The need for strong secure networks has never been more compelling than today.
Why sell Security?

Why Sell Cisco?

Why Security Matters More Than Ever.........................03
Why Sell Security?.........................................................04
Why Comstor?.................................................................06
A Solution To Suit Every Customer.............................07
Why Security Matters More Than Ever

Network Security is an essential and necessary consideration, especially for businesses considering a new or upgrade in ICT infrastructure. The following are key reasons why all businesses need reliable network security:

Maintain Reputation
Today's security challenges put organisations at risk. One data breach can ruin a positive reputation with customers, investors and the marketplace.

Meet Regulatory Compliance Requirements
Every company is subject to some sort of regulation, often related to privacy and protection of customer information. Compliance dictates strong and thoughtful security.

Protect Business Information
Information is at the core of every organisation. The availability, integrity and confidentiality of critical assets must be protected wherever they reside.

Optimise Business Operations
Most companies have difficulty determining the cost of a day's downtime because of the number of direct and indirect factors that must be considered. Among these are lost productivity, loss of business and loyalty, impact on reputation and brand, cost of repair and recovery, and potential legal liability.
Why Sell Security?

Good network security opens doors as well as locking them. In addition to ensuring company assets and data remain safe from interference, appropriate security measures can liberate the workforce to produce a more mobile, effective, yet secure environment for your customers, making their operations more productive – and profitable.

Modern business needs demand that staff can access networks anywhere, anytime and the rise of collaborative network devices are increasingly available to make this a more productive way of working a reality. But, with new opportunities for business, come new threats from hackers and other criminals. Attacks are becoming more intrusive and more innovative and with higher impact, with the sole aim of the attacker to cause maximum damage or optimise their revenue opportunities.

Why Sell Cisco Security?

The Cisco Self-Defending Network provides the most comprehensive, end-to-end approach to network security in the industry. Their world-class solutions not only provide best-of-breed capabilities and features, but also ensure a level of security not available anywhere else, through:

Integration: Critical security functions have been woven into Cisco’s entire line of appliances and network devices, as well as into all of their critical business applications and services, such as unified communications and Data Centre.
Collaboration: An additional layer of security is achieved through unprecedented collaboration between security and network devices, and between different security devices and solutions.

Adaptability: The ability to identify a security event anywhere on the network, and share that information across the network, allows Cisco solutions to dynamically adapt the network’s overall security profile to real-time threats and events.

This integrated, collaborative and adaptive approach to security provides comprehensive, in-depth defense and maximum risk reduction, whilst lowering total cost of ownership – making it the ideal choice for securing networked environments.

For organisations needing to reduce their security and compliance IT risk, IT administrative burden and total cost of ownership, Cisco has the answer. Unlike other security vendors, only Cisco offers the benefits of a combined best-of-breed and systems approach which includes:

- Best-of-breed security addresses emerging threats
- Systems approach addresses pervasive threats, helps to meet compliance regulations, and enables cost-effective management
- History of security innovations since 1995
- Network security market leadership position in firewall technology, virtual private networking, email and web security, and intrusion prevention
- Award-winning products
- Customer validation and success.
Why Comstor?
Cisco offers the broadest and deepest product and services portfolios, and its partners are empowered to design and implement a solution customised to each client’s unique requirements. In addition to a wealth of value-added services, Comstor is the only Distributor currently selling all of Cisco’s security offerings.

Not only do we have the most comprehensive range of Cisco security solutions, we have the most in-depth knowledge and experience of how they work, and how best to deploy them. We know the markets – and the strategies to penetrate and profit from them. If lack of experience is what is currently holding you back, look no further than Comstor – whether your business needs professional services or product training.

The very sophistication of modern network security leads to complexity in planning and deployment. As well as the latest Cisco security technology, Comstor’s Professional Services team has the experience and expertise that your business can call on to ensure every deployment is a success.

In addition, security is a highly emotive issue, with business attitudes varying wildly. Clients often adopt one of two extreme positions in the face of security threats. The first type adopts a laissez faire attitude, believing that their business does not need network security at all and has no real understanding of the potential dangers involved. The second type reacts by completely isolating the network, although their network is safe from attack, it is also cut off from customers, prospects and business opportunities.

A third, more realistic approach, is to view security as an enabling service to manage a productive and secure work force. Clients should be happy with the level of risk exposure to the company and set measures for the necessary steps to protect assets and investments, but request security that allows their employees to be secure on laptops, mobile devices or remote access (VPN), enabling a work anytime anywhere approach.
All three groups are potential clients, and each needs a different approach and strategy to convert into a profitable engagement. This is another area where Comstor can help – with free pre-sales, including planning and advice on client strategy. In short, we offer the added value to help you make a success of the network security market. Take a look at this reference guide and see how network security can grow your business.

A Solution To Suit Every Customer

The Cisco range of network security solutions is comprehensive enough to ensure that all your customers’ businesses can benefit. Below is a comparison chart, illustrating the suitability of different products and services for different enterprises:

<table>
<thead>
<tr>
<th>Description</th>
<th>Product Group</th>
<th>Product Range</th>
<th>SMB</th>
<th>MT</th>
<th>Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-technology Security Appliance</td>
<td>ASA5500</td>
<td>ASA5505</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ASA5510</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ASA5520</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ASA5540</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ASA5550</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ASA5580</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intrusion Prevention System</td>
<td>IPS</td>
<td></td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Router Security</td>
<td>ISR</td>
<td>3800</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2800</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1861</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>7600</td>
<td></td>
<td>●</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ASR</td>
<td></td>
<td>●</td>
<td></td>
</tr>
</tbody>
</table>
## Why sell Security/Why Sell Cisco?

<table>
<thead>
<tr>
<th>Description</th>
<th>Product Group</th>
<th>Product Range</th>
<th>SMB</th>
<th>MT</th>
<th>Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Router Security</strong></td>
<td>ASR</td>
<td>7301</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>7200</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3800</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2800</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1800</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>800</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Switch Security</strong></td>
<td></td>
<td>6500</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Email, Web, Content Security</strong></td>
<td>Email Spam blocker</td>
<td>SVB-BLKR</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Email IronPort</td>
<td>C-Series</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Web IronPort</td>
<td>S-Series</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>ACE Firewall</td>
<td>ACE</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td><strong>Virtual Private Networks</strong></td>
<td>IPSEC VPN</td>
<td>VPN</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>SSL VPN</td>
<td>VPN</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td><strong>End-Point Security</strong></td>
<td>CSA</td>
<td>CSA</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NAC</td>
<td>NAC3300</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td><strong>Management</strong></td>
<td>MARS</td>
<td>CS-MARS</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CSM</td>
<td>CSM</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Secure ACS</td>
<td>CSACS</td>
<td>●</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Getting Started

The Comstor Advantage..................................................09
Get In Contact..................................................................10
The Comstor Advantage

Get Unrivalled Expertise
Network security should be a highly profitable area for you and your company. Comstor has a team of security experts, here to help you make the most from the opportunities this market presents.

Our in-depth knowledge and experience of Cisco solutions, complements our unrivaled portfolio of Cisco security solutions. But – as you will have seen in this booklet – that just scratches the surface of the added value we can bring to your organisation – and your clients.

Get Training
Gain the knowledge you need to succeed – and provide more value added services to your clients. Comstor offers a comprehensive range of training programmes to keep your organisation, and your customers, not only up-to-date, but also ahead of the pack.

As an authorised Cisco Learning Solutions Provider (CLSP), we can help fast-tracking to Premier, Silver and Gold Partner Certifications, by working with you on building a customised training plan to help achieve the required technology specialisations.

And by offering training, such as Security, Data Centre, Unified Communications, Wireless, Routing and Switching to your clients, you can add to your revenues, too.

Get Professional Services
Design installation, consultation, network health checks, network audits and project management – these are all projects that our team of experts are more than qualified to tackle.

Comstor Professional Services is an opportunity for you to add to your offering – and profitability, without adding to your overheads. If you spot an opportunity, but lack the qualifications or experience for a specific project engagement, our team can provide them.
Get In Contact

We hope that you are convinced we can bring real value and profits to your business. If you want to find out how to take advantage of our solutions and services – or simply need clarification on any area – please select the appropriate contact from the following pages.

### Useful Names and Contacts

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comstor Switchboard</td>
<td>Tel: 01285 647000</td>
<td></td>
</tr>
<tr>
<td>Comstor Sales</td>
<td>Tel: 01285 647001 Email: <a href="mailto:sales@comstor.co.uk">sales@comstor.co.uk</a></td>
<td></td>
</tr>
<tr>
<td>Clive Hailstone</td>
<td>Sales Director</td>
<td>Email: <a href="mailto:clive.hailstone@comstor.co.uk">clive.hailstone@comstor.co.uk</a></td>
</tr>
<tr>
<td>Simon Tyler</td>
<td>Sales Manager</td>
<td>Email: <a href="mailto:simon.tyler@comstor.co.uk">simon.tyler@comstor.co.uk</a></td>
</tr>
<tr>
<td>Sarah Day</td>
<td>Team Leader</td>
<td>Email: <a href="mailto:sarah.day@comstor.co.uk">sarah.day@comstor.co.uk</a></td>
</tr>
<tr>
<td>Jay McDonald</td>
<td>Security Product Manager</td>
<td>Email: <a href="mailto:jay.mcdonald@comstor.co.uk">jay.mcdonald@comstor.co.uk</a></td>
</tr>
<tr>
<td>Justin Turner</td>
<td>Business Manager</td>
<td>Email: <a href="mailto:justin.turner@comstor.co.uk">justin.turner@comstor.co.uk</a></td>
</tr>
<tr>
<td>Dominic Roden</td>
<td>UC Product Manager</td>
<td>Email: <a href="mailto:dominic.roden@comstor.co.uk">dominic.roden@comstor.co.uk</a></td>
</tr>
<tr>
<td>Ian Barough</td>
<td>Smartnet Product Manager</td>
<td>Tel: 07775 755828 Email: <a href="mailto:ian.barough@comstor.co.uk">ian.barough@comstor.co.uk</a></td>
</tr>
</tbody>
</table>
# Getting Started

## Training

<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Matthew Hathorn</td>
<td><a href="mailto:matthew.hathorn@comstor.co.uk">matthew.hathorn@comstor.co.uk</a></td>
</tr>
<tr>
<td>Sarah Godwin</td>
<td><a href="mailto:sarah.godwin@comstor.co.uk">sarah.godwin@comstor.co.uk</a></td>
</tr>
<tr>
<td>Becky Chinnick</td>
<td><a href="mailto:rebecca.chinnick@comstor.co.uk">rebecca.chinnick@comstor.co.uk</a></td>
</tr>
<tr>
<td>General Enquiries</td>
<td><a href="mailto:train@comstor.co.uk">train@comstor.co.uk</a></td>
</tr>
</tbody>
</table>

## Professional Services

<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>John Saunders</td>
<td><a href="mailto:john.saunders@comstor.co.uk">john.saunders@comstor.co.uk</a></td>
</tr>
<tr>
<td>General Enquiries</td>
<td><a href="mailto:techassist@comstor.co.uk">techassist@comstor.co.uk</a></td>
</tr>
</tbody>
</table>

## Marketing

<table>
<thead>
<tr>
<th>Name</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warwick Taylor</td>
<td><a href="mailto:warwick.taylor@comstor.co.uk">warwick.taylor@comstor.co.uk</a></td>
</tr>
<tr>
<td>Victoria Reglar</td>
<td><a href="mailto:victoria.reglar@comstor.co.uk">victoria.reglar@comstor.co.uk</a></td>
</tr>
<tr>
<td>Kym Marshall</td>
<td><a href="mailto:kym.marshall@comstor.co.uk">kym.marshall@comstor.co.uk</a></td>
</tr>
</tbody>
</table>
Customer Requirements

Register Now
Register Now
Comstor’s Reseller partners have access to support, tools and programmes that ensure success in Advanced Technology. Comstor can help you quickly and easily respond to the demands of your customers to provide complete networking solutions using best-of-breed products and services.

To become a Comstor Reseller, you must register by filling in an application form that can be downloaded from: www.westcongroup.com/sites/comstor-uk/partners/reseller-partners/become-a-reseller

Are you a Cisco Partner?
One condition of being a Comstor Reseller Partner is that your business must also be a Cisco Partner. If you are not, don’t worry - becoming one is a straightforward process, and well worth the small effort involved in order to enjoy the expertise, training and professional services Comstor has to offer.

Part one:
a. Go to Cisco.com registration:
b. Register with Cisco, Step One of Three: fill in the requested information and click on “submit”
c. Cisco.com Registration, Step Two of Three: Fill out your interests, hit “submit” or “skip this step” as this is not mandatory
d. Complete Registration, Step Three of Three: You will receive an email from Cisco, with the request to activate your account by clicking on the URL in the email. After doing so, you will receive confirmation of your account. You now have guest-access.
Comstor Customer Requirements

Part two:

a. Review the Partner Registration User Guide:
b. Apply to the Registered Partner Program:
   http://tools.cisco.com/WWChannels/IPA/welcome.do
c. Review and accept the terms of the Indirect Channel Partner Agreement (ICPA):
   www.cisco.com/web/partners/pr11/pr193/requirement.html
d. Submit the application.

Obtaining Approval
Cisco will instantly review your application and you will be notified within 24 hours. If approved, your company will receive Registered Partner status, be granted partner-level access to Cisco.com, and be eligible to participate in the Cisco Channel Partner Program – as well as apply as a Comstor Reseller. Please note that status as a registered partner is valid for 12 months and must be renewed annually.

Associate people with your company
Once registered as a Cisco Registered Reseller, you can use Partner Self-Service Portal (PSS):
http://tools.cisco.com/WWChannels/GETLOG/login.do to register your company’s details, partner tool administrators and people associated with your company. You can download a User Guide and Quick Reference guide from this portal as well.

Receive additional rebates
As a Cisco Registered Reseller, you are eligible to enroll onto the Registered Reseller Payment Program:
www.ciscopartners.com/rrpp/home.aspx?disti=comstor. With this programme, you can enjoy further financial rewards for selling products and services.
SMB
Product Guide

Small Business Pro - UTM ...................................................... 14
Firewall (ASA) ........................................................................ 16
Intrusion Prevention Systems ............................................... 20
Cisco Router Security (ISR) ................................................ 23
Content Security (CSC Module) .......................................... 25
Virtual Private Networks (VPN) .......................................... 27
Cisco Spam and Virus Blocker .......................................... 31
Cisco SA 500 Series Security Appliances

Small Business Pro – UTM

Cisco SA 500 Series Security Appliances are all-in-one security solutions for businesses with fewer than 100 employees. Designed specifically for small business, they combine firewall, virtual private network (VPN), and optional email and web security capabilities. Whether in the office or working remotely, your employees can securely access the resources they need, while your business is protected from unauthorised access and Internet threats.

- **All-in-one device**: Combines firewall, email and web security, and secure access in one box.
- **Secure wireless and remote access**: Easily allow mobile workers and branch offices to remotely and securely access the network with flexible and easy to use built-in VPN support.
- **Low overhead**: Reduce costs associated with deployment and ongoing management and monitoring of the security solution by using a single, easy-to-install, easy-to-use solution.
- **Affordable service coverage**: The Cisco Small Business Pro Service delivers service value and peace of mind at a price you can afford.
Optional email and web security capabilities provide additional layers of security:

- Trend Micro ProtectLink Gateway is a cloud-based service that provides strong, automatically updated email and web security to help block spam, viruses, spyware, phishing, and inappropriate web browsing.
- The optional VeriSign Identity Protection (VIP) support provides an easy and effective second level of authentication before granting remote network access.

Part Codes

<table>
<thead>
<tr>
<th>Part Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA520-K9</td>
</tr>
<tr>
<td>SA520W-K9</td>
</tr>
<tr>
<td>SA540-K9</td>
</tr>
</tbody>
</table>

Firewall (ASA)

Overview

The firewall protects the resources of a private network from unauthorised access to applications, networks and data by internal or external users. Cisco firewall solutions provide integrated network security services, including:

- Stateful packet inspection
- Application-layer and protocol inspection
- Inline intrusion prevention
- Rich multimedia and voice security.

Products

Cisco offers multiple firewall solutions, including Cisco ASA 5500 Series Adaptive Security Appliances, Cisco IOS Firewall on Cisco routers, and Cisco Catalyst 6500 Series Firewall Services Module (FWSM) for environments needing greater scalability.

Benefits

- Enables organisations of all sizes to protect their critical networks from unauthorised access
- Protects applications and network services from attack with advanced application inspection capabilities
- Offers multiprotocol support to enable dynamic routing for improved network reliability and performance
- Makes it easy to centrally administer and manage all firewall solutions using Cisco Security Manager
- Provides an extremely resilient security infrastructure with high-availability capabilities
- Maximises network uptime, resulting in improved productivity
- Enables secure deployment of next-generation unified communications and multimedia applications.
The following figure shows how Cisco firewall solutions fit in a network:

![Diagram showing network architecture with Cisco ASA 5500 Series Adaptive Security Appliances]

**Cisco ASA 5500 Series Adaptive Security Appliances**

**Overview**

The Cisco ASA 5500 Series is a UTM (Unified Threat Management) appliance, meaning it is not just a firewall, but converges full-featured, high-performance firewall (including application firewall services), intrusion prevention, content security, IPsec/SSL VPN, and secure unified communications technologies in a single, easy-to-use security appliance.

Now you can provide industrial-strength security to networks, while reducing cost and complexity by converging multiple security functions into a high-performance appliance. Cisco ASA 5500 Series integrated security platforms provide the scalability to meet the security needs of businesses of all sizes.
Benefits

- Reduces cost and complexity by providing firewall, SSL and IPsec VPN, intrusion prevention, network content security services, and secure unified communications on a single hardware platform
- Delivers high performance with multiple security services for the same cost as a firewall alone
- Adapts to new security threats
- Provides thorough remote-office protection to protect data and voice for remote workers
- Provides an integrated threat protection solution on a single device, for both SSL and IPsec VPN connectivity.

Cisco ASA 5500 Series Firewall Edition Bundles

<table>
<thead>
<tr>
<th>Model</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA5505-BUN-K9</td>
<td>ASA 5505 Appliance with SW, 10 Users, 8 ports, 3DES/AES</td>
</tr>
<tr>
<td>ASA5505-50-BUN-K9</td>
<td>ASA 5505 Appliance with SW, 50 Users, 8 ports, 3DES/AES</td>
</tr>
<tr>
<td>ASA5505-UL-BUN-K9</td>
<td>ASA 5505 Appliance with SW, UL Users, 8 ports, 3DES/AES</td>
</tr>
<tr>
<td>ASA5505-SEC-BUN-K9</td>
<td>ASA 5505 Sec Plus Appliance with SW, UL Users, HA, 3DES/AES</td>
</tr>
<tr>
<td>ASA5510-BUN-K9</td>
<td>ASA 5510 Appliance with SW, 5FE, 3DES/AES</td>
</tr>
</tbody>
</table>
## Cisco ASA 5500 Series Firewall Edition Bundles

<table>
<thead>
<tr>
<th>Model</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA5510-SEC-BUN-K9</td>
<td>ASA 5510 Security Plus Appl with SW, HA, 2GE+3FE, 3DES/AES</td>
</tr>
<tr>
<td>ASA5520-BUN-K9*</td>
<td>ASA 5520 Appliance with SW, HA, 4GE+1FE, 3DES/AES</td>
</tr>
<tr>
<td>ASA5540-BUN-K9*</td>
<td>ASA 5540 Appliance with SW, HA, 4GE+1FE, 3DES/AES</td>
</tr>
<tr>
<td>ASA5550-BUN-K9*</td>
<td>ASA 5550 Appliance with SW, HA, 8GE+1FE, 3DES/AES</td>
</tr>
<tr>
<td>ASA5580-20-8GE-K9*</td>
<td>ASA 5580-20 Appliance with 8 GE, Dual AC, 3DES/AES</td>
</tr>
<tr>
<td>ASA5580-40-BUN-K9*</td>
<td>ASA 5580-40 Appliance with 2 GE Mgmt, Single AC, 3DES/AES</td>
</tr>
<tr>
<td>ASA5580-40-8GE-K9*</td>
<td>ASA 5580-40 Appliance with 8 GE, Dual AC, 3DES/AES</td>
</tr>
<tr>
<td>ASA5580-40-10GE-K9*</td>
<td>ASA 5580-40 Appliance with 4 10GE, Dual AC, 3DES/AES</td>
</tr>
<tr>
<td>ASA5580-20-BUN-K9*</td>
<td>ASA 5580-20 Appliance with 2 GE Mgmt, Single AC, 3DES/AES</td>
</tr>
<tr>
<td>ASA5580-20-4GE-K9*</td>
<td>ASA 5580-20 Appliance with 4 GE, Dual AC, 3DES/AES</td>
</tr>
</tbody>
</table>

* Scale beyond SMB and fit within the mid and enterprise networks.
Intrusion Prevention Systems

Overview

The most trusted and widely-deployed IPS in the world, Cisco Intrusion Prevention System (IPS) provides proven protection against over 30,000 threats to help customers secure their confidential data and meet ever-increasing compliance mandates.

Cisco IPS accurately identifies, classifies, and stops malicious traffic, including worms, spyware/adware, network viruses and application abuse, before they affect business continuity. Cisco Anomaly Detection stops zero-day attacks before signature updates are available.

In addition, Cisco IPS collaborates with other key network components for end-to-end network-wide protection. Threat information is shared between Cisco IPS and the host-based IPS Cisco Security Agent and Cisco wireless controller. Available as a dedicated appliance, Cisco IPS is also integrated into Cisco firewall, switch, and router platforms for maximum protection and deployment flexibility.
Benefits
Advanced IPS technology is based on 12 years of IPS innovation and features the following specific features and benefits for your customers:

- Proven protection against more than 30,000 threats
- Tight integration with host-based IPS (Cisco Security Agent) for end-to-end protection
- Tight integration with Cisco Wireless Controller for secure wireless deployments
- Simplified management with Cisco IPS Manager Express for smaller organisations
- Enterprise-class policy management with Cisco Security Manager and Cisco Security Monitoring, Analysis and Response System (Cisco Security MARS)
- Protects against more than just virus outbreaks, such as attacks targeted against a company’s information
- Helps prevent against severe loss due to disruptions, theft, or defacement caused by compromised servers
- Stops worm and virus outbreaks at the network level, before they reach the desktop.

Solutions
Flexible deployment options include:

- Cisco IPS 4200 Series Sensors as standalone IPS appliances
- Integrated Cisco ASA 5500 Series Advanced Inspection and Prevention Security Services Modules (AIP SSM10, AIP SSM20, and AIP SSM40) provide intrusion prevention, firewall and VPN in a single, easy-to-deploy platform
- Cisco AIM-IPS, NME-IPS, or Cisco IPS Sensor Software for integrated services routers
- Cisco Catalyst 6500 Series Intrusion Detection System (IDSM-2) Modules
- Cisco Adaptive Wireless IPS protects the wireless signal from being hijacked by an intruder while Cisco’s network IPS prevents authenticated users (with a legitimate user name and password) from performing malicious or unauthorised activity, such as stealing confidential data.
## Cisco ASA 5500 Series Firewall Edition Bundles

<table>
<thead>
<tr>
<th>Model Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA5505-50-AIP5-K9</td>
<td>ASA 5505 50-user, AIP SSC-5, SW, 3DES/AES</td>
</tr>
<tr>
<td>ASA5505-U-AIP5P-K9</td>
<td>ASA 5505 unlimited user, AIP-SSC-5, SW, Sec Plus, 3DES/AES</td>
</tr>
<tr>
<td>ASA5510-AIP10-K9</td>
<td>ASA 5510 Appliance with AIP-SSM-10, SW, 5FE, 3DES/AES</td>
</tr>
<tr>
<td>ASA5510-AIP10SP-K9</td>
<td>ASA 5510 with AIP-SSM-10, 2GE+3FE, SW, HA,3DES/AES, SEC PLUS</td>
</tr>
<tr>
<td>ASA5510-AIP20SP-K9</td>
<td>ASA 5510 with AIP-SSM-20, 2GE+3FE, SW, HA,3DES/AES, SEC PLUS</td>
</tr>
<tr>
<td>ASA5520-AIP10-K9</td>
<td>ASA 5520 Appliance w/ AIP-SSM-10, SW, HA, 4GE+1FE, 3DES/AES</td>
</tr>
<tr>
<td>ASA5520-AIP20-K9</td>
<td>ASA 5520 Appliance w/ AIP-SSM-20, SW, HA, 4GE+1FE, 3DES/AES</td>
</tr>
<tr>
<td>ASA5540-AIP20-K9</td>
<td>ASA 5540 Appliance w/ AIP-SSM-20, SW, HA, 4GE+1FE, 3DES/AES</td>
</tr>
<tr>
<td>ASA5520-AIP40-K9</td>
<td>ASA 5520 Appliance w/ AIP-SSM-40, SW, HA, 4GE+1FE, 3DES/AES</td>
</tr>
<tr>
<td>ASA5540-AIP40-K9</td>
<td>ASA 5540 Appliance w/ AIP-SSM-40, SW, HA, 4GE+1FE, 3DES/AES</td>
</tr>
</tbody>
</table>

Please refer to:

Cisco Router Security (ISR)

Overview
It is crucial to secure an organisation’s critical network infrastructure, including Cisco routers – and Cisco Router Security (ISR) adds important security features that result in an excellent return on investment (ROI). Cisco Router Security provides the following capabilities to your customers’ branch routers:

- Site-to-site VPN
- IPsec and SSL remote-access
- VPN
- Common Criteria/EAL4-certified stateful firewall
- Content filtering
- Inline intrusion prevention
- Network Admission Control (NAC)
- Security management.

Like any good business continuity design, Cisco Router Security includes encrypted dual WAN links, remote network access during disasters, and stateful failover of critical services. In addition, Cisco Router Security can enable other network services such as secure unified communications (voice and video) and secure wireless LAN.

Benefits
Maximises ROI by greatly increasing router value:

- Enables wireless LAN and unified communications services such as voice and video
- Offers a secure, cost-effective, easy-to-manage, and scalable solution for site-to-site business communications
- Enables compliance with US federal and state data and network privacy laws (eg, Payment Card Industry [PCI] requirements)
- Simplifies management burden by converging security and other services in a single network device.
The following figure shows how the Cisco Router Security fits in the network:

Selected Part Numbers and Ordering Information
Cisco 1800, 2800, 3800, 7200 Series and 7301 router platforms. ASR 1000 (Supports full feature set) Cisco 800, Series router platform includes all firewall features with the exception of authentication proxy. For a list of part codes please go to www.cisco.com/go/routersecurity
Content Security (CSC Module)

Content Security on the Cisco ASA 5500 Series

Overview

The Cisco ASA 5500 Series Adaptive Security Appliance with the Content Security and Control Security Services Module (CSC-SSM) is an all-in-one threat defense appliance that takes advantage of Cisco’s leadership in firewall and VPN technology and Trend Micro’s expertise in anti-malware and gateway content security.

Together, they allow network and security administrators to accurately identify, classify and stop malicious traffic, including worms, spyware/adware, network viruses, and application abuse, before they affect business continuity.

Filtering content at the gateway provides a consistent layer of content protection for company-owned and guest computers, regardless of the type or status of antivirus protection on those computers. The CSC-SSM provides a comprehensive set of content security services, including antispam, URL filtering and blocking, antiphishing and antispyware, in addition to antivirus services.
Benefits
The CSC-SSM solution is low-maintenance – updates and filtering are carried out automatically, once setup is complete. It protects desktops, servers, and email, blocking 90% of spam and 100% of traffic to and from disreputable sites. As a result, unwanted content does not clutter the network or system, and bandwidth is not wasted on unnecessary data. Other benefits include:

- All-in-one appliance
- Minimises day-to-day management
- Better operational efficiency than separate solutions
- Provides Firewall and VPN security
- URL and email filtering
- Protection from viruses, spam, spyware and phishing
- Fully configurable spam filters.

### Cisco ASA 5500 Series Content Security Edition Bundles

<table>
<thead>
<tr>
<th>Bundle Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA5510-CSC10-K9</td>
<td>ASA 5510 Appl w/ CSC10, SW, 50 Usr AV/Spy, 1 YR Subscript</td>
</tr>
<tr>
<td>ASA5510-CSC20-K9</td>
<td>ASA 5510 Appl w/ CSC20, SW, 500 Usr AV/Spy, 1 YR Subscript</td>
</tr>
<tr>
<td>ASA5520-CSC10-K9</td>
<td>ASA 5520 Appl w/ CSC10, SW, 50 Usr AV/Spy, 1 YR Subscript</td>
</tr>
<tr>
<td>ASA5520-CSC20-K9</td>
<td>ASA 5520 Appl w/ CSC20, SW, 500 Usr AV/Spy, 1 YR Subscript</td>
</tr>
</tbody>
</table>
Virtual Private Networks (VPN)

Site-to-Site VPNs

Overview
VPNs enable the deployment of fast, reliable and secure connectivity for remote offices, business partner locations, and other branch sites. The data, voice and video communications between these locations are kept confidential across untrusted networks. Cisco offers a variety of VPN solutions that provide cost-effective and highly manageable secure connectivity. They all provide integrated, threat-protected VPN features that guard against malware and hackers, without the cost and complexity of deploying additional security equipment.

Cisco offers multiple VPN technologies, including IPsec VPN, Dynamic Multipoint VPN (DMVPN), and Group Encrypted Transport VPN (GET VPN), integrated on a single platform, reducing equipment cost and management complexity.

Solutions
Cisco VPN solutions include:
Cisco routers: Cisco’s most advanced site-to-site VPN solution plus integrated remote-access, firewall, intrusion prevention system (IPS) and content security services.

Cisco ASA 5500 Series: Cisco’s most advanced remote access VPN solution, delivering integrated site-to-site VPN, remote-access VPN, firewall, IPS and content security services.

Cisco Catalyst 6500 Series: Cisco’s most scalable VPN platform plus integrated firewall and IPS services.
Benefits

Securely connect office locations utilising the Internet to decrease costs and increase flexibility:

- Support for multiple VPN technologies from a single platform reduces cost and complexity
- Enables VPN services customised to the deployment environment
- Delivery of any application, including voice and video, to any location with a high level of integrity
- Defend network threats without the need for additional security equipment.

### Cisco ASA 5500 Series VPN Edition Bundles

<table>
<thead>
<tr>
<th>Model</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA5505-SSL10-K9</td>
<td>ASA 5505 VPN Edition w/ 10 SSL Users, 50 FW Users, 3DES/AES</td>
</tr>
<tr>
<td>ASA5505-SSL25-K9</td>
<td>ASA 5505 VPN Edition w/ 25 SSL Users, 50 FW Users, 3DES/AES</td>
</tr>
<tr>
<td>ASA5510-SSL50-K9</td>
<td>ASA 5510 VPN Edition w/ 50 SSL User License, 3DES/AES</td>
</tr>
<tr>
<td>ASA5510-SSL100-K9</td>
<td>ASA 5510 VPN Edition w/ 100 SSL User License, 3DES/AES</td>
</tr>
<tr>
<td>ASA5510-SSL250-K9</td>
<td>ASA 5510 VPN Edition w/ 250 SSL User License, 3DES/AES</td>
</tr>
<tr>
<td>ASA5520-SSL500-K9</td>
<td>ASA 5520 VPN Edition w/ 500 SSL User License, HA, 3DES/AES</td>
</tr>
<tr>
<td>ASA5540-SSL1000-K9</td>
<td>ASA 5540 VPN Edition w/ 1000 SSL User License, HA, 3DES/AES</td>
</tr>
<tr>
<td>ASA5540-SSL2500-K9</td>
<td>ASA 5540 VPN Edition w/ 2500 SSL User License, HA, 3DES/AES</td>
</tr>
<tr>
<td>ASA5550-SSL2500-K9</td>
<td>ASA 5550 VPN Edition w/ 2500 SSL User License, HA, 3DES/AES</td>
</tr>
<tr>
<td>ASA5550-SSL5000-K9</td>
<td>ASA 5550 VPN Edition w/ 5000 SSL User License, HA, 3DES/AES</td>
</tr>
<tr>
<td>ASA5580-20-10K-K9</td>
<td>ASA 5580-20 VPN Edition w/ 10K SSL, Dual AC, HA, 3DES/AES</td>
</tr>
</tbody>
</table>
Remote-Access VPNs

Overview
Cisco VPN solutions provide integrated threat protection that guards against malware and hackers without the cost and complexity of deploying additional security equipment. Remote-access VPNs enable fast, reliable, and secure connectivity to the corporate network from practically anywhere, anytime, with any device – including PDAs, smartphones, public kiosks, personal laptops and shared computers. They allow secure remote access to the network based on user roles, whether they are remote workers, employees, contractors or business partners.

Solutions
Cisco offers a variety of VPN solutions, including IP Security (IPsec) and Secure Sockets Layer (SSL) VPN, that provide cost-effective and highly manageable remote connectivity. Cisco VPN technologies are integrated on a single platform, which reduces equipment cost and management complexity. Collectively, these solutions represent the most comprehensive and scalable VPN portfolio in the industry and include:

**Cisco ASA 5500 Series:** Cisco’s most advanced remote access VPN solution, which delivers concurrent user scalability from 10 to 10,000 sessions, plus integrated site-to-site VPN, firewall, intrusion prevention system (IPS), and content security services.

**Cisco routers:** Cisco’s most advanced site-to-site VPN solution plus integrated remote-access, firewall, and IPS services.

**Cisco Catalyst 6500 Series:** Cisco’s most scalable VPN platform plus integrated firewall and IPS services.

Benefits
Reduce cost, complexity, and management overheads:
- Enable VPN services customised for the deployment environment
- Remote-access VPNs support IPsec and clientless SSL VPN
- VPNs deliver any application, including voice and video, to any location with a high level of integrity
- Defend against viruses, spyware and hackers traversing the VPN connection
- No need for additional security equipment
- Simplified administration through remote-access connectivity through any Internet-enabled location with a standard web browser.

### Cisco ASA 5500 Series VPN Edition Bundles

<table>
<thead>
<tr>
<th>Model</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA5505-SSL10-K9</td>
<td>ASA 5505 VPN Edition w/ 10 SSL Users, 50 FW Users, 3DES/AES</td>
</tr>
<tr>
<td>ASA5505-SSL25-K9</td>
<td>ASA 5505 VPN Edition w/ 25 SSL Users, 50 FW Users, 3DES/AES</td>
</tr>
<tr>
<td>ASA5510-SSL50-K9</td>
<td>ASA 5510 VPN Edition w/ 50 SSL User License, 3DES/AES</td>
</tr>
<tr>
<td>ASA5510-SSL100-K9</td>
<td>ASA 5510 VPN Edition w/ 100 SSL User License, 3DES/AES</td>
</tr>
<tr>
<td>ASA5510-SSL250-K9</td>
<td>ASA 5510 VPN Edition w/ 250 SSL User License, 3DES/AES</td>
</tr>
<tr>
<td>ASA5520-SSL500-K9</td>
<td>ASA 5520 VPN Edition w/ 500 SSL User License, HA, 3DES/AES</td>
</tr>
<tr>
<td>ASA5540-SSL1000-K9</td>
<td>ASA 5540 VPN Edition w/ 1000 SSL User License, HA, 3DES/AES</td>
</tr>
<tr>
<td>ASA5540-SSL2500-K9</td>
<td>ASA 5540 VPN Edition w/ 2500 SSL User License, HA, 3DES/AES</td>
</tr>
<tr>
<td>ASA5550-SSL2500-K9</td>
<td>ASA 5550 VPN Edition w/ 2500 SSL User License, HA, 3DES/AES</td>
</tr>
<tr>
<td>ASA5550-SSL5000-K9</td>
<td>ASA 5550 VPN Edition w/ 5000 SSL User License, HA, 3DES/AES</td>
</tr>
<tr>
<td>ASA5580-20-10K-K9</td>
<td>ASA 5580-20 VPN Edition w/ 10K SSL, Dual AC, HA, 3DES/AES</td>
</tr>
</tbody>
</table>
Cisco Spam and Virus Blocker

Overview

The Cisco Spam and Virus Blocker includes everything you need to stop email threats immediately (hardware, software, updates, and product support), in a single package. This allows highly-skilled IT staff to focus on other responsibilities and leave the email issues to Cisco.

It can be deployed in minutes, just behind a network firewall. Once installed, the solution uses award-winning filtering technology to process all email traffic coming into your client’s business, and it identifies even the latest spam and malware attacks.

Benefits

- Protect against dangerous email threats
- Improve the productivity of employees by eliminating spam
- Reduce the time spent managing spam and email security threats
- Increase the performance of the network, servers, and personal computers by getting rid of unwanted email
- Reduce liability for a spam or virus attack that is unintentionally propagated through the network
- A complete solution for complete peace of mind.
## Cisco Spam and Virus Blocker Bundles

<table>
<thead>
<tr>
<th>Bundle Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BLKR-SVB-250U-3Y</td>
<td>Cisco Spam and Virus Blocker</td>
</tr>
<tr>
<td></td>
<td>- 250 User - 3 year</td>
</tr>
<tr>
<td>BLKR-SVB-50U-1Y</td>
<td>Cisco Spam and Virus Blocker</td>
</tr>
<tr>
<td></td>
<td>- 50 User - 1 year</td>
</tr>
<tr>
<td>BLKR-SVB-50U-3Y</td>
<td>Cisco Spam and Virus Blocker</td>
</tr>
<tr>
<td></td>
<td>- 50 User - 3 year</td>
</tr>
<tr>
<td>BLKR-SVB-100U-1Y</td>
<td>Cisco Spam and Virus Blocker</td>
</tr>
<tr>
<td></td>
<td>- 100 User - 1 year</td>
</tr>
<tr>
<td>BLKR-SVB-100U-3Y</td>
<td>Cisco Spam and Virus Blocker</td>
</tr>
<tr>
<td></td>
<td>- 100 User - 3 year</td>
</tr>
<tr>
<td>BLKR-SVB-250U-1Y</td>
<td>Cisco Spam and Virus Blocker</td>
</tr>
<tr>
<td></td>
<td>- 250 User - 1 year</td>
</tr>
</tbody>
</table>
Mid-Tier
Product Guide

Cisco IronPort Web Security (Content Security)......33
Cisco IronPort Email Security.................................35
Cisco Security Agent (End-Point Security).............37
Cisco Web Security Gateway Appliances

Overview
The number of security threats introduced by web traffic has reached epidemic proportions. Traditional gateway defenses are proving to be inadequate against a variety of web-based malware, leaving corporate networks dangerously exposed. According to industry estimates, approximately 75% of corporate PCs are infected with spyware, yet less than 10% of corporations have deployed perimeter malware defenses.

The Cisco IronPort® S-Series Web Security Gateway Appliance is the industry’s first and only appliance to combine traditional URL filtering, reputation filtering and malware filtering on a single platform.

By stopping malware threats at the network perimeter with the Cisco IronPort S-Series, organisations can significantly reduce administrative costs, prevent attacker “phone home” activity on networks, reduce support calls, enhance worker productivity and eliminate the business exposure that accompanies these threats.

The industry’s first web reputation filters provide a powerful outer layer of defense. Cisco IronPort Web Reputation Filters use SenderBase technology to analyse more than 50 different web traffic and network-related parameters, to accurately evaluate a URL’s trustworthiness.
Mid-Tier Product Guide

Benefits

- Guard against security, resource and compliance risks
- Significantly reduce administrative costs
- Reduce support calls
- Enhance worker productivity
- Eliminate business exposure
- Generate awareness and increase education to help mitigate security risk
- Single platform that contains a complete, in-depth defense
- Easy setup and management minimises administrative overhead
- Automated updates, and comprehensive monitoring and alerting
- Real-time and historical security information.

This is a license/service/solution build, please speak to your Comstor account manager with the following for quotes: Does the end user want Web Security? If so:

Selected Part Numbers and Ordering Information

- What vertical is the end user, corporate, education, government?
- Do they want A = URL Filtering?
- AB = URL Filtering, Web Reputation?
- ABC = URL Filtering, Web Reputation, Anti-Malware?
- How many years do they want this over, one or three?
- How many users is this for (Exact numbers required)?
Cisco IronPort Email Security

Overview
- Cisco provides the world’s most powerful multi-layered approach to email security. The Cisco® IronPort® C-Series provides world-class spam protection, data loss prevention, preventative virus outbreak filters and signature-based reactive filters, combined with content filtering and best-of-breed encryption technology, to deliver the highest level of email security available today.
- Today’s email-borne threats consist of virus attacks, spam, false positives, Distributed Denial-of-Service (DDoS) attacks, spyware, phishing (fraud), regulatory compliance violations and data loss. The unparalleled performance of the Cisco IronPort email security appliance delivers industry-leading protection from inbound spam, virus attacks and outbound data loss possibilities, in an easy-to-use appliance.

Benefits
- Quickly and accurately protect customers from spam outbreaks
- Combines SenderBase Reputation Filters with content-level analysis and Cisco IronPort Anti-Spam, to protect customers with an industry best: removing 99% of spam with near-zero false positives
- Enables a significant reduction in TCO by consolidating email operations and security into a single platform. The unparalleled performance of the C-Series delivers dial-tone availability – saving hours of productivity and thousands of dollars during peak traffic times
- Provides system administrators with the necessary information to make critical security decisions and demonstrate ROI.
Selected Part Numbers and Ordering Information

Does the end user want Email Security? If so:

- What vertical is the end user, corporate, education, government?

Do they want:

- S = Anti Spam Only?
- SQ = Anti Spam, Anti Virus?
- SQR = Anti Spam, Anti Virus, Virus Outbreak Filter?
- SQRT = Anti Spam, Anti Virus, Virus Outbreak Filter, Encryption?
- How many years do they want this over? One or three?
- How many users is this for? (Exact numbers required)
Overview

- Cisco® Security Agent is the first endpoint security solution that combines zero-update attack protection, data loss prevention and signature-based antivirus in a single agent. This unique blend of capabilities defends servers and desktops against sophisticated zero-day attacks, and enforces acceptable-use and compliance policies within a simple management infrastructure.
- Your clients will save on their security budget with better security. Cisco Security Agent 6.0 includes antivirus at no additional cost and no charge for renewals.
- Data loss prevention is integrated with Cisco Security Agent. Endpoint security: A single agent and single management console protects both the integrity of the endpoint and confidential data.
- Cisco Security Agent provides certified PCI protection.
- Cisco Security Agent is the industry leader in defending endpoints against targeted attacks, malicious mobile code, rootkits, worms, and zero-day attacks.

Benefits

- Zero-update protection reduces emergency patching in response to vulnerability announcements, minimising patch-related downtime and IT expenses.
- Visibility and control of sensitive data protects against loss from both user actions and targeted malware.
- Predefined compliance and acceptable use policies allow for efficient management, reporting, and auditing of activities.
- “Always-vigilant” security means that your client’s system is always protected, even when users are not connected to the corporate network or lack the latest patches.
The following figure shows how Cisco Security Agent fits in a network:

![Network Diagram]

**Cisco Security Agent**

<table>
<thead>
<tr>
<th>Product Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSA-PROFILER-K9</td>
<td>Cisco Security Agent Profiler</td>
</tr>
<tr>
<td>CSA-SRVR-K9=</td>
<td>Cisco Security Agent [1 Server Agent Bundle]</td>
</tr>
<tr>
<td>CSA-STARTER-K9=</td>
<td>CSA Starter Bundle</td>
</tr>
<tr>
<td>CSA-B10-SRVR-K9</td>
<td>Cisco Security Agent [10 Server Agent Bundle]</td>
</tr>
<tr>
<td>CSA-B25-SRVR-K9</td>
<td>Cisco Security Agent [25 Server Agent Bundle]</td>
</tr>
<tr>
<td>CSA-B50-SRVR-K9</td>
<td>Cisco Security Agent [50 Server Agent Bundle]</td>
</tr>
<tr>
<td>CSA-B100-SRVR-K9</td>
<td>Cisco Security Agent [100 Server Agent Bundle]</td>
</tr>
<tr>
<td>CSA-B25-DTOP-K9</td>
<td>Cisco Security Agent [25 Desktop Agent Bundle]</td>
</tr>
<tr>
<td>CSA-B100-DTOP-K9</td>
<td>Cisco Security Agent [100 Desktop Agent Bundle]</td>
</tr>
<tr>
<td>CSA-B250-DTOP-K9</td>
<td>Cisco Security Agent [250 Desktop Agent Bundle]</td>
</tr>
<tr>
<td>CSA-B500-DTOP-K9</td>
<td>Cisco Security Agent [500 Desktop Agent Bundle]</td>
</tr>
<tr>
<td>CSA-B1000-DTOP-K9</td>
<td>Cisco Security Agent [1,000 Desktop Agent Bundle]</td>
</tr>
</tbody>
</table>
AT Product Guide
(Advanced Technology)

Cisco Application Control Engine (ACE) .......................................................... 39
Firewall & Load balancing .................................................................................. 39
Cisco Network Admission Control (NAO) ......................................................... 41
Switch Security ..................................................................................................... 43
Cisco Monitoring, Analysis and Response System (MARS) ................................. 45
Cisco Security Manager ....................................................................................... 47
Cisco Application Control Engine (ACE) Web Application Firewall and Load Balancing

Overview
The Cisco Application Control Engine (ACE) Web Application Firewall is especially designed to help secure organisations that store, process and transmit credit card data to comply with the current Payment Card Industry (PCI) Data Security Standard (DSS) requirements. It combines deep web application analysis with high-performance Extensible Markup Language (XML) inspection and management, to address the full range of threats to web applications, including identity theft, data theft, information leakage, application disruption, fraud and targeted attacks. Because of its unique blend of HTML and XML security, the Cisco ACE Web Application Firewall provides a full compliance solution for PCI DSS sections 6.5 and 6.6, which mandate the implementation of a web application firewall.

Benefits
- PCI DSS regulation compliance
- Out-of-the-box customisable PCI policies and securing, auditing and reporting on web application activity
- Full-proxy security for both traditional HTML-based web applications and modern XML-enabled web services applications
- Authentication and authorisation enforcement to block unauthorised access
- Best-in-industry scalability throughput for managing XML application traffic in the largest of Data Centres
- Positive and negative security enforcement to keep bad traffic patterns out and identify and allow only good traffic through
- Enterprise-wide, user-friendly management accessible anywhere on the network, through the web GUI.
The following figure shows how a Cisco ACE Web Application Firewall fits in a network:

Application Control Engine (ACE) XML Gateway

<table>
<thead>
<tr>
<th>Model</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACE-XML-K9</td>
<td>ACE XML Gateway</td>
</tr>
<tr>
<td>ACE-XML-NF-K9</td>
<td>ACE XML Gateway Non FIPS</td>
</tr>
<tr>
<td>ACE-XML-NONFIPS</td>
<td>ACE XML Gateway Non FIPS Hardware Option</td>
</tr>
<tr>
<td>ACE-XML-SW-5.0</td>
<td>ACE XML Gateway Software</td>
</tr>
<tr>
<td>ACE-XML-SW-6.0</td>
<td>V6.0 software with AXG and WAF. Use Flex Lic for G/W and MGR</td>
</tr>
<tr>
<td>ACE-WAF-GAT-LICFX=</td>
<td>ACE Web App Firewall FlexLM License</td>
</tr>
<tr>
<td>ACE-WAF-MGT-LICFX=</td>
<td>ACE WAF Manager FlexLM License</td>
</tr>
</tbody>
</table>
Cisco Network Admission Control (NAC)

Overview

Cisco NAC protects sensitive data and prevents unauthorised access, by confirming a user’s identity before access to the network is granted, and allows noncompliant devices to be quarantined and brought into compliance. As a result, it minimises the risks associated with noncompliant devices, regardless of system type, ownership, or access methods, resulting in a more resilient and secure network.

The optional Cisco NAC Profiler automates discovery and inventory of all LAN-attached endpoints, including non-PC devices, such as IP phones and printers. It simplifies NAC deployment by using the device information to apply appropriate Cisco NAC policies. In addition, the optional Cisco NAC Guest Server supports the entire guest access lifecycle, i.e. provisioning, notification, management and reporting.
Benefits

- Enforces security policy compliance at the network level
- Proactively protects against infrastructure disruptions (such as viruses and worms)
- Controls and reduces large-scale infrastructure disruptions
- Reduces operating expenses and maintains higher employee productivity
- Prevents unauthorised access
- Controls network access based on user and device credentials, to maintain security and protect confidential information
- Provides effective controls for guest access and partner connections
- Provides complete services (user authentication, device posture validation, policy enforcement, remediation, device profiling and secure guest) to meet customer business needs
- Profiling service reduces IT burden by automating device discovery and inventory
- Guest service provides secure guest access and guest satisfaction
- Supports all use cases, including campus, branch offices, wireless and VPN
- Secures both company-owned and non-company-owned devices
- Can be deployed for Layer two or Layer three, in-band or out-of-band
- Reduces IT security risks and addresses compliance requirements.

Selected Part Numbers and Ordering Information
NAC3310, NAC3350 – Server, Manager and Profile required. For a full list of part codes, please go to www.cisco.com/go/NAC
Switch Security

Cisco Catalyst 6500 Series Security Services Modules

Overview
Cisco delivers integrated network security with a suite of advanced security modules for Cisco Catalyst 6500 Series Switches, including firewall, intrusion prevention system (IPS), IP Security (IPsec) VPN, Secure Sockets Layer (SSL) acceleration, Distributed Denial-of-Service (DDoS) and content switching modules. These security modules enable integrated, highly available, adaptive and scalable security for network connectivity, services and applications.

Benefits
- Ability to increase security while using existing Cisco Catalyst 6500 Series investment
- Tightly integrated infrastructure security solutions
- Highest-performance security solutions, offering multi-gigabit performance in a single Cisco Catalyst 6500 Series Switch
- Application-level visibility into the infrastructure
- Critical platform for collaboration of emerging technologies (such as application networking).
### Catalyst 6500 Service Modules - Top Sellers

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-SVC-FWM-1-K9</td>
<td>Firewall blade for 6500 and 7600, VFW License Separate</td>
</tr>
<tr>
<td>WS-SVC-FWM-1-K9=</td>
<td>Firewall blade for 6500 and 7600, VFW License Separate (Spare)</td>
</tr>
<tr>
<td>WS-C6503-E-FWM-K9</td>
<td>Cisco Catalyst 6503E Firewall Security System</td>
</tr>
<tr>
<td>WS-C6506-E-FWM-K9</td>
<td>Cisco Catalyst 6506E Firewall Security System</td>
</tr>
<tr>
<td>WS-C6509-E-FWM-K9</td>
<td>Cisco Catalyst 6509E Firewall Security System</td>
</tr>
<tr>
<td>WS-C6513-FWM-K9</td>
<td>Cisco Catalyst 6513 Firewall Security System</td>
</tr>
<tr>
<td>WS-6506-EXL-FWM-K9</td>
<td>C6506 FW Sys, C6509, FWSM, SUP720-3BXL, FAN</td>
</tr>
<tr>
<td>WS-6509-EXL-FWM-K9</td>
<td>C6509 FW Sys, C6509, FWSM, SUP720-3BXL, FAN</td>
</tr>
<tr>
<td>WS-6509EXL-2FWM-K9</td>
<td>Cisco Catalyst 6509E 3BXL Security System with two FWSMs</td>
</tr>
<tr>
<td>WS-6513XL-2FWM-K9</td>
<td>Cisco Catalyst 6513 3BXL Security System with two FWSMs</td>
</tr>
<tr>
<td>WS-C6513-XL-FWM-K9</td>
<td>C6513 FW Sys, C6513, FWSM, SUP720-3BXL, FAN</td>
</tr>
</tbody>
</table>
Cisco Security Monitoring, Analysis, and Response System (MARS)

Overview
The Cisco Security Monitoring, Analysis and Response System (Cisco Security MARS) is a family of high-performance, scalable appliances for threat management, monitoring and mitigation. Cisco Security MARS helps customers achieve greater security and make more effective use of network and security devices.

Benefits
- Collects, analyses, and correlates data from a diverse set of Cisco devices
- Shows a graphical attack path using topology awareness
- Suggests mitigation for rapid threat containment
- Links with Cisco Security Manager for policy provisioning and event lookup
- Optimised for Cisco ASA and Cisco IPS troubleshooting
- Delivers high performance: A single Cisco Security MARS appliance can handle up to 15,000 events per second.
The following figure shows how Cisco Security MARS fits in a network:

**Cisco Security Monitoring, Analysis and Response System (MARS)**

<table>
<thead>
<tr>
<th>Model</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS-MARS-25-K9</td>
<td>CSMARS 25 Appliance</td>
</tr>
<tr>
<td>CS-MARS-25R-K9</td>
<td>CSMARS 25R 1RU Appliance; 75 EPS; 250 GB</td>
</tr>
<tr>
<td>CS-MARS-55-K9</td>
<td>CSMARS 55 1RU Appliance; 1500EPS; 500GB, RAID 1, Redundant</td>
</tr>
<tr>
<td>CS-MARS-110R-K9</td>
<td>CSMARS 110R 2RU Appliance; 4500EPS; 1500GB, RAID 10, Redundant</td>
</tr>
<tr>
<td>CS-MARS-110-K9</td>
<td>CSMARS 110 2RU Appliance; 7500EPS; 1500GB, RAID 10, Redundant</td>
</tr>
</tbody>
</table>
Cisco Security Manager

Overview
Cisco Security Manager provides centralised security administration, faster deployment and increased configuration accuracy. It is a powerful, but easy-to-use, solution that centrally provisions all aspects of device configuration and security policies for Cisco firewalls, VPNs, and intrusion prevention systems (IPSs). The solution is effective for managing small networks consisting of fewer than 10 devices, but also scales to efficiently manage large-scale networks composed of thousands of devices.

Benefits
- A single integrated application for managing firewall, VPN and IPS security services on Cisco security appliances and modules, routers and switches
- Reduces operational expenses
- Collaborates with Cisco Security MARS to form a comprehensive security management solution that encompasses security provisioning, event monitoring, threat detection and mitigation
- Improves provisioning accuracy and consistency
- Allows faster response to threats
- Supports provisioning for Cisco router, switch, and security platforms
- Provides superior ease of use with a rich graphical user interface.

Overall, it supports true enterprise-class operational environments with support for multiple simultaneous security administrators, with fine-grained control of access permissions; an optional “workflow” mode allows the security and network operations staff to work together effectively, with the appropriate division of responsibilities.
SMARTnet & SAFE Overview

Services Overview ................................................................. 48
Services for IPS ................................................................. 51
Smart Care ................................................................. 52
Cisco SAFE ................................................................. 54
Services Overview
Cisco offers a wide spectrum of support services designed to meet your customers’ business needs, and assist to effectively manage the network services needed for high-quality network performance. At the same time, they help to control operational costs and ensure that Cisco products and networks also benefit from the most up-to-date system and application software available.

SMARTnet Overview
Cisco SMARTnet Service is an award-winning technical support service that gives anytime access to Technical Assistance Centre (TAC) engineers and Cisco.com resources. With it, your clients’ receive the fast, expert response and the dedicated accountability they require to resolve critical network issues.

SMARTnet facilitates rapid problem resolution, 24-hour business continuity and improved operational efficiency through a combination of expert technical assistance, online tools, and flexible device coverage options. It provides the following device-level support:

- Global access 24 hours a day, 365 days a year to specialised engineers in the Cisco TAC
- Anytime access to the extensive Cisco.com online knowledge base, resources and tools
- Next-business-day advance hardware replacement (premium service level options for two-hour and four-hour replacement also available)
- Ongoing operating system software updates, including both minor and major releases within the licensed feature set.

Cisco SMARTnet Onsite Service is an option that, in addition to the above, provides a field engineer to install replacement parts at your customer’s site.
<table>
<thead>
<tr>
<th>CODE</th>
<th>Service Level</th>
<th>HW Cover</th>
<th>SW Centre Access</th>
<th>IOS updates</th>
<th>TAC Access</th>
<th>On-Site Cover</th>
<th>FEATURES</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNT</td>
<td>8x5xNBD</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>• (24x7)</td>
<td></td>
<td>Advance replacement parts are delivered the next business day from 9 am to 5 pm (provided the request is received before 3 pm local time).</td>
</tr>
<tr>
<td>SNTE</td>
<td>8x5x4</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>• (24x7)</td>
<td></td>
<td>Advance replacement parts are delivered within four hours of determining that part replacement is required (Monday-Friday, 9 am to 5 pm).</td>
</tr>
<tr>
<td>SNTP</td>
<td>24x7x4</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>• (24x7)</td>
<td></td>
<td>4 hour response time, 365 (including holidays).</td>
</tr>
<tr>
<td>S2P</td>
<td>24x7x2</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>• (24x7)</td>
<td></td>
<td>2 hour response time, 365 (including holidays).</td>
</tr>
<tr>
<td>OS</td>
<td>Onsite 8x5xNBD</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>• (24x7)</td>
<td></td>
<td>Advance replacement parts, with a field engineer, are delivered the next business day from 9 am to 5 pm (provided the request is received before 3 pm local time).</td>
</tr>
<tr>
<td>OSE</td>
<td>Onsite 8x5x4</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>• (24x7)</td>
<td></td>
<td>Advance replacement parts, with a field engineer, are delivered within four hours of determining that part replacement is required (Monday-Friday, 9 am to 5 pm).</td>
</tr>
<tr>
<td>OSP</td>
<td>Onsite 24x7x4</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>• (24x7)</td>
<td></td>
<td>4 hour on-site response time, 365 (including hols).</td>
</tr>
<tr>
<td>PREM</td>
<td>Onsite 24x7x2</td>
<td>•</td>
<td>•</td>
<td>•</td>
<td>• (24x7)</td>
<td></td>
<td>2 hour on-site response time, 365 (including hols).</td>
</tr>
</tbody>
</table>
The Cisco Services portfolio also includes two services to support application software:

Cisco Software Application Support (SAS): provides minor updates and technical support services for over 100 Cisco applications. Eg for product SKU CSACS-4.2 WIN-K9

Software Application Support plus Upgrades (SAU): provides the same benefits as SAS plus major upgrades. Eg for CSA-SRVR-K9.
07 SMARTnet and SAFE Overview

Services for IPS

Overview
To be effective, network security needs to be kept constantly up-to-date in order to deal with the latest threats. Delivering timely information, signature-file updates and comprehensive support, Cisco Services for IPS keeps your customer’s Cisco IPS solution current for the latest threats, so that malicious or business crippling traffic is accurately identified, classified and stopped in real time.

Deliverables
The Cisco Services for IPS combines Cisco SMARTnet deliverables with signature-file updates and availability notifications, to provide comprehensive ongoing support and product enhancements for IPS solutions during their operational lifetime.

Cisco Services for IPS includes:
• Notification of availability of updated signature files
• Access to the signature-file library and new signature files
• Support for licensed operating system software for each registered Cisco IPS solution
• Software updates include maintenance, minor and major releases
• Example product SKUs: ASA5510-AIP10-K9 and IPS-4240-K9.

Please note: signature-file updates cannot be obtained without a Cisco Services for IPS contract. Each IPS solution must be under contract.
Smart Care

Overview
This service provides you with many of the tools you need to provide customers with ongoing remote monitoring, proactive network maintenance and comprehensive technical support for their entire voice and data network – as well as add-on services designed and delivered by you – under a single service contract.

Deliverables
Cisco Smart Care Service includes:

- Dashboard visibility into network performance to remotely monitor performance and correct potential problems
- Proactive notifications to simplify the updating of Cisco devices
- Assessment and repair services to identify potential network issues
- Assessment and preparation services simplify the addition of new technologies and applications
- Next-business-day (NBD) advance hardware replacement to the end user
- Partner access to the Cisco TAC for escalations
- Software updates and maintenance releases for qualified Cisco applications
  - Cisco IOS Software support, including maintenance releases and patches, minor releases and major releases
  - Access to Cisco.com and the Cisco Smart Care Service portal and tools
- Single, network-level service contract covering all qualified Cisco devices in the customer’s network.

Additionally, the Assess and Repair service encompasses a thorough evaluation of every Cisco router, switch and other device in a network, to ensure that all device ports and routing protocols are configured optimally, according to Cisco best practices.
SMARTnet and SAFE Overview

Security assessments examine the configuration of the network in multiple areas, including:

- Password encryption and management to prevent unauthorised access to network devices
- Flood management to ensure Distributed Denial of Service (DDoS) attacks cannot overrun network devices and paralyse the network
- Access control to ensure that unauthorised users cannot gain control of the network devices
- Security of remote network management services operating over the Internet or other untrusted networks
- Logging of network and security events
- Secure IP routing.

If a security assessment reveals that the network is not configured optimally, you can alert the customer to the problem and remediate it, often remotely. This enables you to help your customers proactively address potential security flaws – before they cause damage.
Cisco SAFE

Why a Validated Network Architecture?
The network is undergoing tremendous change. Innovations such as virtualisation, cloud computing and web-based access are bringing about a dramatic evolution in nearly every organisation’s infrastructure. From a security standpoint, these innovations have brought with them several new and complex challenges, in the form of threats that attack network and service availability, exploit new applications and network resources, and focus on data and identity theft. Traditional point security solutions are largely unable to address these threats. Organisations need reliable and proven guidance on how they can best secure these new, business-critical services, while protecting against emerging threats. These complex new threats are increasingly targeted at specific networks, new technologies and services. Some include:

- Increasing botnet sophistication and effectiveness
- Emerging mobile phone threats
- Increasingly malicious spyware
- Web application exploits
- Supply chain attacks infecting consumer devices
- Increasingly rigid regulatory and compliance requirements.

Cisco SAFE Validated Security Architectures
Cisco® SAFE is a security reference architecture that is part of the Cisco Validated Design programme. SAFE provides prescriptive design guides, based on best practices, that address the planning, design and deployment of security solutions. SAFE’s modular design addresses the unique requirements of different places in the network, such as campuses, the Internet edge, branches and Data Centres. Cisco SAFE’s defense-in-depth architectural blueprints provide best practices to help secure critical data and transactions across the network. Organisations can strategically position Cisco products and capabilities across the network, and can take advantage of the collaborative nature between security and network platforms. Cisco SAFE designs focus on supporting critical business and network services by helping organisations develop and enhance network visibility and control.
SMARTnet and SAFE Overview

Visibility

- Identify and classify users, services, traffic and endpoints
- Monitor performance, behaviors, usage patterns, events and policy compliance
- Collect, analyse and correlate system-wide events.

Control

- Harden endpoints, services, servers, applications and infrastructure
- Isolate users, systems and services when containment is needed
- Enforce access controls and security policies and mitigate security events.

The result is a validated security strategy, that helps secure the interactions and transactions between and among places in the network, to create a highly secure network environment.

www.cisco.com/go/safe

Benefits

The Cisco SAFE architecture can provide guidance on all aspects of a secure network, so that organisations can create a thoughtful security deployment strategy, based on available budget and critical need.
SMARTnet and SAFE Overview

- Step-by-step network security design and implementation guidance shortens deployment
- Solutions-based approach focuses on risk management rather than product placement
- Layered security design helps prevent a network from being overwhelmed by a large or unexpected attack
- Threat visibility and coordinated response reduces exposure and IT overhead
- Integrated security and network architecture helps ensure business-critical services availability
- Modular design enables a gradual improvement in security, based on organisational priority
- Fully tested and validated designs
- These best practices and functions can help organisations meet their compliance requirements.

Cisco Security Lifecycle Services

SAFE services delivered are based on a lifecycle approach and cover the entire lifecycle process:

- **Strategy and assessment**: Cisco offers a comprehensive set of assessment services to help organisations understand their current security state and plan for the strategic deployment of SAFE security principles.
- **Deployment and migration**: Cisco offers deployment services to support companies in planning, designing and implementing Cisco SAFE validated designs.
- **Remote management**: Cisco Remote Management Services offers engineers and tools to proactively monitor the SAFE security infrastructures and provide incident, problem, change, configuration and reporting services 24 hours a day, 365 days a year.
- **Security intelligence**: Cisco Security Intelligence Operations Services provide early warning intelligence, analysis and proven mitigation techniques, to help security professionals respond to the latest threats.
- **Security optimisation**: The Cisco Security Optimisation Service is an integrated service offering designed to assess, develop and optimise a company's security infrastructure through quarterly site visits and continual analysis and tuning.
Cisco Training from Comstor

Building Capability ................................................................. 57
Cisco Advanced Technologies
Technical Roadmap ............................................................... 58
Cirencester Courses .............................................................. 60
Comstor Training can help identify the easiest route to maximising you or your clients’ profitability, by advising how to gain and maintain the most suitable Cisco Certification and Specialisations – as well as by keeping you aware of the many promotions such as Challenge and Reward, VIP, OIP and PDF.

As an authorised Cisco Learning Solutions Provider (CLSP), we can help your organisation fast track to Premier, Silver and Gold Partner Certifications, by working with you on building a customised training plan to help you achieve the Technology Specialisations shown in the diagram below such as:

- Security
- Data Centre
- Unified Communications
- Wireless
- Routing and Switching.

This process will identify individual training plans, comprising courses and exams that support the goals of your organisation, and will include dates, locations and costs. This will help you to build an ROI case based upon the rewards gained, versus the time and money invested – allowing you to plan and prioritise your activities to succeed in the Cisco market.

**Building Capability**

Comstor Training can help design training plans for both sales and technical personnel, which build capability within your business to sell and support Cisco Advanced Technologies into your customers – as well as by serving your business goals to maximise profitability though effective Certification and Specialisation management. Examples of these are shown below, with further details available on our website, OneTrain. (http://eu.onetrain.comstor.com)
Cisco Advanced Technologies Sales Roadmap: E.g. Cisco Security Sales Specialist

www.cisco.com/web/learning/le3/le2/le41/le85/le54/learning_certification_type_home_extra_level.html

Designed exclusively for Channel Partners, the Cisco Security Sales Specialist demonstrates fundamental understanding of the Cisco Self Defending Network (SDN) Strategy. He or she possesses the skills and knowledge necessary to assess customer needs and to effectively describe and sell components of the Cisco SDN to protect customer assets, increase productivity and reduce costs.
The building block of this Sales Specialist role is the Cisco Sales Expert certification and once this certification has been achieved the Advanced Security for Account Managers (ASAM) course can be viewed free online via the Partner Education Connection web site. This eLearning course prepares you for the ASAM 646-563 exam. Once you have passed this then you are a Cisco Security Sales Specialist.

**Partner Education Connection**

**ASAM**

**ASAM 646-563**

**Cisco Advanced Technologies Technical Roadmap**
Please contact Comstor Training to help you construct a personal training plan around your needs.

**Certification Examples**
- CCNA Security
- CCSP

**Cisco Qualified Specialist Role Examples**
- Cisco ASA Specialist
- Cisco IPS Specialist
- Cisco Network Admission Control Specialist
- Cisco Security Solutions and Design Specialist.
Closed Course and Onsite Courses
Comstor Training can offer onsite courses for groups of 6 or more Partner or end user personnel.

Comstor Training Pass
The Comstor Training Pass is the simplest way of purchasing multiple days of Cisco Technical training at the most competitive rates. It protects budgets and provides a hassle-free solution for delegates who need to book onto courses. For larger customer opportunities, Partners can resell a Comstor Training Pass – which is transferable between personnel of that same customer. Discounts of up to 50% are achievable using the Comstor Training Pass.

Cisco Remote Labs
Comstor offers Cisco Remote Lab Services, through a generic branded portal – www.livelabs.co.uk Currently, livelabs offers CCNA and CCNP labs, which will soon be extended to include CCIP, CCSP and CCVP courses.

Cirencester Courses
Delegates attending courses at Cirencester enjoy these benefits:

- **Extra Lab access:** Access to labs in the evening at no extra charge and at weekends for a nominal charge – using exactly the same interface as in the classroom. Delegates can also re-book lab time later on, when practicing for exams.
- **Real world local lab environment:** Delegates get a tour of the lab facility on campus and can get supervised access of our real world lab environment for troubleshooting. This is unique to Comstor and reflects the environments that delegates work in – most other labs are overseas and cannot be accessed.
- **Pearson VUE Testing Centre:** Delegates often book an exam on the Friday afternoon following a course.
- **Lower Trainer to Delegate Ratios:** Average ratios are 8:1, compared with 16:1 of other providers. This means more trainer time per delegate and higher customer satisfaction.
- **High Customer Satisfaction:** Average CSAT scores exceed 86%
• **Great Hospitality:** Delegates rate and score our hospitality highly – and enjoy “home cooked style” food prepared and cooked on the premises.

• **Low Hotel Costs:** Local BandB’s start at £50 per night and three star hotels from £69 per night.

• **FOC Extras:** ICND/CCNA delegates receive FOC mock exam software, to help them practice before they take the actual Pearson VUE exam.

**Onsite Pearson VUE Testing**

Comstor Training is uniquely positioned as the only mobile Pearson VUE test facility which improves pass rates. This can be taken advantage of when there are six or more people to be tested for, for example, CCNA and CSE. It is especially useful after onsite courses, where the delegates can be tested on the last day of the course. This service reduces the time spent by multiple delegates going to various testing centres. In an example of an onsite CSE with 12 delegates, this service can save up to 12 person days of selling. It can also be offered as another value-add to Partner customers, when sold alongside onsite courses.
Professional Services from Comstor

What We Can Do For You .................................................. 62
Cost .................................................................................. 63
What We Can Do For You

Expand your services, increase your reach and improve your revenues with Comstor’s Technical and Professional Services. Comstor’s continuing commitment is to help you increase sales with maximum profit margin – at minimum overhead cost.

Comstor Professional Services are responsible for additional solution provider services – including design installation, consultation, network health checks, network audits and project management. If you lack the qualifications or experience for a specific project, task or engagement, our team can provide them.

The Comstor Professional Services Team – whose engineering accreditations range from CCNA, CCNP, CCSP, and CCVP to CCIE – is dedicated to the provision of quality services for solution providers. The main focus is on Cisco IP Telephony, Voice over IP (VoIP), Cisco Security and Wireless. We also offer general installation services for Cisco’s core routing and switching technologies.

In short, we provide you with the ability to service the needs of your customers, without the need for you to be fully certified or even have your own technical resource. We provide a competitive edge with no overhead to your business. We offer services through you, as a solution provider, and will work closely with you to nurture and build your relationships with customers.

“We provide you with the ability to service the needs of your customers, without the need for you to be fully certified.”
Cost

Utilising Comstor PS engineers for services such as implementation, audits, fault finding etc, typically costs only £695 to £850 per day, depending on the qualified skill set required for the work – for example, a basic CM express implementation would use a CCVP, with a cost of £695 per day.

We also provide engineering personnel to participate in consultancy meetings – a typical cost for this service is £500.

Please note: all the above charges may be subject to additional costs, relating to traveling and accommodation expenses.