SD-Access (1.1.x) Firewall Integration
Contents

SD-Access policy model overview ........................................................................................................... 4
Border functionality in SD-Access ........................................................................................................... 5
Firewalls in enterprise use cases ........................................................................................................... 6
  Inter-virtual network traffic ..................................................................................................................... 6
  Exiting fabric traffic ................................................................................................................................. 6
Firewall deployment models .................................................................................................................. 7
Firewall interoperability and policy context in SD-Access ..................................................................... 8
Platform Support ...................................................................................................................................... 9
  SD-Access border platform support ....................................................................................................... 9
  SD-Access firewall integration platform support ..................................................................................... 10
Border Cisco TrustSec and AAA configuration (automated) ................................................................. 10
ISE Configuration .................................................................................................................................... 11
  Network device settings ............................................................................................................................ 11
  Cisco TrustSec settings ............................................................................................................................. 12
  RADIUS settings .................................................................................................................................... 15
  Add ASA as an SXP listener ...................................................................................................................... 15
Firewall Cisco TrustSec and AAA configuration .................................................................................. 19
Policy configuration on the border ......................................................................................................... 22
  Automated border Layer 3 handoff configuration - Configuration for the internal or external border (for the Catalyst 3000, Catalyst 6000, Catalyst 9000, Nexus 7000): ................................................................. 25
  BGP configuration for a single context with the border directly connected to the firewall ............... 34
  Policy enforcement ................................................................................................................................. 38
    Configuration for the internal or external border (for the ASR 1000 Series and the 4000 Series ISR): ................................................................. 38
  Automated border Layer 3 handoff configuration - Configuration for the internal or external border (for the ASR 1000 Series and the 4000 Series ISR): ................................................................. 44
Cisco SD-Access provides automation, device, and network monitoring while delivering segmentation to meet the growing demands of a customer’s network. It provides segmentation through Virtual Routing and Forwarding (VRF) instances. Due to the nature of this segmentation, integration with existing (or upcoming) security requires additional design considerations and configuration.

Cisco® Software-Defined Access (SD-Access) is a powerful combination of the Cisco Digital Network Architecture (Cisco DNA), Campus Fabric, Identity Services Engine (ISE), and Assurance and Analytics. Cisco DNA Center is a centralized management application for your network. Cisco DNA Center simplifies network management so IT can move more quickly, using automation to lower costs, assurance and analytics to improve performance, and security segmentation to reduce risk.

SD-Access radically simplifies the work involved in deploying and operationalizing network segmentation through:

- Technologies on the networking infrastructure such as Virtual Extensible LAN (VXLAN)-based overlay and dynamic group-based policy enforcement
- Identity and device profiling mechanisms to dynamically map endpoints, users, and things to Scalable Group Tags (SGT)
- Controller-based automation of underlay and overlay provisioning, services, and policy provisioning
- Intent-based policy operations
- Analytics to assist with the creation of groups and group policies, assurance of policy enforcement, and business intent
- Consistent policy enforcement for wired and wireless access for workloads in private data centers, public clouds, or Software-as-a-Service (SaaS) applications

Due to the segmentation SD-Access provides, additional design and configuration is needed to implement stateful inspection for SD-Access traffic. This document provides the design, use cases, and necessary configuration to implement firewalls in an SD-Access environment.

Campus fabric was initially introduced as a manual basic infrastructure for building virtual networks based on policy-based segmentation constructs. This fabric is built as an underlay and overlay model. The underlay consists of physical devices that are used as IP transport using traditional routing methods. The fabric overlay is a logical topology that provides services such as host mobility and enhanced security through virtual networks, in addition to normal switching and routing capabilities. The fabric overlay consists of user or Endpoint Identifier (EID) space. The EID space is made up of the IP addresses and prefixes that identify the endpoints. EID reachability across Cisco Locator/ID Separation Protocol (LISP) sites is achieved by resolving EID-to-Routing Locator (RLOC) mappings.

SD-Access provides automation of the campus fabric while also providing visibility into and monitoring of the endpoints, clients, and network (Assurance). SD-Access provides seamless connectivity that is independent of physical topology and provides policy application and enforcement at the edges of the fabric.
SD-Access consists of a single or multiple fabrics that each contain one or two control-plane nodes, border nodes, and edge nodes. The control-plane node is based on LISP and is the map server and map resolver for the endpoints and networks in the fabric. The control-plane node is not responsible for any transport of traffic. The edge node is the access device that the endpoints connect to. The border node is the exit point for the fabric and the entry point into another fabric or another Layer 3 domain. The data plane in the fabric is based on VXLAN, and endpoints are encapsulated and decapsulated at the edge device and border devices as they enter and exit the fabric. The policy plane in SD-Access is based on Cisco TrustSec®.

SD-Access policy model overview

SD-Access policy provides two different contexts for both macro-level segmentation (virtual network, or VN) and micro-level segmentation within a VN (scalable group tags, or SGTs).

**Virtual network:** A virtual network is intended to be used for macro-level network segmentation. Every VN has its own independent VRF instance that is separate from other VRF instances. This separation provides a distinct level of segmentation. SD-Access implements a VN by automating the configuration of the VRF instances onto the fabric devices in the fabric. Each VN is assigned a unique VXLAN ID (VNID). While in the fabric, the VNID is carried in the data plane in the VXLAN header. A VN represents a VRF.

To maintain this segmentation outside of the fabric, the VN context is carried in an 802.1Q tag as a VLAN trunk or VRF-Lite instance.

**Scalable group tags:** For micro-level segmentation, SD-Access uses Cisco TrustSec SGTs that are assigned to endpoints. Users, devices, and things are referenced as endpoints in this solution. An SGT is a logical grouping of these endpoints. SGTs are used in Scalable Group Access Control Lists (SGACLs) to define the access policies of these group-to-group relationships. The SGT is part of the VXLAN header, known in the header as the segment ID (Figure 1).

**Figure 1.** VXLAN header
Endpoints are authenticated into the network and then assigned a VN or a VN and SGT by the ISE’s authorization policies. The VN and SGT can be statically or dynamically assigned to the endpoints.

In SD-Access 1.1, firewalls are not supported in the fabric. As a result, a VN’s configuration is not automated on the firewalls. Customers may want to have stateful inspection (using a firewall) for traffic traversing between VNs or between SGTs within a VN, or they may want to maintain their policies from the fabric to another domain (a data center, another fabric, another Layer 3 domain, etc.). This document provides the necessary design considerations, deployment models, and configuration requirements for implementing these policies in an SD-Access environment.

**Border functionality in SD-Access**

SD-Access has two types of borders: internal and external. A border can also be both internal and external. The functionality of these different types of borders is as follows.

**Rest of company (internal):** This option is for a border that connects to a known network (a device that is part of the company’s network). Examples of this are the data center and another fabric.

**Outside world (external):** This option is for a border that connects to an unknown network (a device that is not part of the company’s network). An example of this would be the Internet.

**Anywhere (internal and external):** This option is for a border that connects to both a known network (a device network that is part of the company’s network) and an unknown network (a device that is not part of the company’s network).

Understanding the border functionality is important to integrating a firewall into SD-Access. With the firewall placement currently outside of the SD-Access fabric, traffic needs to traverse the border(s) to traverse the firewalls. Many enterprises use firewalls in their networks, and firewalls are used for stateful traffic inspection in different parts of a network. SD-Access uses fabrics with LISP and VXLAN that today’s firewalls do not support. This document provides details how to continue to provide stateful inspection in the new SD-Access campus environment.
Firewalls in enterprise use cases

**Inter-virtual network traffic**

Due to the VRF instance construct, VN traffic from one VN cannot access traffic in another VN. There may be a requirement for stateful inspection of traffic traveling from one VN to another VN (Figure 2).

**Figure 2.** Virtual network traffic traversing a firewall

**Exiting fabric traffic**

Traffic exiting the fabric and entering any other domain (Internet, data center, etc.) may be kept separate (through VRFs) or may be leaked (depending on the policy requirements) (Figure 3). The deployment model will depend on the use case.

**Figure 3.** Fabric traffic traversing the firewall and entering another domain
Firewall deployment models

Firewalls may be deployed in a single context or in multiple contexts. To maintain segmentation through a firewall, multiple contexts are recommended. A single context can be used to allow communication between multiple VNs. However, segmentation can still be maintained with a single context by implementing Open Shortest Path First (OSPF) instances for each context or by implementing a different routing protocol for each context. VNs can also be tied to a single context, or each VN can be tied to one context as a part of multiple contexts if allowing communication between two VNs on a multiple-context firewall. Additionally, if there is a border that is dedicated to traffic for a single location (such as the Internet) and a single type of traffic (guest), a single-context firewall can be used (Figures 4 and 5).

**Figure 4.** Single-context firewall deployment (do not need to maintain segmentation during stateful inspection)

**Figure 5.** Multiple-context firewall deployment (need to maintain segmentation during stateful inspection)
In SD-Access 1.1, the border configuration (known as the Layer 3 handoff) is automated. This configuration is applied to the border’s external interfaces to extend the VN context. This deployment model is still supported if the customer desires to connect the firewalls multiple hops away from the border, but the configuration is not documented in this guide. If segmentation is needed from the fabric border and firewall, each hop between the border and firewall will need to carry the VN context. The configuration documented in this guide will need to be applied to each of the hops.

SD-Access 1.1 supports Layer 3 (Routed) mode only. There is no support for Transparent mode. With a Routed-mode firewall, the underlay routing protocol options that are supported are Enhanced Interior Gateway Routing Protocol (EIGRP), OSPF, Border Gateway Protocol (BGP), and Intermediate System to Intermediate System (IS-IS).

**Firewall interoperability and policy context in SD-Access**

In SD-Access 1.1, firewall administration is done on the firewall itself. There is no automation support for firewalls. The policy support is also limited in SD-Access 1.1. By default, the firewall does not have knowledge of the VNs. In order for the firewall to leverage the virtual network classification into the firewall policies, it is necessary to transport the context (VNID and SGT) of the traffic from the fabric to the firewall. In addition, the firewall requires the context of the destination group tag in order to apply the Scalable Group Firewall policy (SGFW) on the basis of the source and destination group tags.

In SD-Access, the virtual network context, also known as a VRF instance, is transported through the 802.1Q tag in a Layer 2 trunk interface on the border (if the border is a Cisco ASR 1000 Series router or 4000 Series Integrated Services Router) or through a Switch Virtual Interface (SVI) (if the border is a Cisco Catalyst® 3000, 6000, or 9000 platform or Cisco Nexus® 7000 Series Switch) (Figure 6). The VRFs will each be mapped to a separate interface on the firewall, or in the case of a firewall with multiple contexts, each VRF will be mapped to a single context. The single-context firewall will merge all of these VRFs into the global routing table on the firewall.

**Figure 6.** Firewall data-plane and policy-plane Integration
The source SGTs are provided through inline tagging in the 802.1Q tag or through the SVI. The destination SGT is provided to the firewall through a Security Group Exchange Protocol (SXP) connection between the ISE and the firewall. SXP is the protocol that Cisco TrustSec uses to propagate the IP-to-SGT mappings to the firewall. SXP is a peering protocol, in which one device acts as an SXP speaker and another device acts as an SXP listener. The SXP speaker is responsible for sending the IP-to-SGT mappings, and the SXP listener is responsible for collecting the IP-to-SGT bindings. For the ISE and firewall integration (not specific to SD-Access), the ISE acts as an SXP speaker to the firewall and the firewall acts as an SXP listener. The SXP communication is over the TCP port 64999, so the path between the ISE and the firewall needs to allow this port. The firewall will need to be manually configured for Authentication, Authorization, and Accounting (AAA) and SXP (either through the Command-Line Interface [CLI] or the Cisco Adaptive Security Device Manager [ASDM]).

The Cisco TrustSec policies for the SGTs that pass through the firewall are created as SGFW rules on the firewall. The SGFW is manually configured via the CLI or ASDM, using the source and destination SGTs. This document provides the CLI configuration for the firewall. The Cisco TrustSec policy rule options available are similar to the options for SGACLs for Cisco switches, routers, wireless controllers, and access points. VN policies can be kept by using a multiple-context firewall or by restricting the share of routes through the BGP routing protocol.

Depending on a customer’s requirements, firewalls may be placed between fabrics or between a fabric and another domain (fabric and the Internet, fabric and data center, etc.). This guide discusses how to implement a firewall outside the fabric for traffic exiting the fabric to another domain. The firewall can be in any of the following placements:

- Directly connected to the internal border
- Directly connected to the external border
- Directly connected to the internal and external border
- Directly connected to a fusion router

Platform Support

### SD-Access border platform support

The following SD-Access border platforms and the corresponding software releases support SD-Access firewall interoperability:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Minimum required software version</th>
<th>802.1Q support</th>
<th>SVI support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Catalyst 6500 Series / 6800 Supervisor Engine 2T or 6T</td>
<td>15.4.1</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Cisco Nexus 7700 with M3 line cards</td>
<td>16.6.2</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Cisco ASR 1000-X platform</td>
<td>16.6.2</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Cisco 4000 Series ISR</td>
<td>16.6.2</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Cisco Catalyst 9300 Series</td>
<td>16.6.2</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Cisco Catalyst 9400 Series</td>
<td>16.6.2</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Cisco Catalyst 9500 Series</td>
<td>16.6.2</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Cisco Catalyst 3650 Series</td>
<td>16.6.2</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Cisco Catalyst 3850 Series</td>
<td>16.6.2</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>

*Can be an external border only, so this will be used only for inspecting traffic that is after the external border.
SD-Access firewall integration platform support

The following SD-Access firewall platforms and the corresponding software releases support SD-Access firewall interoperability:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Minimum software version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco ASA 5500-X with FirePOWER™ Services</td>
<td>6.2</td>
</tr>
<tr>
<td>Cisco ASA high range: 5585-X</td>
<td>ASA 9.8.2</td>
</tr>
<tr>
<td>Cisco Adaptive Security Virtual Appliance (ASAv)</td>
<td>ASAv 9.7.1</td>
</tr>
<tr>
<td>Cisco Firepower® 2100 Series, 4110, 4120, 4140, 4150*</td>
<td>ASA 9.8.2</td>
</tr>
<tr>
<td>Cisco Firepower 9300 Security Appliance*</td>
<td>ASA 9.8.2</td>
</tr>
</tbody>
</table>

* Requires ASA code for SGT destination information.

Integration configuration

This document assumes that the fabric has already been deployed and policy has been defined. Please see the [SD-Access Configuration Guide](#) if these have not yet been done.

Border Cisco TrustSec and AAA configuration (automated)

The border communicates with ISE as a network device, similar to the way it communicates with the firewall. However, in SD-Access the AAA and Cisco TrustSec configuration for the border is automated when the device is provisioned to a site and assigned the border role. This configuration is applied to the border device through the device provisioning in Cisco DNA Center.

**Note:** This configuration is automated from Cisco DNA Center.

```
aaa new-model
aaa group server radius <RADIUS group name>
  server name <RADIUS server name>
  ip radius source-interface <interface used to communicate with ISE>
aaa authentication login default local
aaa authentication enable default enable
aaa authentication dot1x default group <RADIUS group name>
aaa authorization network default group <RADIUS group name>
aaa authorization network <cts list name> <RADIUS group name>
aaa accounting dot1x default start-stop group <RADIUS group name>
aaa login server radius dynamic-author
  client <ISE PSN IP Address> server-key dnalab1
aaa session-id common
```
The border’s VLANs are included in Cisco TrustSec for enforcement.

sd-access-core1(config)#cts role-based enforcement vlan-list <VLANs generated on border that will be handed off to FW/fusion>

**Figure 7.** Firewall data plane and policy plane integration – SXP

ISE Configuration

**Network device settings**

The ISE communicates with the firewall via SXP. The firewall needs to be added into the ISE network devices. At a minimum, the network device IP address needs to be added, along with RADIUS settings. You can add additional information (model name, software version), as well as network device group details (location, device type) to be used in authorization profiles.

In ISE, navigate to Work Centers > TrustSec > Components > Network Devices > **Add**.

Specify the name of the device. The hostname can be used. If the hostname is a Fully Qualified Domain Name (FQDN), the Use Device ID for Cisco TrustSec option cannot be selected. The Cisco TrustSec device ID allows only alphanumeric characters. The following screen shots show the required sections. You can populate additional fields or change the default required fields. The IP address needs to be the IP address of the firewall that will be used to communicate with the ISE.
Cisco TrustSec settings

If the device ID has only alphanumeric characters, the Use Device ID for TrustSec box can be selected. If not, the device ID needs to be manually specified in the ISE and then on the firewall.

**Note:** If the device ID contains any nonalphanumeric characters, this field will not be highlighted with an error until the box is initially checked. The box will need to be unchecked and checked again to see whether the device ID contains any unallowed characters.

The device ID needs to be the same as the Cisco TrustSec credentials ID configured on the ASA. The Cisco TrustSec Notifications and Updates configuration determines how often the Cisco TrustSec environment data is downloaded to the firewall. If the SGTs are changed often and must be updated immediately or less than 1 day after a change, the default setting should be changed to the necessary update timing interval.
The Protected Access Credentials (PAC) are used to establish a secure RADIUS connection between the ISE and the firewall for the downloading of the Cisco TrustSec environment data, also known as the security group table. Click Generate PAC to generate these credentials. Complete the Identity, Encryption Key, and PAC Time to Live fields. The PAC will need to be regenerated when it expires. It will need to be saved locally and then uploaded to the firewall.
Save the file. The PAC file needs to be added to the firewall. The firewall can import the PAC file from a USB flash drive or from a remote server via TFTP, FTP, HTTP, HTTPS, or SMB.

**Note:** If using a USB device to upload the PAC file, it will not show up under disk1 if you remove the USB device to copy the PAC file from your machine. You will need to do a reload after inserting the USB device containing the PAC file to view the disk1 contents.

Upload the PAC file to the firewall.

```
   sd-access-fw(config)# cts import-pac disk0:/sd-access-fw.pac password psssst
   PAC file successfully imported
```
RADIUS settings
RADIUS is used to download the Cisco TrustSec environment data, also known as the security group table. The RADIUS shared secret needs to be configured in the ISE as well as in the firewall. These settings need to be the same on both the ISE and the firewall. The minimum required configuration is given below. You can enable IP Security (IPsec) communication between the ASA and ISE. This guide does not provide the steps to do so, but you can find them in the IPsec to Secure NAD Communication document.

### Add ASA as an SXP listener
The ISE needs to be configured with the ASA as an SXP Listener. The ISE will be the SXP speaker. Connect to the ISE.

Firewalls require an SXP password for the connection. If the password field is blank, the connection will not be established.

If using the default password type, the default password is the SXP global password. This needs to first be defined in the ISE under Work Centers -> TrustSec -> Settings. Access the SXP settings on the left side of the window. This password will be the same as the password defined on the ASA.
Navigate to Work Centers ➔ TrustSec ➔ SXP. Click Add. Populate the IP address that will be used for communication with the ASA. This IP address needs to be able to reach the ISE. Select DEFAULT as the password type.
Add Border as an SXP listener

The ISE needs to be configured with the ASA as an SXP Listener/Speaker. The ISE will be the SXP speaker/listener. The recommended is to have them be both. If using the default password type, the default password is the SXP global password. This needs to first be defined in the ISE under Work Centers -> TrustSec -> Settings. Access the SXP settings on the left side of the window. This password will be the same as the password defined on the ASA.

The SXP Connection will need to be established for each VRF using the IP address of the SVI.
ISE configuration

For the policy to be maintained from the fabric domain (border) to the firewall, the SGTs need to be propagated to the upstream device (firewall, fusion, or each device between border and firewall). The ISE needs to be configured to communicate with the Cisco firewall to provide the destination group tags. This guide provides a configuration for connectivity directly to the border node.

ISE SGTs are created within the ISE or can be manually configured on the devices. SGT creation is out of scope for this document. For how to create SGTs, consult the Cisco TrustSec site.

The ISE communicates with the firewall via SXP. The ISE also communicates with the border for propagating and enforcing external traffic. The firewall needs to be added into the ISE network devices. At a minimum, the network device IP address needs to be added, along with RADIUS settings. You can add additional information (model name, software version), as well as network device group details (location, device type) to be used in authorization profiles. The firewall and border need to be added as SXP devices and the Network devices need to have a policy for SGT assignment.

Navigate to Work Centers -> Trustsec -> Trustsec Policy to assign the network device authorization. We will use the default Trustsec_Devices SGT.
For the policy to be maintained from the fabric domain (border) to the firewall and back, the SGTs need to be propagated to the upstream device (firewall, fusion, or each device between border and firewall). The ISE needs to be configured to communicate with the Cisco firewall to provide the destination group tags. This is done via SXP. This guide provides a configuration for connectivity directly to the border node.

Firewall Cisco TrustSec and AAA configuration

The following section gives the configuration that is required on the firewall for AAA and Cisco TrustSec.

Note: The AAA and Cisco TrustSec configuration is currently not automated from Cisco DNA Center and needs to be applied manually to the firewall.

**CLI**

Firewall AAA configuration:

```
sd-access-fw(config)#aaa-server dnac-radius-group protocol radius
sd-access-fw(config)#exit

sd-access-fw(config)#aaa-server dnac-radius-group (<interface used to communicate with ISE>) host <ISE PSN IP Address>
sd-access-fw(config-aaa-server-host)# key 0 ciscodna

e.g.
aaa-server dnac-radius (outside) host 192.168.101.179
```

SXP global configuration:

```
sd-access-fw(config)#cts server-group dnac-radius-group
sd-access-fw(config)#cts sxp enable
sd-access-fw(config)#cts sxp reconciliation period 60
sd-access-fw(config)#cts sxp retry period 60
sd-access-fw(config)# cts sxp connection peer 192.168.101.179 password default mode peer listener
```
To verify that the SXP connectivity is successful, issue the following command:

```
sd-access-fw# sh cts sxp con
```

SXP               : Enabled
Highest version   : 3
Default password  : Set
Default local IP : Not Set
Reconcile period  : 60 secs
Retry open period : 60 secs
Retry open timer  : Not Running
Total number of SXP connections: 1
Total number of SXP connections shown: 1

```
Peer IP           : 192.168.101.179
Source IP         : 192.168.104.50
Conn status       : On
Conn version      : 3
Local mode        : Listener
Ins number        : 1
TCP conn password : None
Reconciliation timer : Not Running
Delete hold down timer : Not Running
Duration since last state change: 0:00:21:33 (dd:hr:mm:sec)
```

Alternatively, it can be verified on ISE under Work Centers ➔ TrustSec ➔ SXP:

Firewall Cisco TrustSec interface configuration:

```
 sd-access-fw(config)#cts manual
 sd-access-fw(config)#policy static sgt <unique from ISE SGT value between 2 and 65519> trusted
```

Once the PAC is on the firewall and the AAA and Cisco TrustSec configuration is added, the firewall will download the Cisco TrustSec environment data. It can be manually downloaded by issuing the following command:

```
 sd-access-fw(config)#cts refresh environment-data.
 sd-access-fw #sh cts environment-data
```

```
CTS Environment Data
Current state = COMPLETE
Last status = Successful
Local Device SGT:
```
SGT tag = 0-00:Unknown

Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
   Server: 172.25.0.179, port 1812, A-ID 5FCDAE5933D9D583F87BC669F1F2F7EB
       Status = ALIVE
           auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins,
               deadtime = 20 secs
Multicast Group SGT Table:
Security Group Name Table:
   0-31:Unknown
   2-31:TrustSec_Devices
   3-31:Network_Services
   4-31:Employees
   5-31:Contractors
   6-31:Guests
   7-31:Production_Users
   8-31:Developers
   9-31:Auditors
   10-31:Point_of_Sale_Systems
   11-31:Production_Servers
   12-31:Development_Servers
   13-31:Test_Servers
   14-31:PCI_Servers
   15-31:BYOD
   16-31:all
   17-31:Camera
   18-31:HVAC
   19-31:Lights
   20-31:IP_Phones
   255-31:Quarantined_Systems
Environment Data Lifetime = 86400 secs
Last update time = 19:04:54 UTC Mon Dec 4 2017
Env-data expires in   0:22:33:36 (dd:hr:mm:sec)
Env-data refreshes in 0:22:33:36 (dd:hr:mm:sec)
Cache data applied           = NONE
State Machine is running
Policy configuration on the border

The virtual networks are now defined and the border is initially provisioned into the fabric (the configuration shown is a result of provisioning a border node without yet configuring the Layer 3 handoff). These are the VRFs that were created through Policy→ Virtual Networks.

```
METRO-C1# sh run | sec vrf
vrf definition Contractors
  rd 1:4099
  !
  address-family ipv4
    route-target export 1:4099
    route-target import 1:4099
  exit-address-family
vrf definition Corporate
  rd 1:4100
  !
  address-family ipv4
    route-target export 1:4100
    route-target import 1:4100
  exit-address-family
vrf definition DEFAULT_VN
  rd 1:4098
  !
  address-family ipv4
    route-target export 1:4098
    route-target import 1:4098
  exit-address-family
vrf definition Guest
  rd 1:4101
  !
  address-family ipv4
    route-target export 1:4101
    route-target import 1:4101
  exit-address-family
vrf definition IoT
  rd 1:4102
  !
  address-family ipv4
    route-target export 1:4102
    route-target import 1:4102
  exit-address-family
vrf definition Mgmt-vrf
  !
  address-family ipv4
```
The BGP configuration that was pushed from the initial border configuration while provisioning the border without yet configuring the Layer 3 handoff is as follows:

```
exit-address-family
!
address-family ipv6
exit-address-family
vrf forwarding Mgmt-vrf
eid-table vrf DEFAULT_VN
eid-table vrf Contractors
eid-table vrf Corporate
eid-table vrf Guest
eid-table vrf IoT
vrf PCI
vrf IoT
vrf DEFAULT_VN
vrf Corporate
snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-up vnet-trunk-down
```

```
METRO-C1#sh run | sec bgp
   route-import database bgp 100 locator-set rloc_d9ad1062-bb97-4503-a478-9bd59e79f27e
   route-import database bgp 100 locator-set rloc_d9ad1062-bb97-4503-a478-9bd59e79f27e
   route-import database bgp 100 locator-set rloc_d9ad1062-bb97-4503-a478-9bd59e79f27e
   route-import database bgp 100 locator-set rloc_d9ad1062-bb97-4503-a478-9bd59e79f27e
   route-import database bgp 100 locator-set rloc_d9ad1062-bb97-4503-a478-9bd59e79f27e
   router bgp 100
     bgp router-id interface Loopback0
     bgp log-neighbor-changes
     !
     address-family ipv4
       network 192.168.100.1 mask 255.255.255.255
     exit-address-family
     !
     address-family ipv4 vrf Contractors
     exit-address-family
     !
     address-family ipv4 vrf Corporate
     exit-address-family
     !
     address-family ipv4 vrf DEFAULT_VN
     exit-address-family
     !
     address-family ipv4 vrf Guest
```
exit-address-family
!
address-family ipv4 vrf IoT
exit-address-family

**Note:** The following needs to manually be applied on the border’s external interface to maintain micro segmentation (if desired).

interface TenGigabitEthernet1/0/40
cts manual

On the external interface that is connected to the ASA/fusion router (the trunk), the following command needs to be applied to carry the Cisco TrustSec tag. For SXP to carry the Trustsec tag, the following needs to be configured:

```
sd-access-core1 (config)#cts sxp enable
ccts sxp default source-ip <source interface IP>
sd-access-core1 (config)#cts sxp connection peer <ISE PSN IP> password none mode local listener hold-time 0 0
sd-access-core1 (config)#cts sxp connection peer <ISE PSN IP> source <VLAN IP for each VRF> 0 password none mode local listener hold-time 0 0 vrf <VRF name>
sd-access-core1 (config)#cts role-based enforcement
sd-access-core1 (config)#cts role-based enforcement vlan-list <vlan number>
```

The following is an example of what has been applied in this guide’s configurations:

```
aaa new-model
aaa group server radius dnac-group
    server name dnac-radius_192.168.101.179
    ip radius source-interface Loopback0
aaa authentication login default group dnac-group local
aaa authentication enable default enable
aaa authentication dot1x default group dnac-group
aaa authorization exec default group dnac-group local
aaa authorization network default group dnac-group
aaa authorization network dnac-cts-list group dnac-group
aaa accounting dot1x default start-stop group dnac-group
aaa server radius dynamic-author
    client 192.168.101.179 server-key cisco123
aaa session-id common
```

The following is an example of what has been applied in this guide’s configurations (for SXP):

```
ccts sxp enable
ccts sxp default source-ip 192.168.104.50
ccts sxp connection peer 172.25.0.179 password none mode local listener hold-time 0 0
ccts sxp connection peer 172.25.0.179 source 192.168.104.50 password none mode local listener hold-time 0 0 vrf Corporate
ccts sxp connection peer 172.25.0.179 source 192.168.104.50 password none mode local listener hold-time 0 0 vrf Contractors
```
cts sxp connection peer 172.25.0.179 source 192.168.104.50 password none mode
local listener hold-time 0 0 vrf Guest
crs role-based enforcement
crs role-based enforcement vlan-list 3001-3003

Automated border Layer 3 handoff configuration - Configuration for the internal or external border (for the Catalyst 3000, Catalyst 6000, Catalyst 9000, Nexus 7000):

Note: For the remaining discussion of configurations in this document, the VNs will be referred to as VRFs.

Figure 8. VRF handoff to firewall

Cisco DNA Center 1.1 provides an automated Layer 3 handoff for the border configuration to support carrying policy outside of the fabric. This configuration can be configured manually if desired.

First, you need to configure an IP pool that will be used for configuring the IP addresses for VRF-Lite. These IP addresses will be subnetted into multiple /30 networks, one for each VRF that will be leaked. The external interface of the border(s) will be configured with this. The other usable IP address in each subnet will need to be manually configured on the neighbor interface on the next hop.

Navigate to Design → Network Settings → IP Address Pools.
Click **Add IP Pool** in the upper right corner. This will bring up the following screen. Populate the subnet to be used and the associated details.
Navigate to the Provision application. Click the fabric to be configured.

**Note:** This guide assumes that the border device(s) are already assigned to a site and provisioned. The provisioning step adds the network setting configuration to the site. This is a requirement before any device is added to a fabric. Additionally, the ISE should already be integrated and VNs created.

Click the device that will be used as the border. Select Add as Border or Add as CP + Border, depending on the desired role.
This will bring up a configuration box on the right side of the screen. Select the option that suits the border’s neighbor, based on the descriptions noted earlier in this document.

![Configuration Box]

The next configuration is the routing protocol that will be configured on the external interface to the neighboring network. In Cisco DNA Center 1.1, only BGP is supported (for automated configuration). Any routing protocol is supported if the configuration is going to be applied to the external interface of the border manually. Select a number to be used as the local AS number.

![BGP Configuration]

In Cisco DNA Center 1.1, only Layer 3 border handoff is supported. This handoff is done by applying VRF-Lite to the external interfaces. The Cisco Catalyst 3000, 6000, and 9000 platforms and Cisco Nexus 7000 platform will be configured with VLANs for each VRF that will be leaked (due to a lack of subinterface support in Cisco IOS XE Release 16.6). The ASR 1000 Series and the 4000 Series ISR will be configured with 802.1Q subinterfaces for each VRF that will be leaked.

The following is the workflow and configuration for the Cisco Catalyst 3000, 6000, and 9000 platforms and the Cisco Nexus 7000 platform:

Click ➤ to expand the Layer 3 handoff configuration.

![Layer 3 Configuration]

VRF-Lite is selected by default. Click ➤ to access the IP pool drop-down.
Click the IP pool that was configured for the Layer 3 handoff.

Click the **next to External Interface to access the list of available interfaces. This will depend on the border device and its configuration. Define the remote AS number that will be used.

**Note:** The remote AS number will need to be configured manually on the remote device as the local AS number. This configuration is not automated on the remote device.
Check the Virtual Network box and click the ▾ to show the virtual networks that have been configured. Select the virtual networks that will be leaked out of the fabric. In this example we are going to leak the Corporate and Contractors VRFs.

**Note:** In Cisco DNA Center 1.1.0 to 1.1.2, the INFRA_VN needs to be selected when doing any border handoff, as this point-to-point link is used to establish the neighborship. This is not needed in Cisco DNA Center 1.1.3 and later.
Scroll down and click Save.

Confirm that the Layer 3 handoff information that was just configured is correct. Click Add.

Border Handoff

- Layer 3

VRF-Lite

L3_Handoff (192.168.104.0/24)

Once this is done, you will need to save the configuration. Click Save in the upper right corner of the fabric page.

Choose to configure the Layer 3 handoff now or to schedule it for a later time.
Once you click Save, Cisco DNA Center will provision the selected border device. In this example, the following additional interface configuration will be applied to the Cisco Catalyst 3000, 6000, or 9000 platform or the Cisco Nexus 7000 platform:

A trunk is created on the link connected to the ASA. This is used to carry the VRFs and SGTs.

```plaintext
interface TenGigabitEthernet1/0/40
  description To ASA-5585
  switchport mode trunk
  device-tracking attach-policy IPDT_MAX_10

#For each VRF that was selected, an SVI is created using the assigned L3_Handoff Subnet of 192.168.104.0/24. The VLAN3001 is created for the Infra_VN. This is used to establish the neighborship between the border and the ASA.

interface Vlan3001
  description vrf interface to External router
  vrf forwarding Corporate
  ip address 192.168.104.1 255.255.255.252
  no ip redirects
  ip route-cache same-interface
!
interface Vlan3002
  description vrf interface to External router
  vrf forwarding Contractors
  ip address 192.168.104.5 255.255.255.252
  no ip redirects
  ip route-cache same-interface
!
interface Vlan3003
  description vrf interface to External router
  ip address 192.168.104.9 255.255.255.252
  no ip redirects
  ip route-cache same-interface
```
The following BGP configuration is applied.

```bash
METRO-C1#sh ru | sec bgp
  route-import database bgp 100 locator-set rloc_d9ad1062-bb97-4503-a478-9bd59e79f27e
  route-import database bgp 100 locator-set rloc_d9ad1062-bb97-4503-a478-9bd59e79f27e
  route-import database bgp 100 locator-set rloc_d9ad1062-bb97-4503-a478-9bd59e79f27e
  route-import database bgp 100 locator-set rloc_d9ad1062-bb97-4503-a478-9bd59e79f27e
  route-import database bgp 100 locator-set rloc_d9ad1062-bb97-4503-a478-9bd59e79f27e
  route-import database bgp 100 locator-set rloc_d9ad1062-bb97-4503-a478-9bd59e79f27e
router bgp 100
  bgp router-id interface Loopback0
  bgp log-neighbor-changes
  neighbor 192.168.104.2 remote-as 200
  neighbor 192.168.104.2 update-source Vlan3001

The loopback network is used for the neighborship establishment (INFRA_VN):

```bash
address-family ipv4
  network 192.168.100.1 mask 255.255.255.255
  redistribute lisp metric 10
  neighbor 192.168.104.10 activate
  neighbor 192.168.104.10 weight 65535
  exit-address-family
```

The BGP neighbor configuration for each VRF-> SVI is added. These are the IP addresses that will be configured on the ASA for each VRF. The update source is configured as the local VLAN associated with the corresponding VRF:

```bash
address-family ipv4 vrf Corporate
  neighbor 192.168.104.2 remote-as 200
  neighbor 192.168.104.2 update-source Vlan3002
  neighbor 192.168.104.2 activate
  neighbor 192.168.104.2 weight 65535
  exit-address-family
!
address-family ipv4 vrf Contractors
  neighbor 192.168.104.6 remote-as 200
  neighbor 192.168.104.6 update-source Vlan3003
  neighbor 192.168.104.6 activate
  neighbor 192.168.104.6 weight 65535
  exit-address-family
!
address-family ipv4 vrf DEFAULT_VN
  exit-address-family
!
address-family ipv4 vrf Guest
```
exit-address-family
!
address-family ipv4 vrf IoT
exit-address-family
!

Note that the L3_Handoff IP pool was applied to the configuration.

<table>
<thead>
<tr>
<th>Virtual Network</th>
<th>Vlan</th>
<th>Local IP</th>
<th>Remote IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate</td>
<td>3001</td>
<td>192.168.104.1/30</td>
<td>192.168.104.2/30</td>
</tr>
<tr>
<td>Contractor</td>
<td>3002</td>
<td>192.168.104.5/30</td>
<td>192.168.104.6/30</td>
</tr>
<tr>
<td>INFRA_VN</td>
<td>3003</td>
<td>192.168.104.9/30</td>
<td>192.168.104.10/30</td>
</tr>
</tbody>
</table>

BGP configuration for a single context with the border directly connected to the firewall

Routing needs to be established between the border and the firewall. In SD-Access 1.1, the routing and Layer 3 handoff for the next-hop device (that is not managed by Cisco DNA Center) is manually configured. This guide provides that configuration.

Any IGP that your border, fusion router, and firewall hardware support is supported. This guide provides configuration examples for BGP based on the Cisco DNA Center automated Layer 3 handoff BGP configuration. This guide can be used as guidance for implementing other routing protocols. Appropriate loop prevention mechanisms should be implemented (distribute-list, prefix-list, route-map, etc.). This guide does not provide the configuration for the general routing table. It provides the CLI configuration only for the ASA OS.

Note: The Cisco Catalyst 3000, 6000, and 9000 platforms and the Cisco Nexus 7000 platform will use SVIs for the VRFs that connect to the firewall. The ASR 1000 Series and the 4000 Series ISR will use 802.1Q subinterfaces for the VRFs that connect to the firewall.

This example uses a single-context firewall, since the traffic will be leaked and inspected during the VRF’s communication.

Recall the border configuration. The ASA configuration will be the same for connecting to the Cisco Catalyst 3000, 6000, or 9000 platform; the Cisco Nexus 7000 platform; or the ASR 1000 Series or 4000 Series ISR. To assist with the configuration steps, we show the configuration for the ASA for both previous examples.

Configuration for the internal or external border (for the Cisco Catalyst 3000, 6000, or 9000 platform or Cisco Nexus 7000 platform):

Note: This configuration needs to be manually applied to the ASA.
Interface configuration

interface GigabitEthernet0/0/1.3001
  description BGP peering for VLAN 3001
  vlan 3001
  nameif Corporate
  security-level 100
  ip address 192.168.104.2 255.255.255.252

interface GigabitEthernet0/0.3002
  description BGP peering for VLAN 3002
  vlan 3002
  nameif Contractors
  mosecurity-level 100
  ip address 192.168.104.6 255.255.255.252

interface GigabitEthernet0/0.3003
  description INFRA-for BGP Neighborship
  vlan 3003
  nameif BGP-Peer
  security-level 100
  ip address 192.168.104.10 255.255.255.252

Routing configuration

Apply the BGP AS number that was configured as the remote AS.
router bgp 200
  bgp router-id interface GigabitEthernet0/0
  bgp log-neighbor-changes
!

Apply the neighbor details on each firewall context for the SVIs configured on the Cisco Catalyst 3000, 6000, or 9000 platform or the Cisco Nexus 7000 platform.

Corporate
address-family ipv4 vrf Corporate

network 174.25.13.1 mask 255.255.255.255
neighbor 192.168.104.1 remote-as 100
neighbor 192.168.104.1 activate
neighbor 192.168.104.1 weight 65535
exit-address-family
**Contractors**
address-family ipv4 vrf Contractors
  network 174.25.14.1 mask 255.255.255.255
  neighbor 192.168.104.5 remote-as 100
  neighbor 192.168.104.5 activate
  neighbor 192.168.104.5 weight 65535
  exit-address-family

**BGP neighborship (INFRA_VN)**
  address-family ipv4
  network 192.168.100.1 mask 255.255.255.255
  neighbor 192.168.104.9 remote-as 100
  neighbor 192.168.104.9 activate
  neighbor 192.168.104.9 weight 65535
  exit-address-family

The BGP configuration should look like the following once complete:

```
router bgp 200
  bgp log-neighbor-changes
  address-family ipv4 unicast
    neighbor 192.168.104.1 remote-as 100
    neighbor 192.168.104.1 activate
    neighbor 192.168.104.1 weight 65535
    neighbor 192.168.104.9 remote-as 100
    neighbor 192.168.104.9 activate
    neighbor 192.168.104.9 weight 65535
    neighbor 192.168.104.13 remote-as 100
    neighbor 192.168.104.13 activate
    neighbor 192.168.104.13 weight 65535
    network 174.25.13.1 mask 255.255.255.255
    network 174.25.14.1 mask 255.255.255.255
    network 192.168.100.1 mask 255.255.255.255
    no auto-summary
    no synchronization
  exit-address-family
```
Policy configuration

The following configuration needs to be added to the ASA physical and subinterfaces to allow the SGT inline tagging. For this example, these are the interfaces GigabitEthernet 0/0, 0/0.3001 to 3003.

```plaintext
cts manual
    policy static sgt 65000 trusted

interface GigabitEthernet0/0
description BGP Neighborship
nameif Border Connection
cts manual
    policy static sgt 65000 trusted
security-level 100
ip address 192.168.104.2 255.255.255.252

interface GigabitEthernet0/0.3001
description BGP peering for VLAN 3001
vlan 3001
nameif Corporate
cts manual
    policy static sgt 65000 trusted
security-level 100
ip address 192.168.104.2 255.255.255.252
!
interface GigabitEthernet0/0.3002
description BGP peering for VLAN3002
vlan 3002
nameif Contractors
cts manual
    policy static sgt 65000 trusted
security-level 100
ip address 192.168.104.6 255.255.255.252

interface GigabitEthernet0/0.3003
description BGP peering for VLAN3003
vlan 3003
nameif INFRA_VN
cts manual
    policy static sgt 65000 trusted
security-level 100
ip address 192.168.104.10 255.255.255.252
```
Policy enforcement

Once the VRFs are leaked to the firewall and the traffic can traverse the firewall, the SG-FWs can be defined. The policies created on the firewall can include specific ports or protocols. The SG-FWs can be configured via CLI or ASDM. For details on configuring the SG-FWs, consult the Service Policy Module for ASA.

sd-access-fw# sh cts sgt-map

Active IP-SGT Bindings Information

<table>
<thead>
<tr>
<th>IP Address</th>
<th>SGT</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.115.217.20</td>
<td>20</td>
<td>SXP</td>
</tr>
<tr>
<td>174.25.13.5</td>
<td>17</td>
<td>SXP</td>
</tr>
</tbody>
</table>

IP-SGT active Bindings Summary

Total number of SXP bindings = 2
Total number of active bindings = 2
Total number of shown bindings = 2

Configuration for the internal or external border (for the ASR 1000 Series and the 4000 Series ISR):

For these steps the same IP pool will be used, so the IP addresses will continue to the next /30 subnets and the VLAN number will also increase accordingly. The same steps will be followed as before, but in this example the device will be selected as an external border only.

Click the device that will be used as the border. Select Add as Border or Add as CP + Border, depending on the desired role.
This will bring up a configuration box on the right side. Select the option that suits the border’s neighbor. For traffic to a domain with known IP prefixes (data center, traditional IP network, another domain within the company), select Internal or Internal and External. For traffic to the Internet or an unknown domain, select External.

The next configuration is the routing protocol that will be configured on the external interface to the neighboring network. In Cisco DNA Center 1.1, only BGP is supported (for automated configuration). Any routing protocol is supported if the configuration will be applied to the external interface of the border manually. Select a number to be used as the local AS number.

Select the IP pool that was configured for the Layer 3 handoff.
Add the external interface(s) that will be configured to communicate with the firewall, and then click

Add Interface

This will take you to the following screen.

Click ![Add Interface](image)
to access the list of available interfaces. This list will depend on the border device and its configuration. Define the remote AS number that will be used.
Check the Virtual Network box and click the ✔️ to show the virtual networks that have been configured. Select the virtual networks that will be leaked out of the fabric. Be sure to include INFRA_VN to establish the neighborhood.

![Virtual Network]

Scroll down and click Save.
Confirm that the Layer 3 handoff information is correct. Click Add.

<table>
<thead>
<tr>
<th>Interface</th>
<th>Number of VN</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet0/0/1</td>
<td>2</td>
</tr>
</tbody>
</table>

Once this is done, you need to save the configuration. Click Save in the upper right corner.

Choose to configure the Layer 3 handoff now or schedule it for a later time.

Once you click Save, Cisco DNA Center will provision the selected border device. In this example, the following additional interface configuration will be applied to the Cisco Catalyst 3000, 6000, or 9000 platform or the Cisco Nexus 7000 platform:

The loopbacks are created for the user VRFs and have the associated gateway IP address for the subnet. The INFRA_VN does not create a loopback, as this uses the primary Loopback0.

```
interface Loopback1021
  description Loopback Border
  vrf forwarding Corporate
  ip address 174.25.13.1 255.255.255.255
dhcp(Border-relay)
!
interface Loopback1022
  description Loopback Border
  vrf forwarding Contractors
  ip address 174.25.14.1 255.255.255.255
dhcp(Border-relay)
!```
Subinterfaces are created for each VRF. These are used to carry the VRFs and SGTs.

```conf
interface GigabitEthernet0/0/1
  description to ASA-5525 gig0/1
  no ip address
  media-type rj45
  negotiation auto

! interface GigabitEthernet0/0/1.3004
  description vrf interface to External router
  encapsulation dot1Q 3004
  ip address 192.168.104.13 255.255.255.252
  no ip redirects

interface GigabitEthernet0/0/1.3005
  description vrf interface to External router
  encapsulation dot1Q 3005
  vrf forwarding Corporate
  ip address 192.168.104.17 255.255.255.252
  no ip redirects

interface GigabitEthernet0/0/1.3006
  description vrf interface to External router
  encapsulation dot1Q 3006
  vrf forwarding Contractors
  ip address 192.168.104.21 255.255.255.252
  no ip redirects
```

The following BGP configuration is applied. The BGP neighbor configuration for each VRF-> subinterface is added. These are the IP addresses that will be configured on the ASA for each VRF. The update source is configured as the local VLAN associated with the corresponding VRF.

```conf
router bgp 200
  bgp router-id interface GigabitEthernet0/0/1
  bgp log-neighbor-changes
  neighbor 192.168.104.14 remote-as 100
  neighbor 192.168.104.14 GigabitEthernet0/0/1.3004
  address-family ipv4
    network 192.168.100.1 mask 255.255.255.255
    neighbor 192.168.104.14 activate
    neighbor 192.168.104.14 weight 65535
  exit-address-family
  !
  address-family ipv4 vrf Corporate
  neighbor 192.168.104.18 remote-as 200
```
neighbor 192.168.104.18 update-source GigabitEthernet0/0/1.3005
neighbor 192.168.104.18 activate
neighbor 192.168.104.18 weight 65535
exit-address-family
!
address-family ipv4 vrf Contractors
network 174.25.14.1 mask 255.255.255.255
neighbor 192.168.104.22 remote-as 200
neighbor 192.168.104.22 update-source GigabitEthernet0/0/1.3006
neighbor 192.168.104.22 activate
neighbor 192.168.104.22 weight 65535
exit-address-family

Note that the L3_Handoff IP pool was applied to the configuration. Click on the device configured for the Layer 3 handoff. Select View Info to see the VLANs configured on the device.

![Image](image_url)

The virtual networks (VRFs), associated VLAN, and local IP are displayed. The remote IP needs to be manually configured on the directly connected interface on the ASA (or next-hop device).

Automated border Layer 3 handoff configuration - Configuration for the internal or external border (for the ASR 1000 Series and the 4000 Series ISR):

Routing configuration
BGP configuration for ASA contexts

This configuration example uses the same VLANs and subinterfaces as in the example for the single-context Cisco Catalyst 3000, 6000, and 9000 platforms and Cisco Nexus 7000 platform.

**Note:** This configuration needs to be manually applied to the ASA.
**Configuration for the internal or external border** (for the internal or external border Cisco Catalyst 3000, 6000, or 9000 platform and Cisco Nexus 7000 platform example)

**Note:** Multiple contexts are recommended when the VRFs need to be kept segmented while traversing the firewall. If the VRFs need to communicate with each other while traversing a firewall, a single context should be used.

Follow the firewall [multi-context configuration guide](#) for the VRFs that will be traversing the firewall. In this guide, the following contexts are created for each VRF.

**Context configuration**

```
 sda-asa-5525(config)# context Contractors
 Creating context 'Contractors'... Done. (3)
 sda-asa-5525(config-ctx)# context Corporate
 Creating context 'Corporate'... Done. (4)
```

Configure the interfaces in their respective contexts. Be sure to configure the correct VLAN in each context that is assigned to each VRF.

The BGP neighborship needs to be configured in each context.

```
interface GigabitEthernet0/0.3004
 description BGP Neighborship
 vlan 3003
 nameif BGP-Peer
 security-level 100
 ip address 192.168.104.14 255.255.255.252
```

Configure the Corporate VLAN in the Corporate context.

```
interface GigabitEthernet0/0/1.3005
 description BGP peering for VLAN 3005
 vlan 3005
 nameif Corporate
 security-level 100
 ip address 192.168.104.18 255.255.255.252
```

Configure the Contractors VLAN in the Contractors context.

```
interface GigabitEthernet0/0.3006
 description BGP peering for VLAN 3006
 vlan 3006
 nameif Contractors
 security-level 100
 ip address 192.168.104.22 255.255.255.252
```
Routing configuration
Apply the BGP AS number that was configured as the remote AS.

```
router bgp 200
  bgp log-neighbor-changes
!
```

Apply the neighbor details for the SVIs configured on the ASR 1000 Series or 4000 Series ISR. Apply the correct VRF neighbor in the respective context.

Apply the neighbor details on each firewall context for the SVIs configured on the Cisco Catalyst 3000, 6000, or 9000 platform or the Cisco Nexus 7000 platform.

Corporate context
```
address-family ipv4
  network 174.25.13.1 mask 255.255.255.255
  neighbor 192.168.104.17 remote-as 100
  neighbor 192.168.104.17 activate
  neighbor 192.168.104.17 weight 65535
exit-address-family
```

Contractors context
```
address-family ipv4
  network 174.25.14.1 mask 255.255.255.255
  neighbor 192.168.104.22 remote-as 100
  neighbor 192.168.104.22 activate
  neighbor 192.168.104.22 weight 65535
exit-address-family
```

BGP neighborship (this needs to be applied in each context)
```
address-family ipv4
  network 192.168.100.1 mask 255.255.255.255
  redistribute lisp metric 10
  neighbor 192.168.104.13 activate
  neighbor 192.168.104.13 weight 65535
exit-address-family
```
Conclusion

SD-Access provides the segmentation many customers require today. With the integration of firewalls, customers are able to increase their security by implementing stateful inspection between the VNs, fabrics, other Layer 3 domains, and the Internet to complement the security SD-Access provides.

Customer Call to Action

For more information, please visit the following:

- SD-Access
- SD-Access Design Guide
- Cisco ASA 9.8 CLI Configuration Guide
- Cisco ASA Firewall ASDM Configuration Guide
- Cisco TrustSec
- VRF-Aware SGT