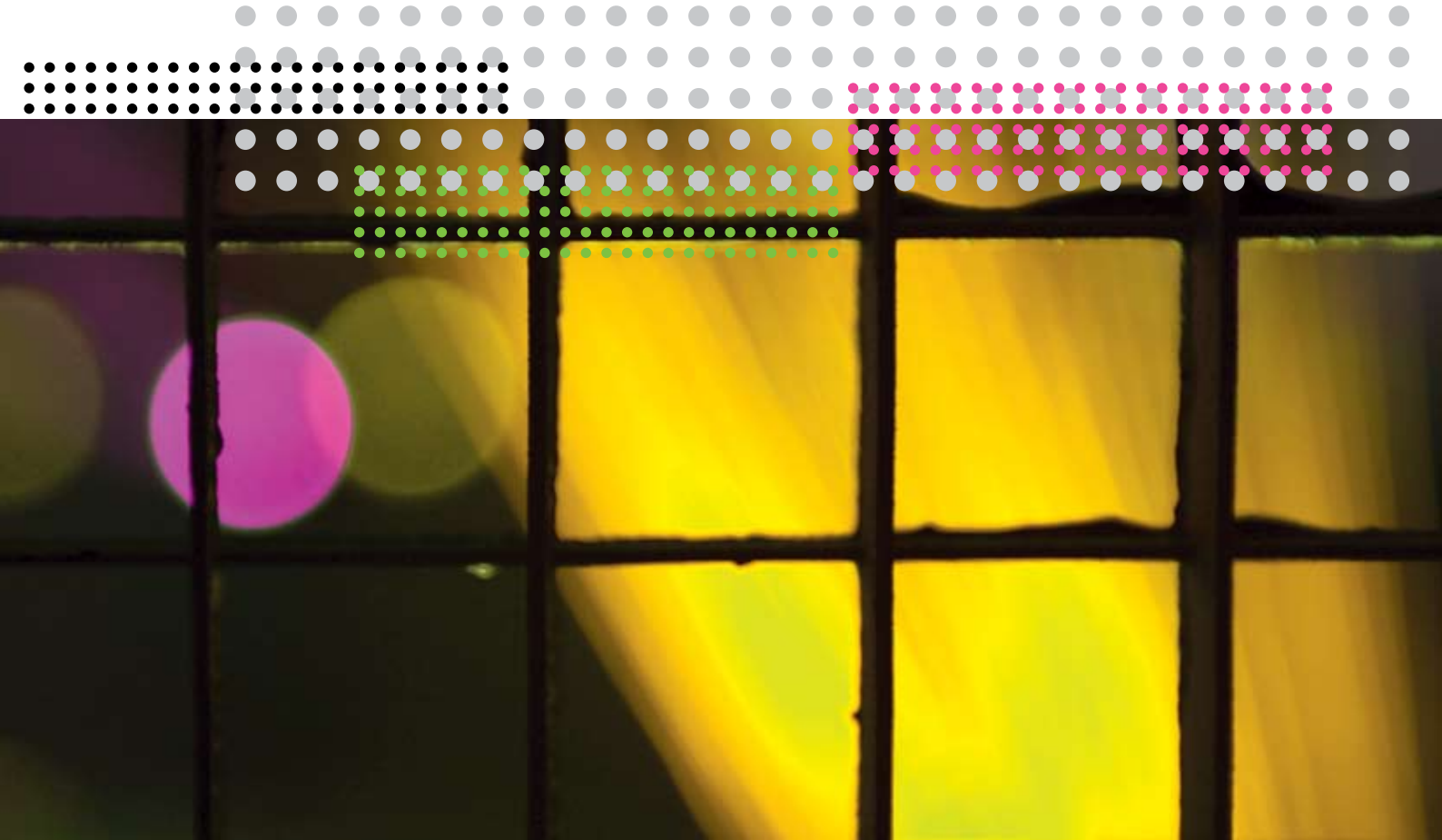
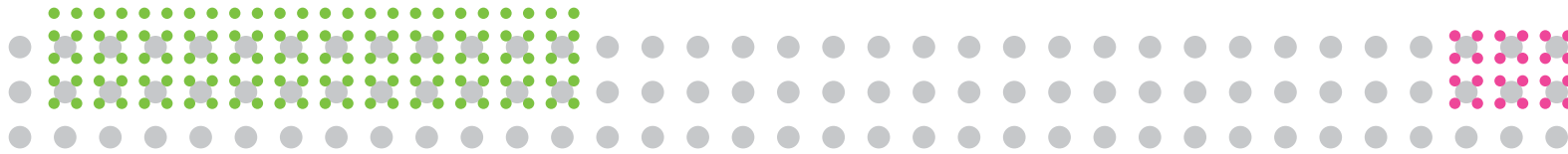


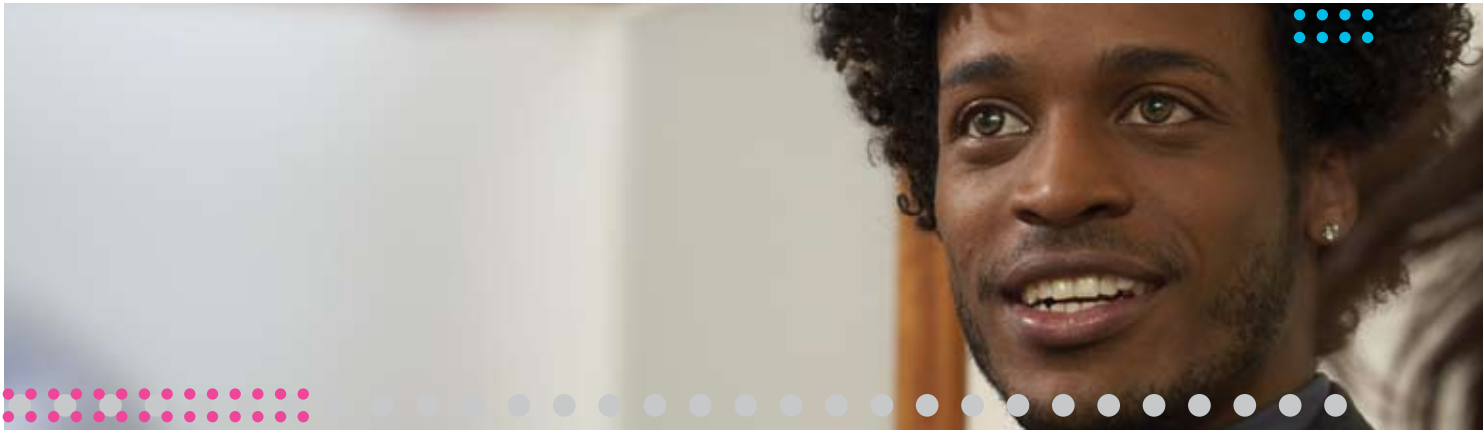
Making Enterprise Security Simple
Carrier class solutions for business





Introduction

Security matters. The internet is, of course, a very public network, which means that protecting private networks from malevolent content and users is a mission-critical priority for communications service providers and enterprises.



And let's not underplay the value of what we're protecting. For most enterprises, the contents of their network are the lifeblood of the business – from proprietary data and designs to R&D and business strategy, intellectual property, customer lists, financial documents and confidential personnel data.

In fact, an enterprise network can be one of a company's most valuable assets.

It's also undeniable that the number of external/internal threats and vulnerabilities associated with such networks continues to increase, with attacks growing in number, complexity and impact. As network users, communications protocols and hackers become more sophisticated, and portable access and storage devices proliferate, it's unsurprising such attacks are becoming more prevalent.



As the edge of corporate networks continues to expand, we're also beginning to see the first wave of viruses in cell phones and PDAs and hackers have already started figuring out ways to hijack VoIP sessions. These are all trends expected to not only continue, but grow.

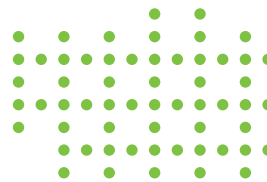
In an enterprise context, we must also consider the challenges associated with greater mobility. It goes without saying that businesses value new communications tools that improve the flexibility and productivity of their workforces.

However, with increased mobility comes the threat from workers who come back to the home office with viruses on their notebooks, phones or PDAs – viruses that are then introduced to enterprise networks.

So for IT managers and administrators, it's not a question of whether security threats are real and present dangers – that's a given. The challenge lies in keeping up to speed on where the next new threat is likely to emerge and how to prioritize defense against those that already exist



In short, modern, progressive businesses can no longer regard carrier-class network security as a 'nice-to-have' add-on. First-rate network security must lie at the heart of every company's communications infrastructure, a routine cost of doing business like building insurance and salaries.



What's the problem?

Figure 1 summarizes the most common types of security threats to corporate networks. For enterprises able to quantify the consequences of such attacks, denial of service (DoS) incidents and the theft of proprietary information are considered the most costly. The nuisance and time-wasting associated with viruses and worms come in a close third.

Denial-of-service attacks are attempts to render services unusable through assaults on network resources like routing devices, email and domain name system (DNS) servers. DoS tactics center on the overload, disruption and destruction of resources. Incidents are characterized according to the focus of the attack and the most common include:

- the consumption of network resources, such as bandwidth, disk space, or CPU time;
- the disruption of configuration information, such as routing information;
- the disruption of physical network components.



Figure 1. The most common types of security threats to corporate networks

| TYPE OF RISK | WHAT DOES THIS MEAN? | RANGE OF BEST-TO-WORST CASE SCENARIO |
|----------------------------------|---|--|
| Denial of service | Traffic over the internet connection slows or stops | Slowed services, order receipts – to – large productivity impairment |
| Malicious code | Viruses, worms, or other harmful code that compromises system performance | Nuisance – to – large productivity impairment |
| Compromised access | Insiders or outsiders gain unauthorized access to system or network resources | Website defacement – to – loss of customer data |
| Theft of proprietary information | Insiders or outsiders steal intellectual property | Minor embarrassment – to – catastrophic loss |
| Financial fraud | Insiders or outsiders use the firm's systems to commit financial fraud | Below-threshold loss – to – catastrophic loss |
| Equipment theft | Thieves steal IT equipment | Replacement required |



The theft of proprietary data often demands we examine security challenges from the outside in. How can businesses protect networks and data from unauthorized internal access?

The growing challenge here is that technology at the disposal of uninformed or dishonest employees and interlopers is becoming more powerful, cheaper and more portable all the time. To understand the scale of the threat, just consider a USB

dumper that, when installed on your computer, will copy files from any USB flash drive installed to it silently in the background. Well, such applications are already on the market. And they don't just copy the files from a USB drive, but actually **make an image** of the USB drive. In other words, anyone employing readily available un-deletion tools has a fair chance of recovering files deleted from the target drive.

Less dramatic, but no less



In a recent report, analysts Forrester Research estimated that a denial of service attack can typically cost a company \$100,000 an hour. The costs to specific types of businesses – for example, those based around financial transactions and e-commerce – could be very much higher.

concerning, just think about the ubiquity of iPod-style devices. Then consider the implications of the new generation of mega-capacity hard-drives associated with such devices. Just how much privileged information could you squeeze on to a tiny, very portable 120Gb drive?

The introduction of debilitating viruses and worms on to the enterprise network can be accomplished all too easily and, once again, with the proliferation of portable hardware, it is becoming

extremely difficult for businesses to manage. For example, a popular technique for security consultants seeking to expose poor enterprise housekeeping is to leave promotional USB memory sticks around the offices of their clients. The sticks are incentivised with some kind of competition or offer but also carry a harmless virus that is transferred to the computer in which the drive is used. Invariably, the vast majority of workers that pick up a stick go on to plug it into their computer to see what happens. Now consider the same scenario in the context of a malevolent attack and the huge

numbers of memory sticks, iPods, PDAs, notebooks and cell phones introduced on to an enterprise network on a daily basis.

Of course the bottom line here is all about *the* bottom line. In the final analysis, enterprise security is focused on protecting enterprise investments. Think about the impact of one serious denial of service incident for a major enterprise. This could mean several thousand people unable to

do business for five or six hours. Imagine the costs of proprietary information falling into the hands of a blackcap hacker as a result of a hijacked session; the costs relating to remediation and clean up – the costs of downtime and loss of productivity across the business. And consider the paralysing effect of the threat of such an attack hanging over a business – they’ve done it once and could do it again.

Screenwriters and novelists have taught us to fear targeted attacks and technically sophisticated espionage. The reality is more prosaic and probably more troubling.

For example, the majority of DoS attacks on networks are likely to come from anonymous hackers simply looking for something to break or damage. More often than not, they won’t even know what they’re targeting. It’s random and meaningless – except what they’re

targeting could be your business. The theft of privileged information by dishonest or disgruntled insiders is also on the rise, driven by low-cost technology and the growing number of technically savvy employees.

In this context, taking a sensible, measured precautionary approach to security simply makes good business sense.

What can enterprises do to protect against attack?

How do responsible businesses defend corporate networks – and, of course, the data on such networks – from outside attack or influence?


In broad terms, what needs to be done is quite straightforward: secure the wireless segments, firewall the wired network, authenticate users, scan data and constantly monitor the entire network. You also need to secure the perimeter of the network. Any connection to the internet or any public network – including a wireless network – needs to have a firewall in place. Simple.

In addition, modern network protection is about adopting a layered approach to security. So, for example, you'll need to have virus scanning on the network, but you will also want virus scanning on individual PCs and devices.

This level of diligence implies high levels of control and functionality,

which is why the armoury of network security is becoming significantly more sophisticated.

Traditionally, firewalls have been regarded as the cornerstones of such systems, but enterprise products need to offer much more than simply a sentry at the front door. Today's businesses will also be looking for



The trick, of course, is to accomplish all this efficiently and cost-effectively; taking into account the differing security demands of different strands of the business – which in global businesses are likely to be geographically remote – and in a manner that is thorough, yet at the same time doesn't adversely impact network performance and throughput.



advanced distributed denial of service (DDoS) attack protection, high-speed content security – including command blocking, URL filtering, virus scanning – strong authentication, real-time monitoring, logging, and reporting.

In many cases, it is becoming advisable for enterprises to employ what are known as intrusion detection systems (IDS) throughout the network, although advanced


firewalls can often deliver much IDS functionality.

As the name suggests, the role of an IDS system is to detect unauthorized access to or misuse of a network. These systems are effectively network burglar alarms, sounding the alert when an intruder or abuser is detected.


A system that combines the blocking capabilities of a firewall with the deep packet inspection of an IDS

product is sometimes referred to as an intrusion prevention system or IPS, although the term is in no way precise.

IPS technology is essentially a proactive defence mechanism that detects malicious packets within normal network traffic, automatically blocking any offending data before it can cause damage.



In general, IDS technology falls into one of two categories – anomaly detection and signature-based detection. Anomaly detectors focus on behaviour that deviates from normal system use. Signature detectors look for behaviour that matches a known attack scenario.



The point here is that these systems are smarter than the conventional IDS products that simply raise an alarm during or after a malicious payload has been delivered.

However, given that ever more hi-spec firewalls, routers, IDS devices and even AV gateways all include some kind of intrusion prevention technology, differentiating an IPS product from any of the above is often more a



matter of marketing than technical capabilities.

It's worth emphasizing the value of a distributed approach to security in which the most effective means of IDS and IPS deployment is to have such systems established around a network in areas other than those where the firewalls are located.

that provides communications – especially IP-based traffic – to end users. Whether you're supporting a few hundred users or a few hundred thousand, today's mission-critical, real-time data communications require each enterprise to become its own carrier, and therefore to protect and support its network traffic as a large carrier would.

If you're starting to suspect this sounds like a recipe for full-blown carrier-class enterprise network security, then your suspicions are justified. The safety and reliability of a secure network is critical to any business

Broadly speaking, there are four key features that ensure carrier class security for any network:

- distributed architecture with centralized control;
- seamless interoperability;
- real-time protocol filtering; *and*
- reliability.

Distributed architecture with centralized control

The value of this feature is related to the holistic nature of effective enterprise security. Protecting any enterprise network means developing strategies that embrace network vulnerability, access control and user security profile



management, secure communication and data privacy, electronic record retention and retrieval, plus any other data security and management procedures relating to the regulatory obligations of your enterprise.

All this suggests high levels of organisation which clearly needs to be orchestrated by some measure of centralized control.

Clearly the security of a network is only as strong as its weakest link. This means ensuring a consistent application of procedure, policy and technology across the entire enterprise, especially when business activity is geographically dispersed. Such an approach implies a winning


combination of shared local knowledge coupled with strategic, centralized control. Let's take the example of a national bank, where the security protocols of multiple branches are centrally managed from HQ.

What are the advantages of such an approach? First, it allows individual firewalls to be managed centrally and this enables an enterprise to establish, maintain and monitor a unified security policy across the group. At the same time, distributed architecture with centralized control facilitates the customization of security at individual branches, according to circumstances and demand.

From the perspective of consistency and logistics, centralized control also allows security personnel to upgrade security systems across a

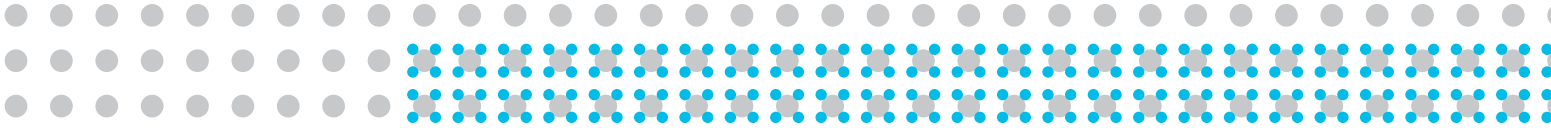
dispersed national or even global business in a matter of hours rather than months. This approach avoids situations in which IT staff have to visit individual branches in order to upgrade systems and also prevents potentially dangerous scenarios where some branches have been upgraded, others not, so the collective enterprise is unsure about the precise level of preparedness at any given moment.

In short, enterprises – like carriers – need an easy-to-use centralized management system that supports scalability and provides full real-time management through integrated security architecture. Whether the network comprises a few nodes and remote users or supports hundreds or even thousands of nodes, the ability to make a change in one central location and distribute it throughout the network instantly is critical to



For larger enterprises, centralized security control means there is no need for experienced IT personnel employed at individual sites. Clearly, because support, monitoring and administration can all be managed from HQ, this can lead to significant headcount savings.

the emergence of best-of-breed security components, so why aggregate key security functionality like firewall, email gateway, spam filter, anti-virus, anti-spyware, IDS, IPS, and vulnerability management into a single unit, effectively employing an under-powered product?



fast, efficient operations. Such a system allows network managers to control thousands of VPN/firewall devices and hundreds of thousands of concurrent VPN tunnels from one place.

Seamless interoperability

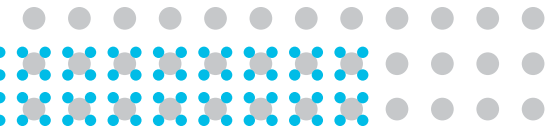
The second key feature of carrier class network security addresses the challenge of developing an efficient, effective approach to what is known

as ‘universal threat management’. As we have seen, today’s enterprises require an arsenal of security technologies to stave off a wide variety of threats.

At present, the common approach to threat management is to create a product that unifies and integrates multiple security features on to a single hardware platform. The trouble is that most enterprises recognize and place high value on

The point here is that running multiple applications from a single box will invariably result in an under powered security system – regardless of the size of box running the applications. You will have also created a single point of failure in the network. If that box goes, your whole network goes. The solution is to distribute the intelligence to a clutch of ‘best-of-breed’ appliances, each handling the tasks they are best at and have been exclusively

designed to tackle. The most effective security architecture places the firewall at the center of the security solution, routing network traffic through the various best-of-breed appliances. This is known as a 'layered' security approach or distributed unified threat management (DUTM).



It's worth noting that even unified products employing best-of-breed solutions can run into problems. For example, this kind of software is always prone to bugs and patches and there's never any guarantee that when you upgrade to fix one piece of software, that in so doing you don't cause problems with other software you have running in the same box.

In practice, for some light enterprise applications it may be desirable to

have all of these functions on one appliance to reduce capex and opex. However, for most medium-to-large enterprises, such a design is extremely limiting and likely to cause network bottlenecks as well as single points of failure in the network.

A much more robust approach and design is one that spreads the security disciplines throughout the network, allowing for free flow of data, best-of-breed technologies in every category as well as interaction between those technologies. In fact, flexibility of interaction is a key differentiator for the elements chosen to be included in such a network design. This kind of system can be described as a *distributed* unified threat management platform.

Having acknowledged the advantages of a best-of-breed solution, the next step is to recognize that different sorts of network

traffic should be treated differently. This introduces the concept of rules-based routing, a routing system based on protocols that can forward data packets, depending on the type of traffic, to the appropriate third party security appliance such as anti-virus scanning, spam filtering, URL blocking, content filtering, etc.

Rules-based routing enables firewall functionality to interoperate seamlessly with any third party best-in-class solution to provide maximum flexibility, enabling traffic segmentation across security zones and freeing individual network components from unnecessary processing loads.

By routing only the traffic that requires scanning, rather than all of the data that passes through a firewall, the overall flow of the network can be much more efficient. Security administrators can determine what they would like scanned by what equipment and what doesn't need to be scanned at all, thus reducing potential bottlenecks on the network.

A rules-based routing solution can be configured to route only the protocols that require scanning, leaving 'clear' traffic free to move quickly and efficiently to its destination.

Real-time protocols

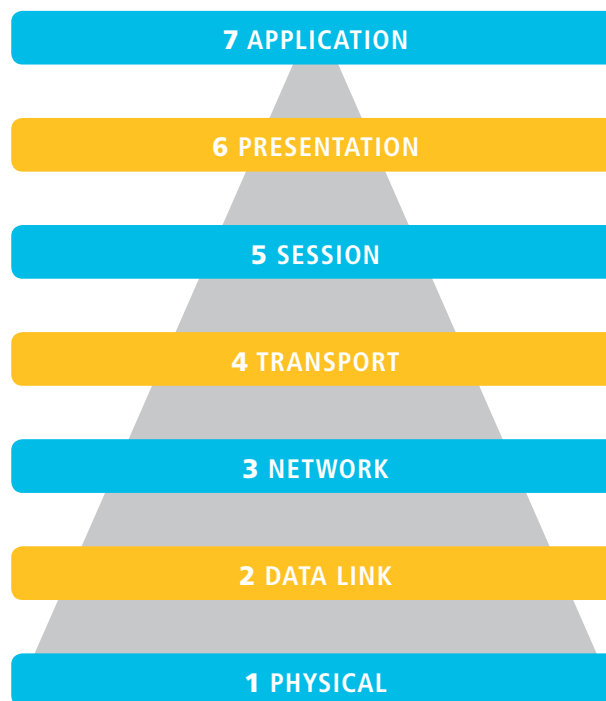
The third characteristic of effective carrier class security is the ability of systems to cope as data networks move to supporting real-time IP communication services such as VoIP and IPTV. In the new service environment, security elements must ensure such communications take place securely, without creating an open back door into the network. In addition, such systems must also

be able to help minimize the impact of latency and handle significant variations in demand, without compromising quality of service for users.

Large enterprise networks have long had to contend with the fact that SIP and H.323 require the use of multiple randomly selected ports to deliver associated data during a

session. This is a great challenge for the firewall in that the randomly selected port range is 64,000 ports. If the firewall were to open all 64,000 ports each time a call was being established there would be nearly no security at all. When a data transfer is completed, the ports are often left open, allowing hackers to conduct a random port scan to gain access to secure networks. In addition,

Figure 2. The seven layers of the OSI model



complex protocols like FTP and Telnet employ a command set that requires filtering at the application layer (ie. layer 7 of the OSI model).

A real-time protocol technique called dynamic pinholing supports VoIP and IPTV types of service without permanently opening ports and exposing the network to attack. The technique means that a firewall can listen in on port negotiation during call set-up for SIP and H.323 in order to open the ports between the two negotiating endpoints to allow the call, yet keep the other 64,000 possible ports closed. In the context of VoIP, many enterprises will also want to ensure that dynamic pinholing can be combined with network address translation (NAT) technologies for signalling and transport to ensure the connectivity and control of IP phones in 'private' environments.

In addition, application or layer 7 filtering (ie. assessing traffic at the application layer) has been developed to recognize IP communication packets and dynamically open ports on the

system to move the packets only between the initiation point and the endpoint, closing the ports when the call is terminated.

Effective bandwidth management is also becoming a hot topic in the context of real-time services like VoIP. Clearly, bandwidth management has always been an important element of network performance, simply because applications can perform poorly or fail if too much bandwidth is allocated to or demanded by any class of traffic. Successful bandwidth management is always about maintaining an appropriate mix of high- and low-priority traffic.

However, emerging real-time communications services require highly granular bandwidth management control, functionality that enables administrators to prioritize quality of service (QoS) by managing bandwidth at the level of the interface, the rule-set, the rule and the session. This level of control is critical when working with any real-time application, since the ability to guarantee bandwidth



for each individual session enforces good QoS for the VoIP call or other real time session.

Imagine if you only had bandwidth management at the physical interface. You might have hundreds of real-time applications like VoIP calls active at any given time. You might also have other data users on that interface. So if some heavy data application or download starts

running on that interface you could lose all or some of your VoIP calls or reduce them to a quality that is so poor that the users would hang up.

In addition, administrators must be able to provision server-level QoS with bandwidth limits to ensure that web servers are further protected against DDoS attacks. In this context, it is becoming increasingly important to be able to restrict the number of new sessions per second to defend against malicious disruption.

Clearly, network reliability and security have always been important. However, in recent years, ensuring such high standards has become an issue of legal compliance in most developed countries.

information processing standards and EAL-4 in order to do business.

In many industries, the failure to take proactive action to ensure robust, secure networks is now as much a matter for corporate lawyers as IT professionals. In the US, for example, the HIPAA's security rule requires that all healthcare organizations adopt 'reasonable and appropriate administrative, technical and physical safeguards':

- to ensure the integrity and confidentiality of patient information;
- to protect against any reasonably anticipated threats or hazards to the security or integrity of the information;
- to protect against unauthorized use or disclosure of the information;
- to otherwise ensure compliance among employees or officers.

At customer level, QoS control must ensure that one customer isn't starving other customers of bandwidth in shared hardware environments.

Reliability & compliance

Finally, the fourth key element for carrier-class security relates to reliability. There are two dimensions to this issue. The first is adherence to standards and best practices that address security in all of its many dimensions.

With regulations like the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act in the US, and the implications of initiatives like Basel II in Europe, security has suddenly become a C-level imperative for the majority of companies.

In addition, enterprises that interact with government or other security intensive systems often require assurance certification like federal



Until case law and negotiation establishes agreed-upon baselines as to what comprises the appropriate safeguards, technology and procedures, businesses would be wise to seek compliance with international industry standards. Deploying systems based on key international standards such as the International Telecommunications Union's X.805 and the ISO 18028-2 standard ensures not just reliability, but also enables businesses to be seen to be making every effort to protect both networks and data.

Hot failover is failover without perceptible downtime, a capability that is especially important in the context of emerging real-time services like video conferencing, VoIP and IPTV

Other key features that contribute to reliable network security include hack-proof, carrier-hardened operating systems and firewalls that employ faster and more robust flash memory rather than hard-drive based technology.



The second dimension to ensuring reliability is the fundamental security architecture of networks. Delivering reliability in the network infrastructure requires features such as hot failover without dropping sessions. Failover is, of course, an ability to switch over automatically to a redundant or standby system in the event of failure or abnormal termination of the active system without human intervention.



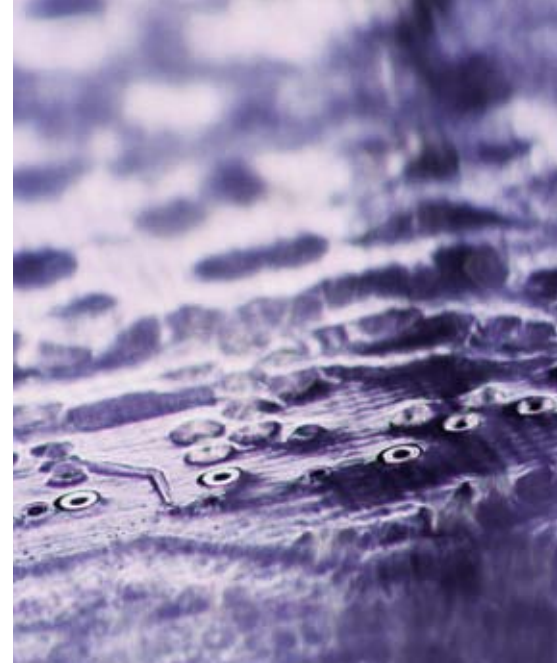
Alcatel-Lucent for carrier-class network security

Alcatel-Lucent's Bell Labs division has recognized the need to provide innovative security solutions to help reduce the growing number of threats confronting today's enterprise networks. In response to these needs, Bell Labs developed the Alcatel-Lucent VPN Firewall portfolio, a unique three-tier security architecture that includes:

- **VPN Firewall Brick® platforms:** Security appliances that integrate deep packet inspection firewall functionality with advanced VPN capabilities.
- **Alcatel-Lucent Security Management Server:** Software for robust, tightly synchronized firewall, VPN, service quality, VLAN and virtual firewall policy management.
- **Alcatel-Lucent IPSec Client:** Easy-to-use IPSec software delivering secure remote access to VPN services.

Collectively, these unique elements comprise a world-class solution that addresses all four key criteria that ensure carrier class security for any network:

- distributed architecture with centralized control;
- seamless interoperability;
- real-time protocol filtering; *and*
- reliability.



Distributed architecture with centralized control

Alcatel-Lucent's approach to enterprise network security architecture is founded on a central management platform that controls all firewall bricks directly, even in global networks. This is an important advantage for mid-sized and large enterprises, where the cost of administration outweighs all other cost factors in the deployment of a security solution.

At the heart of this centralized architecture is the Alcatel-Lucent Security Management Platform. This tool manages and monitors all aspects of the Alcatel-Lucent



VPN Firewall Brick and Alcatel-Lucent IPSec clients and provides a wealth of management capabilities, including:

- Hierarchical management tiers rapidly to provision and manage up to 20,000 Brick appliances and 500,000 clients from a single cluster.
- Full redundancy/failover capabilities for load-sharing and disaster recovery operation.
- Seamless integration of firewall, VPN, bandwidth management, virtual LAN (VLAN) and virtual firewall policy management – centralized real-time monitoring, robust logging and customized reporting capabilities.

In addition, Alcatel-Lucent's approach to security management helps reduce delays, IT staff time and headcount across an enterprise by facilitating centralized control of software upgrades and patches. This also means administrators can ensure consistent levels of security in all parts of a business, even when that business is dispersed nationally or even globally.

Seamless interoperability

Mission critical networks require a multi-tiered security approach. As we have seen, in most cases an architecture in which all security features reside in a single appliance is not the best approach. A better solution is to adopt a 'distributed universal threat management' strategy that controls the interaction of a range of 'best-of-breed' appliances from each of the security disciplines.

Flexibility of interaction is a key differentiator for the devices selected to protect the network. And the ability to route according to protocol at the rule level in each of the firewalls provides the flexibility to build a true multi-tiered secure network.

Alcatel-Lucent's Security Management Server version 9.1 enables a new Bell Labs-developed feature called Rules Based Routing. This technique allows routing based on protocols and forwards data packets, depending on the type of traffic, to the appropriate third party security appliance such as anti-virus

scanning, spam filtering, URL blocking, content filtering, etc. This enables the Alcatel-Lucent device to interoperate with any third party best-in-class solution to provide maximum flexibility and interoperability. This in turn enables traffic segmentation across security zones and frees individual network components from unnecessary processing loads.

Alcatel-Lucent security solutions also efficiently address the need

to contain operations outlays by making efficient use of in-house technical expertise and protecting network investments. Introducing them requires no costly network retrofits. As a true layer 2 network device, Alcatel-Lucent's VPN Firewall Brick security appliance was also designed to integrate seamlessly into existing corporate networks, with little or no network reconfiguration required. Although operating as a layer 2 network device the bricks filter all the way up to layer 7 of the OSI model, see *Figure 2. p14*.



Unlike many competitive products, VPN Firewall Brick platforms are built as security-specific devices and, in contrast to traditional router-based systems, they operate as intrinsically secure ethernet-layer bridges that are virtually invisible to hackers scanning a network.

Completely segregated from the routing process, these security appliances are not vulnerable to dynamic routing protocol attacks. In many instances, they are literally undetectable, protecting enterprises with a high level of stealth security.

Real-time protocols

Alcatel-Lucent's VPN Firewall Brick platforms have evolved to support real-time, latency-sensitive, IP-based multimedia services such as VoIP and IP videoconferencing. One of the key innovations in this area is the implementation of a technology called dynamic pinholing. As we have seen, this technique means a firewall can listen in on port negotiation during call set-up for SIP and H.323 in order to open the ports between the two negotiating

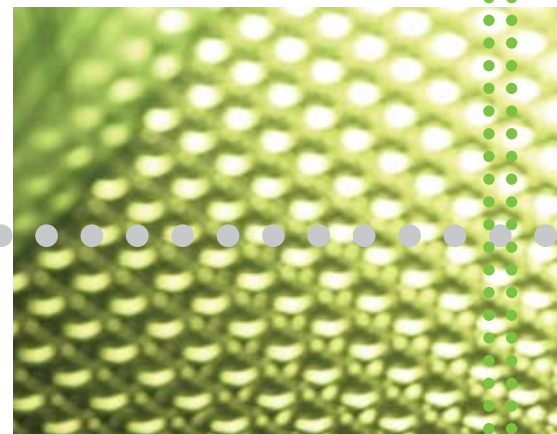
endpoints to allow the call, yet keep the other 64,000 possible ports closed.

This is a powerful improvement over existing models for IP-based voice traffic, which employ a firewall device permanently or temporarily opening a range of ports to allow IP voice calls. The control of dynamic pinholing reduces the chance that malicious hackers can exploit these open ports to gain entry to an Alcatel-Lucent protected network through this technique.

Most firewall technology filters at layers 4 and 3 (transport and IP). This is fine for simple protocols. However, there are protocols that are much more complex and require filtering at the application layer (7), see *Figure 2. p14*. Consider protocols that have commands embedded in them like H.323, SIP or maybe something more familiar like FTP where you can use Put and Get commands. These types of protocols require a system that allows the protocol through the network,

yet is also able to finely tune it so administrators have control over the actual commands within the protocol.

Alcatel-Lucent's VPN Firewall Brick platforms allow application or layer 7 filtering (ie. assessing traffic at the application layer) to facilitate more granular control of traffic.



Network security and quality of service can be increased through sophisticated Bell Labs engineered bandwidth management methods, which incorporate a robust implementation of class-based queuing (CBQ) technology for committed-rate bandwidth control and traffic prioritization.

From a security perspective, bandwidth limits help defend against flood attacks, while bandwidth guarantees also enhance end user experiences and can be enforced at the server and user levels. Traffic can be classified by physical interface, virtual firewall, policy rule and session, enabling simplified yet precisely targeted security implementations. This is essential to ensure that next-generation, time-sensitive IP applications, such as VoIP and IPTV, meet the service level quality requirements required for effective implementation.

Reliability

Bell Labs, the research organization that pioneered 'five-nines' reliability in the circuit-switched world, is now focused on applying its security insights, technologies, architectures, and standards to the new converged wireline and wireless enterprise network.

This means a high-availability architecture is built into every component of the Alcatel-Lucent's

VPN Firewall portfolio. This ensures there is no single point of failure solution-wide. All VPN Firewall Brick systems support native subsecond failover to a standby unit. In an outage, services continue uninterrupted. Out-of-band management capabilities help ensure continued service even if communications are lost due to a network outage.

For added reliability, Alcatel-Lucent's Security Management Server software can be distributed across multiple geographically dispersed operations centers for active/active network redundancy. This enables immediate disaster recovery in the event of a catastrophe at the primary management location.

In addition, Alcatel-Lucent's standards driven approach to security ensures an environment that places reliability and interoperability at the top of the agenda. Bell Labs' security model, now the basis of both the ITU X.805 standard (generally geared toward service providers) and an

ISO 18028-2 standard (generally for enterprises), is a Bell Labs pioneered approach to assessing, planning, managing and maintaining secure computer and telecommunications networks, regardless of which technologies or vendors are used.

Bell Labs' security model provides a systematic framework that addresses these challenges for ensuring network security, filling a void in existing security standards by providing a holistic network security architecture that is applicable to the end user, management and control or signalling of network infrastructures, services and applications.

The framework helps enterprise customers and service providers combat network security threats across several network dimensions and potentially save millions of dollars in security vulnerabilities by identifying the security investments that can drive more efficiency into the supply chain and thereby lower costs and raise productivity.

Alcatel-Lucent's VPN Firewall (LVF) portfolio

The Alcatel-Lucent VPN Firewall portfolio offers flexible deployment options to suit service provider, government, and enterprise network strategies.

PORTFOLIO BENEFITS AND FEATURES INCLUDE:

- **SIMPLIFIED MANAGEMENT**
 - unique client/server design; centralized staging, real-time monitoring and no-touch management of all VPN, security and service quality assurance capabilities via scalable, proven Alcatel-Lucent SMS.
- **FULL-FEATURED BRIDGING** – enables stealthy, depth-of-defence security that conventional router-based firewalls cannot match.
- **ADVANCED SECURITY SAFEGUARDS** – denial-of-service attack protection; high-speed content security; premium authentication services; with no occurrences of reported advisories or vulnerabilities and no backdoors.
- **UNIQUELY GRANULAR BANDWIDTH MANAGEMENT**
 - maximize service quality via flexible class-based queuing (CBQ) technology, server level and user level limits and guarantees.
- **CARRIER-GRADE RELIABILITY**
 - native high availability architecture with no single point of failure.
- **RULES-BASED ROUTING** – Routes all packets matching the rule to a proxy server, router or other device utilizing third party software to perform content filtering functions such as command blocking, URL filtering and virus scanning. Allows transparent interaction with any third party equipment.
- **HIGH-PERFORMANCE PACKET PROCESSING** – supports up to 4 million simultaneous sessions, 1100 virtual firewalls, 20,000 VPN tunnels.
- **ULTRA-THIN, HIGHLY SECURE OPERATING SYSTEM** – virtually impenetrable to hacker attacks; frees memory for packet processing, policy management.
- **VIRTUAL FIREWALL AND VLAN SUPPORT** – easily assign and enforce security policies for diverse user groups.
- **PLUG-AND-PLAY DEPLOYMENT**
 - implement secure mission critical applications without costly, time intensive network reconfiguration.
- **LOW OWNERSHIP COSTS** – no ongoing feature-licensing expenses; easy installation, management and upgrades save IT staff time and effort; high performance, high capacity features reduce the need to purchase additional equipment.

Alcatel-Lucent's VPN Firewall Brick Family

TECHNICAL SPECIFICATIONS

IPSec Client 9.0

- Easy to use IPSec w/IKE Auto policy download
- Stateful Firewall Client "status logs"
- Managed client option
- Interoperable w/full portfolio

Alcatel-Lucent Security Management Server (LSMS)

- Software for robust, tightly synchronized firewall, VPN, service quality, VLAN and virtual firewall policy management



Brick 50

- 3 x 10/100 ports
- 195 Mbps firewall
- 75 Mbps 3DES
- 135,000 sessions
- 1000 VPN tunnels
- 50 virtual firewalls



Brick 150

- 4 x 10/100 ports
- 330 Mbps firewall
- 127 Mbps 3DES
- 245,000 sessions
- 1000 VPN tunnels
- 150 virtual firewalls



Brick 700

- 8 x 10/100/1000 ports
- 1.7 Gbps firewall
- 425Mbps 3DES
- 350Mbps AES
- 1,000,000 sessions
- 20,000 new sessions/s.
- 7500 VPN tunnels
- 350 virtual firewalls



Brick 1200

- 10 gigabit ports
- 2 x GBIC & 8 x 10/100/1000
- 3 Gbps firewall
- 1.1 Gbps 3DES/AES
- 2,000,000 sessions
- 30,000 new sessions/s
- 10,000 VPN tunnels
- 500 virtual firewalls



Brick 1200 HS

- 20 gigabit ports
- 6 x GBIC & 14 x 10/100/1000
- 4.75 Gbps firewall
- 1.7 Gbps 3DES/AES
- 3,000,000 sessions
- 45,000 new sessions/s.
- 20,000 VPN tunnels
- 1100 virtual firewalls



SOHO
ROBO



Small
enterprise



Mid
enterprise



Large enterprise
Data center



Conclusion

If you think carrier class security is just for large carriers, then think again. The safety and reliability of a secure network is critical to any business that provides communications – especially IP-based traffic – to end users.

Whether you're supporting a few hundred users or a few hundred thousand, today's mission-critical real-time data communications require each enterprise to become its own carrier, and therefore to protect and support its network traffic as a large carrier would.

Alcatel-Lucent's standards-based VPN Firewall portfolio founded on distributed architecture with centralized control, with powerful features like Rules Based Routing, provides a best in class multi-tiered secure network solution for today's enterprises.

To reduce headcount and administration costs, mid-sized and large enterprises require security solutions with centralized management capabilities designed for the managed services space.

Today's enterprise networks also require a multi-tiered security approach. This means adopting a distributed universal threat management strategy, applying best-of-breed security controls while maximizing network efficiency.

For both service provider and enterprise customers, Alcatel-Lucent's Bell Labs division continues to innovate: designing strategies that protect critical infrastructures from disasters and attacks, developing products that help secure networks, databases and key information against hackers and corruption, and integrating features into Alcatel-Lucent's products that make them some of the most reliable and secure solutions in the market.

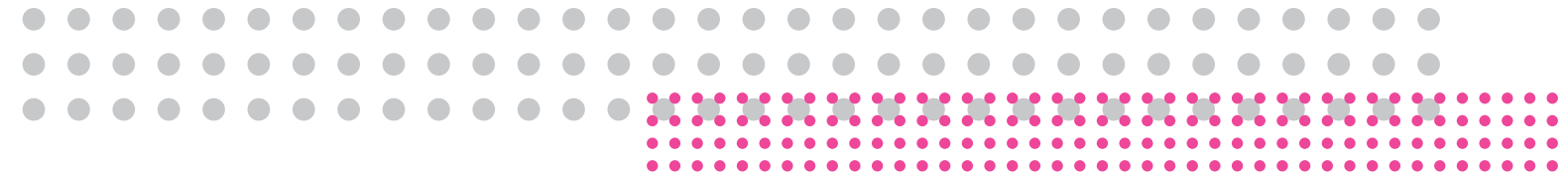




Abbreviations

| | | | |
|--------|---|-------|---|
| 3GPP | Third Generation Partnership Project | IPTV | internet protocol television |
| A/V | audio/visual | ISUP | integrated services digital network user part |
| ADSL | asymmetric digital subscriber line | ISV | independent software vendor |
| ALG | application layer gateway | LAN | local area network |
| ARP | address resolution protocol | LMDS | local multipoint distribution system |
| ARPU | average revenue per user | MPLS | multiprotocol label switching |
| ATM | asynchronous transfer mode | MSPP | multiservice provisioning platform |
| BRAS | broadband remote access server | NAT | network address translation |
| BSA | broadband service aggregator | NGN | next generation network |
| BSR | broadband service router | NOC | network operations center |
| BSS | business support system | ONT | optical network termination |
| CDR | call detail record | OSS | operations support system |
| CO | central office | PDA | personal digital assistant |
| CPE | customer premises equipment | PIP | picture-in-picture |
| DBS | direct broadband satellite | PLMN | public land mobile network |
| DHCP | dynamic host configuration protocol | PSTN | public switched telephone network |
| DNS | domain name system | PVR | personal video recorder |
| DoS | denial of service | QoS | quality of service |
| DRM | digital rights management | RDP | remote desktop protocol |
| DSL | digital subscriber line | RPR | resilient packet ring |
| DUTM | distributed unified threat management | SD | standard definition |
| ETSI | European Telecommunications Standards Institute | SDH | synchronous digital hierarchy |
| FTTN | fiber to the node | SIP | session initiation protocol |
| GPON | gigabit passive optical network | SLA | service level agreement |
| GPRS | general packet radio service | SONET | synchronous optical network |
| HD | high definition | STB | set-top box |
| HDTV | high definition television | TDM | time division multiplexing |
| HIPAA | Health Insurance Portability and Accountability Act | UDP | user datagram protocol |
| HSI | high-speed Internet | UMTS | Universal Mobile Telecommunications System |
| HTTP | hypertext transport protocol | VHO | video hub office |
| IGMP | Internet group management protocol | VLAN | virtual LAN |
| IMS IP | multimedia subsystem | VoD | video on demand |
| INAP | intelligent network application part | VoIP | voice over IP |
| IP | internet protocol | VPLS | virtual private LAN service |
| | | VSO | video service office |





Alcatel, Lucent, Alcatel-Lucent and the Alcatel-Lucent logo are trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners. Alcatel-Lucent assumes no responsibility for the accuracy of the information presented, which is subject to change without notice.

© 05 2007 Alcatel-Lucent. All rights reserved. Brochure ref. SimpleSec0507.

www.alcatel-lucent.com

