FROLGATE TECHNOLOGY GROUP
Helping You Serve Your Customers Better

Customer Experience offers for Secure Remote Worker

Increase Remote Access VPN capacity, provide DNS security and advanced malware protection to end users, and manage security risks effectively with Cisco CX.

With the unexpected outbreak of the COVID-19 pandemic, and customers acclimatizing to the new reality of remote working, organizations need to ensure more than ever that their VPN Remote Access capacity and connectivity can manage the incremental workload, while keeping security intact.

Cisco Customer Experience (CX) understands the need and has introduced a suite of enhanced security service packages for Remote Access, based on CX expertise and best practices to help you maintain business continuity. Cisco Consulting, Design and Implementation, Business Continuity Triage, and Incident Response Services help analyze your current VPN design and configuration, and contain recommendations for additional VPN capacity planning, design and configuration. Deploy Umbrella and Amp for Endpoints on remote clients rapidly to provide DNS security and malware protection. Manage security risks and incident response in the event of security breaches with Cisco Talos Incident Response Retainer. Cisco is also offering free Self-Help resources such as Ask the Expert webinar sessions, where Cisco SMEs help you address your VPN connectivity challenges to manage your remote policies.

Cisco Security experts engage with you via Cisco's remote collaboration platform, and all services packages offer specific customer deliverables in the form of summary recommendations, security remediation guidance, and post-implementation support to ensure efficient deployment and operationalization.

Benefits

- Get the support you need during the COVID-19 pandemic with our Customer Experience (CX) expertise, best practices, and analytical insight
- Accelerate deployment of VPN capabilities to enhance capacity and deliver endpoint security with Umbrella and AMP for Endpoints
- Manage security risks with advisory support and ensure incident response preparedness with Cisco Talos Incident Response Retainer

FROLGATE TECHNOLOGY GROUP
Helping You Serve Your Customers Better

Cisco Customer Experience offers for Secure Remote Worker

Expert and Self-Help Resources Free (90 days)

Free Ask the Expert sessions, free videos and instructions

SME Consulting Services for Remote Access

SME consulting support and recommendations

VPN Capacity Design and Implementation Service (Small)

Design, configuration, and implementation of VPN-related capabilities (1 VPN cluster)

VPN Capacity Design and Implementation Service (Medium

Design, configuration, and implementation of VPN-related capabilities (up to 2 VPN clusters)

Cisco Services for DNS Implementation for Remote Workers

Fast deployment of Cisco Umbrella DNS security using proven practices

Cisco Services for AMP for Endpoints Security Deployment

Design, configuration, and implementation services for Endpoint Security with AMP

Business Continuity Triage Services

Security experts assess the security posture and provide recommendations

Cisco Talos Incident Response Retainer

Triage, coordination, investigation (analysis and forensics), and containment

FROLGATE TECHNOLOGY GROUP
Helping You Serve Your Customers Better

What it does

Expert and Self-Help resources with Ask The Expert Webinars

One-to-many interactive technical sessions led by Cisco experts, focused on helping with VPN implementation and onboarding.

Cisco SME Consulting Services for Remote Access

Offers VPN capacity planning, configuration review and design recommendations. Cisco SMEs start by reviewing your IT environment spanning VPN configuration, security policies, hardware capacity, licensing, and bandwidth requirements. Based on thorough assessment, CX experts recommend design, resiliency and configuration recommendations to help increase VPN capacity and accelerate Remote Access. Simultaneously, Cisco Security experts focus on identifying any security vulnerabilities and gaps, and recommend policy-based security remediation measures to ensure uninterrupted VPN connectivity.

Key CX deliverables:

- Cisco delivers a Recommendation Summary Report supported by up to 40 hours of remote expert guidance to help your IT team speed VPN capacity planning and accelerate security management

Cisco Services for VPN Capacity Design and Implementation (Small)

Offers design, configuration and implementation services to help increase capacity of VPN Remote Access. Support includes one pair of Firewalls [Firepower Threat Defense (FTD) or Adaptive Security Appliance (ASA)], with up to 5 group policies, with CX Experts reviewing VPN configurations, security policies, hardware capacity, and bandwidth needs to determine your current technical set-up. We then help configure the firewall for basic configuration requirements (e.g. IP addressing, routing, high availability, etc.), and deliver documentation with strategic recommendations based on current/ future utilization requirements.

Key CX deliverables:

- Recommendation Summary Report
- Implementation details of Firewall VPN-related capabilities
- Integration with one (1) existing authentication system
- Maintenance window rollback script
- 8-hours of post-implementation support **Services for Business Continuity Triage**

Cisco Services for VPN Capacity Design and Implementation (Medium)

Offers a broader scope of deployment with up to two (2) VPN clusters, three (3) devices per cluster (FTD or ASA), and up to 10 group policies. The Medium services package includes all of the VPN capabilities and security measures covered in the Small package- including assessment of VPN configurations, security policies, hardware capacity, bandwidth requirements etc., and also covers a larger pool of VPN clusters and group policies at a more cost-effective price.

Key CX deliverables:

- Recommendation Summary Report
- Implementation of Firewalls VPN related capabilities
- Integration with one (1) existing authentication system
- Maintenance window roll back script
- 8-hours post-implementation support

Cisco Services for Business Continuity Triage

Offers a dedicated Cisco Enterprise Security Advisor (ESA), that ensures alignment of security programs to business goals, defines the security architecture for the computing environment, and ensures that security policies are properly designed, implemented and enforced. Based on an agreed-upon scope, Cisco experts focus on reviewing the current security posture of your environment, then determine the right security engagement model by administering some of the recommendations that best align to your business goals.

- Revisiting shifting IT security priorities during a global health crisis
- Providing a view of IT risks and the potential impact on your operational/ financial strategies
- Developing a risk remediation roadmap that includes recommended risk treatment options
- Recommending strategies to support the COVID-19 response and mitigate data privacy concerns

Key CX deliverables:

- An Executive Summary Report, short-term Business Continuity roadmap, and Risk Heatmap focused on Cisco security and network solutions

FROLGATE TECHNOLOGY GROUP
Helping You Serve Your Customers Better

Cisco Services for DNS Security Implementation for Remote Workers

Cisco Services for DNS Security Implementation for Remote Workers offers fast deployment of Cisco Umbrella DNS security using proven practices, reduced downtime leveraging expert planning, and reduced risk during and after implementation based on Cisco's vast experience. Cisco CX experts conduct remote customer consultation to gather requirements and then configure Umbrella dashboards for roaming computer traffic. We then configure and deploy up to 10 Umbrella Roaming Clients (URC or AnyConnect Roaming Security Module (AC-RSM) endpoint clients and help integrate with one Active Directory (AD) domain. This protects remote workers from malicious Internet sites and helps easily enforce web content category filtering by leveraging specialized CX security experts and best practices on DNS security deployment.

Key CX deliverables:

- Solution Design Document
- Implementation of Umbrella Off-Network Endpoint Security
- Post Implementation Support and Knowledge Transfer

Cisco Services for AMP for Endpoints Security Deployment

Cisco Services for AMP for Endpoints Security Deployment offers design, configuration, and implementation services to enhance Endpoint Security with AMP. CX experts conduct a pre-deployment review session for strategy and design elements, collaboratively define AMP for Endpoints policies, and validate an alpha implementation. Post-deployment, CX engineers help validate the performance of the deployment and provide remote tuning support by leveraging expert guidance and strategic recommendations on configuration, deployment and verification.

Key CX deliverables:

- Provides pre-deployment, deployment, and post-deployment activities
- Small: Up to five thousand (5,000) customer endpoints
- Large: Up to twenty-five thousand (25,000) customer endpoints
- Endpoints interacting with Cisco's securely hosted cloud from the Internet (Public Cloud); Out of scope: *Private Cloud*

Cisco Talos Incident Response Retainer

Cisco Talos Incident Response Retainer provides emergency Incident Response which includes triage, coordination, investigation (analysis and forensics), and containment. Customers can leverage Talos consultants through Insights on Demand, and also gain access to one or more proactive services like Readiness Assessment, Compromise Assessment, Threat Hunting, Table Top Exercises, Cyber Range, and Plans and Playbooks. Customers get actionable threat intelligence through enhanced services that are based on the latest malware campaigns, as well as full access to Cisco's tools during an incident, providing a broader understanding of all threats within the network. This helps accelerate faster response time due to the combination of world-class incident response and threat intelligence capability from CX experts.

Key CX deliverables:

- Emergency Incident Response Report
- Proactive Assessment Report which may include one or more of the following
  - Incident Readiness Assessment Report
  - Incident Plan and Playbook
  - Tabletop Exercises Report
  - Threat Hunting Report
  - Compromise Assessment Report

Next Steps

Contact Frolgate Technology for a DEMO, Presentation or Proof of Concept

sales@froltech.co.zw | www.froltech.co.zw

We enable and empower businesses and people to achieve more with less