Application Centric Infrastructure Security

Extended Abstract

Rick Lahaye
rick.lahaye@outlook.com

Intern System Engineer
Cisco Systems

Student Informatie en Communicatie Technologieën
Specialisatie Infrastructure Design
ZUYD Hogeschool

Plaats en datum	Amsterdam, 6 Januari 2016
Opdrachtgever	Cisco Systems
Opdrachtnemer	Rick Lahaye ZUYD Hogeschool
Periode	september 2015 - januari 2016
Bedrijfsbegeleider	Andre Brugman
Schoolbegeleider	Daniël Heynen

Abstract

Dit Extended Abstract geeft inzicht in het uitgevoerde afstudeerproject bij Cisco Systems in Amsterdam.

De afstudeeropdracht betreft het adviseren van de opdrachtgever met betrekking tot de integratie van Cisco Security producten en Cisco Application Centric Infrastructure.

De reden voor deze opdracht is het ontbreken van kennis over deze integratie bij zowel het security als het data center team van Cisco. Dit gebrek aan kennis is ontstaan door de nieuwe en snelle ontwikkelingen binnen Cisco ACI en de Cisco Security devices.

ACI is een Software Defined Networking (SDN) oplossing van Cisco. ACI biedt het volgende: automatie, security, zichtbaarheid en abstractie van het netwerk en workflows van het data center.

Security binnen ACI vindt plaats door middel van een distributed stateless firewall Voor de huidige geavanceerde cyber-attacks is dit niet voldoende. Een combinatie van Cisco ACI en Cisco Security producten biedt extra security door middel van Deep Packet Inspection en anti-malware solution.

Het advies is gegeven door middel van het beantwoorden van de volgende vraag:

- Welke Cisco Security devices kunnen er geïntegreerd worden met Cisco ACI en wat is de beste manier om dit te doen?

Uit de resultaten blijkt dat ASA with FirePOWER het beste geïntegreerd kan worden door middel van de Layer 4 to Layer 7 Service Insertion feature van ACI. Redenen voor deze conclusie zijn de automatie die deze feature biedt en de zichtbaarheid die gegeven wordt binnen het geïntegreerde device.

Inleiding

Dit Extended Abstract beschrijft het project dat tijdens de afstudeerstage is uitgevoerd. Deze afstudeerstage is uitgevoerd bij het Nederlandse Sales team van het bedrijf Cisco Systems tijdens het vierde jaar van de opleiding Informatie en Communicatie Technologieën (ICT), specialisatie Infrastructure Design (ID), aan het Hoger Beroeps Onderwijs (HBO) ZUYD Hogeschool.

Het project betreft het adviseren van Cisco over de integratie van Cisco ACI en Cisco Security devices. Deze opdracht is tot stand gekomen tijdens het eerste kennismakingsgesprek tussen de opdrachtgever en de opdrachtnemer.

Cisco Systems in Amsterdam heeft meerdere architectuurgroepen met specialisten, waaronder een security- en data center team. Deze teams richten zich onder andere op Cisco ACI en Cisco Security devices en zijn expert in deze producten, die ook als alleenstaand verkocht worden.

Door middel van een integratie van Cisco ACI en Cisco Security devices kan er extra security gewaarborgd worden. Echter door de vele en snelle ontwikkelingen binnen Cisco ACI en de Cisco Security devices ontbreekt er kennis over de integratie van deze producten. Deze ontwikkelingen vinden plaats om bij te blijven met de trends op de markt: security om klanten te beveiligen tegen cyber-attacks, en Software Defined om automatie en schaalbaarheid te kunnen bieden.

Door de beperkte kennis met betrekking tot de integratie is er behoefte aan advisering en hiermee de kennis van de teams te vergroten. Dit is tevens het doel van het project.

Het advies is gegeven door het uitvoeren van de afstudeeropdracht: het beantwoorden van de hoofdvraag.

Dit project is waardevol voor iedere ACI-omgeving en voor de integratie van security binnen ACI. Dit project geeft inzicht in de security features van ACI, hoe deze verbeterd kunnen worden en hoe dit in zijn werk gaat. Echter om deze integratie uit te kunnen voeren is enige kennis van ACI noodzakelijk.

Het project hanteert de softwareversies die tijdens de start van de afstudeerstage actueel waren:

- Cisco APIC: release 1.1(4e)
- Cisco ASA: release 9.5(x)
- Cisco FirePOWER: release 5.4(x)

Opdracht

De afstudeeropdracht betreft het geven van advies door middel van het beantwoorden van de hoofdvraag. Deze hoofdvraag is beantwoord met de resultaten van de deelvragen.

De hoofdvraag luidt als volgt:

- Welke Cisco Security devices kunnen er geïntegreerd worden met Cisco ACI en wat is de beste manier om dit te doen?

De betreffende deelvragen zijn:

- Wat is ACI?
- Wat zijn de security features van ACI in vergelijking met die van Cisco Security devices?
- Hoe kunnen de security features van Cisco Security devices geïntegreerd worden met Cisco ACI en wat zijn de voordelen hiervan?
- Wat zijn de installatie en integratie best practices?

De producten die opgeleverd zijn: Plan van Aanpak, prestatieplan, literatuuronderzoek, interviewrapport, notulen rapport, voortgangsrapport, reflectierapport, hoofdonderzoek, Extended Abstract en Proof of Concept. Deze producten zijn terug te vinden in de project portfolio.

Het Plan van Aanpak bevat informatie over het project met betrekking tot de doel- en probleemstelling, onderzoeksopdracht, scope, eisen, op te leveren producten, planning, risicoanalyse en communicatieplan.

Het prestatieplan bevat de geleverde prestaties van de student aan de hand van bewijsmiddelen.

Het literatuuronderzoek is een rapport dat gebruikt is als vooronderzoek en is geschreven met als doel: het vergaren van informatie door middel van deskresearch ter beantwoording van deelvragen in het hoofdonderzoek.

Het interviewrapport is een rapport met alle informatie die vergaard is door middel van interviews

voor het beantwoorden van deelvragen in het hoofdonderzoek.

Het notulenrapport bevat notulen van bijgewoonde of gegeven demonstraties, presentaties, trainingen en sessies.

Het voortgangsrapport bevat de wekelijkse voortgang en is gebruikt om overzicht te houden op het verloop van het project.

Het reflectierapport bevat een zelfreflectie van het uitgevoerde project.

Het hoofdonderzoek is het rapport waar de hoofd- en deelvragen in beantwoord worden. Dit rapport geeft tevens de conclusie met aanbevelingen voor Cisco.

Het Extended Abstract geeft inzicht in het uitgevoerde project door middel van het beschrijven van de context van de opdracht, probleem- en doelstelling, opdrachtomschrijving, gebruikte methodes, resultaten, discussie en conclusie.

Het Proof of Concept zal de inzetbaarheid van de resultaten van dit onderzoek tonen.

Voor het beantwoorden van de afstudeeropdracht diende er kennis opgedaan te worden over hoe ACI omgaat met routing en switching en hoe deze geconfigureerd kunnen worden zodat een Cisco Security device geïntegreerd kan worden.

Scope

De scope van het project limiteert Cisco Security devices tot Cisco ASA with FirePOWER.

Methode

Onderzoek

De methode die gebruikt is voor het onderzoek betreft kwalitatief onderzoek. Er is gekozen voor kwalitatief onderzoek aangezien het onderzoek gericht is op het verkrijgen van informatie over de integratie van producten, om daarmee de waarom vraag te beantwoorden. De gebruikte kwalitatieve onderzoeksmethodes zijn: deskresearch, interviews en observaties. Deze methodes zijn gekozen voor enerzijds het vergaren van informatie om mijn kennis te verbreden, anderzijds om de ervaringen van personen die met deze producten werken in kaart te brengen.

Project

De methode die gebruikt is voor projectmanagement is Prince2. Prince2 gebruikt een gecontroleerde en lerende benadering voor het project door middel van fases, planning, versiebeheer, zelfreflectie en met focus op de op te leveren producten.

Fasen

De volgende fasen zijn gebruikt bij het project: oriëntatiefase, onderzoeksfase, analysefase, adviesfase, en realisatiefase. De volgende fase start wanneer de vorige fase succesvol is afgerond.

De eerste fase, oriëntatie, omvat de eerste 3 weken van het project. Deze fase is gebruikt voor het formuleren van de probleemstelling, doelstelling, onderzoeksopdracht met hoofd en deelvragen, scope en producten die opgeleverd dienen te worden. Deze informatie wordt genoteerd in het Plan van Aanpak.

De tweede fase, onderzoek, omvat 7 weken. Deze fase is gebruikt voor het vergaren van informatie voor het onderzoek. De kwalitatieve onderzoeksmethoden die gebruikt zijn betreffen deskresearch en interviews. De informatie die vergaard is door middel van deskresearch kan gevonden worden in het literatuuronderzoek en de interviews in het Interview Report.

De derde fase, analyse, omvat 4 weken. Deze fase is gebruikt voor het verwerken en analyseren van de vergaarde informatie uit de onderzoeksfase. In deze fase is het onderzoeksrapport opgesteld voor het beantwoorden van de deelvragen.

De vierde fase, advies, omvat 3 weken. Deze fase is gebruikt voor het schrijven van de conclusie; het beantwoorden van de hoofdvraag en het geven van een advies. In deze fase is ook het Extended Abstract gemaakt en het project portfolio met alle op te leveren producten opgeleverd.

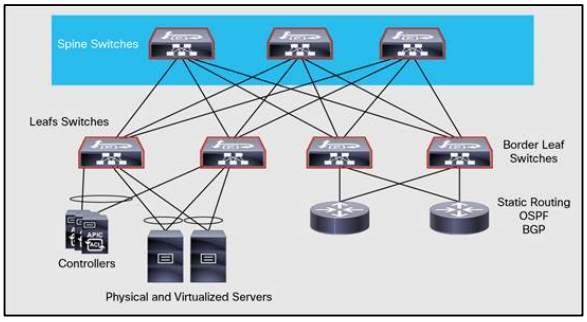
De vijfde fase, realisatie, omvat 3 weken. Deze fase bevat de afsluiting van het project. In deze fase zal het project gepresenteerd en verdedigd worden door middel van een eindsessie bij ZUYD Hogeschool. Tevens zal er een Proof of Concept gemaakt worden voor het bewijzen van de resultaten van het onderzoek.

Resultaat

ACI

Application Centric Infrastructure (ACI) is een SDN oplossing door Cisco. Deze oplossing biedt automatie, abstractie, zichtbaarheid en security voor het netwerk en workflows in het data center. ACI draait op een serie Nexus 9000 switches die met elkaar verbonden zijn door middel van een leaf spine model. Dit is een model zonder een distributie laag in tegenstelling tot het traditionele 3 lagen model. De spine switches representeren de core laag, de leaf switches de access laag.

Figuur 1 laat de ACI Fabric zien met de leaf spine topology:



Figuur 1: ACI Fabric

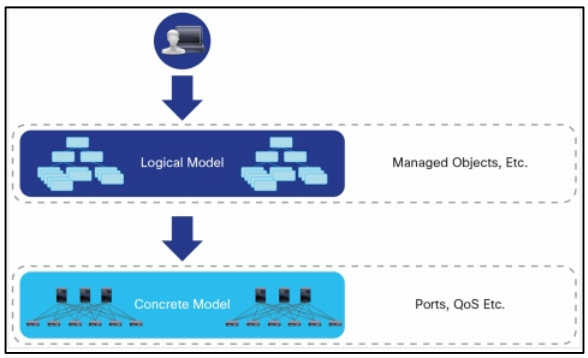
ACI wordt beheerd door middel van een programmeerbare centrale controller: de Application Policy Infrastructure Controller (APIC). Deze bevindt zich niet in het data plane. Dit houdt in dat het netwerk onafhankelijk kan opereren als de APIC losgekoppeld of verplaatst wordt. Het netwerk is programmeerbaar door middel van een Northbound en Southbound API die aangeboden wordt door de APIC. De Northbound API maakt het mogelijk om het netwerk te beheren door middel van scripting en de Southbound API maakt het mogelijk om producten of devices te configureren vanuit de APIC. De APIC wordt via de leaf switch aan de fabric verbonden.

De zichtbaarheid wordt geleverd door de APIC binnen het netwerk. De APIC kent de configuratie van elk object en dus de fysieke en virtuele infrastructuur. Verder gebruikt het verschillende protocollen om informatie te vergaren van het netwerk en de workflows.

De automatie voor ACI wordt geleverd door het aanbieden van onder andere deze API en de mogelijkheid tot het managen van het netwerk vanuit een centraal punt.

Abstractie vindt plaats door het Object-Oriented Model dat ACI gebruikt. Bij dit model is elke configuratie van het netwerk, inclusief de fysieke laag en de workflows, gerepresenteerd als een object. Dit object en zijn eigenschappen kunnen geconfigureerd en hergebruikt worden.

Figuur 2 laat zien dat dit logisch model met objecten gepusht wordt naar de hardware door middel van een concreet model:



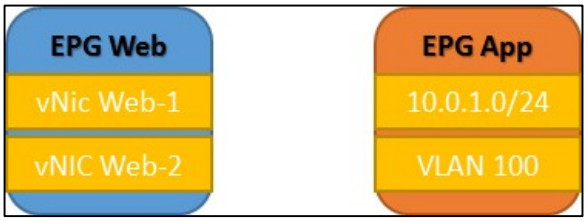
Figuur 2: Logisch Model naar Concreet Model

Workflows binnen ACI worden gepresenteerd als Endpoint Groups (EPG), dit is een groep van endpoints die onder dezelfde policy vallen. Een EPG wordt gedefinieerd door middel van de volgende attributen:

- VLAN
- VXLAN
- VMware Port Group of Naam
- IP of subnet
- DNS
- Interface

Een EPG kan zowel een fysiek als een virtueel endpoint representeren, of en Layer 2 of Layer 3 External Network (interface).

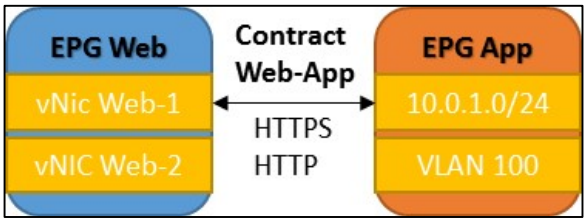
Figuur 3 laat een EPG Web zien met virtuele endpoints en een EPG App dat een VLAN en een subnet bevat:



Figuur 3: EPG's

Security voor ACI wordt mogelijk gemaakt door de zero-trust architectuur en de distributed stateless firewall. Dit betekent dat verkeer tussen EPG's niet toegestaan is, tenzij het expliciet is gespecificeerd. Dit specificeren wordt gedaan door middel van een contract. Een contract is vergelijkbaar met een Access Control List (ACL) en specificeert welk verkeer toegestaan is, en hoe dit afgehandeld moet worden. Verkeer dat toegestaan is door middel van een contract is standaard bidirectioneel, tenzij anders gespecificeerd.

Figuur 4 laat een EPG Web en App zien met een contract Web-App dat HTTP en HTTPS toestaat:



Figuur 4: EPG's met Contract

Integratie

Integratie van Cisco Security devices met Cisco ACI kan op 2 methodes gedaan worden:

- Layer 4 to Layer 7 Service Insertion
- External Network

Methode Layer 4 to Layer 7 Service Insertion

Met Layer 4 to Layer 7 (L4-L7) Service Insertion is het mogelijk om een (security) device te integreren tussen 2 EPG's (workflows).

Bij het integreren van zo'n device zal verkeer wat toegestaan is tussen EPG's gerouteerd worden over het geïmplementeerde device. Dit device kan dan een service leveren zoals: Deep Packet Inspection, stateful firewalling en anti-malware protection. Een eis bij het gebruik van deze methode is dat beide EPG's zich niet bevinden in hetzelfde Layer 2 netwerk, ook wel Bridge Domains genoemd binnen ACI. Het device wat geïntegreerd gaat worden, zal dan connectiviteit leveren tussen de Bridge Domains.

Het leveren van deze connectiviteit tussen de Bridge Domains kan op 2 manieren gedaan worden:

- Go Through mode (Layer 2)
- Go To mode (Layer 3)

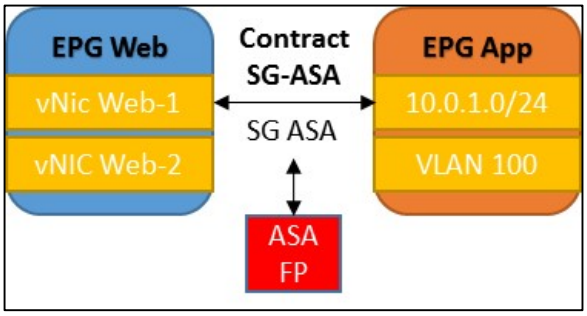
In de Go Through mode worden de Bridge Domains van elke EPG met elkaar gebridged. Deze bridge wordt gerealiseerd door het geïntegreerde device. Een eis bij het gebruik van deze mode is dat de EPG's zich in hetzelfde subnet moeten bevinden, maar niet in hetzelfde Bridge Domain. Om verkeer van EPG naar EPG te laten gaan moet het verkeer het Bridge Domain uit, en wordt het geswitcht over het geïntegreerde device door middel van Layer 2.

In de Go Through mode worden de Bridge Domains van de EPG's met elkaar verbonden door middel van routing. Routing wordt gerealiseerd door het geïntegreerde device die dient als routed hop. Hierbij dient ieder EPG een verschillend subnet en Bridge Domain te hebben, met het IP van het geïntegreerde device als default gateway. Een EPG wat connecteert naar een ander EPG, die zich bevindt in een ander subnet, zal gerouteerd worden over de routed hop, het geïntegreerde device, door middel van Layer 3.

Het geïntegreerde device kan zowel virtueel als fysiek zijn en kan zich overal bevinden zolang het aan de ACI leaf switch gekoppeld is.

De configuratie van de Layer 4 to Layer 7 Service Insertion wordt gedaan door middel van een object, namelijk een Service Graph. Een Service Graph is een template wat specificeert wat voor device geïntegreerd moet worden tussen EPG's, de configuratie van het device, en met welke mode. Ook is het mogelijk om meerdere devices achter elkaar te gebruiken. Een Service Graph is altijd gelinkt aan een contract. Het contract zorgt ervoor dat connectiviteit tussen de 2 EPG's toegestaan is en gerouteerd wordt over het device in de Service Graph.

Figuur 5 laat 2 EPG's zien met een contract SG-ASA ertussen wat gelinkt is naar een Service Graph ASA met een ASA with FirePOWER device:



Figuur 5: EPG's met Contract gelinkt aan Service Graph met ASA with FirePOWER

Elk device dat een device package heeft kan geïntegreerd worden met deze feature. Aangezien ACI een Open Security Framework heeft, is het mogelijk om voor elk device zelf een device package te scripten. Een device package vertelt de APIC wat voor device het betreft, hoe het te beheren en te configureren valt, en wat voor functies het kan leveren.

Dit betekent dat de APIC het device kan beheren, wat een mate van automatie en zichtbaarheid biedt. Automatie wordt geleverd door het Object-Oriented Model, waarbij objecten, en dus configuraties, makkelijk naar verschillende devices uitgerold kunnen worden. Verder kan de APIC het uitgerolde device monitoren, wat zichtbaarheid geeft door middel van health scores en fouten. Health scores kunnen gebaseerd worden op hardware benutting of status en fouten op log level of noodsignalen.

Methode External Network

Een andere methode voor de integratie kan het gebruik van external networks zijn. ACI kan verbinding maken met external networks. Hierbij bevindt 1 EPG zich in de ACI Fabric als fysiek of virtueel, en 1 EPG buiten de fabric als Layer 2 of Layer 3 External Network. In dit external network zou er security toegepast kunnen worden.

Een external network is een Layer 2 of 3 netwerk dat zich buiten de ACI Fabric bevindt en gepresenteerd wordt als een EPG voor ACI. Dit wordt gebruikt als gateway naar buiten toe: het internet, een WAN verbinding of een traditioneel data center. Hoe het verkeer in dit external network wordt afgehandeld staat los van ACI. In dit external network zou security geïntegreerd kunnen worden voor verkeer wat naar buiten toe gaat. Als het verkeer daarna ook nog terug gerouteerd wordt, is er security toegepast tussen 2 EPG's binnen de fabric.

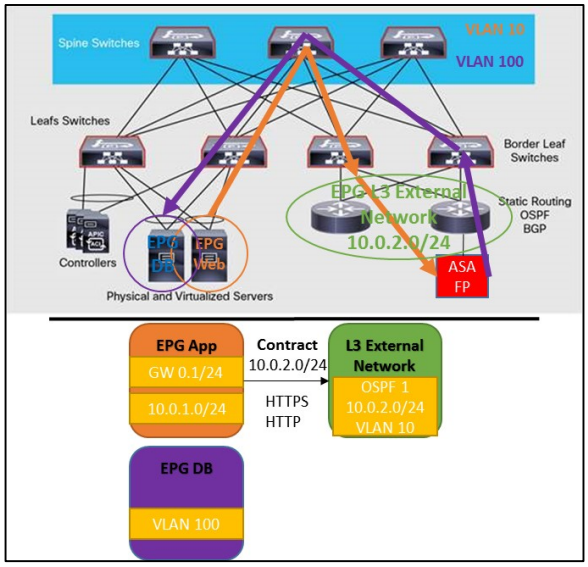
Deze verbinding met het external network kan gemaakt worden op 2 manieren:

- Layer 2 External Network (Bridged)
- Layer 3 External Network (Routed)

Bij Layer 2 wordt er verbinding gemaakt, door middel van interface bridging, met een switch (eventueel ASA with FirePOWER) dat het external network representeert.

Met Layer 3 wordt er verbinding gemaakt, door middel van routing, met een router (eventueel ASA with FirePOWER) dat het external network representeert.

Figuur 6 laat een voorbeeld zien hoe deze methode gebruikt kan worden tussen 2 EPG's die zich in de fabric bevinden. Dit figuur laat een EPG App zien die een contract heeft naar een EPG L3 External Network. De systemen in de EPG App hebben als default gateway 10.0.1.1. Wanneer er verbonden wordt naar het 10.0.2.0 subnet, zal de default gateway het door routeren op VLAN 10 naar de Border Leaf Switch, en dan naar de external router wat het external network representeert. De external router routeert het door naar de ASA, ASA filtert het verkeer, en geeft het een tag VLAN 100. Verkeer komt terug aan op de Border Leaf Switch, en verkeer met VLAN 100 wat naar subnet 10.0.1.0 moet, komt terug aan in de EPG DB.



Figuur 6: Security als External Network

Dit is een oplossing om security te integreren tussen ACI en de buitenwereld, of als het een device betreft zonder device package. Verder kan er met deze methode ook route redistribution plaatsvinden. Het gebruik van deze methode brengt complexiteit met zich mee omdat het verkeer vanuit het External Network terug gerouteerd moet worden naar de ACI Fabric. Dit kan niet geconfigureerd worden door ACI. Ook mist de automatie en zichtbaarheid binnen het device en heeft het verkeer een hogere latency vanwege het aantal benodigde hops.

Integratie Voordelen

ASA with FirePOWER kan geïntegreerd worden met ACI door middel van beide methodes wanneer de standaard security van ACI niet zou voldoen. Deze integratie levert extra security tussen EPG's (workflows) met onder andere stateful firewalling, anti-malware protection, Deep Packet Inspection en contextueel inzicht binnen het netwerk.

Tabel 1 laat de voordelen van een integratie zien met betrekking tot security features voor beide methodes:

Feature	ACI	ASA	Integratie
Stateless Network Firewall	Ja	Ja	Ja
Segmentation	Ja	Ja	Ja
Stateful Network Firewall	Nee	Ja	Ja
Reputation Based IP and URL Filtering	Nee	Ja	Ja
Application Firewall	Nee	Ja	Ja
Next Generation Intrusion Prevention System (NGIPS)	Nee	Ja	Ja
SSL Decrypting	Nee	Ja	Ja
Contextual Awareness	Nee	Ja	Ja

Tabel 1: Security Features Integratie

Best Practices

De best practices voor deze implementatie zijn als volgende gedefinieerd:

- Security should be included from the start, not considered after
- Consider what, where, and how security needs to be implemented
- Involve all datacenter teams when implementing security
- Respect number 1 rule in Datacenter; Don't break traffic
- Work with implementation phases
- Consider using SPAN port instead of inline for implementation
- Use automation with use of scripting
- Consider if using transparent or routed mode
- Consider using High Availability mode or cluster for scaling
- Use multiple contexts for multi tenancy

Meer gedetailleerde best practices zijn te vinden in het hoofdonderzoek.

Advies

Het advies voor de integratie van Cisco Security devices en ACI is:

- Gebruik de Layer 4 to Layer 7 Service Insertion;
- Volg de best Practices.

Het is raadzaam om bij het eerste design van een ACI-omgeving direct na te denken over security. Dit omdat bij het gebruik van de Layer 4 to Layer 7 Service Insertion de EPG's zich moeten bevinden in een verschillend Bridge Domain. Als er later security geïmplementeerd moet worden tussen EPG's die zich bevinden in hetzelfde Bridge Domain, doordat er niet nagedacht is over security, moet dit gewijzigd worden.

Hetzelfde geldt voor waar de security geïmplementeerd moet worden. Is dit tussen ACI en een WAN verbinding, of tussen de applicaties? En welke applicaties gaan dit dan worden, high risk of low risk?

Ook throughput tussen EPG's is belangrijk. Als er te veel data over het geïntegreerde device gerouteerd wordt kan dit het netwerk tussen de EPG's onderuithalen. Een advies is dus om uit te rekenen hoeveel throughput er plaats vindt tussen de EPG's voordat er security geïmplementeerd wordt. Throughput kan verhoogd worden door middel van een cluster en virtual port channels. Een cluster is het bundelen van ASA nodes met dezelfde configuratie waartussen dan load balancing plaats vindt. Een cluster kan maximaal 16 node bevatten wat een throughput[1] levert van 224gbps, een enkele node kan 20gbps leveren.

De virtual port channel zorgt ervoor dat een ASA verbonden kan worden met meerdere interfaces van 2 switches wat gezien wordt als een enkel interface. Voordeel is dat meerdere interfaces gebruikt kunnen worden en dus de throughput verhoogd wordt.

Een cluster en virtual port channel verhogen niet alleen de throughput, maar leveren ook redundantie wanneer een switch, ASA node of kabel niet meer werkt.

Discussie

De scope van het onderzoek limiteert Cisco Security devices tot Cisco ASA with FirePOWER. Als er geen rekening gehouden zou worden met deze scope kan elk device geïntegreerd worden met de Layer 4 to Layer 7 Service Insertion, mits het een device package heeft. Als het device geen device package heeft kan er gebruik worden gemaakt van de external network methode, mits het device routing of switching ondersteunt.

Verder blijkt dat de beste manier om deze implementatie te doen is door middel van de Layer 4 to Layer 7 Service Insertion feature. Hierbij is in acht genomen dat de meeste klanten waarde hechten aan automatie aangezien het ACI betreft (Cisco, n.d.). Vandaar dat er gekozen is voor de methode die de meeste automatie biedt. Een eis voor deze methode is dat het device dat geïntegreerd gaat worden een device package heeft. Als de klant geen waarde hecht aan automatie en zichtbaarheid kan ook de external network methode gebruikt worden wat extra complexiteit met zich mee brengt.

Echter is het aan de klant zelf om keuze te maken tussen het implementeren van security door middel van een external network of de Layer 4 to Layer 7 Service Insertion. Dit is afhankelijk van wat de klant ziet als "het beste". Om een weloverwogen beslissing te nemen inzake een methode is het raadzaam om een aantal vragen te stellen:

- Wat voor device betreft het?
- Is een device package beschikbaar?
- Wil je security met de traditionele managent tool beheren of met de APIC?
- Wil je security laten beheren door het data center/netwerk team in plaats van het security team?
- Wil je dat een data center product inzicht heeft binnen een security product?

Met de laatste ACI release genaamd Brazos[2] is het gebruik van een device package geen eis meer bij de Layer 4 to Layer 7 Service Insertion. Deze release is uitgebracht op 23 december 2015. Met de laatste release is een device package optioneel en kan gebruikt worden wanneer automatie voor het device, en zichtbaarheid binnen het device, gewenst is. Het gebruik van een device package wordt ook wel "managed" mode genoemd. Het gebruik zonder device package wordt dan "unmanaged" mode genoemd. Zonder device package kan elk device geïntegreerd worden, maar mist dan de automatie en zichtbaarheid. Bij deze mode is ACI alleen bewust van de uitgaande en inkomende poort op de leaf switch. Wat er gebeurt met het verkeer tussen de uitgaande- en de inkomende poort is niet relevant bij deze mode.

Ik heb dit project met veel plezier en motivatie uitgevoerd, dit door de vele brede kennis wat het mij gebracht heeft. Deze kennis is in mijn ogen zeer waardevol omdat het gebaseerd is op market trends.

Het project was lastig uit te voeren door de vele en snelle ontwikkelingen binnen ACI en ASA with FirePOWER. Het gevolg hiervan was dat literatuur vaak sprak over outdated versies, of versies die nog niet uitgebracht zijn. Ook de complexiteit van de

[1] Throughput met betrekking tot stateful Inspection

[2] Versie 1.2(1k) of hoger

nieuwe technieken waar ACI gebruik van maakt, maakte het uitvoeren van het project extra lastig.

In dit Extended Abstract wordt omschreven hoe security geïmplementeerd kan worden tussen EPG's, echter bij een implementatie is dit ingewikkelder omdat er rekening gehouden moet worden met Bridge Domains en VRF's. Dit zijn objecten die de infrastructuur configureren en vergelijkbaar zijn met Layer 2 en Layer 3 netwerken.

Conclusie

De hoofdvraag betreft:

- Welke Cisco Security devices kunnen er geïntegreerd worden met Cisco ACI en wat is de beste manier om dit te doen?

Het antwoord op deze hoofdvraag is: ASA with FirePOWER kan het beste geïntegreerd worden door middel van de Layer 4 to Layer 7 Service Insertion.

De reden hiervoor is dat de Layer 4 to Layer 7 Service Insertion automatie biedt voor het device en zichtbaarheid biedt binnen het device. Dit integendeel met security integreren als external network wat extra complexiteit met zich mee brengt.

Met behulp van het hoofdonderzoek kan een administrator security implementeren binnen ACI. Om de inzetbaarheid te tonen van dit onderzoek zal er een Proof of Concept geleverd worden met een implementatie van Cisco ASA with FirePOWER en Cisco ACI.

Aanbevelingen

Een aanbeveling is: het verder onderzoeken van multi tenancy met betrekking tot ASA with FirePOWER. ACI is een data center product en bij data centers is multi tenancy belangrijk om aan de business van verschillende klanten te voldoen.

Bronnenlijst

Cisco. (sd). *Case Studies*. Opgeroepen op 12 18, 2015, van Cisco: http://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/customer-case-study-listing.html

Lahaye, R. (2016). *ACI Security - Interview Report.*

Lahaye, R. (2016). *ACI Security - Literature Research Report.*

Lahaye, R. (2016). *ACI Security - Minutes Report.*

Lahaye, R. (2016). *ACI Security - Performance Plan.*

Lahaye, R. (2016). *ACI Security - Progress Report.*

Lahaye, R. (2016). *ACI Security - Project Initiation Document.*

Lahaye, R. (2016). *ACI Security - Reflective Report.*

Lahaye, R. (2016). *ACI Security - Research Report.*