Preface

Document Purpose

This guide discusses the Cisco SAFE best practices, designs and configurations, and provides network and security engineers with the necessary information to help them succeed in designing, implementing and operating secure network infrastructures based on Cisco products and technologies.

Document Audience

While the target audience is technical in nature, business decision makers, senior IT leaders, and systems architects can benefit from understanding the design driving principles and fundamental security concepts.

Document Organization

The following table lists and briefly describes the chapters and appendices of this guide:

Chapter	Description
Chapter 1, “SAFE Overview.”	Provides high-level overview of the Cisco SAFE design.
Chapter 2, “Network Foundation Protection.”	Describes the best practices for securing the enterprise network infrastructure. This includes setting a security baseline for protecting the control and management planes as well as setting a strong foundation on which more advanced methods and techniques can subsequently be built on.
Chapter 3, “Enterprise Core.”	Describes the core component of the Cisco SAFE design. It describes types of threats that targets the core and the best practices for implementing security within the core network.
Chapter 4, “Intranet Data Center.”	Describes the intranet data center component of the Cisco SAFE design. It provide guidelines for integrating security services into Cisco recommended data center architectures.
Chapter 5, “Enterprise Campus.”	Describes the enterprise campus component of the Cisco SAFE design. It covers the threat types that affect the enterprise campus and the best practices for implementing security within the campus network.

Chapter	Description
Chapter 6, “Enterprise Internet Edge.”	Describes the enterprise Internet edge component of the Cisco SAFE design. It covers the threat types that affect the Internet edge and the best practices for implementing security within the enterprise Internet edge network.
Chapter 7, “Enterprise WAN Edge.”	Describes the enterprise WAN edge component of the Cisco SAFE design. It covers the threat types that affect the enterprise WAN edge and the best practices for implementing security within the WAN edge network.
Chapter 8, “Enterprise Branch.”	Describes enterprise branch component of the Cisco SAFE design. It covers the threat types that affect the enterprise branch and the best practices for implementing security within the branch network.
Chapter 9, “Management.”	Describes the management component of the Cisco SAFE design. It covers the threat types that affects the management module and the best practices for mitigation those threats.
Chapter 10, “Monitoring, Analysis, and Correlation.”	Describes the security tools used for monitoring, analysis, and correlations of the network SAFE design network resources.
Chapter 11, “Threat Control and Containment.”	Describes the threat control and containment attributes of the Cisco SAFE design.
Chapter 12, “Cisco Security Services.”	Describes the security services designed to support the continuous solution lifecycle.
Chapter A, “Reference Documents.”	Provides a list of reference documents where users can obtain additional information.
Glossary	Lists and defines key terms and acronyms used in this guide.

About the Authors

This section provides information about the authors who developed the content of this guide.

Justin Chung, Manager, CMO Enterprise Solutions Engineering (ESE), Cisco Systems

Justin is a Technical Marketing Manager with over twelve years of experience in the networking industry. During his eleven years at Cisco, he managed various security solutions such as Dynamic Multipoint VPN (DMVPN), Group Encrypted Transport VPN (GET VPN), VRF-Aware IPSec, Network Admission Control (NAC), and others. He is a recipient of the Pioneer Award for the GET VPN solution. He is currently managing the Enterprise WAN Edge, Branch, and Security solutions.

Martin Pueblas, CCIE#2133, CISSP#40844—Technical Leader, CMO Enterprise Solutions Engineering (ESE), Cisco Systems

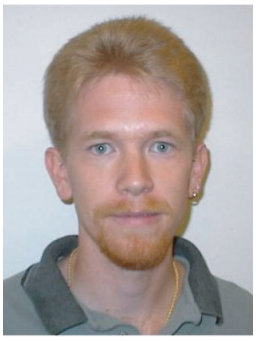
Martin is the lead system architect of the Cisco SAFE Security Reference Architecture.

He is a network security expert with over 17 years of experience in the networking industry. He obtained his CCIE certification in 1996 and CISSP in 2004. Martin joined Cisco in 1998 and has held a variety of technical positions. Started as a Customer Support Engineer in Cisco's Technical Assistance Center (TAC) in Brussels, Belgium. In 1999 moved to the United States where soon became technical leader for the Security Team. Martin's primary job responsibilities included acting as a primary escalation resource for the team and delivering training for the support organization. At the end of 2000, he joined the Advanced Engineering Services team as a Network Design Consultant, where he provided design and security consulting services to large corporations and Service Providers. During this period, Martin has written a variety of technical documents including design guides and white papers that define Cisco's best practices for security and VPNs. Martin joined Cisco's Central Marketing Organization in late 2001, where as a Technical Marketing Engineer, he focused on security and VPN technologies. In late 2004, he joined his current position acting as a security technical leader. As part of his current responsibilities, Martin is leading the development of security solutions for enterprises.

Alex Nadimi, Technical Marketing Engineer, CMO Enterprise Solutions Engineering (ESE), Cisco Systems

Alex has been at Cisco for 14 years. His expertise include security, VPN technologies, MPLS, and Multicast. Alex has authored several design guides and technical notes.

Alex has over 15 years experience in the computer, communications, and networking fields. He is a graduate of University of London and Louisiana State University.

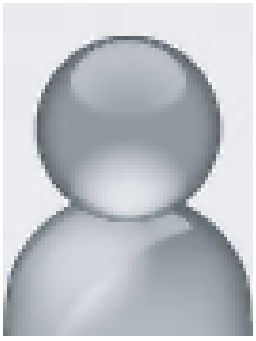


Dan Hamilton, CCIE #4080 —Technical Leader, CMO Enterprise Solutions Engineering (ESE), Cisco Systems

Dan has over 15 years experience in the networking industry. He has been with Cisco for 9 years. He joined Cisco in 2000 as a Systems Engineer supporting a large Service Provider customer. In 2004, he became a Technical Marketing Engineer in the Security Technology Group (STG) supporting IOS security features such as infrastructure security, access control and Flexible Packet Matching (FPM) on the Integrated Security Routers (ISRs), mid-range routers and the Catalyst 6500 switches. He moved to a Product Manager role in STG in 2006, driving the development of new IOS security features before joining the ESE Team in 2008.

Prior to joining Cisco, Dan was a network architect for a large Service Provider, responsible for designing and developing their network managed service offerings.

Dan has a Bachelor of Science degree in Electrical Engineering from the University of Florida.



Sherelle Farrington, Technical Leader, CMO Enterprise Solutions Engineering (ESE), Cisco Systems

Sherelle is a technical leader at Cisco Systems with over fifteen years experience in the networking industry, encompassing service provider and enterprise environments in the US and Europe.

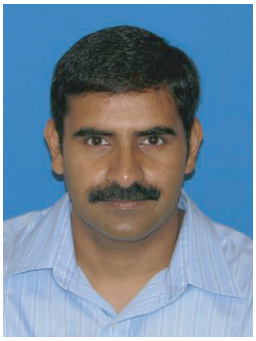
During her more than ten years at Cisco, she has worked on a variety of service provider and enterprise solutions, and started her current focus on network security integration over four years ago. She has presented and published on a number of topics, most recently as co-author of the Wireless and Network Security Integration Solution design guide, and the Network Security Baseline paper.

David Anderson, CCIE #7660, CISSP#57547—Senior Technical Marketing Engineer, CMO Enterprise Solutions Engineering (ESE), Cisco Systems

David is a Senior Technical Marketing Engineer in CMO - Enterprise Solutions Engineering (ESE), Cisco Systems. In this role, David focuses on security and virtualization in data center solutions. David also works cross-functionally to develop data center solutions with Cisco business units and partners.

David joined Cisco in 1999 as a solution engineer for service provider dial-access architectures. His roles at Cisco include Systems Engineer, Technical Marketing Engineer, and Senior Product Manager. In 2001 David was part of the initial team that began focusing on data center related solutions for Cisco. After several years, he moved to the role of Senior Technical Marketing Engineer and Product Manager to help establish and grow the Cisco Network Admission Control product line.

David is a frequent speaker at Cisco Live (Networkers) and other industry events and forums. Prior to joining Cisco, David was a Senior Network Engineer for the Department of Emergency Communications and E-911 Center in San Francisco. David holds CCIE and CISSP certifications and has a Bachelor of Science degree in Management Information Systems from Florida State University.



Srinivas Tenneti, CCIE#10483—Technical Marketing Engineer, CMO Enterprise Solutions Engineering (ESE), Cisco Systems

Srinivas is a Technical Marketing Engineer for WAN and branch architectures in Cisco's ESE team. Prior to joining the ESE team, Srinivas worked two years in Commercial System Engineering team where he worked on producing design guides, and SE presentations for channel partners and SEs. Before that, he worked for 5 years with other Cisco engineering teams. Srinivas has been at Cisco for 8 years.