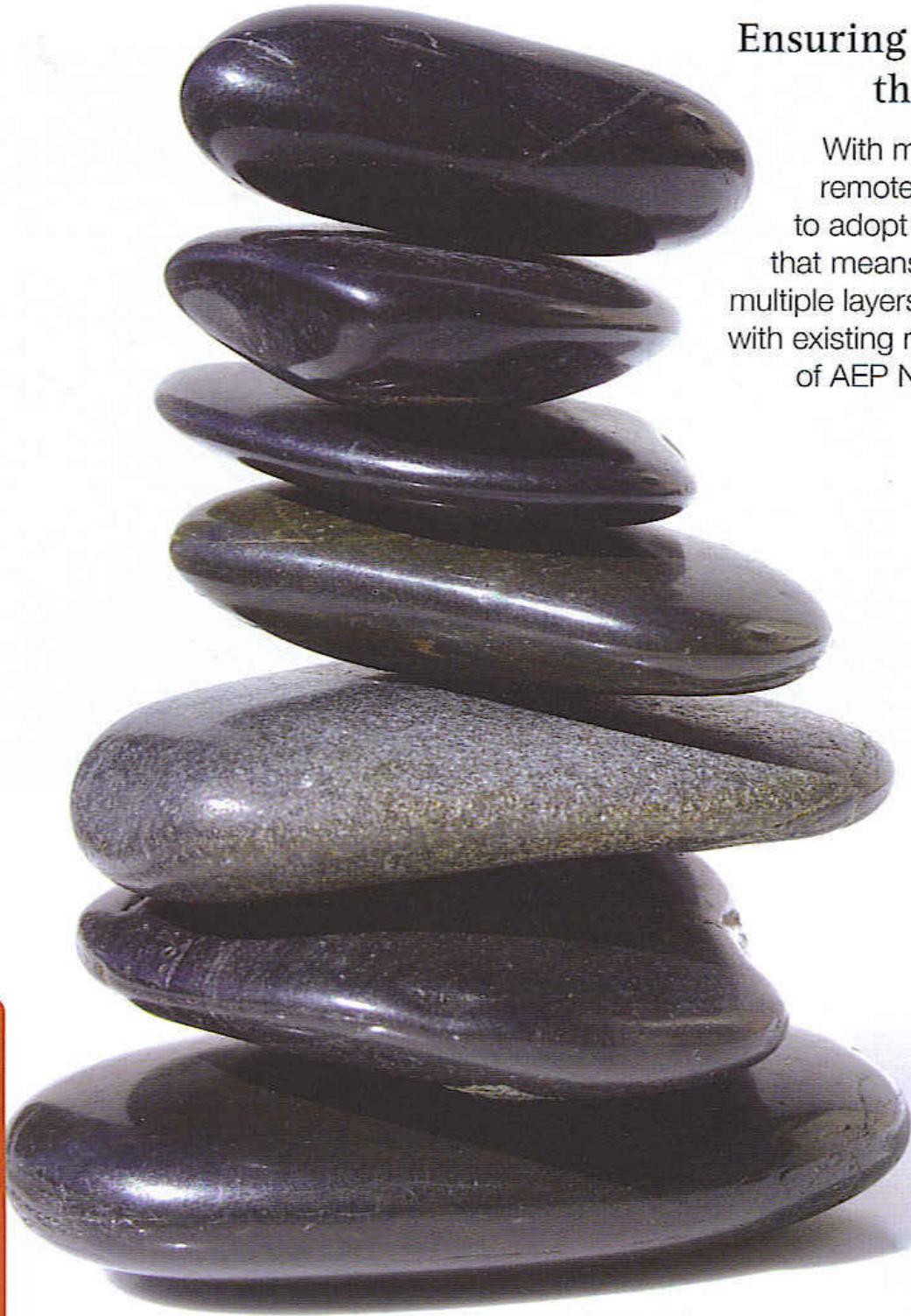


The Balancing act

Ensuring security and compliance through policy networking

With more and more organisations using remote technology, it's become essential to adopt a new approach to security – and that means policy networking which involves multiple layers of security solutions all operating with existing network systems. **Reginald Best**, of AEP Networks, explains how it all works





Reginald P. Best brings nearly 20 years of experience in engineering and business management to AEP Networks. Prior to the merger of AEP Systems, Ltd and Netilla Networks, Inc. in December 2004, Reggie was co-founder, President and CEO of Netilla Networks. Before that, Reggie founded AccessWorks Communications, an Internet/remote access company acquired by 3Com Corporation. Reggie has a B.S. degree in Electrical Engineering from City College of New York and an M.S. degree in Electrical Engineering from Columbia University.

It organisations must perform a tricky balancing act when working to provide access to their network resources, for teleworkers, for general remote access and for partner collaborations, for example, while at the same time securing those resources to prevent misuse and attack from unauthorised users.

To safeguard their assets and meet regulatory compliance, enterprises worldwide are now turning to the layered security of Policy Networking. Policy Networking (PN) involves multiple layers of security solutions all interoperating with existing network systems, and it enables organisations to enforce policies that govern network admission as well as access to high-value resources.

PN also serves to ensure compliance with industry and government regulations by verifying policy enforcement with audit trails.

The broad demands of application use, as well as compliance with government and industry regulations, mean that systems have to be protected from internal users and systems as well as "outsiders". Controlling access through the network has become much more

important, motivating an evolution to a policy-based perspective.

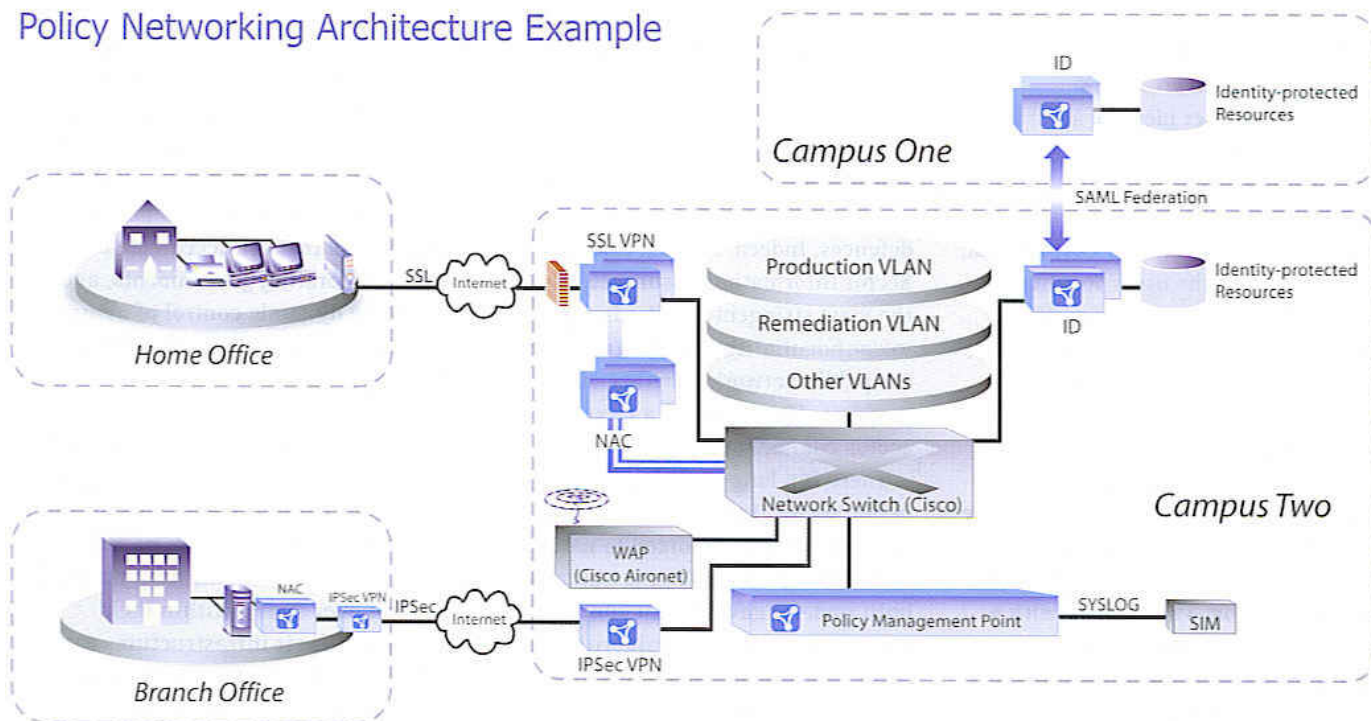
Admission to the Network

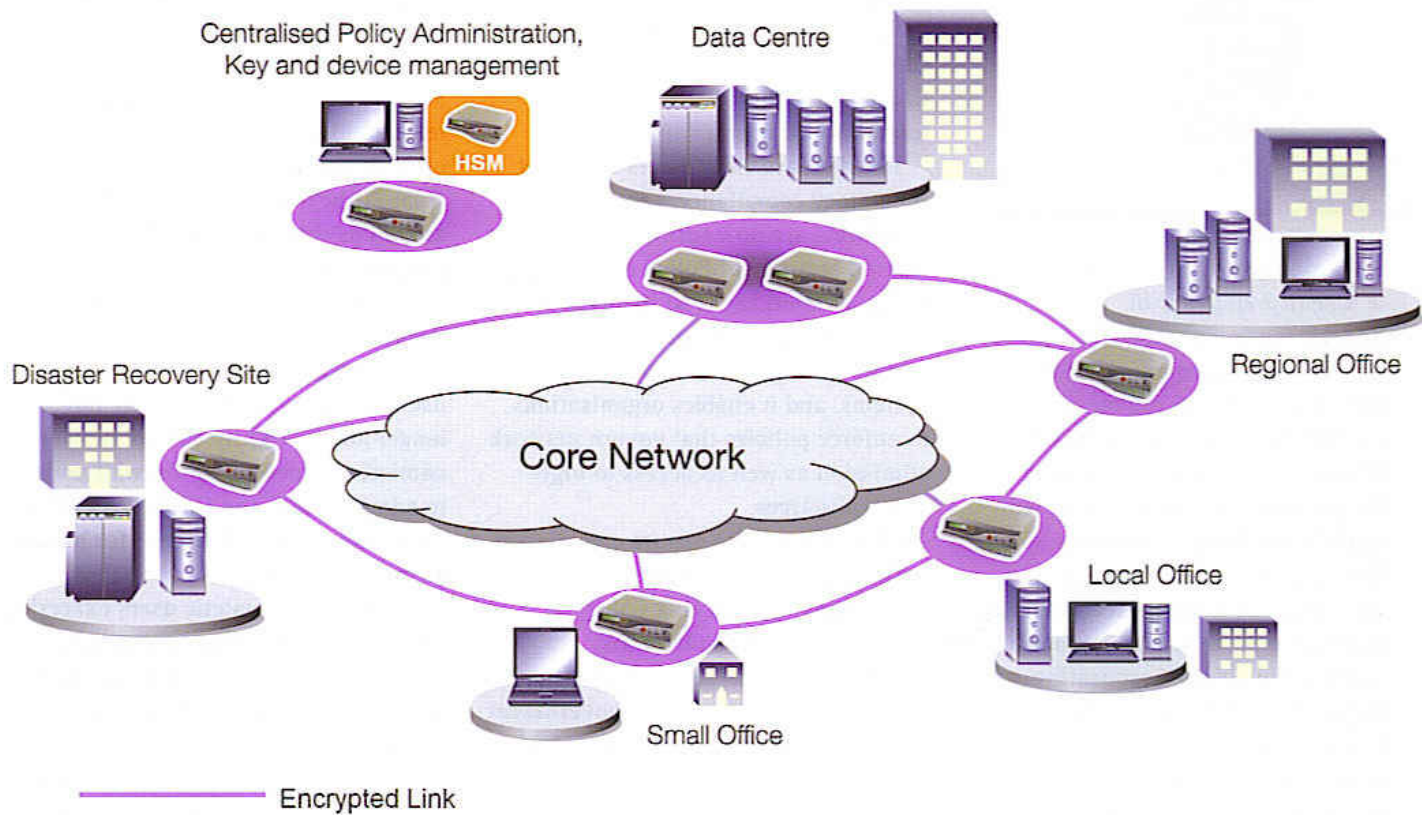
The most basic network security ensures that only authorised users enter the infrastructure. Today, however, more and more of these users are telecommuters, mobile employees and other remote staff who require access from far beyond the LAN perimeter, as well as third-party users like partners, suppliers, consultants and contractors who may require access to the enterprise network.

While traditional firewalls remain useful security tools, they are no longer able to tightly control network admission. Opening up firewall ports to admit remote and third-party users provides potential gateways for hackers or malicious code.

Moreover, peripatetic users exacerbate risks because their devices are often beyond the control of administrators. Although anti-viral software can deter online threats, there is no guarantee that off-site employees and third parties update their computers with the latest filters and security patches, and they may have acquired malicious software

Policy Networking Architecture Example





from other networks.

To protect enterprises, PN authenticates user identity according to policy, beginning with the very first security decision point – network admission. The functionality of Network Admission Control (NAC) ensures that, independent of the users' locations, endpoint devices or access methods, only trusted users enter the network, and it also verifies the security configuration of each user's terminal, permitting only policy-compliant devices into the infrastructure.

Importantly, and to maintain business continuity, admission control must be coupled with the capability to take remedial action. Thus, a user with a non-compliant terminal should be quarantined while the unit is updated with the latest patch or anti-virus signature and, once compliant, allowed into the network.

Secure Remote Access / VPNs

While regulatory compliance is increasingly focused on identifying and managing users once they have entered the infrastructure, it would be very unwise to neglect the perimeter defences. Indeed, in most Public Sector Information Assurance models the most stringent standards apply to confidentiality and integrity over the public network, whether on the corporate WAN or over a remote access connection.

There is a long tradition in the public sector that communications security must be enforced to national standards often employing equipment built under a government contract and implementing national algorithms. However, this sits uncomfortably in the era of joined-up government and international collaboration against threats such as terrorism. It also seems to be an anathema to public sector

agencies to allow remote access to sensitive data or to share such data.

The challenge to the security industry is to develop communications security products that integrate into the PN model, that are flexible, implement algorithms that are acceptable to the collaborating governments, and facilitate dynamic control of assured data separation such as Closed User Groups.

Controlling the network's interior

Organisations, particularly those with stringent regulatory mandates such as government and financial and healthcare institutions, must maintain control over traffic within their networks. Their infrastructures can no longer be open systems in which all users have unfettered access to every resource. Servers containing critical business, financial, healthcare or government assets must be restricted to

only those users who need these resources.

To attain security and compliance, PN offers Layer 3 policy enforcement to safeguard data and applications from unauthorised access. Identity Enforcement (ID) controls traffic at critical junctions within the network according to enterprise-wide governance, enforcing resource availability based on identity and policy.

An ID appliance serves as a proxy for identity-protected servers. Upon receiving an access request for the resource, the ID queries policy stores (e.g. LDAP), as well as policy

While traditional firewalls remain useful security tools, they are no longer able to tightly control network admission.

configurations on the ID itself. If the user and the request conform to policies, it is forwarded to the target servers. Otherwise, the ID denies the user even visibility of restricted components, concealing their locations, preventing pings and eliminating potential risks.

When the ID detects offending behavior, it works in concert with NAC. The ID can take such measures as instructing the NAC to place the questionable user into quarantine or even shutting down the user's port. Furthermore, it can alert administrators of the aberrant conduct.

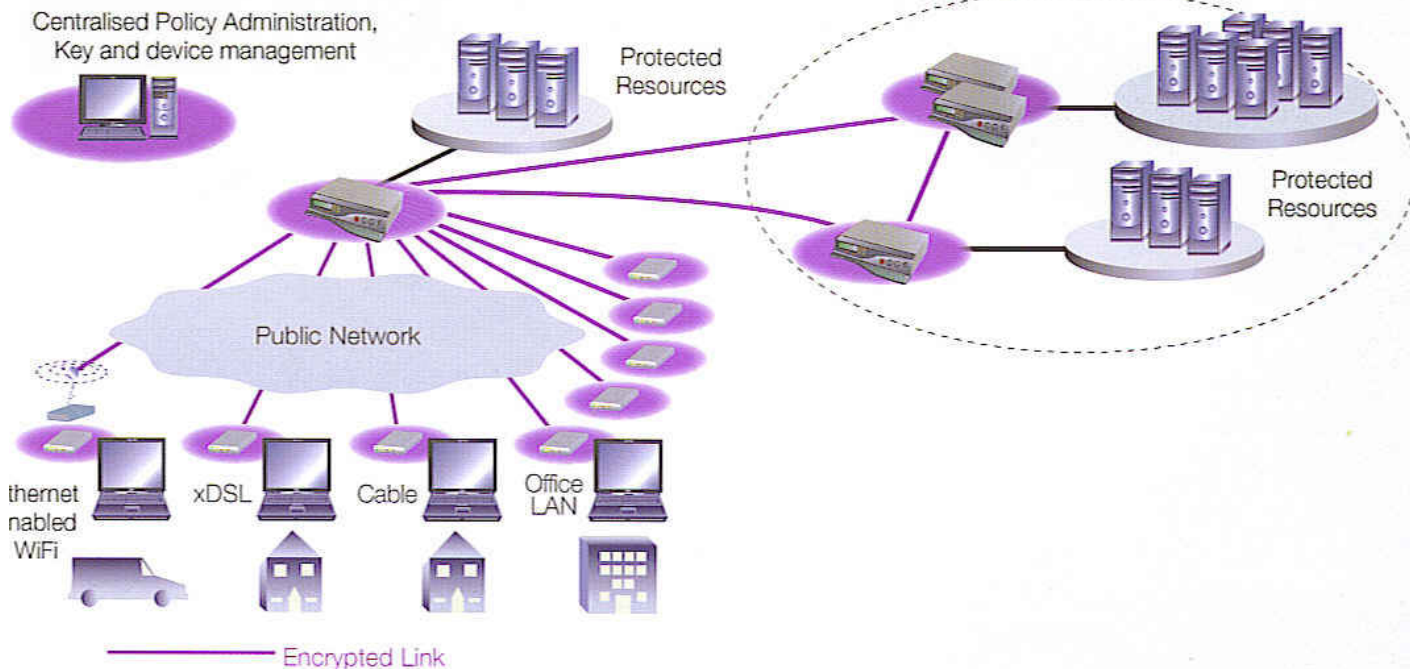
Scenario: A Government Agency Controls Admission

Of all the organisations that require secure access, government agencies are, perhaps, the most accountable. Unauthorised users must never be allowed to access classified resources, databases or personnel information. Any failure could compromise missions and place people in jeopardy. Yet, their field operatives, as well as colleagues from other agencies, must access the network to share data and coordinate operations.

To build defence-in-depth the agency deploys government standard encryption to protect public network communications and remote access and, within the perimeter, implements NACs to secure separate domains.

For an employee connecting his laptop to the network at a remote site or plugged directly into an Ethernet port at his office, the method for admission is identical. He submits to an authorisation process using a username, password and token. The edge switch notifies the NAC of the request, which confirms the user's identity according to policies. The NAC then places the employee in a quarantined zone while it assesses the health status of his terminal. After ensuring he complies with security policies, NAC permits the user into the production network. If not, then the user's session is quarantined until remedial measures are complete.

Remote Access Security



Achieving comprehensive security

By using PN to control access by identity and enforce usage policies at network decision points, enterprises can secure and police user traffic from desktops, across the public network, within and beyond the LAN perimeter. They can ensure adherence to policies for user identity, endpoint device configuration and health as well as the servers each user is allowed to access and the permitted interactions with applications. Organisations can achieve operational security by imposing access and use policies for assets, operational robustness by protecting resources

.....
Network Admission Control ensures that, independent of the users' locations, endpoint devices or access methods, only trusted users enter the network
.....

from attacks and vulnerabilities, business governance by complying with established policies and mandates and operational effectiveness by meeting the imperatives of collaborative working.

Policy Networking can help enterprises across all industries meet the most stringent compliance needs while eliminating the risks and vulnerabilities that can compromise their operations. **eS**

What is a Policy-based Network?

.....
According to Internet Research Group [Policy-based Networks: An Overview, September 2006], an ideal policy-based network would operate in the following manner:

- Policies would exist that define trust and authority requirements for access to and use of network-based resources.
- The authority and trust of each user would be maintained in an authoritative directory.
- A user would have to authenticate his identity to gain use of the network.
- At the time of user authentication, the state of the user's computer would be assessed against established software security policies.
- Depending on your identity, system profile and the resulting trust, the network would provide suitable connectivity.
- After the initial connection, if anything changed (you were fired; your system started acting as if infected by a worm; a new application was commissioned; general system conditions changed dramatically), a policy driven network would automatically reconfigure to reflect the modified access appropriately.