CISCO VALIDATED PROFILE

Routing
Private WAN—GETVPN Vertical

April 2016

Table of Contents

Profile Introduction

Cisco is transforming the network edge with Cisco ASR 1000 Series Aggregation Services Routers and Cisco 4000 Series Integrated Services Routers (ISRs), new lines of midrange routers that establish a new price-to-performance class offering, benefiting both enterprises and service providers. These routers provide a great opportunity for simplifying the WAN edge and significantly decreasing network operating expenses (OpEx). By efficiently integrating a critical set of WAN edge functions such as WAN aggregation, Internet edge services, firewall services, VPN termination, etc. into a single platform, enterprises can meet their business objectives by facilitating deployment of advanced services in a secure, scalable, and reliable manner while minimizing the total cost of ownership (TCO).

Cisco WAN aggregation solutions distinguish themselves from other solutions by offering multiservice routers with the highest performance, availability, and density for concurrent data, security, voice, and application-acceleration services with maximum headroom for growth. The solutions feature embedded security, performance, and memory enhancements, and high-performance interfaces featuring the latest WAN technologies can help enterprises meet the needs of the most demanding WAN network.

Cisco provides the most feature-rich and flexible VPN solutions in the industry. Cisco VPN solutions integrate advanced network intelligence and routing to deliver reliable transport for complex mission-critical traffic, such as voice and client-server applications, without compromising communications quality. These solutions are built on the underlying VPN technologies:

- Dynamic Multipoint VPN (DMVPN–GRE tunnel-based)
- Group Encrypted Transport VPN (GETVPN–tunnel-less)
- Easy VPN, SSL VPN, IPSec sVTi, IPSec dVTi (virtual template-based)
- Static & dynamic crypto maps

Each technology has it benefits and is customized to meet specific Enterprise WAN deployment requirements.

This documents covers the GETVPN solution in a Private WAN network.

The Cisco IOS Group Encrypted Transport VPN (GETVPN) is a tunnel-less VPN technology that provides end-to-end security for network traffic. Cisco IOS GETVPN preserves the original source and destination IP addresses information in the header of the encrypted packet for optimal routing. Hence it is largely suited for an enterprise running over a private multiprotocol label switching (MPLS)/IP-based core network.

Because GETVPN is deployed in a Private WAN network, this profile is named the *Private WAN GETVPN profile*.

Table 1 summarizes the key areas on which this profile focuses.

Table 1 *Profile feature summary*

Deployment areas	Features
Security	GETVPN GM with GDOI/G-IKEv2 GETVPN KS with mixed group COOP KS Group Security Association Time-based anti-replay (TBAR) PKI-based authentication FailClose ACL, local ACL on GETVPN group member (GM)
Services	QoS, AVC, FNF, ZBFW
IPv6 migration	IPv4 only, IPv6 only, dual stack
Network planning & trouble-shooting	Flexible NetFlow (FNF) Application Visibility & Control (AVC) Embedded Packet Capture (EPC) MPLS, BGP
Efficient network management	LiveAction

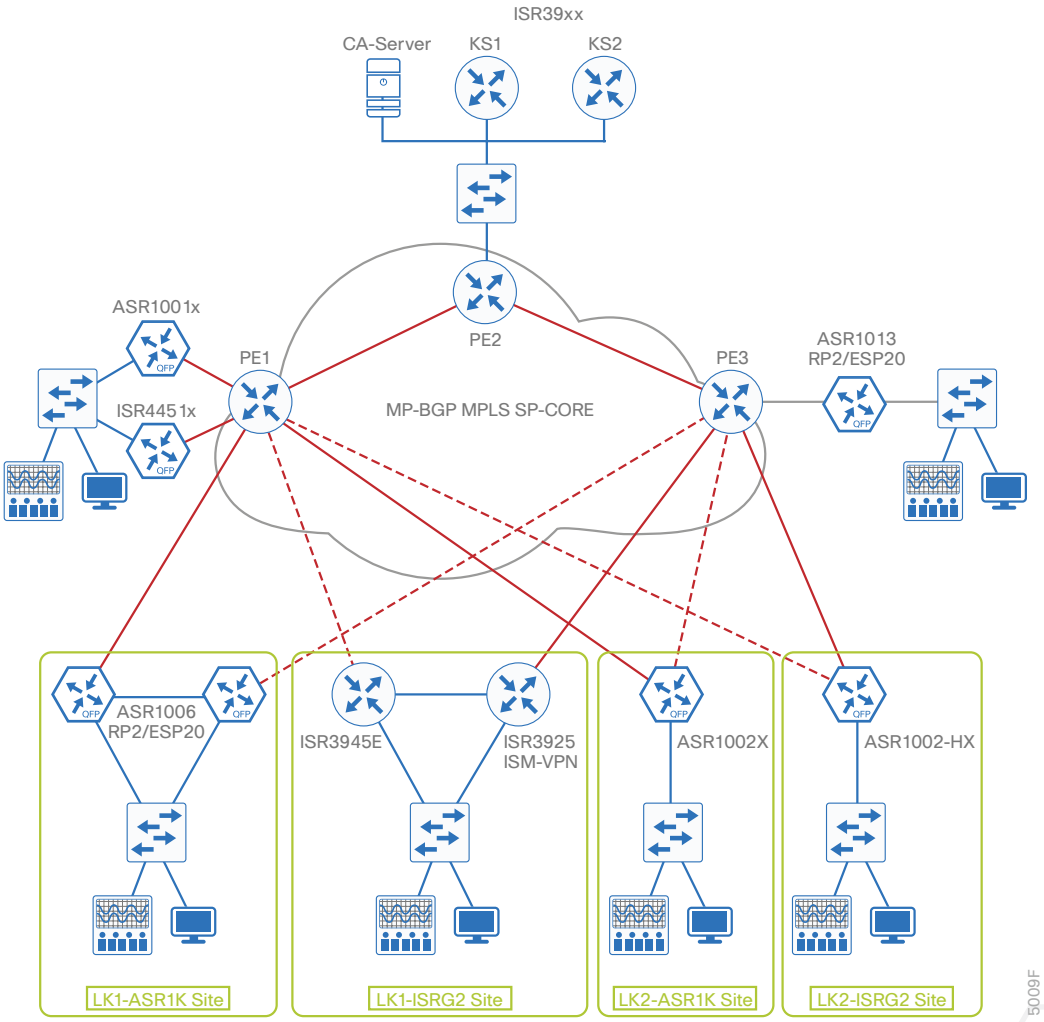
Network Profile

Based on the research, customer feedback, and configuration samples, the Private WAN GETVPN Profile is designed with a generic deployment topology that you can easily modify to fit any specific deployment scenario.

TOPOLOGY DIAGRAM

Figure 1 shows the topology for Private-WAN GETVPN profile.

Figure 1 *Topology overview*



HARDWARE & FEATURE SPECIFICATIONS

This section of describes the 3-D feature matrix where the hardware platforms are listed along with their place-in-network (PIN)

Key Vertical Features

Table 2 defines the 3-D hardware, PIN, and the features deployed. The scale of these configured features, the test environment, list of endpoints, and hardware/software versions of the network topology are defined later.

Table 2 *3-D Feature Summary with Hardware and PIN*

Deployment layer (PIN)	Platforms	Critical vertical features
Key server (KS)	Primary KS—ISR3945/ASR1001x Secondary COOP KS—ISR2951	GDOI group Mixed group with GDOI/G-IKEv2 Time-Based Anti-Replay (TBAR) CTS SGT Inline Tagging TEK/KEK Lifetime Suite-B/Non-Suite-B algorithms COOP Key Server PKI Based Authentication SNMP (GDOI MIB) GETVPN CoPP
Group member	ASR1002x ASR1001x ASR1013(RP2/ESP200) ASR1002-HX ISR4451x ASR1006(RP2/ESP40) ISR3925 ISR3945e	GDOI/G-IKEv2 vrf-lite GM PKI Based Authentication IPv4/IPv6/Dual-Stack Local ACL/Fail-Close ACL QoS ZBFW Application Visibility Control (AVC)/Flexible NetFlow (FNF) SNMP (GDOI MIB) GM Routing Awareness Dual-Homed/Multi-Homed GM site IPSLA EPC Vrf-aware GDOI GETVPN with SGT-inline tagging
MPLS-Core	PE1—ASR1004 PE2—ASR1006 PE3—ASR1004	MPLS BGP
IOS CA	CA Server—ISR3925	PKI

Hardware Profile

Table 3 defines the set of relevant hardware, servers, test equipment, and endpoints that are used to complete the end-to-end deployment.

This list of hardware, along with the relevant software versions and the role of these devices, complement the actual physical topology defined in Figure 1.

Table 3 Hardware profile of servers and endpoints

VM and HW	Software versions	Description
Ixia	IxNetwork and IxExplorer version X	Generate traffic streams and to emulate dot1x clients
Spirent	Spirent Test Center	Generate dual stack traffic
SNMPMibToaster	SNMPMibtoaster Tool	To run snmp mib walk and to do access testing, range testing, syntax testing on a MIB
LiveAction	Version 4.0	To collect the FNF statistics
ISIC Tool	Version 4.0	ISIC is a suite of utilities to exercise the stability of an IP Stack and its component stacks (TCP, UDP, etc.)

TEST ENVIRONMENT

This describes of the features and the relevant scales at which the features are deployed across the physical topology. Table 4 lists the scale for each feature.

Table 4 Private WAN GETVPN: feature scale validated in this profile

Feature	Scale
KS scale	
Group membersGM per group	ISR-G2 KS: 4000 ASR1000 KS: 4000
Group membersGM per KS	ISR-G2 KS: 4000 ASR1000 KS: 4000
Groups per KS	100
Registration rate	40 GMs/second
Groups per KS	20
KS ACL	Up to 100 Cisco Application Control Engines (ACEs) per ACL
GM scale	
VRF-lite GMs per box	100 (ASR1K)
Registration rate	40 GMs/second

Use Case Scenarios

TEST METHODOLOGY

The use cases listed in Table 5 are executed using the Topology shown in Figure 1, along with the test environment shown in Table 4.

With respect to the longevity for this profile setup, the CPU and memory use are monitored overnight as well as during the weekends, along with any mem-leak checks. In order to test the robustness, certain negative events are triggered during use-case testing.

USE CASES

Table 5 describes the use cases that are executed on the Private-WAN GETVPN Profile. These use cases are divided into buckets of technology areas to show the complete coverage of the deployment scenarios.

These technology buckets comprises are composed of system upgrade, security, network services, monitoring & troubleshooting, simplified management, and system health monitoring, along with system and network resiliency.

Table 5 *List of use case scenarios*

No.	Focus area	Use cases
System upgrade		
1	GM upgrade	Network admin wants to upgrade GMs from GDOI to G-IKEv2 seamlessly. ▪ All of the configuration should be migrated seamlessly during the upgrade/downgrade operation. ▪ In Service Software Upgrade (ISSU)
2	GDOI to G-IKEv2 migration	Network admin wants to migrate from GDOI to G-IKEv2. ▪ Bring up KS and GM with GDOI ▪ Make the GDOI group on the KS mixed, which can accept GDOI and G-IKEv2 GMs ▪ Configure G-IKEv2 profile under the GDOI group on GM ▪ Registration is successful and GM is upgraded seamlessly.
3	KS upgrade	Network administrator should be able to perform KS upgrade and downgrade between releases seamlessly. ▪ All of the configuration should be migrated seamlessly during the upgrade/downgrade operation. ▪ ISSU ▪ Upgrade secondary KS to the new image and then the primary KS.

Table 5 continued

Security		
4	GM routing awareness	Network admin wants to have routing based on crypto status. ▪ Dual Homing Scenario ▪ Configure EOT and associate it to the gdoi group. Verify the traffic goes through other GM when there is a crypto error on the first GM through which the traffic was going initially
5	Fail-Close ACL	Network admin wants to drop unencrypted traffic ▪ Apply Fail-Close ACL on the WAN interface of the Group Member. Traffic between the GMs drops until the both the GMs register successfully.
6	Suite-B	Network admin wants to use Suite-B algorithms for encryption ▪ Configure Key Server with Suite-B encryption algorithms ▪ GMs registration is successful and traffic passes through seamlessly
Network services		
7	QoS	Network admin needs to enhance user experience by ensuring traffic and application delivery using QoS policies for GETVPN interfaces. ▪ Traffic types: VOIP, Video, Data ▪ Policing and shaping
8	ZBFW	Network admin to secure the traffic using ZBF ▪ Inspect traffic based on type of traffic or source/destination address
9	CoPP	Network admin to apply control plane policing for the GETVPN control traffic ▪ Inspect Configure Access-lists to segregate desirable (OSPF/BGP/LDP) & undesirable control-plane traffic like (TCP/UDP/ICMP/fragments) & normal traffic (like ICMP) and deny the rest ▪ Configure class-maps to match these ACLs ▪ Configure policy-map with policing for these classes, apply the policy-map under the control-plane
Monitoring & troubleshooting		
10	EPC	Network admin should be able to troubleshoot the network by capturing and analyzing the traffic. ▪ Embedded Packet Capture ▪ Wireshark
11	NetFlow	Enable IT admins to determine network resource use and capacity planning by monitoring IP traffic flows using Flexible NetFlow ▪ Traffic types: IPv4, IPv6 ▪ LiveAction

Table 5 continued

12	SNMP	Network admin should be able to use SNMP for monitoring. ▪ SNMP mibwalk
13	AVC	Enable IT admins to determine network resource use and capacity planning by monitoring IP traffic flows using Application Visibility and Control. ▪ Traffic types: IPv4, IPv6, HTTP ▪ LiveAction
14	IPSLA	Network admin should be able to troubleshoot the network by enabling the IPSLA. ▪ IPSLA probes from GM to KS ▪ IPSLA probes from GM to remote GM
Simplified management		
15	Prime-Trouble-shooting	Simply network troubleshooting and debugging for IT admins ▪ Monitor network for alarms, syslogs, and traps
System health monitoring		
16	System health	Monitor system health for CPU use, memory consumption, and memory leaks during longevity
System & network resiliency, robustness		
17	System resiliency	Verify system-level resiliency during the following events: ▪ Active RP failure/RP Switchover ▪ Active/Standby ESP failure ▪ WAN/LAN Interface flaps ▪ SIP/SPA reload/OIR
18	Network resil-iency	Verify that the system holds well during a network level resiliency ▪ GETVPN primary and COOP KS split ▪ KS aggressive rekey

Table 5 continued

19	Negative events, triggers	Verify that the system holds well and recovers to working condition after the following negative events are triggered: ▪ Config changes–add/remove config snippets, config replace ▪ Routing protocol interface flaps ▪ IPSec, GDOI, G-IKEv2 events such as clear gdoi sessions, clear sa counters, change TEK/KEK lifetimes, modify KS ACL on the fly ▪ QoS events such as adding/removing QoS policy, modifying the ACL, modifying the class map ▪ Adding/deleting/appending/prepending ACEs in the KS ACL and issuing rekey ▪ Enable/disable TBAR on KS and rekey ▪ Enable/disable SGT inline tagging on KS and rekey

Appendix A

You can find example configurations at the following location:

http://cvddocs.com/fw/cvpconfig-routing

Please use the feedback form to send comments and suggestions about this guide.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.