MICRODASYS

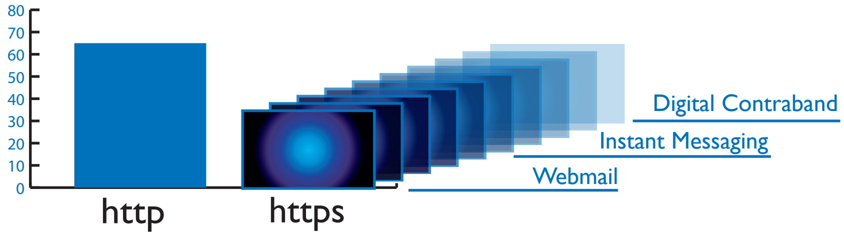
THE NEED TO CONTROL, INSPECT AND MANAGE ENCRYPTED WEBTRAFFIC

If you allow encrypted ("https", "SSL", "TLS") internet traffic in and out of your intranet you are vulnerable to viruses, malicious code and other common attacks.

SSL Encryption is one of the cornerstones of todays eCommerce and business to business applications. However, it is impossible for firewalls and content scanners to inspect encrypted webtraffic, hence making encryption an easy backdoor for hackers. Weak registration processes and ineffective revocation checking of digital certificates only add to the problem.

> *"...since SSL traffic is encrypted, the use of SSL can actually detract from overall network security.*
> *"It is impossible for security devices to inspect SSL traffic to determine if the data conforms to an organisation's security policy.*
> *Intrusion Detection Systems (IDSs) are rendered useless since they rely on examining the traffic for known attack signatures."*
>
> - Steven McLeod
> Australian Defence Signals Directorate

On average, more than 30% of webtraffic is encrypted. Hence, at least one third of the traffic that is entering and leaving your network is not inspected, and/or subject to any security policy.



SCIP ENCRYPTED CONTENT SECURITY

THE SOLUTION

SCIP Encrypted Content Security software enables you to secure your network from attack by encrypted web traffic. SCIP lets you set, and automatically apply, security policies to all encrypted inbound and outbound Internet traffic. The data is decrypted, forwarded to your content scanner for inspection, then re-encrypted and sent to its destination. All digital certificates are checked for validity (common name, expiration date, revocation status, valid issuer CA). All security policies that apply to standard http traffic, now also apply to SSL encrypted traffic.

Unlike simple "SSL bridging" or a "reverse proxy" that can not protect your internal network from encrypted attacks, SCIP is defending you from the inside.

FEATURE HIGHLIGHTS

Decryption and encryption of all inbound and outbound SSL ("https") traffic.
Security policy enforcement, even if the traffic is encrypted.
All certificates are inspected and allowed or denied at the gateway level, based on security policies, not the discretion of the client user.
Automatic revocation checking with CRL and OCSP support.
Extensive exception handling and incident management capabilities.
Supports unlimited, multiple accounts with role-based, multi-admin administration.

TECH SPECS

SUN Solaris (SPARC), Win 2000 / 2003 Server, Linux
Support for ICAP and Proxy mode
SSLv2, SSLv3, TLSv1 with all ciphers
SSL hardware accelerator support
SSL enabled, web based administration console
Scaleable to any network size with HA and LB support
LDAP and Active Directory support

MICRODASYS
BRIDGING THE GAP IN CONTENT SECURITY

Microdasys Inc.
2620 Regatta Drive, Suite 102
Las Vegas, NV 89128, USA

Vox: +1 702 240 5275
Fax: +1 702 240 5310

www.microdasys.com
info@microdasys.com