Security Group Access for BYOD

Revised: March 6, 2014

What's New: In the previous version of the BYOD CVD, TrustSec in the use of security group tags was addressed in a Centralized Unified Wireless Design within a campus, where users attaching to the wireless network based on authentication credentials in the respective authorization were assigned a security group tag.

In this version of the BYOD CVD, the use of security group tags as a means for enforcing policy is expanded to include a Centralized Unified Wireless Design incorporating the Cisco CT 5760 wireless controller as well as in a Converged Access infrastructure using the Cisco Catalyst 3850. In the CUWN design both the CT 5508 and the CT 5760 wireless controllers are used in parallel to terminate wireless devices in the campus. Additionally, policy enforcement for wireless access via the Catalyst 3850 and its integrated controller, when deployed in the campus access layer, is expanded to include the use of security group tags in addition to access control lists used in the previous version of the BYOD CVD.

As in the previous version of the BYOD CVD, this version continues to demonstrate the use of security group tags for policy enforcement in the same two scenarios using both SG ACLs on Nexus and Catalyst switches for the first scenario and the ASA security appliance in conjunction with the Security Group Firewall (SG-FW).

The following section describes the infrastructure used in this CVD and provides an outline of the two deployment scenarios used to enforce policies based on Security Group Tags. These deployment scenarios are not mutually exclusive and may be used together to satisfy an organization's requirements. Configuration details for the infrastructure are also provided.

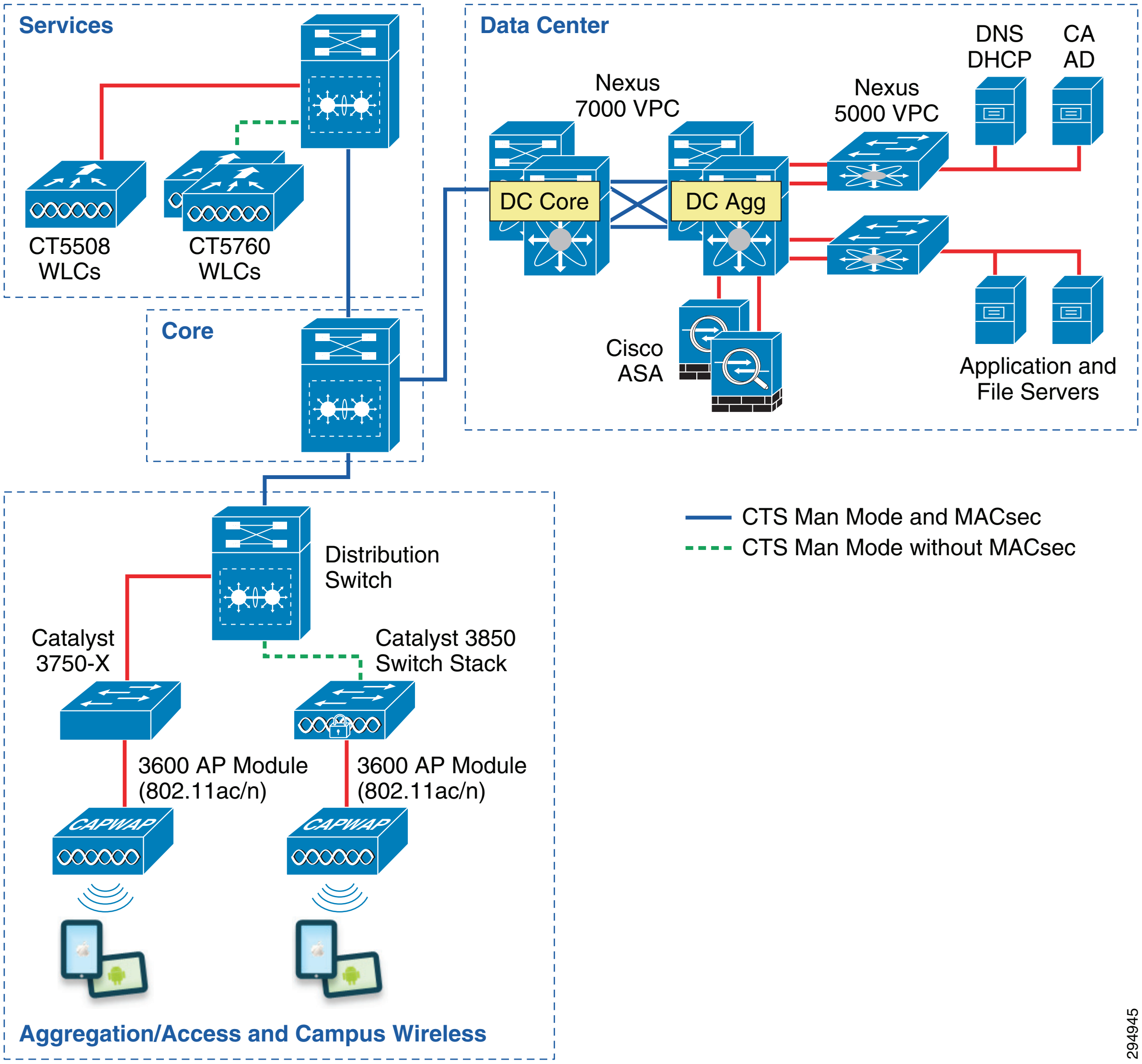
Unified Infrastructure Design to Support SGA

In this current version of the BYOD CVD, Security Group Tags are used as a means to enforce role-based access policies for Campus wireless users (as in the previous version of this CVD). New to this CVD however is the introduction of the CT-5760 wireless controller as well as the Catalyst 3850 for campus wireless access and the ability to natively tag traffic accessing the network through these devices. Two specific infrastructure deployment scenarios are examined in this CVD. The first use case makes use of TrustSec Policy defined at the Identity Services Engine and the resulting SGACLs being dynamically exchanged with the Catalyst 6500 and 3850 switches, the CT-5760 wireless controller, and the Nexus 7000 infrastructure. The second use case once again makes use of the TrustSec Policy defined at the Identity Services Engine, but policy is enforced through the configuration of Security Group Firewall (SG-FW) policies defined on an ASA providing secure access to data center resources.

The wireless access design using the CT-5508 wireless controller validated in the previous release of this CVD will continue to be used to support access to data center resources by wireless devices using the CT-5508 instead of the CT-5760, identical to that demonstrated in the previous release of this CVD.

Figure 12-1 depicts the infrastructure that is used for purposes of SGA validation within the CVD.

Figure 12-1 TrustSec Infrastructure for BYOD v2.5 CVD

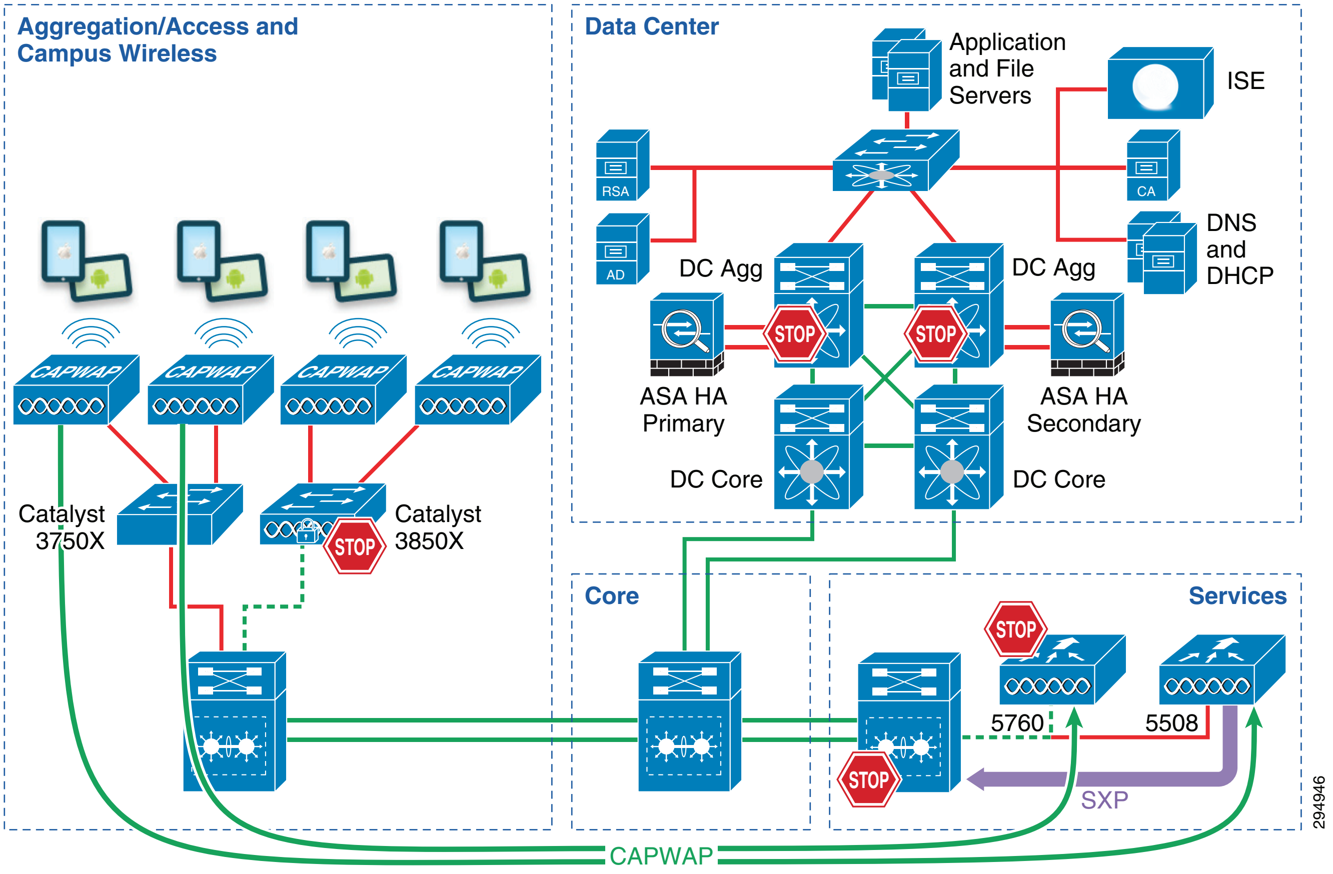


In Figure 12-1, the links extending between the Catalyst 6500 VSS in Shared Services to the Catalyst 6500 VSS in the core and extending to the Nexus 7000 are 10GE links. On the Catalyst 6500s, WS-X6904 linecards with the FourX Adapters provide the 10GE interfaces while the N7K-M108X2-12L and N7K-F248XP-25E linecards (last eight ports) provide the Nexus 7000 interfaces. The links between the Nexus 7000 and the Nexus 5548 are likewise connected to N7K-M108X2-12L linecards at the Nexus 7000 and 10GE ports on the Nexus 5548. All other network connectivity for wireless controllers, ASA firewalls, ISE, and the miscellaneous servers depicted are 1GE links.

Policy Configuration for SGACLs in Scenario 1

For Deployment Scenario 1, refer to Figure 12-2.

Figure 12-2 Infrastructure Deployment Scenario 1 SGT Enforcement



In this first scenario, wireless users, upon successful authentication and authorization, will be associated with a specific role and an IP to SGT mapping will be created on the wireless controller with the device's IP Address and the appropriate SGT. In Deployment Scenario 1 wireless device traffic will have the SGT inserted at different networking devices and this insertion point is dependent on which wireless controller the device is terminating at for network access.

Table 12-1 summarizes where the SGT will be inserted.

Table 12-1 SGT Insertion

Architecture	Wireless Controller	Device	Explanation
Converged	3850	3850 switches	3850 Switch supports inline tagging capability
Centralized	5760	5760 wireless controller	5760 wireless controller supports inline tagging capability
Centralized	5508	6500 Shared Services	5508 does not support in-line tagging. Therefore SXP is used between 5508 and 6500. Tags imposed at 6500.

In Deployment Scenario 1, CUWN traffic with Security Group Tags will be forwarded from the Shared Services Catalyst 6500 VSS where the wireless controllers are attached or from the 3850 converged access switches connected to the Catalyst 6500 Distribution switch. These tags are then propagated through the Core of the BYOD infrastructure en route to servers located in the data center. In Figure 12-2, the links depicted in a solid green line will be configured for SGT forwarding as well as manually configured for 802.1ae MACsec. Links with a dashed green line will be configured to support SGT forwarding only as they do not support MACsec with current software but will in the future.

Note As of IOS-XE 3.3.0, the Catalyst 3850 and CT-5760 wireless controller will impose and propagate the SGT as well as enforce SGACLs. Although these platforms have the necessary ASICs for MACsec support, the software has yet to be enabled as of the writing of this CVD.

As this traffic traverses the SGT-capable Core, this tag will be propagated hop-by-hop en route to the Nexus 7000s that compose the data center switching infrastructure within which the various servers are located. As shown in the Figure 12-3, a wireless user accessing the network using centralized wireless architecture is assigned a tag value of 12 after successful authentication and authorization; similarly, a wireless user accessing the network using a converged access medium is assigned a tag value of 10.

As 802.1X is not used to authenticate the servers residing in the Nexus data center infrastructure, the server IP Address to SGT mapping can either be manually defined on the Nexus 7000 Data Center Aggregation switch or at the ISE server which would subsequently “push” that mapping to the Nexus 7000. For purposes of the CVD, specific IP/SGT mappings have been manually defined on the Nexus 7000 data center Aggregation Switches as well as through the use of VLAN to SGT mapping.

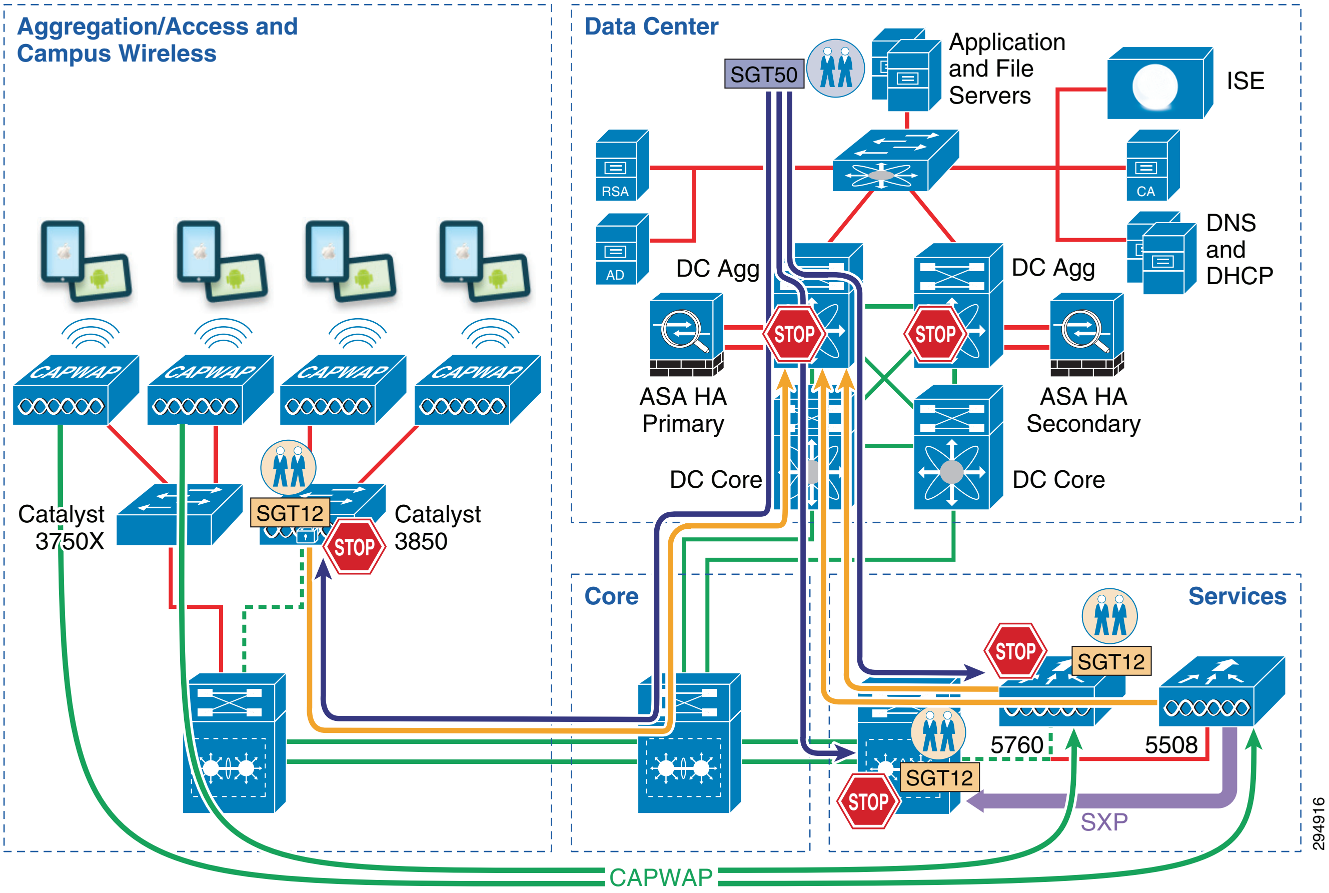
As tagged user traffic arrives at the Nexus 7000 data center switch where the manual SGT mappings for the servers have been created, the traffic will be matched against TrustSec Policy (SGACL) defined either centrally at ISE or locally and will be either forwarded or dropped as applicable. For example, as shown in Figure 12-3, the traffic with SGT 10 arriving from converged access wireless user with full access is permitted by the Nexus aggregation switch and the traffic with SGT12 from a CUWN wireless user who has partial access is denied access to the servers.

As discussed earlier, all SGT mappings for the servers have been manually created on the Nexus 7000 aggregation switches. As the servers are connected to the Nexus 5548 switches depicted in Figure 12-3, traffic from the Nexus 5548s egresses untagged as no mappings have been created there. Once this traffic passes through the Nexus 7000 Aggregation switch, the resident SGT mappings will be examined and the appropriate SGT imposed upon egress from the aggregation switch. The SGT mappings can be implemented on the Nexus 7000 via IP/SGT mapping or by VLAN/SGT mapping. The details for this configuration are covered later in this document. In the event that traffic would be initiated by a server associated with an SGT in the data center, the tagged traffic would then leave the Nexus 7000 data center switches traversing the Catalyst 6500 Core and Shared Service infrastructure with the SGT propagated at each hop towards the destination, the wireless controllers attached to the Shared Services 6500, or wireless devices accessing the network through the Catalyst 3850s.

If destined for CUWN wireless controllers, upon arrival at the Shared Services 6500, the traffic will be matched against local TrustSec Policy (SGACL) and will be either forwarded or dropped depending on the controller to which it is destined. If destined for the CT-5508, SGACL policies will be enforced at the Shared Services C6500 VSS as the CT-5508 does not support tagging or SGACLs and only advertises the IP/SGT mappings to the Shared Services C6500 VSS for enforcement. If destined for the CT-5760 with its support for SGT tagging and SGACLs, the IP/SGT mappings for those devices accessing the network at the CT-5760 will be created and stored at the 5760 and hence the SGACL enforced there as well.

If destined for the Catalyst 3850 and the converged access wireless users, the SGACL policy will be enforced on the Catalyst 3850 to which the wireless user is associated.

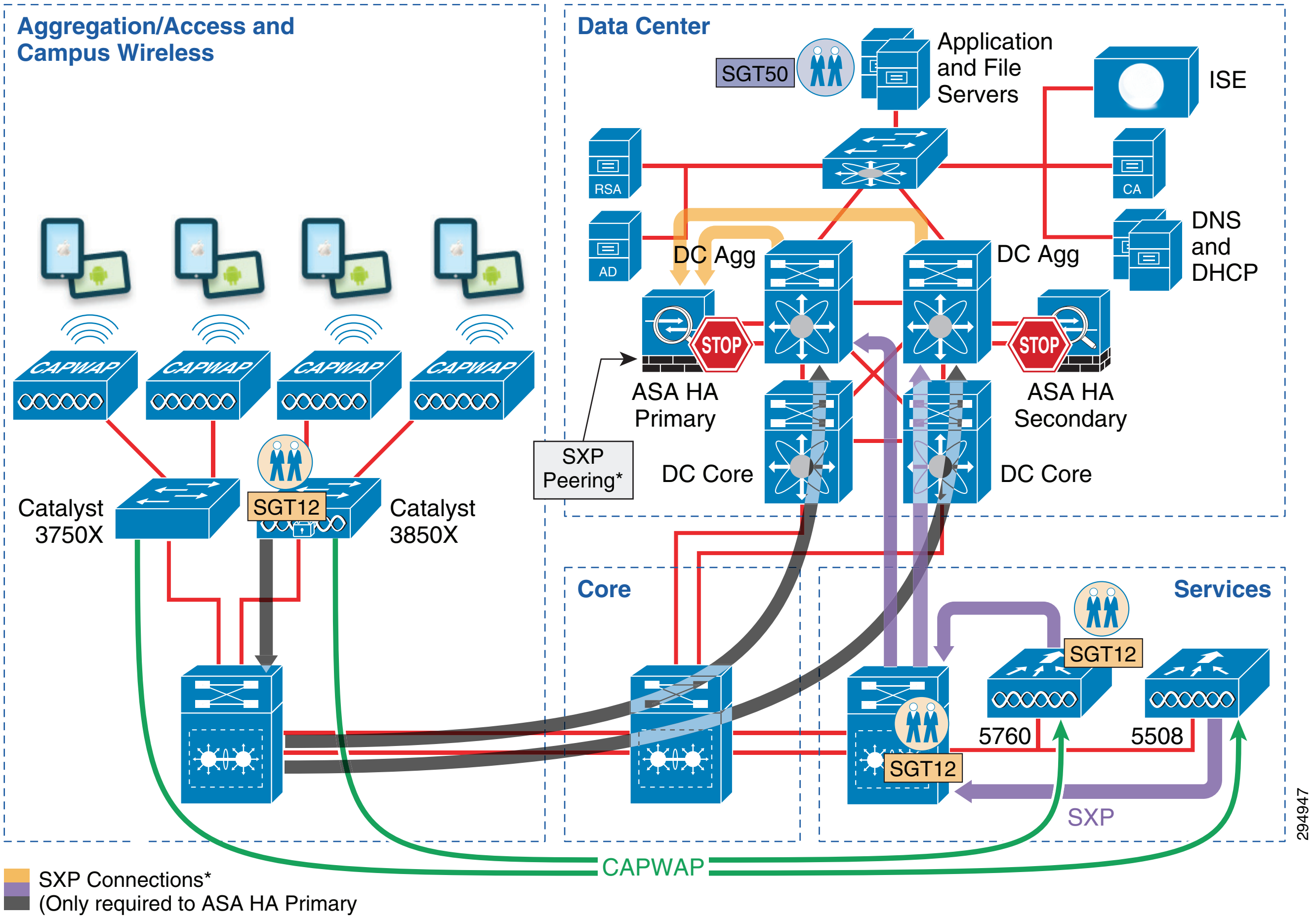
Figure 12-3 Policy Enforcement in Deployment Scenario 1



Policy Configuration in Scenario 2

For the topology used in Deployment Scenario 2, refer to Figure 12-4.

Figure 12-4 Deployment Scenario 2 Configuration



With Deployment Scenario 2 an alternate means other than SGACLs will be used to enforce TrustSec policy. In Scenario 2 an ASA running version 9.0(2) will be used as a Security Group Firewall (SG-FW) securing data center resources from outside access. Unlike Scenario 1, the 10GE infrastructure between the Shared Services Catalyst 6500 VSS and the data center does not need to be enabled to support Security Group Tag forwarding or SGACLs. As the ASA does not presently support native SGT tagging on its Ethernet interfaces, Security Group Tag Exchange Protocol (SXP) must be used for it to learn IP/SGT mappings from other areas of the network where they have been dynamically learned or statically configured. It is by virtue of these SXP advertisements that the ASA is capable of inspecting the untagged traffic and, through the use of these IP/SGT mappings, that SG-FW policies are enforced

As in the case of the first deployment scenario, wireless users, upon successful authentication and authorization, will be associated with a specific role and an IP to SGT Binding will be created on the wireless controller with the device's IP Address and the appropriate SGT.

Once the IP/SGT mappings have been created upon wireless device access to the respective controller, SXP will be used as the primary method through which these mappings are communicated to the ASA firewall. As depicted in Figure 12-4, the 3850 converged access switches and both the CT-5760 and CT-5508 wireless controllers must communicate their respective IP/SGT mappings to the ASA Firewall. In this design we have chosen the following method to minimize the number of SXP tunnels needed to the ASA Firewall:

- The CT-5760 and CT-5508 wireless controllers have an SXP peering to the Shared Services C6500 VSS, which also has an SXP peering to each of the Nexus 7000 data center aggregation switches.

- Access layer Catalyst 3850 switches establish an SXP tunnel to the C6500 VSS campus distribution switch, which then establishes a tunnel to each of the Nexus 7000 data center aggregation switches. The primary advantage in this approach is to aggregate what may be hundreds of Catalyst 3850s peering at the respective campus distribution switch(es) and then creating a single SXP peering to the data center.
- All SXP tunnels from the Campus infrastructure are aggregated at each of the Nexus 7000 data center aggregation switches.
- The IP/SGT mapping information is aggregated and sent by each of the Nexus 7000 aggregation switches to the HA primary ASA Firewall including all of the server mappings created through static IP/SGT mappings or VLAN/SGT mappings at the Nexus switches. By doing this, the ASA does not have to maintain numerous SXP peerings to different devices.

Table 12-2 summarizes the SXP peering that is used in the CVD:

Table 12-2 SXP Peering

Device	Role	Intfc	Dst Device	Role	Intfc
CT-5760	Speaker	Lo0	Shared Svcs C6500 VSS	Listener	Lo0
CT-5508	Speaker	Mgmnt.	Shared Svcs C6500 VSS	Listener	Lo0
Shared Svcs C6500 VSS	Speaker	Lo0	N7K-Agg-1	Listener	Lo0
Shared Svcs C6500 VSS	Speaker	Lo0	N7K-Agg-2	Listener	Lo0
Catalyst 3850 Access	Speaker	Lo0	Distribution C6500 VSS	Listener	Lo0
Distribution C6500 VSS	Speaker	Lo0	N7K-Agg-1	Listener	Lo0
Distribution C6500 VSS	Speaker	Lo0	N7K-Agg-2	Listener	Lo0
N7K-Agg-1	Speaker	Lo0	ASA Firewall HA Primary	Listener	Out
N7K-Agg-2	Speaker	Lo0	ASA Firewall HA Primary	Listener	Out

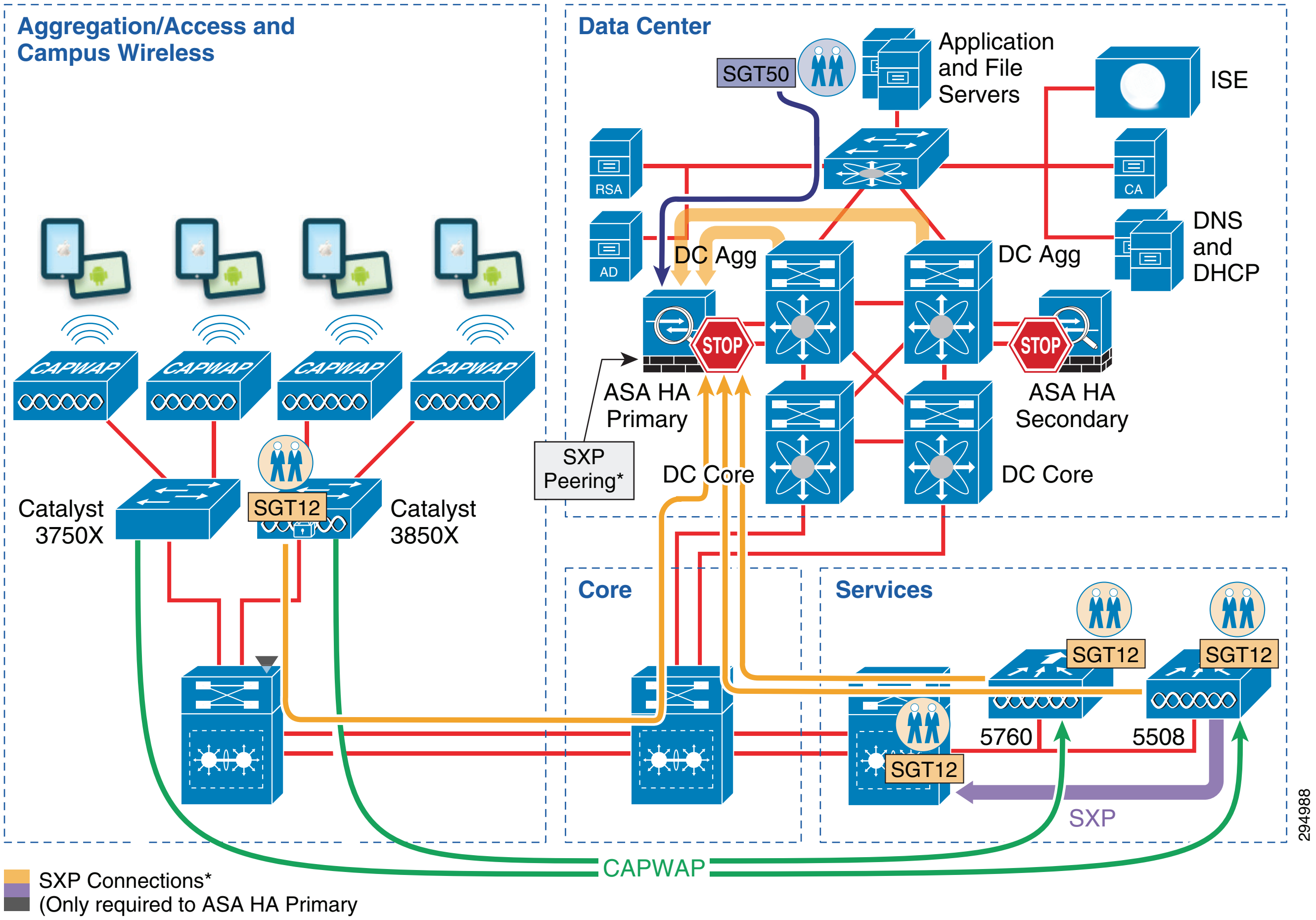
As previously discussed, the ASA firewall that will be used to enforce SG-FW policies must be manually configured with SGT policies as dynamic updates via ISE is presently not supported in the ASA. The details regarding these SG-FW policies will be discussed later.

As wireless traffic egresses the Shared Services Catalyst 6500 VSS en route to the data center, the traffic will be untagged and will simply be propagated through the Core, enter the data center switching infrastructure, and ultimately arrive at the ASA firewall where the appropriate SG-FW policy will be enforced. As shown in Figure 12-5 all the traffic going from the user to the server is passing through the ASA firewall.

In the unlikely event that any traffic would be sourced from a server in the data center, it would likewise egress the Nexus 7000 aggregation switch untagged and be forwarded to the ASA firewall where any applicable SG-FW policy will be enforced

Figure 12-5 depicts the infrastructure used in Deployment Scenario 2 and the means by which security group policies will be enforced.

Figure 12-5 SGA Policy Enforcement Using SXP and SG-FW



TrustSec Summary

For information regarding the detailed, platform-specific configuration steps, refer to the TrustSec section in Chapter 23, "BYOD Policy Enforcement Using Security Group Access."

Note Minimally, Patch 1 for ISE 1.2 **MUST** be installed in order for NDAC (Network Device Admission Control) to function properly between the network device and ISE. Without Patch 1, the network device will be unable to authenticate with ISE in order to derive TrustSec environment data, PAC file, and security group policies when CTS Manual Mode is configured and, additionally, the credentials required to authenticate peers/TrustSec links when CTS Dot1x Mode is configured. Due to issue between ISE and new behavior in iOS7 for Apple devices, it is recommended to deploy ISE 1.2 Patch 5. Refer to the ISE 1.2 Release Notes for additional information regarding this **very important** information.