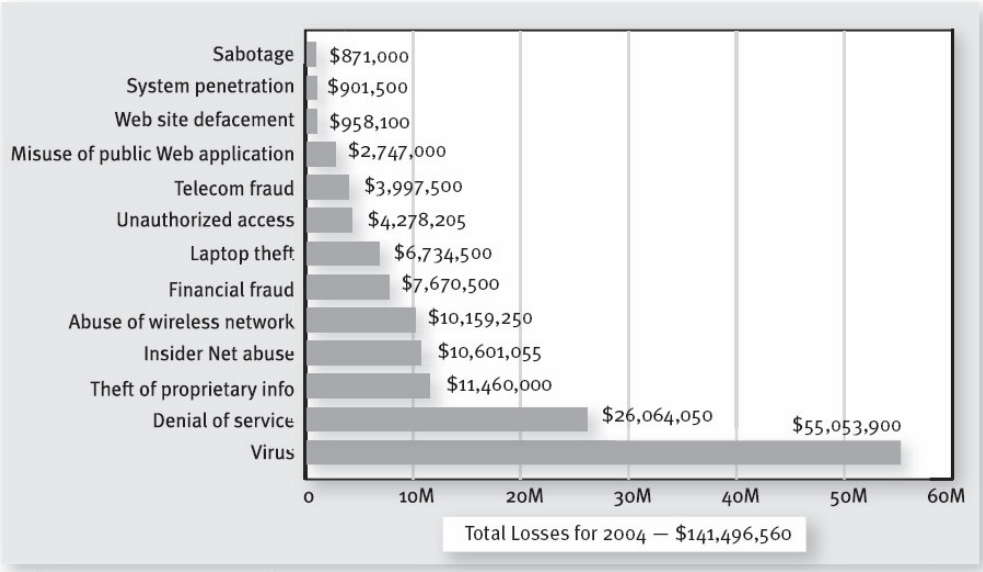

Figure 1: Average cost of security breaches from surveyed organizations, by category

Just as the openness of the Internet has created an opportunistic environment for malicious users to attempt to break into private networks and steal or alter their sensitive data or initiate denial of service attacks, the openness of internal Ethernet and IP networks has created a hospitable environment for insider security breaches. Organizations that bristle with external network protection to deny unauthorized access, allow trivially easy access to their entire enterprise-wide internal networks at any available Ethernet jack. The implications for security and regulatory compliance risks are obvious—trivial access to the network by unauthorized devices constitutes a significant threat to the integrity of the organization's data and business operations.

The Internal Network Access Control Landscape

Beyond physical connectivity, IP network access requires the combination of an Ethernet and a unique IP address to enable communication. Most organizations utilize a combination of dynamically (DHCP) and statically (manually) assigned IP addresses for their networked devices, typically in an 80/20 ratio. Once connected, users must log-on to various servers to access applications such as email. However, without adequate and comprehensive authorization mechanisms over device access to the Ethernet and IP layer of the network, a security gap is opened that allows employees, contractors and even visitors to easily connect unauthorized devices to the network that create significant data privacy and security risks. Even without malicious intent, unauthorized servers can be placed on the network without It's knowledge that haven't received proper security patches or software applications or that have open ports and applications that are vulnerable to attack, or that might circumvent other security measures such as standard VPN access methods. Employees can connect personal laptops or network drives and download corporate data without authorization, then end up storing sensitive data on poorly protected home networks and unsecured computers.

Unfortunately, the vast majority of IT organizations have no effective and timely control over Ethernet and IP addresses and network access. The current landscape of network access and address controls is a hodge-podge of elements that are either impractical or can't provide a comprehensive system of controls over basic internal network access.
Table 1 analyzes four common methods for tracking or controlling Ethernet/IP network access in use today:

Access Control Method	Description	Pros and Cons
Address allocation tracking systems	Ranging from simple Excel spreadsheets to home-grown databases, these tools are used by administrators to keep documentation on what IP address has been assigned to which user	Pro: Better than nothing Con: Depends on human effort to notice and document changes in the network—usually days or weeks behind the real state of the network. No enforcement and therefore no control. Difficult to keep current, even as a documentation method. 80% of organizations operate at least a portion of their network in this fashion.
Ethernet Switch Port-Address Locking	Administrator must manually assign a valid Ethernet address to a particular physical Ethernet switch port	Pro: If administered consistently, provides high degree of integrity Con: Impractically difficult and time-consuming to administrate, thus not widely utilized. Doesn't cover IP addresses
DHCP Address Management Solutions	Administrators can specify IP addresses to assign to particular Ethernet addresses, deny other address requests.	Pro: Eases monitoring and administration of DHCP address assignment. Con: doesn't provide enforcement on any statically assigned IP address. Only 20% of all organizations have a third-party DHCP address mgmt solution.
Wireless Encryption	Prevents 802.11 Wi-Fi access without appropriate crypto key	Pro: Prevents war-driving Con: Wi-Fi encryption keys are equivalent to physically securing access to an Ethernet port. No further controls over address allocation or addressing is provided

Table 1: The Ethernet/IP Network Access Control Landscape

The current weak state of fundamental Ethernet/IP network access and address control is of growing concern to many IT managers for a variety of reasons. Not only does it pose a security and regulatory

compliance risk, but poorly administered IP address resources can also cause network disruptions. According to Forrester, 15% of all application downtime is caused by network issues, and a majority of the root causes of network-based downtime are due to IP addressing problems. IP address conflicts that bring down connectivity to key servers, or worse, to key routers can cause costly network downtime. This level of risk is unacceptable since organizations are relying on IP networks to carry sensitive converged Voice and Video communications traffic, in addition to ever more demanding data applications.

IPScan—Comprehensive, Network-Wide Access Control

IPScan is the industry's leading solution for comprehensive Ethernet/IP network access and address control, deployed by hundreds of enterprises, government and military agencies, service providers, and educational institutions today to centrally administer and enforce policy-based controls over network access and address resources. IPScan monitors the entire network in real-time, learning all Ethernet and IP addressed devices attempting to communicate on the network, and enforcing centrally defined policies for network access and address allocation for Ethernet and both dynamic and static IP addresses. IPScan empowers IT with control over Ethernet/IP access in a transparent, user-friendly manner that requires no client software, eliminates inefficient manual address inventorying and tracking, and provides a continuous audit trail of all device activity. IPScan's high degree of automation, enforcement and audit trail capabilities make it an indispensable component of regulatory compliance systems.

How IPScan Works

IPScan is a system of distributed probes and centralized server software that controls network device access by authorizing the combination of the device's IP address, Ethernet MAC address and optionally its host name. This flexible approach provides IPScan with visibility and control over all devices, whether dynamically or statically addressed.

Low-cost IPScan probe appliances are deployed in conjunction with Ethernet switches throughout the network to provide total visibility of all Ethernet/IP devices that attach to the network, as seen in Figure 2. Probes monitor all network devices and send continuous updates as well as alerts to the IPScan server, which stores a real-time monitoring view as well as an auditable history in a database. Probes also automatically enforce centrally defined authorization policies and real-time commands sent down from the Server. The IPScan Server and database are centrally deployed and are managed via an administrative console. Network administrators can define users, user groups and policies, monitor all devices that have historically attempted connections to the network, and their real-time status, and view alerts sent from the probes. Since the probes automatically detect and update the central database with all network devices, manual entry of addresses is greatly reduced. Administrators can also shut down network access to any device in real-time from the console.

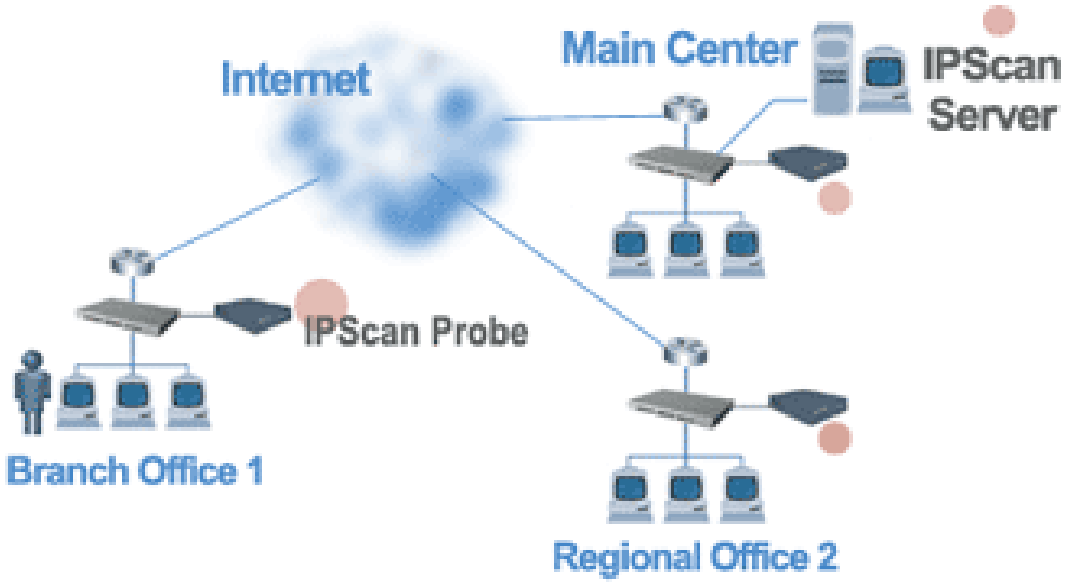

Figure 2: IPScan Deployment Architecture

Access can be granted to guests and contractors for limited amounts of time (hours/days/weeks/months). Access can also be limited to certain parts of the network or can be limited to business hours. In addition, the IPScan solution offers sophisticated reporting for audit trails and intelligent management. IT managers can view the entire network on one screen, including every remote office, thus creating accountability within each remote branch.

Benefits of IPScan

Comprehensive and Easily Integrated Access Control

IPScan enables organizations to have centralized control over the internal network edge. IPScan provides comprehensive visibility, and automates policy enforcement. IPScan fits seamlessly into any networked environment—since it is transparent to users, and does not disrupt existing equipment, nor does it require other network management systems to be reconfigured.

Enhanced Security

IPScan provides greatly enhanced network security risk mitigation

- 99.99% secure network access control.
- No device can access your internal network without policy-based IT department clearance
- Continuously maintains and archives network access and security logs in real-time

Streamlined Operations

IPScan greatly reduces the overhead needed to properly administrate and control all network addresses, while dramatically increasing the speed, confidence and responsiveness of IT managers in meeting customer and business requirements.

- Real-time, network-wide visibility of all networked devices
- Seamless integration of monitored addresses into policy configuration database, reducing manual tasks
- Comprehensive user, and departmental policy creation capabilities
- Automatic policy enforcement

Reduced Downtime

IPScan prevents downtime caused by IP address conflicts

- Estimated 18% reduction in overall network downtime for compelling ROI
- Protects critical servers and network infrastructure devices from IP conflicts.
- Centralized, network-wide visibility for enhanced monitoring and troubleshooting and reduced MTTR

Enhanced Regulatory Compliance

The IP blocking and the reporting/IT audit trail functionality within IPScan help companies to comply with industry regulations and internal policies

- Sarbanes-Oxley Act of 2002– Section 404
- Health Insurance Portability and Accountability Act of 1996 (HIPPA)
- Gramm-Leach Bliley Act
- ISO-17799
- Internal Policies

Conclusion

IPScan is the only solution available that enforces complete IT control over all Ethernet and IP activity throughout an entire network from a centralized location, automatically. It is also the only solution that offers automatic, real-time detection of every IP device on the network, recorded and archived in a policy server database, with included reports. IPScan provides a critical component in ensuring ongoing security, availability and regulatory compliance of IP networks. To learn more about IPScan, please visit our website at http://www.viascope.com or send email to: sales@viascopeus.com