

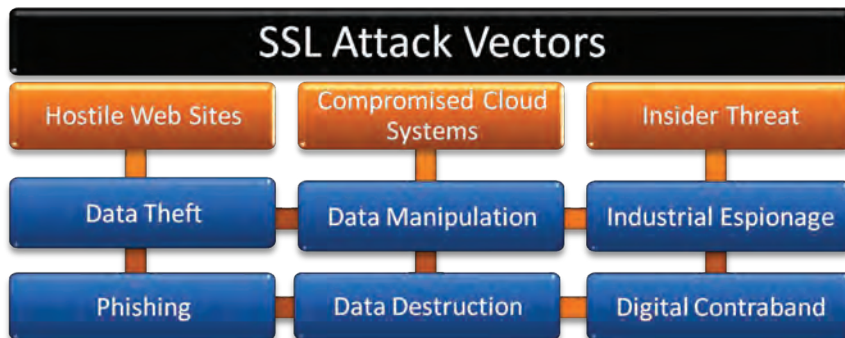


# SCIP SSL Content Proxy 3.4

*Essential gateway protection from encrypted web threats*

Cloud computing and eCommerce make SSL encryption a necessity to protect confidential data. For internet criminals however, SSL encryption provides the easiest attack vector to circumvent enterprise security scanners and policies, as it establishes an uncontrollable tunnel between the client desktop and the SSL server. Company insiders can use SSL to create their very own "Black VPN" and practically send and receive data to and from any system in the world without detection.

**SCIP SSL Content Proxy** provides immediate enterprise wide protection at the gateway from hostile or compromised internet SSL hosts and effectively stops company insiders that try to circumvent enterprise security policies through SSL. As the market leading SSL Content Proxy, it automatically detects and blocks access to SSL servers with untrustworthy digital certificates and decodes the datastream for inspection by Anti Virus, Data Loss Prevention and other content security scanners.



## KEY FEATURES

### ENTERPRISE VALIDATION AUTHORITY

Inspects and validates digital server certificates by Expiration Date, URL-Common Name Match, Revocation Status, Trusted Issuer

### SSL DECRYPTION AND ENCRYPTION

Enables existing content scanners to inspect SSL data and apply identical security policies to both, SSL and non-SSL web traffic.

### INCIDENT MANAGEMENT

Extensive administration features for easy exception handling and white and blacklisting

### CLUSTER SUPPORT

Enables central administration of multiple SCIP servers, central issuance and management of certificates and creation of unique incident ticket IDs.

## PROTECTION POINT

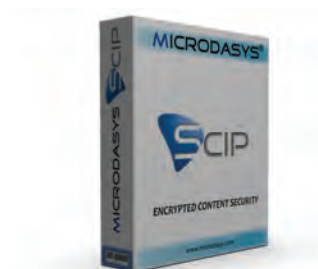
- Internet Gateway

## THREAT PROTECTION

- Encrypted Web Traffic
- Invalid and bogus digital server certificates
- Revoked Certificates
- Black VPNs
- All web threats associated with unencrypted web traffic

## KEY BENEFITS

- Inspects all server certificates at the gateway
- Blocks access to SSL encrypted web servers with expired, revoked or self signed certificates
- Removes decision authority from the user
- Decrypts SSL web traffic for inspection by content security devices
- Extensive Management, Whitelisting and Exception Handling
- Maximises ROI of existing security infrastructure



## NETWORK INTEGRATION

The SCIP SSL Content Proxy is designed to easily integrate into small to very large scale and complex network infrastructures. The software is continuously tested with leading content security devices to ensure seamless integration and interoperability.

NETWORK INTERFACES AND PROTOCOLS	
PROTOCOLS	HTTPS, HTTP 1.1, HTTP, WCCP v2, ICAP
NETWORKMODE	Proxy, Transparent Proxy, ICAP
AUTHENTICATION	Basic, NTLM v1, NTLM v2
ENCRYPTION	SSL v2, SSL v3, TLS v1
DIRECTORY SUPPORT	LDAP, Active Directory

MINIMUM SYSTEM REQUIREMENTS			
PLATFORM	WINDOWS	LINUX	SOLARIS
OPERATING SYSTEM	2003 Server or higher	Kernel 2.4, glibc 2.2 or higher <b>RECOMMENDED:</b> RedHat Enterprise Linux AS 4 Novell SUSE Linux Enterprise Server 10	Solaris 8, 9, 10 (SPARC)
CPU	Pentium IV	Pentium IV	UltraSPARC IIIi
	<b>RECOMMENDED:</b> Quad Core System or better		
RAM	512 MByte		
	<b>RECOMMENDED:</b> 2 GByte or better		

## MICRODASYS

Microdasys develops leading edge content security software that enable enterprises to securely and successfully conduct business over the internet.

Microdasys was first to market with SCIP, the first SSL Content Proxy that set the standard for SSL encrypted content scanning.

## COMPLEMENTARY PRODUCTS

Microdasys XSG Gateway  
Web 2.0, XML and Web Services  
Content Security Software.

## CONTACT

Americas, Asia Pacific:

Microdasys Inc.  
385 Pilot Rd., Ste A  
Las Vegas, NV 89119

Phone: +1-702-577-2889  
eMail: sales@microdasys.com

Europe, Middle East, Africa:

Microdasys Inc.  
Geisenhausener Str. 11a  
81379 Munich, Germany

Phone: +49-89-374 18 778  
eMail: saleseu@microdasys.com

[www.microdasys.com](http://www.microdasys.com)