MyFloridaNet-2
VPN SERVICE DESCRIPTIONS

KELLY CANNON

MFN-2 Training

Revised: August 31, 2018

Agenda

- VPN Services Overview
- Centralized - Client To LAN VPN
- Centralized - Clientless VPN
- Centralized - LAN To LAN VPN
- Distributed - Site To Site VPN
- Distributed - Dynamic VPN - GET VPN

VPN Services Overview

- There are 5 different VPN services in two categories available on MFN-2
  - Centralized VPN
    - Tunnel established remotely and terminating on Cisco Firepower Firewall acting as VPN gateway at IAGs
      1. Client-to-LAN
      2. Clientless
      3. LAN-to-LAN
  - Distributed VPN
    - Tunnel established remotely and terminating on customer CPE or beyond it on a rented VPN appliance
      1. Site-to-Site
      2. Dynamic VPN (GET VPN)

VPN Services Descriptions

HARRIS

VPN Type	Description	Example Application
Centralized – Client-to-LAN	Remote user Cisco AnyConnect tunnel to MFN-2 VPN appliance at IAG	User connects to an agency server on an agency network via laptop in a hotel
Centralized - Clientless	SSL/HTTPS proxy between remote user computer and agency applications via MFN-2 VPN appliance at IAG	User logs in to time card server and completes and signs time card via a browser (HTTPS)
Centralized – LAN-to-LAN	Tunnel from remote VPN router/appliance to MFN-2 VPN appliance at IAG	Agency partner connects to an agency's network over the Internet
Distributed – Site-to-Site	Tunnel from remote VPN router/appliance to MFN-2 agency premise router or VPN appliance	Agency partner connects to an agency's network over the Internet
Distributed - Dynamic VPN (GET VPN)	Multiple MFN-2 sites communicate via dynamic tunnels using group key encryption	State agency encrypts sensitive data over MFN-2 core

Centralized VPN Features and Benefits

HARRIS®

Features	Benefits
VPN session tunnels terminate connections at the MFN-2 centralized VPN appliance	Alleviates the need to implement VPN hardware at multiple agency locations within MFN-2
	Guards MFN-2 customers against network attacks as the unencrypted traffic is inspected and monitored through IDS and additional cloud firewalls in the IAGs
Digital certificates provide global load balancing at geographically diverse IAGs	Minimizes disruptions to customer services
Provisioned, managed, and monitored by the MFN-2 NOC/SOC	Account creation and activation
	Service level performance guarantees
	Leverages MFN-2 Security Information and Event Management (SIEM) capability

Client-to-LAN Features and Benefits

HARRIS

Features	Benefits
Cisco AnyConnect Secure Mobility Client	Tunnel is built from client computer to outside interface of the MFN-2 centralized VPN appliance
	Traditional IPSEC client-based VPN
2-factor authentication	Username (ex. johnadams) and passcode (PIN + token)
Downloadable ACLs	Permits VPN clients to only access the locations their agency requires for them such as web servers, applications, and networks
Split tunneling option	Allows agency defined traffic through the VPN while all other Internet traffic is routed outside the VPN tunnel through the client's ISP
	Without this option, traffic that is not intended for agency resources will be dropped
Posture Validation	Checks remote user configuration for active firewall, operating system, software patches, and antivirus software

Client-to-LAN Details

- User downloads and installs VPN client via MFN-2 centralized VPN appliance
- User launches the Cisco AnyConnect Security Mobility client application
- User authenticates with MFN-2 VPN appliance using 2-factor authentication
- Centralized VPN appliance performs posture validation using Cisco Identity Services Engine (ISE)

Remote Location

MFN-2 Internet Access Gateway

Internet

Internet Access Gateway

MFN-2 Core Network

Agency VRF

Agency Data Center

Encrypted Tunnnel

Application Data Flow

Split Tunneling

Any Connect

MFN-2 Core Router

Edge Router

Notes:
- *Internet access is provided by remote location*
- *Resource accessibility is based on user group association and VPN permission profiles*
- *Agency administrator pre-defines resource accessibility*
- *Split tunneling is an option at an additional cost*

Client-to-LAN Ordering and Pricing

HARRIS®

- Subscription to this service, as well as the optional split tunneling service, and the agency resources reachable via this service, must be:
  - Authorized by the agency administrator
  - Ordered in CSAB
  - Approved by DMS
- VPN profile must be loaded in CSAB by agency administrator

Order	NRC	MRC
Client-to-LAN cost per user	$ 80.25	$5.89
Split tunnel cost per user	$ 53.50	$1.07

Client-to-LAN in the CSAB

Client-to-LAN in the CSAB

Client-to-LAN in the CSAB

Clientless Features and Benefits
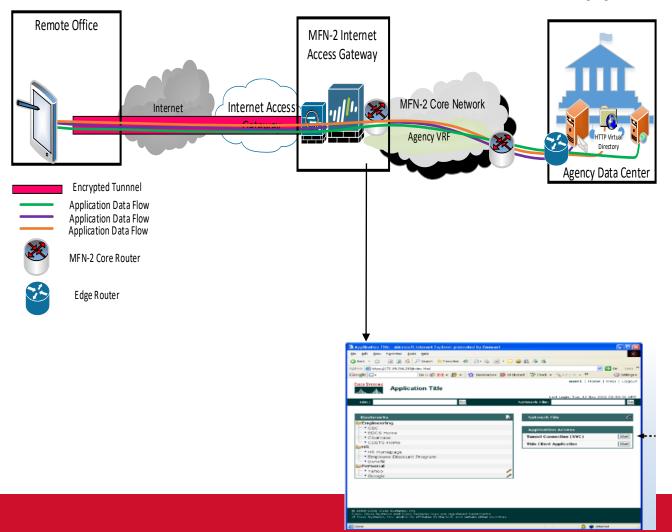
HARRIS®

Features	Benefits
HTTPS interface	Tunnel is built from client computer to web interface of the MFN-2 centralized VPN appliance No Cisco AnyConnect Secure Mobility Client application necessary
2-factor authentication	Username (ex. johnadams) and passcode (PIN + token)
ACLs	Permits VPN clients to only access the web services their agency requires for them

Clientless Details

- User enters URL of MFN-2 VPN server via web browser
- User authenticates with MFN-2 VPN appliance using 2-factor authentication

- User is presented with webpage of agency specific web applications such as Outlook and Citrix Desktop
- Layer 7 session proxies IP traffic between remote device and MFN-2 agency

Notes:
- *Internet access is provided by remote location*
- *Agency administrator predetermines applications presented*
- *Resource accessibility is based on user group association and VPN permission profiles*
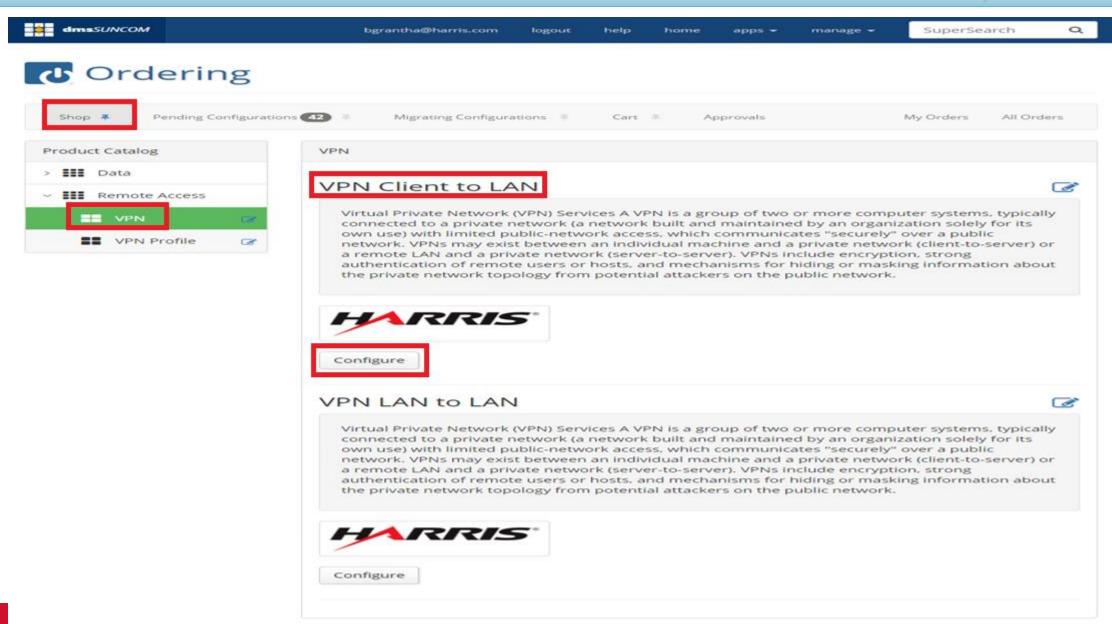
Clientless Ordering and Pricing

- Subscription to this service and the agency resources reachable via this service, must be:
  - Authorized by the agency administrator
  - Ordered in CSAB
  - Approved by DMS
- VPN profile must be loaded in CSAB by agency administrator
- List of servers and/or URLs for access must be provided

Order	NRC	MRC
Clientless per user	$ 80.25	$5.35

Clientless in the CSAB

Clientless in the CSAB

Clientless in the CSAB

LAN-to-LAN Details

- VPN tunnel is provisioned between MFN-2 centralized VPN appliance and another VPN appliance device at remote office
  - Remote device could be router or firewall
  - Remote termination is on host specific public IP address

- Ability to perform NAT on MFN-2 inbound traffic into DMS specified IP range for routing across Common Services VRF

Notes:
- *Agency administrator and DMS predefine agency's network accessibility (VRFs)*
- *Remote partner provides their VPN appliance and associated software*
- *MFN-2 provider works with agency partner to configure partner's tunnel endpoint*

Partner Office

MFN-2 Internet Access Gateway

Agency Data Center

Internet

Internet Access Gateway

MFN-2 Core Network

Agency VRF

Encrypted Tunnnel

Application Data Flow

Edge Router

MFN-2 Core Router

VPN Appliance

Agency Router
(Harris Provided or Customer provided)
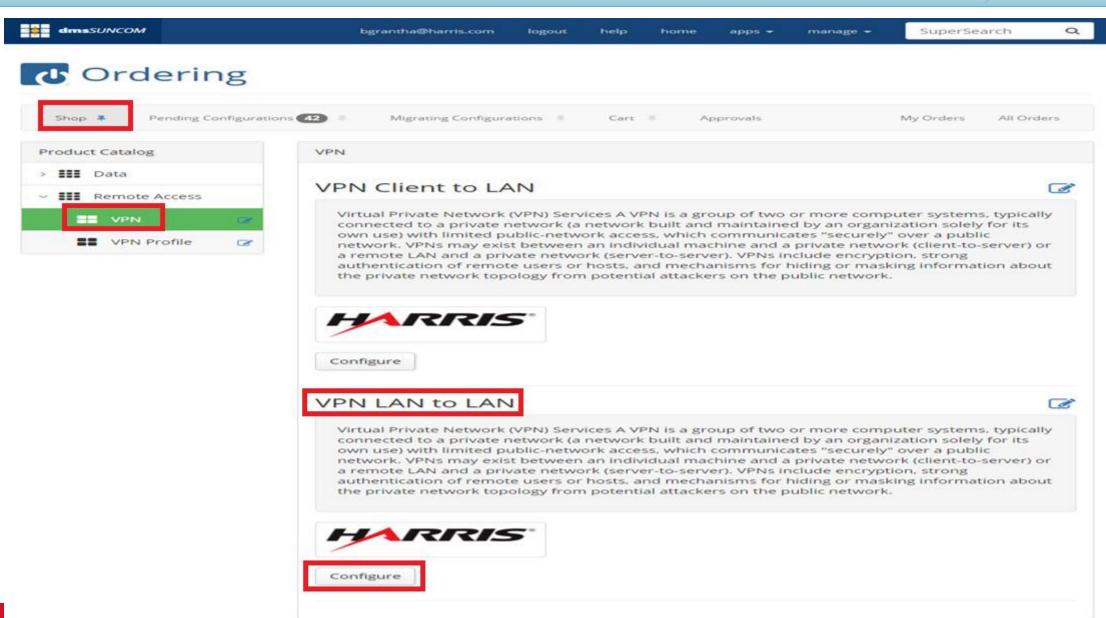
LAN-to-LAN Ordering and Pricing

HARRIS®

- Price depends on whether the agency CPE is provided by Harris or the agency
- Subscription to this service and the agency resources reachable via this service, must be:
  - Authorized by the agency administrator
  - Ordered in CSAB
  - Approved by DMS

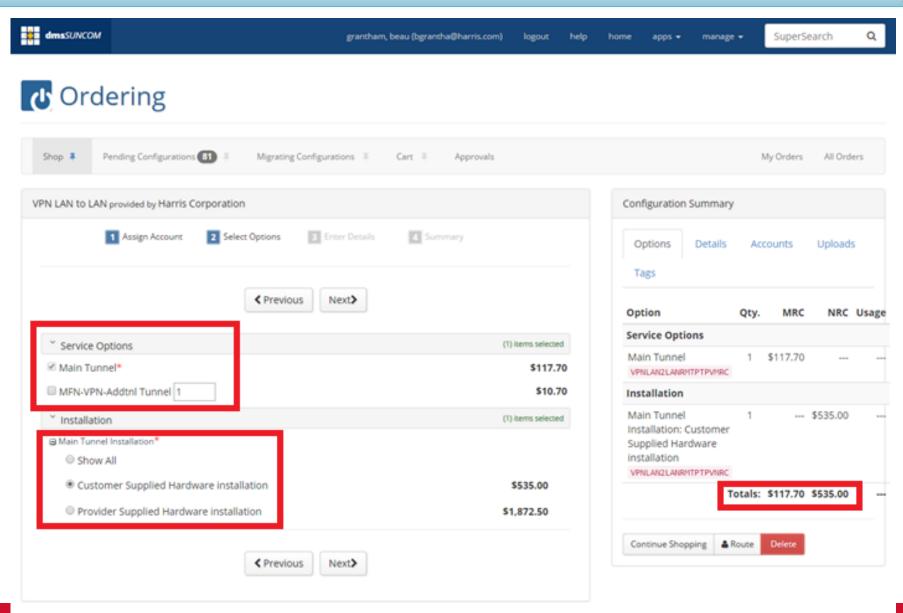| CPE	Description	NRC	MRC
Harris provided	Includes installation and configuration of router or VPN appliance plus first tunnel on a per agency basis	$1,872.50	$117.70
Customer provided	Remote partner provides their hardware appliance including software configurations Includes first tunnel on a per agency basis	$535.00	$117.70
Any	Rate per tunnel for each additional LAN-to-LAN tunnel	$53.50	$10.70

LAN-to-LAN in the CSAB
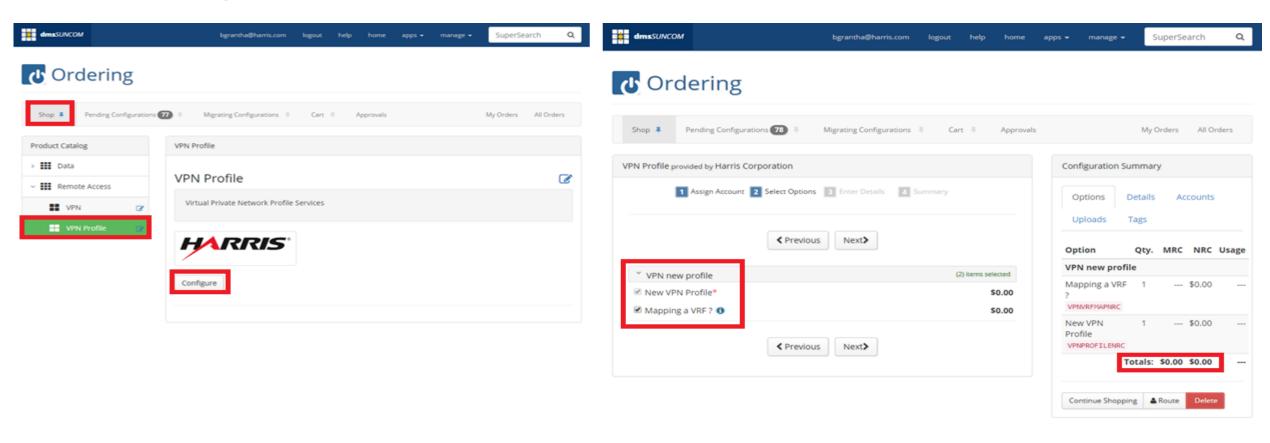
LAN-to-LAN in the CSAB

LAN-to-LAN in the CSAB

Centralized VPN Profiles

- All centralized versions of VPN orders require VPN Profile information which serves as an access list

- If customer does not already have a profile, they must create a new one in the CSAB

- If customer wants to map their profile to VRF other than Common Services VRF, they must check to select **Mapping a VRF?**

Centralized VPN Profiles

Distributed Site-to-Site Features and Benefits

Features	Benefits
VPN session tunnels terminate connections at agency premise hardware, either router or firewall	Leverages existing hardware of agency customer
Multiple VPN design models available, such as IPSec, GRE, and FlexVPN	Individualized design
Bypasses MFN-2 centralized VPN gateway	True end-to-end tunnel
Over Internet or Intranet	

Distributed Site-to-Site via MFN-2 Intranet

- Securely connects MFN-2 customer sites to MFN-2 customer sites over MFN-2 Intranet

- VPN tunnel terminates between originating MFN-2 agency VPN appliance and destination MFN-2 agency VPN appliance

- Termination is on IP address provided by State or by agency

- Typically uses standard IPSec tunnels

Notes:
- *VPN termination hardware can be MFN-2 provided or agency provided*
- *Harris managed router required to tunnel to partner office on Common Services VRF*
- *MFN-2 provider works with agency to configure tunnel endpoints*

Agency Data Center

MFN-2 Internet Access Gateway

MFN-2 CPE

MFN-2 Core Network

Customer VRF

MFN-2 CPE

Agency Data Center

MFN-2 CPE

Encrypted Tunnel

Application Data Flow

MFN-2 Core Router

Agency Router
(Harris Provided or Customer provided)

Agency VPN Appliance
(Harris Provided or Customer provided)

Distributed Site-to-Site via Internet

HARRIS®

- Securely connects remote partner sites to MFN-2 customer sites over unsecure Internet

- VPN tunnel terminates between MFN-2 agency VPN appliance and partner VPN appliance

- Termination is on public IP address provided by State and partner public IP address
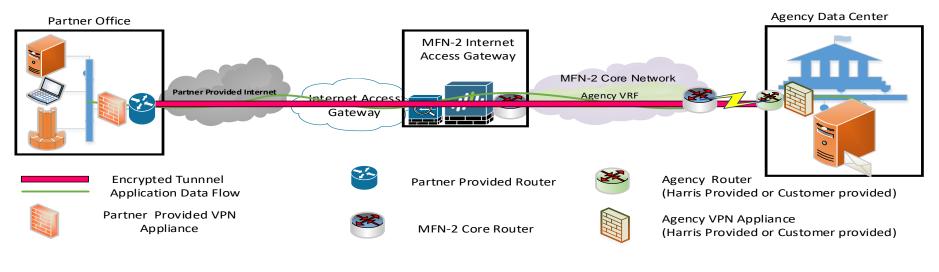
- Typically uses standard IPSec tunnels

Notes:
- *Agency VPN termination hardware can be MFN-2 provided or agency provided*
- *Harris managed router required to tunnel to partner office on Common Services VRF*
- *Remote partner provides VPN hardware for remote location*
- *Remote VPN tunnel endpoint and Remote LAN IP address ranges need to be provided by Customer*
- *MFN-2 provider works with agency to configure tunnel endpoints*

Partner Office

MFN-2 Internet Access Gateway

Partner Provided Internet

Internet Access Gateway

MFN-2 Core Network
Agency VRF

Agency Data Center

Encrypted Tunnel
Application Data Flow

Partner Provided VPN Appliance

Partner Provided Router

MFN-2 Core Router

Agency Router
(Harris Provided or Customer provided)

Agency VPN Appliance
(Harris Provided or Customer provided)

Distributed Site-to-Site Ordering and Pricing

HARRIS®

- Harris managed router is required

- Price is cost of management fee

- No selection in CSAB for Distributed Site To Site VPN
  - When ordering this service, customer should check to select **Encryption (Static)**

- Then on **Summary** page of CSAB, select **Uploads** tab and click to **Attach File** with all the particulars of the distributed VPN

Order	NRC	MRC
Harris managed CPE (mandatory)	$0.00	$30.90

Distributed Site-to-Site in the CSAB

Distributed Dynamic VPN Features and Benefits

HARRIS®

Features	Benefits
Group encryption	Ensures low latency and jitter by enabling full-time, direct communications between sites, without requiring transport through a central hub
Key server	Eliminates complex peer-to-peer key management with group encryption keys
Tunneless	Preserves actual source and destination IP addresses rather than using tunnel addresses thereby avoiding overlay routing
Unicast and multicast	Both supported

Distributed Dynamic VPN Details

HARRIS®

- Unicast and multicast encryption across the MFN-2 core

- Based on Cisco GET VPN which uses group key for encryption and decryption

- Key servers distribute keys and policies to group members (CPE)

Key Servers
- Validate Group Members
- Manage Security Policy
- Create Group Keys
- Distribute Policy Keys
- Replicate data between other Key Servers

MFN-2 Internet Access Gateway Tallahassee

MFN-2 Internet Access Gateway Miami

Key Management Server

Primary Key Server To CPE

Secondary Key Server To CPE

Router with Encryption Key SW

Common Services VRF

MFN-2 Core Network

Customer VRF

MFN-2 CPE

MFN-2 CPE

MFN-2 CPE

Notes:
- *VPN termination hardware can be Harris provided or agency provided*
- *Harris managed router required*
- *DMVPN is also available on a case-by-case basis*

Group Members
- CPE Routers
- Encryption Devices
- Route secure and unsecure data based on policy

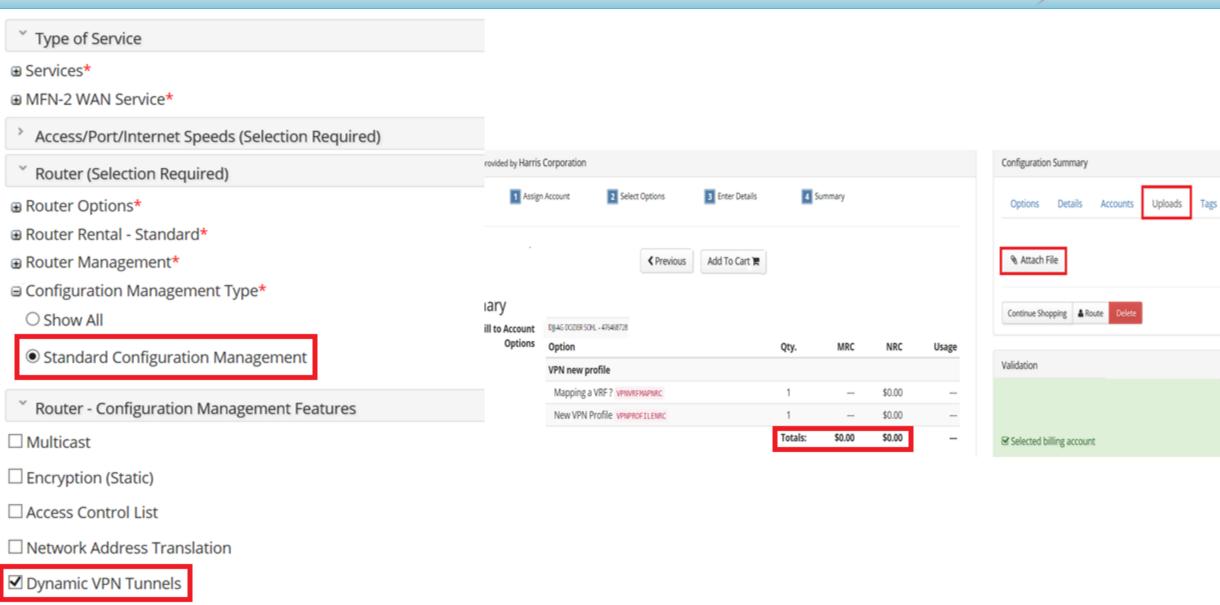# Distributed Dynamic VPN Ordering and Pricing

HARRIS®

- Harris managed router is required
- Price is cost of management fee
- No selection in CSAB for Distributed Dynamic VPN
  - When ordering this service, customer should check to select **Dynamic VPN Tunnels**
- Then on **Summary** page of CSAB, select **Uploads** tab and click to **Attach File** with the particulars of the distributed VPN

Order	NRC	MRC
Harris managed CPE (mandatory)	$0.00	$30.90

Dynamic VPN in the CSAB

HARRIS®

End of VPN Service Description