Cisco Secure Firewall Service Overview

WHAT WE DELIVER

BTA delivers a structured deployment and migration to Cisco Secure Firewall using our proven SIMPLE methodology. Whether the customer is deploying net-new firewalls or migrating from an existing platform (Palo Alto, Fortinet, Check Point, etc.), this service provides next-generation threat protection, application visibility, and segmentation controls — reducing attack surface, supporting compliance initiatives, and strengthening cyber insurance posture.

As a partner, you bring the customer relationship. BTA handles the design, migration, deployment, and knowledge transfer.

WHY YOUR CUSTOMERS NEED THIS

- **Cyber insurance requirements** increasingly mandate next-generation firewall capabilities and network segmentation
- **Ransomware and advanced threats** require IPS, malware detection, and application-aware security policies
- **Compliance frameworks** (NIST, CMMC, PCI-DSS, HIPAA) require perimeter and internal segmentation controls
- **Lateral movement** is the leading attack vector — firewall segmentation directly addresses this risk

KEY OUTCOMES

- Next-generation firewall protection at the network edge or data center
- Application-aware and identity-based security policies
- Improved visibility into network traffic and threats
- Reduced lateral movement through segmentation policies
- Documented architecture and operational runbook

IN-SCOPE CAPABILITIES

- Cisco Secure Firewall architecture and deployment
- Migration from existing firewall platform (policy translation, rule conversion)
- Firewall device provisioning and base configuration
- Secure Firewall Management Center (FMC or cdFMC) deployment or integration
- Network and security zone design
- Access control policy creation
- Intrusion prevention (IPS) configuration
- NAT and routing configuration
- VPN configuration (site-to-site or remote access, optional)
- SSL/TLS decryption policy design (optional)
- Logging and SIEM integration
- Knowledge transfer and operational documentation

BTA Cisco Secure Firewall Service Overview

BTA'S SIMPLE METHODOLOGY

START

Project Initiation and Alignment
- Project kickoff and stakeholder alignment
- Define business objectives and success criteria
- Confirm scope, timeline, and roles

Deliverables: Project plan and kickoff documentation

IMMERSE

Environment Discovery and Requirements Gathering
- Current firewall and network architecture review
- Existing firewall configuration analysis (rule count, NAT complexity, feature usage)
- Security policy and rulebase analysis
- Application and traffic flow review
- VPN tunnel inventory (site-to-site and remote access)
- SSL/TLS decryption requirements
- Management platform assessment (migrating to FMC or cdFMC)
- Logging and SIEM integration requirements
- Compliance and cyber insurance requirements
- Pilot scope definition

Deliverables: Current state assessment and pilot scope

MAP

Architecture and Policy Design
- Firewall architecture and placement design
- Network segmentation and zone model
- Access control and IPS policy framework
- NAT and VPN design
- Migration and rollout plan

Deliverables: Architecture diagram and design document

PROVE

Pilot Validation
- Firewall installation and base configuration
- FMC deployment or integration
- Pilot policy implementation
- Limited user or application cutover
- Threat detection and policy testing
- Success criteria validation

Deliverables: Pilot results report and validated configuration

LAUNCH

Production Deployment
- Production firewall rollout
- Full policy implementation
- Application and user migration
- Final tuning and validation

Deliverables: Production deployment completion

EVOLVE

Optimization and Operational Transition
- Policy refinement and threat tuning
- Operational runbooks and documentation
- Knowledge transfer sessions
- Executive closeout

Deliverables: Low-level design document, operational runbook, and final project report

sales@GoBTA.com 678-951-8980 GoBTA.com

Schedule A Call

Cisco Secure Firewall Service Overview

ENGAGEMENT SCOPE

Deployment Size	Firewalls	Rule Count	Advanced Features	Engineer Hours	PM Hours	Duration
Small	Up to 2	Up to 200	Basic (ACL, NAT)	60–100	24	3–5 Weeks
Mid-Size	Up to 6	Up to 500	Up to 2 (e.g., IPS, VPN, SIEM)	100–160	40	5–8 Weeks
Large	> 6	> 500	> 2 (e.g., SSL decryption, IPS tuning, HA, complex VPN)	Custom	Custom	Custom

CUSTOMER RESPONSIBILITIES

- **Provide access to network diagrams and firewall policies**
- **Supply application and traffic flow documentation**
- **Support pilot communications and change management**
- **Provide required Cisco firewall hardware, licenses, and rack/VM resources**

OPTIONAL ADD-ON SERVICES

- Advanced IPS tuning and threat hunting
- Micro-segmentation architecture
- Integration with Cisco ISE or Zero Trust initiatives
- Managed firewall operations
- Cyber insurance and compliance advisory

HOW TO ENGAGE BTA

When you identify a customer opportunity, BTA will:

1. Scope the engagement — Joint call to qualify the opportunity and size the deployment
2. Deliver a proposal — BTA provides a statement of work for your customer
3. Execute the project — BTA engineers deliver using the SIMPLE methodology
4. Transition to operations — Knowledge transfer and runbook handoff to the customer

Contact your BTA partner representative to get started.