

# CSG

## Cisco Validated Profile Series

### Enterprise Routing

Cisco Secure Branch with Cisco ISR 4000/ISR  
1000/ASR 1000 Routers

---

# Table of Contents

<b>1. Profile introduction</b> .....	<b>3</b>
<b>2. Network profile</b> .....	<b>4</b>
a. Topology diagram and hardware specifications .....	4
2.1. ISR4451 as a branch .....	6
2.2. ISR4221 as a branch .....	7
2.3. C1101 as a branch.....	7
2.4. C1113-8P as a branch .....	8
2.5. ISR4351 as a branch .....	8
2.6. ISR4461 as a branch .....	9
i. Key vertical features .....	9
ii. Hardware profile .....	10
b. Test environment .....	10
<b>3. Use-case scenarios</b> .....	<b>11</b>
3.1. Test methodology .....	11
3.2. Use cases .....	11
3.2.1. Security in a branch.....	11
3.2.1.1 Routing .....	11
3.2.1.2 Security.....	11
3.2.1.3 Network services .....	11
3.2.1.4 Simplified management .....	12
3.2.1.5 System health monitoring .....	12
3.2.1.6 System and network resiliency, robustness.....	12
<b>4. Appendix A: Notes</b> .....	<b>12</b>
<b>5. Appendix B: Configurations</b> .....	<b>13</b>

---

## 1. Profile introduction

Cisco is transforming the network edge with Cisco® ASR 1000 Series Aggregation Services Routers, Cisco 4000 Series Integrated Services Routers, Cisco 1000 Series Integrated Services Routers, 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. 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 that can help enterprises meet the needs of the most demanding WAN network.

This Secure Branch profile outlines a typical branch office with an Internet link. Hence, security is very important. Cisco provides a secure branch-in-a-box solution equipped with features described in this document.

With integrated security in the enterprise branch, we get protection against sophisticated threats while maintaining outstanding performance and lowering costs.

With router security we can

- Simplify branch management and save time and money with an all-in-one platform – physical or virtual.
- Respond quickly to threats, mitigate security vulnerabilities, and protect your branches.
- Get visibility and analytics by extending visibility into the branch network and gaining security intelligence.
- Lower costs by using an Internet path to consume less bandwidth and improve application performance.

Highly secure connectivity in the branch is provided by VPN technologies. They protect sensitive enterprise communications.

Branch threat defense is provided by IOS zone-based firewall (ZBFW), Snort IPS, and Cisco Umbrella™ Branch. These features protect the data from malware, intrusions, denial-of-service attacks, and advanced threats.

Visibility allows you to see network traffic and understand a baseline. Analytics uncover anomalous behavior for you to act on. Flexible NetFlow, Application Visibility and Control (AVC), and Encrypted Traffic Analytics (ETA) along with Stealthwatch®, provide the visibility and analytics for the Enterprise Branch.

WAN optimization is provided by Cisco Wide Area Application Services (WAAS). WAAS is a set of WAN optimization solutions that minimize enterprise bandwidth use and accelerate application performance.

This Profile is designed to integrate key requirements in any WAN-aggregation router and to validate the feature interoperability in a typical deployment.

**Table 1.** Secure Branch Profile feature summary

Deployment areas	Features
Security	D MVPN, PKI, ETA, DCA, Cisco Umbrella, IPS/IDS, NAT/PAT, ZBFW
Network planning and troubleshooting	NBAR, FNF, Adaptive QoS, Tunnel QoS
Management and monitoring	SNMP, Syslog Server
System resiliency	Interface flapping, Route Flapping
Network services	OSPF, BGP

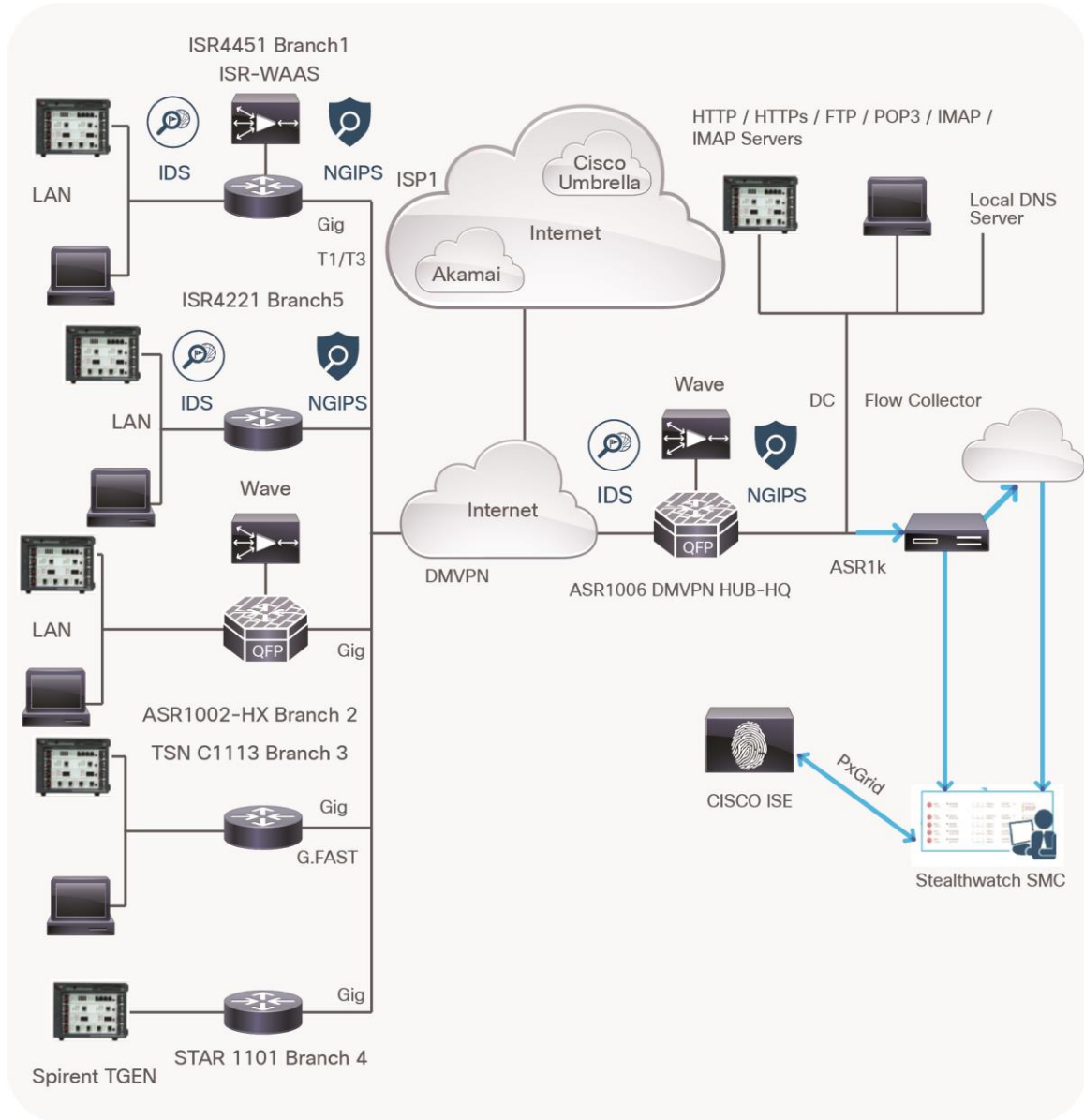
## 2. Network profile

Based on research, customer feedback, and configuration samples, the Security in a Branch with Cisco ISR4000/ASR1000/ISR1K Router Profile is designed with a generic deployment topology that can easily be modified to fit any specific deployment scenario.

### a. Topology diagram and hardware specifications

1. **Disclaimer:** The links between the different network layers in the topology are mainly to facilitate this profile validation across different platform combinations, and the actual deployment could vary based on specific requirement.

**Figure 1.** Secure Branch topology



The left-portion of the topology represents the Enterprise branches. The right portion is the data center hub where the ETA Flow collector and Certificate Authority (CA) server are present. Table 1 provides the hardware specifications and the features tested

**Table 2.** Hardware specifications, platform, and features tested

Network device	Platform	Features/functionalties tested
<b>Data center hub</b>	ASR1004 (RP2/ESP40)	BGP as overlay, OSPF as underlay routing protocols
<b>Core</b>	ASR1006	DMVPN with IKEv2 (Phase 2 and Phase 3)
<b>Branches</b>	ISR4451 (16 GB) ISR4221 (8 GB) ASR1002-HX	PKI-based authentication

	C1101 C1113-8P (G.FAST) ISR4351 (16 GB) ISR4461 (32 GB)	
<b>Certificate Authority (CA) server</b>	Microsoft Certificate Authority	Cisco Umbrella / Direct Cloud Access (DCA)
<b>Encrypted Traffic Analytics (ETA) tools</b>	Cisco Stealthwatch® / Cognitive Threat Analytics (CTA)	IPS/IDS
<b>Links</b>	All 1G links	ETA with Stealthwatch / CTA NAT/PAT Zone-Based FireWall NBAR ISR WAAS FNF AVC Adaptive QoS / Tunnel QoS NETCONF / YANG for ZBFW, ETA and Cisco Umbrella for provisioning the branch

## 2.1. ISR4451 as a branch

Features/functionalities tested on the DMVPN tunnel
• IPsec (IKEv2)
• ETA
• ZBFW
• AVC
• Adaptive QoS / Tunnel QoS
• NBAR
• FNF
• ISR WAAS
• Snort IPS

#### Features/functionalities tested on the LAN/WAN interfaces

- Umbrella Connector / Direct Cloud Access (DCA)
- ETA
- ZBFW
- AVC
- QoS
- NBAR
- Snort IPS
- FNF
- NAT

## 2.2. ISR4221 as a branch

#### Features/functionalities tested on the DMVPN tunnel

- IPsec (IKEv2)
- ETA
- ZBFW
- AVC
- Adaptive QoS / Tunnel QoS
- NBAR
- FNF

#### Features/functionalities tested on the LAN/WAN interfaces

- Umbrella Connector / DCA
- ETA
- ZBFW
- NAT
- QoS
- NBAR
- FNF

## 2.3. C1101 as a branch

#### Features/functionalities tested on the DMVPN tunnel

- IPsec (IKEv2)
- ETA
- ZBFW
- Adaptive QoS / Tunnel QoS
- NBAR

#### Features/functionalities tested on the LAN/WAN interfaces

- Umbrella Connector / DCA
- ETA
- ZBFW
- NAT
- QoS
- NBAR

## 2.4. C1113-8P as a branch

#### Features/functionalities tested on the DMVPN tunnel

- IPsec (IKEv2)
- ETA
- ZBFW
- Adaptive QoS / Tunnel QoS
- NBAR

#### Features/functionalities tested on the LAN/WAN interfaces

- Umbrella Connector / DCA
- ETA
- ZBFW
- NAT
- QoS
- NBAR

## 2.5. ISR4351 as a branch

#### Features/functionalities tested on the DMVPN tunnel

- IPsec (IKEv2)
- ETA
- AVC
- Adaptive QoS / Tunnel QoS
- NBAR
- TrustSec

#### Features/functionalities tested on the LAN/WAN interfaces

- Umbrella Connector / DCA
- ETA
- ZBFW
- NAT
- QoS
- NBAR
- AVC
- TrustSec



## 2.6. ISR4461 as a branch

Features/functionalities tested on the DMVPN tunnel
<ul style="list-style-type: none"> <li>• IPsec (IKEv2)</li> </ul>
<ul style="list-style-type: none"> <li>• ETA</li> </ul>
<ul style="list-style-type: none"> <li>• AVC</li> </ul>
<ul style="list-style-type: none"> <li>• Adaptive QoS</li> </ul>
<ul style="list-style-type: none"> <li>• NBAR</li> </ul>
<ul style="list-style-type: none"> <li>• TrustSec</li> </ul>

Features/functionalities tested on the LAN/WAN interfaces
<ul style="list-style-type: none"> <li>• Umbrella Connector / DCA</li> </ul>
<ul style="list-style-type: none"> <li>• ETA</li> </ul>
<ul style="list-style-type: none"> <li>• AVC</li> </ul>
<ul style="list-style-type: none"> <li>• NAT</li> </ul>
<ul style="list-style-type: none"> <li>• QoS</li> </ul>
<ul style="list-style-type: none"> <li>• NBAR</li> </ul>
<ul style="list-style-type: none"> <li>• TrustSec</li> </ul>
<ul style="list-style-type: none"> <li>• ZBFW</li> </ul>

### i. Key vertical features

Table 2 defines the 3-D hardware, Place-In-Network (PIN), and the features deployed. The scale of these configured features, the test environment, the list of end-points, hardware, and software of the network topology will be defined in the following sections of this guide.

#### 2.4.1.1. Security in a branch

Deployment layer	Platforms	Critical vertical features
<b>Data center hub</b>	ASR1004 (RP2/ESP40)	BGP as overlay, OSPF underlay DMVPN with IKEv2 (Phase 2 and Phase 3) PKI-based authentication ETA with Stealthwatch/CTA Adaptive QoS / Tunnel QoS
<b>Core</b>	ASR1006	OSPF underlay
<b>Branch</b>	ISR4451 (16 GB) ISR4221 (8 GB) ASR1001-HX C1101 C1113-8P (G.FAST) ISR4351 (16 GB) ISR4461 (32 GB)	BGP overlay, OSPF underlay DMVPN with IKEv2 (Phase 2 and Phase 3) PKI-based authentication ETA with Stealthwatch / CTA DCA / Cisco Umbrella IPS/IDS NAT/PAT Zone-Based Firewall NBAR ISR WAAS FNF AVC Adaptive QoS / Tunnel QoS NETCONF/YANG for ZBFW, ETA and cisco Umbrella TrustSec (covered by ISR4461 and ISR4351 only)

**Disclaimer:** Refer to appropriate Cisco.com documentation for release/feature support across different platforms.

## ii. Hardware profile

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

This list of hardware, along with the relevant software versions and the roles of these devices, complements the physical topology defined in Figure 1 of the previous section.

**Table 3.** Hardware profile of servers and endpoints

Virtual machine (VM) and hardware	Software versions	Description
Stealthwatch		Flow exporter for ETA
CTA		For analyzing exported flows from ETA
Cisco UCS®	ESXi 5.5.0	For management and hosting of Windows Virtual Machines, Ixia traffic tool, etc.
Spirent	Spirent CyberFlood	Test tool to generate AppMix traffic and malware traffic
Windows Virtual Machine Clients	Windows 7	Endpoints for testing end-to-end traffic
Ixia	IxLoad	Test tool to generate HTTP, FTP, and DNS traffic

## b. Test environment

This section contains the relevant scales at which the features are deployed across the physical topology. Table 4 lists the scale for each respective feature.

### Disclaimer:

Table 4 captures a sample set of scale values used in one of the use cases. Please refer to appropriate Cisco.com documentation and data sheets for comprehensive scale data.

**Table 4.** Scale for each feature

Feature	Scale
<b>IVRF scale</b>	ISR4451 – 100 ISR4221 – 50 C1101 – 25 C1113 – 30 ASR1001-X - 100 Note that the scales were measured without any feature interactions, such as QoS, AVC, or NBAR, on the tunnel/LAN/WAN interfaces
<b>Traffic scales</b>	ISR4451 - Max 4400 flows with 8k html pages ASR1001-X – Max 7900 flows with 4k html pages TSN – Max 1460 flows with 8k html pages

### 3. Use-case scenarios

#### 3.1. Test methodology

The use cases listed in Table 5, below, will be executed using the topology defined in Figure 1 along with the test environment (see Table 4), already explained in this document.

Images are loaded on the devices under test via the TFTP server using the management interface.

To validate a new release, the network topology is upgraded with the new software image with the existing configuration, comprising the use cases and relevant traffic profiles. New use cases acquired from the field or from customer deployments are added to the existing configuration.

During each use case execution, the Syslog would be monitored closely across the devices for any relevant system events, errors, or alarms. With respect to longevity for this profile setup, CPU and memory usage leaks would be monitored during the validation phase. Furthermore, to test the robustness of the software release and platform under test, typical network events would be triggered while executing the use cases.

#### 3.2. Use cases

Table 5 describes the use cases that were executed on the Secure Branch profile. These use cases are divided into buckets of technology areas to see the complete coverage of the deployment scenarios. Use cases continuously evolve based on the feedback from the field.

These technology buckets comprise Security, Network Services, Monitoring and Troubleshooting, simplified management, system health monitoring, and system resiliency.

##### 3.2.1. Security in a branch

No.	Focus area	Use cases
<b>3.2.1.1 Routing</b>		
1	BGP overlay and OSPF underlay	<ul style="list-style-type: none"><li>• OSPF is used for the underlay.</li><li>• BGP is used for overlay between DMVPN hub and branches.</li></ul>
<b>3.2.1.2 Security</b>		
1	DMVPN	<ul style="list-style-type: none"><li>• DMVPN with IKEv2 between hub and branches</li><li>• DNS queries sent to Umbrella cloud</li></ul>
1	Umbrella Connector without DCA	
2	Umbrella Connector with DCA	<ul style="list-style-type: none"><li>• Umbrella Connector with DCA but no policy enforcement at Umbrella</li><li>• Umbrella Connector with direct cloud access with policy enforcement at cloud</li><li>• Umbrella Connector with DCA but no EDNS or DNSCrypt</li></ul>
3	ETA on branch	<ul style="list-style-type: none"><li>• ETA on branch: enables ETA on WAN/LAN interfaces of branch and export the TLS information to Stealthwatch/CTA.</li></ul>
4	ETA on hub	<ul style="list-style-type: none"><li>• ETA on hub: enables ETA on WAN/LAN interfaces of hub and exports the TLS information to Stealthwatch/CTA.</li></ul>
5	IPS/IDS	<ul style="list-style-type: none"><li>• Snort IPS/IDS on the branch</li></ul>
<b>3.2.1.3 Network services</b>		
1	NAT/PAT	<ul style="list-style-type: none"><li>• Dynamic NAT</li><li>• PAT with interface overload</li></ul>
2	ZBFW	<ul style="list-style-type: none"><li>• Zone-based firewall on the LAN/WAN/DMVPN tunnel interface</li></ul>
3	NBAR	<ul style="list-style-type: none"><li>• NBAR-enabled on the LAN/WAN/DMVPN tunnel interface</li></ul>
4	FNF	<ul style="list-style-type: none"><li>• FNF-enabled on LAN/WAN/DMVPN tunnel interface</li></ul>

No.	Focus area	Use cases
5	AVC	<ul style="list-style-type: none"> <li>• AVC-enabled on the LAN/WAN/DMVPN tunnel interface</li> </ul>
6	QoS	<ul style="list-style-type: none"> <li>• Adaptive QoS on DMVPN hub and spoke</li> <li>• Remove Adaptive QoS and Per Tunnel QoS</li> </ul>
7	AppNav WAAS	<ul style="list-style-type: none"> <li>• ISR WAAS on branch</li> <li>• Also use one-side optimization with Akamai</li> </ul>
<b>3.2.1.4 Simplified management</b>		
6	Monitoring	Exports and monitors logs from the Syslog server
<b>3.2.1.5 System health monitoring</b>		
7	System health	Monitors system health for CPU usage, memory consumption, and memory leaks during longevity
<b>3.2.1.6 System and network resiliency, robustness</b>		
8	System resiliency	Verifies system level resiliency during the following events: <ul style="list-style-type: none"> <li>• Router reload</li> <li>• Interface flaps</li> <li>• Module failures</li> </ul>
9	Negative events, triggers	Verifies that the system holds good and recovers to working condition after the following negative events are triggered: <ul style="list-style-type: none"> <li>• Config changes, including adding/removing config snippets and config replacements</li> <li>• Routing-protocol interface flaps</li> <li>• QoS events such as adding/removing QoS policy, modifying the ACL, modifying the class map</li> </ul>

#### 4. Appendix A: Notes

- Virtual services commands are not visible when a boost license is enabled on ISR4K. ISR WAAS and Snort IPS/IDS cannot be used if a boost license is enabled.
- A network interface module solid-state drive (NIM-SSD) is not supported on ISR4221 (ISR WAAS cannot be used).
- T3/E3 NIMs are also not supported on ISR4221; therefore, testing is not done for T3/E3 interfaces.
- When a boost license is enabled on ISR4221, no difference in crypto throughput is observed either with or without an HSECK9 license. We are hitting the maximum throughput limit on the platform before hitting the maximum crypto throughput.
- FNF is not supported on the LAN VLAN interface on C1101 and C1113.
- ISR WAAS and Snort IPS/IDS are not supported on C1101 and C1113.
- QFP DRAM exhaustion issues are observed on C1101s with features like FNF, AVC, and ETA. QFP DRAM spikes from 60 percent to 90 percent because of which we start to notice %FMFP-3-OBJ\_DWNLD\_TO\_DP\_FAILED messages. We need to be cautious when enabling CPU-intensive features on C1101.
- VLAN scaling was tested up to 30 on C1113 and up to, 25 on C1101.

#### Disclaimer:

Below are some sample configuration snippets to give a general idea of the configuration used in some of the use cases; actual deployments would require further customization. For detailed configuration options and best practices, please refer to the Cisco.com documentation.

---

## 5. Appendix B: Configurations

### Base configuration with DMVPN (with IKEv2) on branch:

```
interface Loopback0
  ip address 21.1.1.4 255.255.255.255
!
interface Loopback1
  description "for pki"
  ip address 9.45.48.8 255.255.255.255
  shutdown
!
interface Loopback2
  ip address 1.1.1.1 255.255.255.255
!
interface GigabitEthernet0/0/0
  description "WAN Interface"
  ip address 11.1.1.1 255.255.255.0
  media-type sfp
  negotiation auto
!
interface GigabitEthernet0/0/1
  description "LAN Interface"
  ip address 50.1.1.1 255.255.255.0
  negotiation auto
!
crypto pki trustpoint TP-self-signed-3077088137
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-3077088137
  revocation-check none
  rsakeypair TP-self-signed-3077088137
!
crypto pki trustpoint test
  enrollment mode ra
  enrollment url http://9.44.49.253:80/certsrv/mscep/mscep.dll
  revocation-check crl
  source interface GigabitEthernet0/0/0
  rsakeypair test 1024
!
```

```
crypto ikev2 proposal CRP_ike-proposal
  encryption aes-cbc-256
  integrity sha256
  group 16
!
crypto ikev2 policy CRP_ike-policy
  match address local 11.1.1.1
  proposal CRP_ike-proposal
!
crypto ikev2 keyring CRP_ike-keyring
  peer DC
    address 0.0.0.0 0.0.0.0
    pre-shared-key cisco123
!
!
crypto ikev2 keyring 10
!
!
crypto ikev2 profile CRP_ike-profile
  match identity remote address 0.0.0.0
  authentication remote pre-share
  authentication local pre-share
  keyring local CRP_ike-keyring
  lifetime 1800
  dpd 120 10 on-demand
!
!
!
crypto ipsec security-association replay window-size 1024
!
crypto ipsec transform-set citi-trans-AES esp-aes 256 esp-sha-hmac
  mode tunnel
!
crypto ipsec profile CRP_ipsec-profile
  set security-association lifetime seconds 900
  set transform-set citi-trans-AES
  set pfs group16
  set ikev2-profile CRP_ike-profile
```

```
!  
!  
interface Tunnell  
  ip address 192.168.1.3 255.255.255.0  
  no ip redirects  
  ip mtu 1400  
  ip nhrp authentication cisco  
  ip nhrp map 192.168.1.1 15.1.1.1  
  ip nhrp map multicast 15.1.1.1  
  ip nhrp network-id 40  
  ip nhrp holdtime 7200  
  ip nhrp nhs 192.168.1.1  
  ip nhrp registration timeout 2400  
  ip nhrp redirect  
  ip tcp adjust-mss 1360  
  cdp enable  
  tunnel source GigabitEthernet0/0/0  
  tunnel mode gre multipoint  
  tunnel key 40  
  tunnel protection ipsec profile CRP_ipsec-profile  
!  
router ospf 1  
  network 1.1.1.1 0.0.0.0 area 0  
  network 11.1.1.0 0.0.0.255 area 0  
  network 21.1.1.4 0.0.0.0 area 0  
  network 22.1.1.1 0.0.0.0 area 0  
!  
router bgp 101  
  template peer-policy NRP_ppt-to-sbal  
    soft-reconfiguration inbound  
    send-community  
  exit-peer-policy  
!  
  bgp router-id 21.1.1.4  
  bgp log-neighbor-changes  
  timers bgp 20 60  
  neighbor 192.168.1.1 remote-as 101  
  neighbor 192.168.1.1 update-source Tunnell
```

```
!  
address-family ipv4  
  network 50.1.1.0 mask 255.255.255.0  
  neighbor 192.168.1.1 activate  
  neighbor 192.168.1.1 inherit peer-policy NRP_ppt-to-sba1  
exit-address-family  
!
```

### **Zone-Based Firewall:**

```
class-map type inspect match-all CMAP2  
  match access-group name zone_acl1  
class-map type inspect match-all CMAP1  
  match access-group name zone_acl  
policy-map type inspect PMAP1  
  class type inspect CMAP1  
    inspect  
  class class-default  
    pass  
policy-map type inspect PMAP2  
  class type inspect CMAP2  
    inspect  
  class class-default  
    drop  
!  
ip access-list extended zone_acl1  
  permit ip any any  
  permit tcp any any  
  permit udp any any  
!  
zone security LAN  
zone security WAN  
zone security WAN1  
zone security LAN1  
zone-pair security LAN-WAN source LAN destination WAN  
  service-policy type inspect PMAP1  
zone-pair security LAN1_WAN1 source LAN1 destination WAN1  
  description zonepair  
  service-policy type inspect PMAP2  
zone-pair security WAN-LAN source WAN destination LAN
```



```
service-policy type inspect PMAPI
!
interface Tunnell
  zone-member security WAN1
!
interface GigabitEthernet0/0/0
  description "WAN Interface"
  zone-member security WAN1
!
interface GigabitEthernet0/0/1
  description "LAN Interface"
  zone-member security LAN1
!
```

#### **App Firewall:**

```
ip access-list extended INTERNET
  deny udp any any eq isakmp
  permit ip 192.168.10.0 0.0.0.255 any
  permit ip 192.168.14.0 0.0.0.255 any
!
class-map type inspect match-any cm1
  match access-group 1
  match access-group name INTERNET
  match protocol dns
  match protocol tcp
  match protocol udp
  match protocol icmp
!
class-map match-any nbar-class
  match protocol amazon
  match protocol amazon-web-services
!
class-map match-any nbar-class-1
  match protocol rediff-com
  match protocol yahoo
  match protocol attribute category consumer-internet
  match protocol attribute category consumer-streaming
!
policy-map type inspect avc nbar-policy
```

```

class nbar-class
  deny
class class-default
  allow
!
policy-map type inspect avc nbar-policy
class nbar-class-1
  allow
!
policy-map type inspect pml
class type inspect cml
  inspect
service-policy avc nbar-policy
class class-default
  drop
!
zone security lan_zone
zone security int_zone
!
zone-pair security lan_zone-int_zone source lan_zone destination int_zone
service-policy type inspect pml
!
interface GigabitEthernet0/0/0
  description "WAN Interface"
  zone-member security int_zone
!
interface GigabitEthernet0/0/1
  description "LAN Interface"
  zone-member security lan_zone
!

```

**Adaptive QoS:**

```

class-map match-any CLASS_AF31
  match dscp af31
  match access-group name ACL_VESSEL_CONTROL_NETWORK_AF31
  match protocol http
!
class-map match-any CLASS_AF41
  match ip dscp af41

```

```
match access-group name ACL_VESSEL_CONTROL_BUSINESS_AF41
match dscp af41
!
policy-map HUB-SAT-CHILD
class CLASS_AF31
set dscp tunnel af31
set ip dscp af31
bandwidth remaining percent 40
class CLASS_AF41
set ip dscp af41
set dscp tunnel af41
!
policy-map HUB-SAT-PARENT
class class-default
shape adaptive upper-bound 4000000000 lower-bound 112000
service-policy HUB-SAT-CHILD
!
ip access-list extended ACL_VESSEL_CONTROL_NETWORK_AF31
permit udp 30.1.1.0 0.0.0.255 50.1.1.0 0.0.0.255
permit udp 50.1.1.0 0.0.0.255 30.1.1.0 0.0.0.255
permit tcp 30.1.1.0 0.0.0.255 50.1.1.0 0.0.0.255
permit tcp 50.1.1.0 0.0.0.255 30.1.1.0 0.0.0.255
!
ip access-list extended ACL_VESSEL_CONTROL_BUSINESS_AF41
permit udp 30.1.1.0 0.0.0.255 50.1.1.0 0.0.0.255
permit udp 50.1.1.0 0.0.0.255 30.1.1.0 0.0.0.255
permit tcp 30.1.1.0 0.0.0.255 50.1.1.0 0.0.0.255
permit tcp 50.1.1.0 0.0.0.255 30.1.1.0 0.0.0.255
permit tcp 50.1.1.0 0.0.0.255 71.1.2.0 0.0.0.255
permit tcp 71.1.2.0 0.0.0.255 50.1.1.0 0.0.0.255
permit udp 71.1.2.0 0.0.0.255 50.1.1.0 0.0.0.255
permit udp 50.1.1.0 0.0.0.255 71.1.2.0 0.0.0.255
!
interface Tunnell
nhp group SPOKE-SAT
nhp map group HUB-SAT service-policy output HUB-SAT-PARENT
!
```

### FNF and ETA Configs:

```
flow record CYBER-RECORD
  match ipv4 tos
  match ipv4 protocol
  match ipv4 source address
  match ipv4 destination address
  match transport source-port
  match transport destination-port
  match interface input
  collect routing next-hop address ipv4
  collect ipv4 dscp
  collect ipv4 ttl minimum
  collect ipv4 ttl maximum
  collect transport tcp flags
  collect counter bytes
  collect counter packets
  collect timestamp sys-uptime first
  collect timestamp sys-uptime last
!
!
flow exporter CYBER-EXPORTER
  description lancope stealthwath flow collector
  destination 20.0.0.100
  source GigabitEthernet0/0/0
  transport udp 2055
!
!
flow monitor CYBER-MONITOR
  description Main NetFlow Cache for the stealthwatch
  exporter CYBER-EXPORTER
  cache timeout inactive 60
  cache timeout active 60
  record CYBER-RECORD
!
et-analytics
  ip flow-export destination 23.1.1.2 2055
!
interface Tunnell
```

```
ip flow monitor CYBER-MONITOR input
ip flow monitor CYBER-MONITOR output
et-analytics enable
!
interface GigabitEthernet0/0/0
description "WAN Interface"
ip flow monitor CYBER-MONITOR input
ip flow monitor CYBER-MONITOR output
et-analytics enable
!
interface GigabitEthernet0/0/1
description "LAN Interface"
ip flow monitor CYBER-MONITOR input
ip flow monitor CYBER-MONITOR output
et-analytics enable
!
```

**AVC:**

```
performance monitor context ezPM profile application-experience
exporter destination 1.1.1.1 source GigabitEthernet0/0/0 port 9999
traffic-monitor all
!
!
performance monitor context ezPM1 profile application-statistics
exporter destination 1.1.1.1 source GigabitEthernet0/0/0 port 999
traffic-monitor application-client-server-stats
!
interface Tunnell
performance monitor context ezPM
performance monitor context ezPM1
!
interface GigabitEthernet0/0/0
description "WAN Interface"
performance monitor context ezPM
performance monitor context ezPM1
!
```

---

**NBAR:**

```
interface Tunnell
  ip nbar protocol-discovery
!
interface GigabitEthernet0/0/0
  description "WAN Interface"
  ip nbar protocol-discovery
!
interface GigabitEthernet0/0/1
  description "LAN Interface"
  ip nbar protocol-discovery
!
```

**PAT:**

```
ip access-list extended INTERNET
  permit ip 50.1.1.0 0.0.0.255 any
  permit ip host 1.1.1.1 any
!
route-map nat2primary permit 1
  match ip address INTERNET
!
ip nat pool NATPOOL 50.100.1.1 50.100.1.100 prefix-length 24
ip nat inside source route-map nat2primary interface GigabitEthernet0/0/0
overload
!
interface GigabitEthernet0/0/0
  description "WAN Interface"
  ip nat outside
!
interface GigabitEthernet0/0/1
  description "LAN Interface"
  ip nat inside
!
```

---

### DCA/Umbrella Connector:

```
class-map match-any umbrella-direct-access
  match protocol dns in-app-hierarchy
  match protocol attribute application-set saas-apps office365
  match protocol google-docs
  match protocol amazon
  match protocol facebook
  match protocol cnn
  match protocol bbc
  match protocol microsoftds
!
policy-map type umbrella umbrella_dca_policy
  class umbrella-direct-access
    direct-cloud-access
!
parameter-map type regex local_domain
  pattern www.cisco.com
  pattern www.cisco1.com
  pattern www.cisco2.com
  pattern www.cisco3.com
  pattern www.4.com
  pattern www.5.com
  pattern www.6.com
  pattern www.7.com
  pattern www.8.com
  pattern www.1.com
!
parameter-map type umbrella global
  token <token>
  local-domain local_domain
  dnscrypt
  udp-timeout 5
!
interface GigabitEthernet0/0/0
  description "WAN Interface"
  umbrella out
!
interface GigabitEthernet0/0/1
```

---

```
description "LAN Interface"  
umbrella in direct-cloud-access umbrella_dca_policy test1  
!
```

**IPS/IDS:**

```
interface VirtualPortGroup0  
 ip address 18.1.1.1 255.255.255.252  
 no mop enabled  
 no mop sysid  
!  
interface VirtualPortGroup1  
 ip address 19.1.1.1 255.255.255.252  
 no mop enabled  
 no mop sysid  
!  
virtual-service UTDIPS  
 vnic gateway VirtualPortGroup0  
  guest ip address 18.1.1.2  
 vnic gateway VirtualPortGroup1  
  guest ip address 19.1.1.2  
 activate  
!  
utd engine standard  
  threat-inspection  
  threat protection  
  policy security  
utd engine advanced  
utd  
  all-interfaces  
  redirect interface VirtualPortGroup1  
  engine standard  
!
```

**ISR WAAS:**

```
class-map type appnav match-any SN_OR_WCM  
  match access-group name SN_OR_WCM  
class-map type appnav match-any RTSP  
  match access-group name RTSP  
class-map type appnav match-any AUTOWAAS
```



```
match access-group name AUTOWAAS
class-map type appnav match-any MAPI
  match protocol mapi
class-map type appnav match-any HTTP
  match access-group name HTTP
class-map type appnav match-any HTTPS
  match access-group name HTTPS
class-map type appnav match-any CIFS
  match access-group name CIFS
class-map type appnav match-any Citrix-CGP
  match access-group name Citrix-CGP
class-map type appnav match-any Citrix-ICA
  match access-group name Citrix-ICA
class-map type appnav match-any NFS
  match access-group name NFS
class-map type appnav match-any EPMAP
  match access-group name EPMAP
!
policy-map type appnav AUTOWAAS
  description AUTOWAAS global policy
  class SN_OR_WCM
    pass-through
  class HTTP
    distribute service-node-group AUTOWAAS-SNG
    monitor-load http
  class MAPI
    distribute service-node-group AUTOWAAS-SNG
    monitor-load mapi
  class HTTPS
    distribute service-node-group AUTOWAAS-SNG
    monitor-load ssl
  class CIFS
    distribute service-node-group AUTOWAAS-SNG
    monitor-load cifs
  class Citrix-ICA
    distribute service-node-group AUTOWAAS-SNG
    monitor-load ica
  class Citrix-CGP
```

```

    distribute service-node-group AUTOWAAS-SNG
    monitor-load ica
class EPMAP
    distribute service-node-group AUTOWAAS-SNG
    monitor-load MS-port-mapper
class NFS
    distribute service-node-group AUTOWAAS-SNG
    monitor-load nfs
class AUTOWAAS
    distribute service-node-group AUTOWAAS-SNG
!
interface VirtualPortGroup31
    ip address 40.0.0.1 255.255.255.0
    no mop enabled
    no mop sysid
!
interface AppNav-Compress1
    ip unnumbered VirtualPortGroup31
    no keepalive
!
interface AppNav-UnCompress1
    ip unnumbered VirtualPortGroup31
    no keepalive
!
virtual-service AUTOWAAS
    profile ISR-WAAS-750
    vnic gateway VirtualPortGroup31
    guest ip address 40.0.0.2
    activate
!
service-insertion service-node-group AUTOWAAS-SNG
    description "AUTOWAAS"
    service-node 40.0.0.2
    node-discovery enable
!
service-insertion appnav-controller-group AUTOWAAS-SCG
    description "AUTOWAAS"
    appnav-controller 40.0.0.1

```

```
!  
service-insertion service-context waas/1  
  appnav-controller-group AUTOWAAS-SCG  
  service-node-group AUTOWAAS-SNG  
  service-policy AUTOWAAS  
  vrf default  
  enable  
!  
interface Tunnell  
  service-insertion waas  
!
```

#### **TrustSec:**

```
aaa authorization network cts-mlist group ISE  
cts authorization list MLIST  
crypto ikev2 cts sgt  
no ip redirects  
cts sgt inline  
cts role-based sgt-map sgt 4  
cts role-based sgt-cache egress  
cts manual  
  cts role-based sgt-cache ingress  
cts role-based enforcement  
!  
aaa authentication dot1x default group ISE  
aaa authorization network default group ISE  
aaa authorization network MLIST group ISE  
aaa authorization network cts-mlist group ISE  
aaa authorization auth-proxy default group ISE  
aaa accounting dot1x default start-stop group ISE  
username cisco privilege 15 one-time password 0 cisco  
!  
radius server ISE_SERVER  
address ipv4 10.104.54.195 auth-port 1812 acct-port 1813  
pac key cisco123  
!  
aaa group server radius ISE  
server name ISE_SERVER  
ip radius source-interface GigabitEthernet0/0/0
```

```
!
aaa new-model
aaa session-id common
!
!
interface Tunnell
  cts sgt inline
  cts role-based sgt-map sgt 4
  cts role-based sgt-cache egress
!
interface GigabitEthernet0/0/2
  description "LAN interface"
  cts manual
  policy static sgt 3
  no propagate sgt
  cts role-based sgt-cache ingress
```




---

**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 <https://www.cisco.com/go/offices>.

 Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)