Security

As technologies increasingly converge onto a single IP based network it is becoming increasingly common for organisations to be vulnerable to security breaches from internal and external threats. Organisations require stringent network security reassurance through in-depth security reviews across their network devices.

Visibility

Most networks have evolved over a period of time housing a mixture of technologies and vendors across both legacy and current networking devices and software. For this reason alone organisations need to formulate an inventory of their network in order to understand the complexities surrounding the security of their business systems. This audit provides the foundations for future network expansion and should be constantly reviewed and updated. As part of any unified network it is important to have a network security policy in place that identifies and mitigates any form of attack or disruption to a business whilst conforming to privacy and legal compliances.

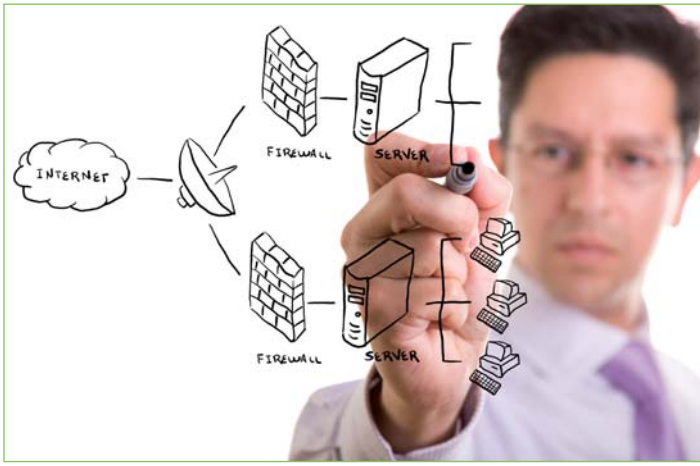
Evolved has a team of security specialists who assist customers across a broad spectrum of network security areas. These may include firewalls, VPN access, router & switch security and endpoint security all of which require the same high level of technical expertise and industry knowledge.

All Evolved technology specialists are trained to deal with the most complex network scenarios and because of Evolved's specialist support services customer's benefit from utilising this resource without the need for employing specialists of their own, ensuring overhead is kept to a minimum.

Security services

Security policy development

> The first step for security is to develop a security policy defining acceptable use and administration of the network
> Hand hold client through the creation of a security policy
> **Deliverable:** Completed security policy customised to match the customer's requirements



Network security audit

> "Do you know what is being added to your network?"
> Designed to gain an understanding of what is there and how it is put together with a focus on security
> A basic audit including; kit lists, configurations, connections
> Network capture only to look for types of traffic, P2P, IM traffic
> Allows a company to gain control back where networks have evolved
> Use automated tools/checklists to review configs or best practice
> **Deliverable:** Summary report on the state of the network
  – What is there
  – Generalisations about what it is, or is not doing
  – Noted issues observed

Security design audit

> In depth review of the current environment (or output of the network audit)
  – Kit and configurations
  – LAN, WAN and perimeter design
  – Security features used and un-used
> Deliverable: In depth report providing best practice design recommendations
  – Security device positioning
  – VPN design
  – Scalability
  – Redundancy
  – Shopping list of recommendations
  – Recommended implementation processes
  – Training suggestions
  – Recommended implementation processes
  – Training suggestions

evolved

Security device review

> A customer may only have a single device, or may only have concerns about the configuration of one or two devices. Therefore they may not want to have a full audit. This review is designed to provide an in depth review on specific devices.
> What devices can be reviewed?
- Firewall policy
  - Rule set
  - Nat configuration
  - Device access
  - Additional service (IPS, VPN, AV etc)
  - Software versions
- IPS/IDS Policy
  - Software versions
  - Signature updates
  - Configuration signatures
  - Monitoring configuration (inline etc.)
  - Device access
  - Blocking functions
- VPN access policies
  - VPN design and access
  - Authentication process
  - IPSEC policies used
  - Performance issues
- Router security
  - Routers can provide many security functions, firewall, IPS, VPN (all which can be reviewed)
  - Device access
  - Routing protocol security
  - QOS
- Switch security
  - Switches can have many of the security requirements of routers
  - In addition, layer 2 functions, would be reviewed, port security, storm control etc

Installation Services

> Managed using Prince 2 methodology
> Provide installations for a wide range of security technologies
> Subject matter experts on all market leading devices
> Able to provide engineers who can look at the bigger picture, not just the security device, to integrate the solution into your network.
- Layer 2 & Layer 3
- WAN optimisation
- Content switching

Security testing services

> Vulnerability assessment
- An automated audit of the network from the inside or outside of the network
- Use of industry recognised tools to produce a report
- The report will also include an engineer summary detailing prioritising issues and identifying false positives

> Wireless testing
- A test of your network to review the security of the wireless infrastructure that would include:
  - Signal leakage
  - Encryption security
  - Authentication

> Penetration testing
- A custom designed manual audit of the network, this audit could include aspects of:
  - Vulnerability assessment
  - Wireless testing
  - External & internal testing
  - Social engineering

Management & monitoring

> Firewall management
- Adds, moves and changes (max no. set per year)
- Hardware maintenance
- Software support
- Installation of software updates (as released by manufacturer)
- Configuration backup and recovery

> IPS management
- Adds, moves and changes (max no. set per year)
- Hardware maintenance
- Software support
- Installation of software updates (as released by manufacturer)
- Installation of patches
- Configuration backup and recovery

> Managed VPN connectivity
- Site adds, moves and changes (max no. set per year)
- Hardware maintenance
- Software support
- Installation of software updates (as released by manufacturer)
- 2nd & 3rd line remote user VPN support
- Configuration backup and recovery

Security training

> Administrator training
> End user training

Primary technologies supported

Security technologies

- Identity
  - 802.1x
  - NAC (Network Access Control)
  - AAA
  - 2 factor authentication
- Access
  - WAN
  - LAN Security
  - Wireless
  - VPN
  - Site to Site
  - SSL
  - Remote
- Protection
  - Firewall
  - Integrated Service Routers
  - Endpoint security
- Monitoring
  - IDS/ IPS
  - Content monitoring
  - AV/ Spam filtering
  - Security agent

Network edge technologies

- WAN optimisation
- Content switching

Evolved Information Solutions
Feltimores Park, Chalk Lane, Harlow
Essex, CM17 0PF

T: +44 (0) 1279 437 444 F: +44 (0) 1279 437 445
www.evolvedis.com