WHITE PAPER

Best Practices for Securing the LAN

CONSENTRY™ NETWORKS

The need to protect the business – its assets and operations – is nothing new; what is new is the need to do so from within. The LAN has emerged as a new focus area for security, and its openness is its Achilles' heel. Internal threats, such as the use of wireless, the need to support guests and contractors, and the constant migration of laptops between "trusted" and "untrusted" Internet connections, now match if not exceed the danger posed by external threats.

Yet connectivity and high performance remain essential to the operation of the LAN, which makes securing it a complex challenge. To meet this challenge, IT needs a new set of LAN security best practices that complement existing approaches. What follows are ten best practices that bring the LAN infrastructure under the overall security umbrella, strengthening protection of critical enterprise assets.

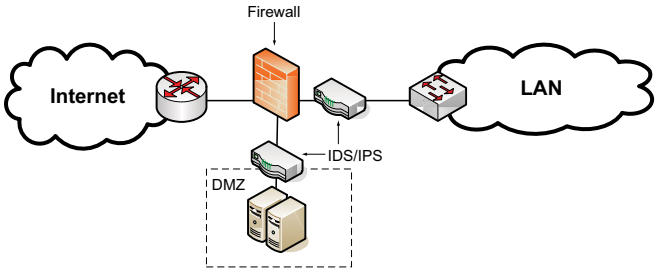
1 – Practice Defense in Depth

Defense In Depth

Area of Protection	Security Technology or Technique
Perimeter	firewalls, VPNs, and intrusion prevention systems
Data Center/Apps	application firewalls, encryption, patch management, and physical security
LAN	NAC plus post-admission controls and LAN-speed threat containment
Clients/Desktop	posture check, anti-virus software, and personal firewalls

Defense in depth involves using multiple security techniques in layers across an enterprise to ensure that no single device or infrastructure layer poses a significant vulnerability. Each technique and layer, from the firewall at the LAN-WAN boundary to the anti-virus software running on desktops, deflects a different threat. And each adds more protection by mitigating the damage that could result if one defense is compromised or circumvented. LAN security is yet another layer of protection, based on techniques specifically designed to counter threats to the LAN infrastructure and the data it houses.

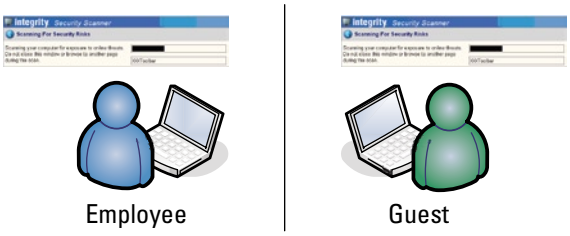
2 – Continue Perimeter Security



Perimeter security is crucial to preventing malicious traffic from entering your network via the WAN. Perimeter devices such as firewalls and intrusion detection/prevention systems recognize known threats and prevent these from propagating onto the LAN and its attached resources. Mature, well-established perimeter security products are available to guard the critical LAN-WAN boundary, and you should continue to take advantage of their protection.

3 – Protect the Client

Scan Known and Unknown Machines



Threats against clients and attacks that use clients as their launching point evolve quickly. Since client security products primarily protect against known threats, it's important that client protection be kept up to date. Host posture check, for example, ensures end points are in compliance with corporate standards and are running an approved operating system with current patches and fixes as well as an updated anti-virus program. In addition, clients should be protected from worms, spyware, and adware. Only clients that pass host posture check should be given access to the LAN.

The majority of today's client solutions are geared to managed desktops, but an effective client security solution must span both managed and unmanaged desktops. Look for a solution that can protect your LAN from attacks launched by guest or contractor devices as well as by employee devices. In addition, to avoid the overhead of manually installing an agent on every desktop, look for client solutions that automate deployment.

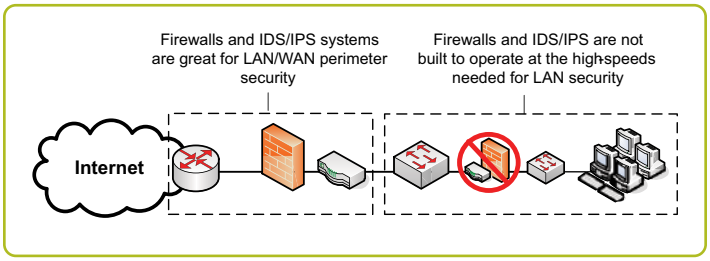
4 – Protect the Data

Data "leakage," the transfer of confidential or sensitive data outside the enterprise, can result in significant losses – in revenue, customer confidence, and regulatory penalties. Content monitoring and filtering products are among the newest tools for protecting critical resources from unauthorized transmission. Look for solutions that protect data stored on both servers and desktops and can monitor data in transmission via e-mail, instant messaging, and web communications. A content monitoring and filtering solution should monitor and decode multiple protocols, including FTP, HTTP, and TCP/IP; be capable of blocking traffic that violates policies; and operate on inbound as well as outbound communications.

5 – Protect the Network Itself

Every enterprise knows the cost of network down time, and many businesses have suffered extensive down time due to worm outbreaks and other malware. Protecting the network infrastructure is as important as protecting the WAN perimeter, clients, and data center and is paramount to ensuring network availability. Given the LAN's ubiquitous connectivity, a LAN security solution must protect against a range of threats, from misuse to the propagation of zero-hour malware. A LAN security solution must provide visibility into and control over user activities and application traffic, allowing IT to protect the network from the inside out.

6 – Use Purpose-Built Devices



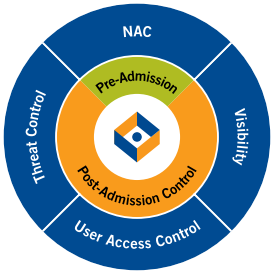
To get the most effective security protection, select and deploy security products that are designed for a specific use or location in the IT infrastructure. Purpose-built devices have the capabilities, performance, scalability, and price point appropriate to their usage. Avoid deploying security products designed for one area and problem set into another area. For example, deploying firewalls on internal links may seem like a good way to control malicious traffic across the LAN. However, firewalls are designed for the perimeter; they lack the performance needed on LANs, aren't designed to inspect and control the broad range of traffic on LANs, and are too expensive to be deployed throughout the LAN.

Just as you would select a security product purpose-built for the perimeter, client, or data center, look for a LAN security solution purpose-built for the LAN. A LAN security solution must operate at LAN speeds and be located close to the user to provide granular visibility into and control over LAN traffic. Visibility is key to control for all security devices – you can't control what you can't see. And securing the LAN requires a solution capable of monitoring the significant volume and range of traffic running on LANs and acting on that traffic based on containment policies.

7 – Look Beyond NAC to Post-Admission Controls

NAC plus Post-Admission

Only valid people, systems get on the LAN
» Authentication and posture check



Threat containment
» The unknown

Full L2-L7 visibility
» Tied to the user

Role-based provisioning
» Universal access control, L7 policies

Many enterprises are focused on network admission control (NAC), and rightly so. NAC encompasses user authentication and host posture check, allowing you to control who connects to the network and scanning their machines for compliance with security measures. Look for a NAC solution that leverages your existing investment in identity stores, such as Active Directory and RADIUS, and does not require you to pre-install a client agent for host posture check.

NAC is essential for controlling who gains access to the network. However, you also need post-admission controls so you can see and control where users go on the LAN and what they access. Post-admission monitoring and control is also essential for detecting anomalous traffic symptomatic of a zero-hour attack. A LAN security solution should provide visibility in the form of deep packet inspection on a per-user, per-application flow basis up to Layer 7, including details within Layer 7 such as the file name involved in an FTP. Comprehensive traffic visibility is a pre-requisite for access control and auditing as well as for granular threat control.

A LAN security solution must provide user-based, post-admission access controls, so IT can define rights and control actions based on a user's role in the organization. And an effective LAN security solution must detect malware – even malicious code never seen on the network before – and prevent it from propagating throughout the LAN.

8 – Architect for Simplicity

Architect each layer of security so that you leverage as much of your existing IT infrastructure as possible and can enable capabilities in a phased fashion. Look for security solutions that integrate into the infrastructure in a way that optimizes their functionality and minimizes operational overhead and can add value to your existing security processes. For example, at the perimeter, look for platforms that integrate firewalling and basic routing in a single device. At the client, expect NAC to be built into the next rev of Microsoft OSes.

At the data center, look for products with broad coverage, capable of monitoring and filtering content on multiple channels, and with robust attack protection. If you want to get a picture of how sensitive data is moving in your organization before you begin filtering, select a product that allows you to turn on transmission prevention in phases.

Similarly, a LAN security solution must work with your existing infrastructure and support functions such as NAC without requiring a switch upgrade. Likewise, it should enhance your existing security techniques, providing you more information about and more control over your business. For example, it should be possible to start with access controls based on a few simple groupings – for example, guest, contractor, and employee – and move to more granular, role-based provisioning, such as one set of permissions for a finance user vs. an engineer. In addition to interoperating with your existing LAN infrastructure, a LAN security solution should interoperate with your existing identity store(s), such as Active Directory or RADIUS. Look to simplify role-based provisioning by demanding that the LAN security platform be able to automatically learn a user's role during authentication.

9 – Enable Pervasive Security

Eliminate the Trade-Offs

LAN security = pervasive security
But LAN security cannot sacrifice performance or simplicity

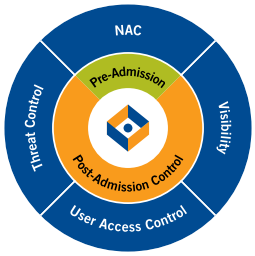
Just as you want to practice defense in depth, you need LAN security to cover the entire LAN. Deploying security pervasively ensures no "holes" exist in a given defense layer – all WAN traffic enters the enterprise through a firewall, all clients are protected, all confidential content in the data center is subject to monitoring and filtering.

Likewise, for LAN security to be effective, you must be able to deploy it pervasively. You may choose to implement a LAN security solution in phases, beginning with the most vulnerable areas, just as you would with any layer of security. However, the product must have an architecture, performance, and cost structure (including capital outlay and ongoing operational expenses) that allows for deployment across all LAN segments.

10 – Implement a LAN Security Architecture – Not Point Products

Architecture vs. Point Products

- NAC/802.1x/user authentication
- Wireless access
- Open live Ethernet jacks



- Zero-hour malware control
- Internal IPS

- L7 visibility
- Policy-based session capture

- Regulatory compliance
- Role-based provisioning

- Guest/contractor/patient access
- LAN segmentation

Given that the LAN touches all pieces of the IT infrastructure, LAN security must encompass many capabilities: user authentication and host posture check, complete visibility into data flows, user access control, and threat control. Purchasing a series of point products to get each of these capabilities is complex and expensive and provides more limited functionality since each feature is isolated. In addition, such a patch-work approach cannot scale.

To be effective, a LAN security solution must be holistic, with the component capabilities architected to leverage each other and work with the existing IT infrastructure. Only when a platform addresses the broad set of LAN security functions can IT be confident they're meeting the requirements for an effective solution in terms of capabilities and budget.

LAN security presents IT with a new set of challenges for protecting the business. By following these 10 Best Practices, IT can confidently embark on deploying a LAN security architecture to meet today's and tomorrow's demands.

About ConSentry Networks

ConSentry Networks delivers comprehensive LAN security, enabling businesses to protect their corporate assets, ensure continuity of operations, and dramatically reduce the risk of security breaches. ConSentry enables this pervasive security while lowering IT's cost of operations through its flexible, high-performance platform powered by ground-breaking custom silicon and revolutionary LAN security software. Backed by blue-chip venture capital firms that include Accel Partners, INVESCO Private Capital, and Sequoia Capital, ConSentry is headquartered in Milpitas, California. For more information, visit the company's web site at www.consentry.com.

Corporate Headquarters

ConSentry Networks
1690 McCandless Drive
Milpitas CA 95035

Tel: 408-956-2100
Toll-Free: 866-841-9100
Fax: 408-956-2199
Email: sales@consentry.com

Germany Office

ConSentry Networks
Lyoner Strasse 26 D-60528
Frankfurt Germany

Tel: +49 69 677 33 422
Fax: +49 69 677 33 200

United Kingdom Office

ConSentry Networks
Lakeside House 1, Furzeground Way
Stockley Park, Heathrow, UB11 1BD

Tel: +44 (0) 2086 22 3020
Fax: +44 (0) 2086 22 3200

Japan Office

ConSentry Networks
Hibiya Central Bldg. 14F
1-2-9, Nishi Shinbashi, Minato-ku
Tokyo 105-0003 Japan

Tel: +813-5532-7630
Fax: +813-5532-7373