Security Infrastructure

Inleiding en instructies

Voor Security Infrastructure zal je een computernetwerk configureren en beschermen met een firewall. Als firewall zullen we gebruik maken van een Palo Alto networks vm series. Dit is een virtuele uitvoering van de firewall, die via de private cloud van de opleiding bruikbaar wordt.
Je kan individueel een opstelling opstarten via https://cloud.ikdoeict.gent/.

Je zal zelf voor een groot stuk op zoek moeten naar de configuratiestappen die je moet nemen om de opstelling aan de praat te krijgen en te voldoen aan de richtlijnen in deze opgave. Deze informatie kan je onder andere terugvinden in de documenten die je op Toledo kan vinden, de presentaties van de theorielessen en in het online curriculum van Palo Alto. Je bereidt best de relevante hoofdstukken voor, vooraleer je naar het labo komt.

Deze volledige opgave bestaat uit twee soorten opgaven. De eerste reeks zijn de basisopgaven en vormen de verschillende checkpoints van een opgave waar een pass/fail beoordeling aan is gekoppeld. De andere opgaven zijn aanvullende opdrachten die individueel punten opleveren. De punten die je kan verdienen worden uitgedrukt in procenten. Als je die percentages optelt kom je boven de 100% uit. Je score wordt beperkt tot het maximum voor de extra opgaven (8 punten op 20) als je meer dan 100% verzamelt en wordt proportioneel berekend als je daar onder zit.
Je kan zelf kiezen welke opgaven je uitwerkt. Deze opgaven worden in deze tekst verwerkt en aangeduid met een aangepaste opmaak (kader met grijze achtergrond):

Extra opgave

Zowel de extra opgaven als de onderdelen van de pass/fail-opgave worden verbeterd volgens een binair syteem. Je kan er met andere woorden geen deelpunten voor scoren als je het gedeeltelijk in orde hebt.

Naar begeleiding wordt er bij het uitwerken van de extra opgaven ook meer zelfstandigheid verwacht. Als je vast zit met een opgave, kan je altijd vragen stellen, maar reken in dat geval niet op een pasklare oplossing, maar eerder op hulp om de oorzaak van het probleem vast te stellen.

Hieronder vind je een planning voor de verschillende deelopgaven van de pass/fail opgave:

opgave	**planning checkpointcontrole**
basis config	week 1
app id, decryption/content id	week 2
content id / decryption	week 3
DMZ access	week 4
site-to-site VPN	week 5
Remote Access VPN	week 6
user-id	week 7

Een opgave laten controleren doe je tijdens de labo sessies. In de opgave worden een aantal zaken vermeld die je klaarzet als je de controle aanvraagt. Deze zaken neem je ook op in je logboek. In het logboek kan je daarnaast uiteraard ook configuratiestappen en aandachtspunten opnemen. Het logboek zal door de docenten aangemaakt worden en met jou gedeeld tijdens het eerste labo.

Tijdens de labo sessies is het niet alleen de bedoeling om checkpoints te laten controleren, maar uiteraard ook om te werken aan je opgave. Als je daarbij stuit op problemen, kan je terecht bij de begeleidende docent voor ondersteuning. Belangrijk daarbij is dat je het probleem goed omschrijft en aantoont wat je ondernomen hebt om het op te lossen en waarom je geen mogelijke oplossing ziet (“het werkt niet” voldoet niet aan deze omschrijving).

Naast de labosessies zijn er ook nog zogenaamde “begeleide werksessies”. Tijdens deze online momenten is het de bedoeling dat studenten met een achterstand op het schema actief opgebeld worden via teams. Studenten die wel op schema zitten, kunnen uiteraard ook gebruik maken van het moment. Zij sturen in eerste instantie een chatbericht met een omschrijving van het probleem waarmee ze kampen en worden dan opgebeld.

In de opstelling zitten een aantal vm’s, waarvan je voor sommige zelf kan kiezen of het windows of linux machines zijn. De standaard paswoorden die zijn ingesteld zijn:

- op windows: Azerty123 (voor gebruiker student of administrator)
- op linux: student (voor gebruiker student)

- op de firewalls: student (voor gebruiker student), best aan te passen na de eerste login

Extra opgave: Theorie (15%)

Een eerste mogelijke keuze als extra opgave is het afleggen van theorietesten. Aan de theorielessen zijn geen evaluaties voorzien, maar er is ook een online moodle cursus waar je sowieso extra uitleg en inspiratie voor de oplossingen kan vinden. Naast de extra informatie kan je er ook module testen afleggen. Voor de testen van de Firewall essentials cursus kan je punten verdienen als je op elke quiz de door Palo Alto vastgelegde minimumscore haalt. Je mag de testen meerdere keren afleggen en je hoogste score telt.
Je moet wel rekening houden met onderstaand tijdschema. Het lijkt een beetje willekeurig, maar het is een schema, waarmee de modules gemapt worden met de deadlines van de basisopgave waarvoor ze relevant zijn

- week 2: modules 2,3
- week 3: modules 5,6,8
- week 4: modules 7,10,11,13
- week 7: modules 1,4,9,12,14 en final

Als een deadline in een bepaalde week ligt, dan betekent het dat je de test ten laatste op de vrijdag van die week moet afleggen

Laat controleren: zodra je alle testen hebt afgelegd (met een pass-resultaat) stuur je een mail of teams bericht naar je docent (deadline vrijdag week 7).

Initiële configuratie

Een opstelling deploy je op https://cloud.ikdoeict.gent/. Deze opstelling bevat twee virtuele firewalls (PA-vm), een client en een server.

De firewall heeft een basisconfiguratie gekregen, zodat je meteen via de webinterface aan de slag kan. Om van buitenaf (dus bijvoorbeeld vanaf een PC in het labo of van thuis uit via de vpn) verbinding te maken met de webinterface, maak je een **https** verbinding naar het IP adres van de firewall (onder general).
Deze interface krijgt dynamisch een IP adres toegewezen in 10.129.[32-39].0/21. In principe leert de cloud dit IP adres ook, maar dat duurt lang en je kan ten allen tijde het IP adres van je firewall opvragen door verbinding te maken met de webconsole, aan te melden met gebruikersnaam **student** en paswoord **student**. Vervolgens kan je het IP adres opvragen met het commando `show system info`. Met een beetje geluk staat de output van de DHCP aanvraag ook nog gewoon zichtbaar boven de login.

Als je via de webinterface verbinding maakt, kan je als één van de eerste stappen het paswoord van het student account aanpassen (Device - administrators), zodat niemand anders toegang kan krijgen tot je firewall. Voor de docenten is een apart account

voorzien. Als je dit laat bestaan, dan kan je makkelijk geholpen worden, zonder paswoorden te moeten delen.
Hoewel niet strikt noodzakelijk, kan je via Device - Setup - management de tijd aanpassen. Dit kan later relevant zijn om makkelijker de logs te interpreteren.
Je kan ook via ssh verbinding maken met dit IP adres (met een ssh client als putty, mobaXterm…). Je krijgt dan toegang tot de Command Line Interface van de firewall. De CLI biedt vooral extra mogelijkheden bij het testen en troubleshooten.

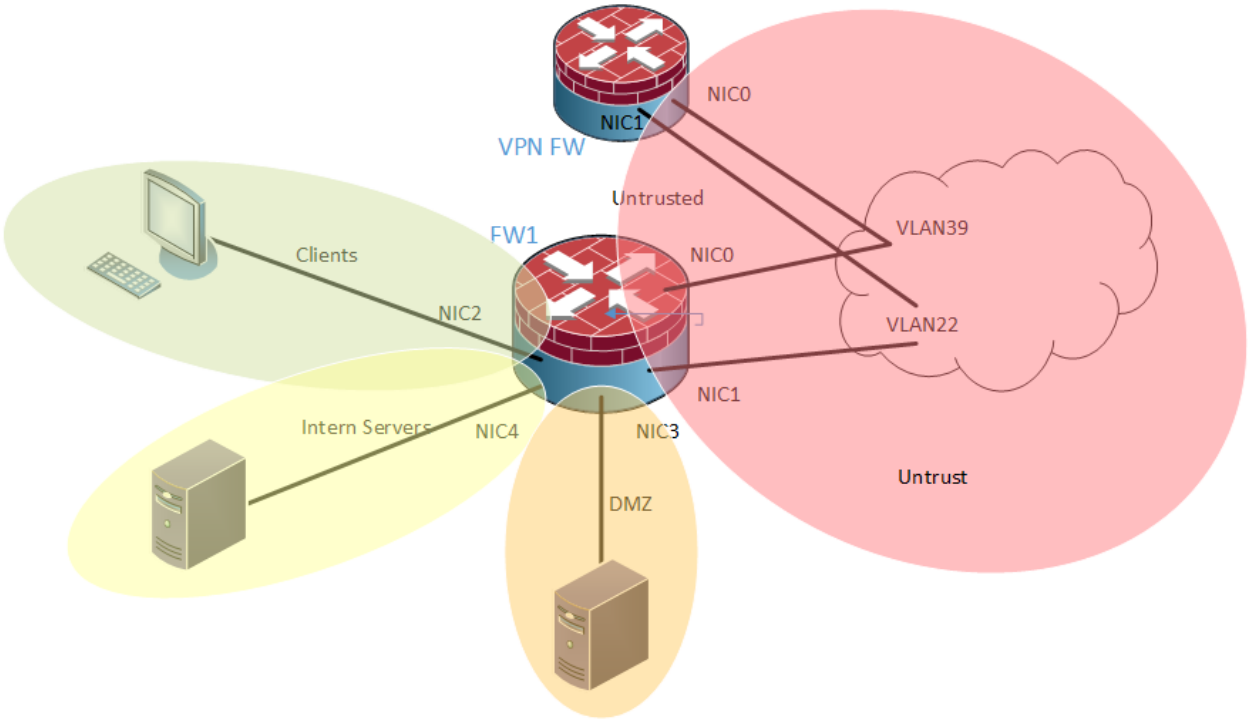
Opmerkingen:
De management interface kan niet gebruikt worden voor dataverkeer. Merk ook op dat in deze labo opstelling de management interface verbonden is met het externe netwerk. Het zou duidelijk moeten zijn dat dit niet meteen de meest veilige opstelling is en dat ze dus in de praktijk ook niet op deze manier zal toegepast worden. Voor de specifieke situatie van het labo is het wel de meest efficiënte. Dit maakt wel dat iedereen van binnen het schoolnetwerk je firewall kan beheren. Het is dus echt een goed idee om je paswoord aan te passen.

Bij een Palo Alto firewall is het cruciaal om te weten dat een verandering in de configuratie geen ogenblikkelijke invloed heeft op de werking van het toestel. Deze invloed komt er pas nadat je een "**commit**" hebt gedaan. Vergeet dus niet om telkens de veranderingen toe te passen.

Als je een deel van de configuratie gedaan hebt, kan het ook interessant zijn om je configuratie op te slaan (save named configuration in device-operations). Als je dan een fout maakt bij de configuratie kan je makkelijk terugkeren naar deze toestand.

Je bent zelf verantwoordelijk voor jouw opstelling en het documenteren van je configuratie. In het geval van een rampscenario zal het van die documentatie afhangen hoe vlot je de toestand kan herstellen.

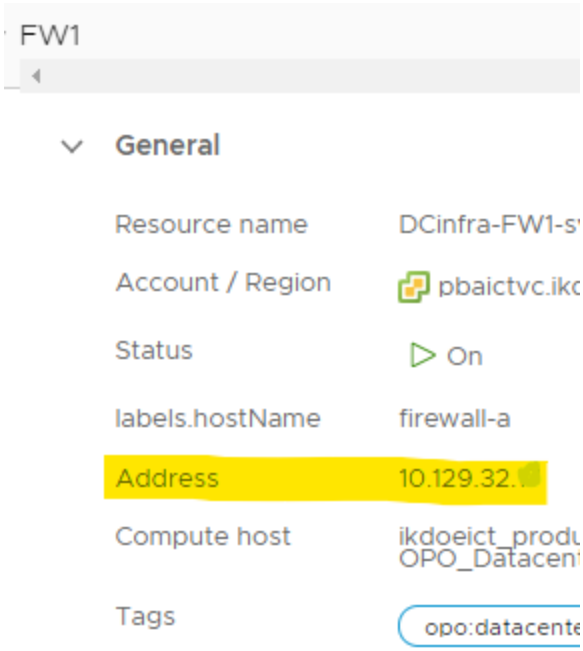
Topologie



Firewall 1			
Cloud Interface	**Firewall interface**	**IP adres vorm**	**opmerkingen**
NIC0	MGMT	10.129.[32-39].a	Dynamisch, af te lezen in cloud omgeving of via externe console
NIC1	e1/1 (untrusted)	10.129.22.x	zie overzicht
NIC2	e1/2 (clients)	zelf te kiezen in 172.21.x.0/24	zie overzicht
NIC3	e1/3 (dmz)	zelf te kiezen in 172.22.x.0/24	zie overzicht
NIC4	e1/4 (internal servers)	zelf te kiezen in 172.23.x.0/24	zie overzicht

Firewall 2			
Cloud Interface	**Firewall interface**	**vCloud IP**	
NIC0	MGMT	10.129.[32-39].b	Dynamisch, af te lezen in cloud omgeving of via externe console
NIC1	e1/1 (untrusted)	10.129.22.(x+2)	zie overzicht

In de cloud omgeving zijn enkel de adressen belangrijk in het bereik 10.129.32-39.0/24. Voor alle andere interfaces zal je zelf de configuratie moeten doen om te zorgen dat ze (op de gewenste manier) het netwerk kunnen gebruiken. De adressen die je daarbij mag gebruiken voldoen aan het patroon in de tabel. Concrete waarden kan je opsporen in dit overzicht. Afwijken van deze adressen kan ervoor zorgen dat jouw oplossing niet werkt.
De management interfaces zijn geconfigureerd met DHCP om de initiële config eenvoudiger te maken, het gevolg is wel dat het adres kan veranderen. Controleer dus zeker of je met je eigen firewall verbinding maakt.
De cloud geeft het management IP weer onder general (niet onder network) zodra die zich bewust is van het IP adres (dat kan wel even duren):



Basisconfiguratie

In dit deel van de opgave zal je ervoor zorgen dat de de computers in het “clients” netwerk verbinding kunnen maken met het internet. De Windows 10 machine bevindt zich in dit netwerk en zal je dus kunnen gebruiken om te testen.

Er moeten een aantal zaken ingesteld worden. Om te beginnen moet op de interface die verbinding maakt met het extern Odisee netwerk (ethernet 1/1) een IP adres toegekend worden (controleer het adres dat de cloud aan de interface toekent, het heeft de vorm 10.129.22.x/24).
Ook op de interface in het “clients netwerk” zal je een IP adres nodig hebben. Dit IP adres kies je zelf in de range 172.21.x.0/24. Om IP instellingen te kunnen doen, moet je bij het configureren van de interfaces het type op L3 zetten.

Bij de configuratie van de interfaces zal je de interfaces ook moeten toekennen aan een security zone. Creëer daarvoor twee Layer 3 security zones, noem ze ClientsFamilienaam en Untrusted (in het vervolg van de opgave zullen de namen clients en untrusted gebruikt worden). Op een Palo Alto firewall beveilig je het verkeer niet tussen interfaces, maar tussen security zones.

Bij de configuratie kan je ook een management profile instellen. Dit bepaalt op welke protocollen de firewall interface zal reageren (merk op dat dit iets totaal anders is dan het verkeer dat de firewall zal toelaten). Maak management profiles aan zodat je enkel ping toelaat op de untrusted interface en op de interne interface ping, ssh en https toelaat.

In het clients netwerk moet de firewall nog de rol van dhcp laten spelen. Daarvoor creëer je op de firewall een dhcp server. Ken die toe aan de correcte interface (ethernet 1/2) en zorg ervoor dat die de adressen van 50 tot 100 kan uitdelen in het 172.21.x.0/24 netwerk. Als DNS servers geef je 10.129.28.232 en 10.129.28.230 mee. Vergeet niet om het juiste default gateway adres mee te geven aan je DHCP clients.

Nu moeten de interfaces nog toegekend worden aan een virtuele router. Maak daarvoor een nieuwe virtuele router aan “VR-voornaam”, zorg ervoor dat beide interfaces hieraan worden toegevoegd en creëer een statische route die al het verkeer naar het untrusted netwerk stuurt (next hop 10.129.22.254).
Controleer of je client in het interne netwerk geconfigureerd is voor DHCP en controleer of je een adres gekregen hebt in het juiste bereik (vergeet “commit” niet op de firewall). Het moet nu mogelijk zijn om de firewall vanaf de interne pc te bereiken via de protocollen die je definieerde in het management profile (onder andere ping en https). Als dit niet lukt, troubleshoot je eerst voordat je verder gaat.

Op dit ogenblik is er nog geen security policy gedefinieerd, dit betekent dat al het interzone verkeer wordt geblokkeerd. Maak een erg eenvoudige policy aan die al het verkeer van clients naar untrusted toelaat. Je moet in deze policy dus geen onderscheid maken in adressen of applicaties. Let er in de laatste tab op dat verkeer standaard pas gelogd wordt aan het einde van een sessie. Hou hiermee rekening als je de logs gaat raadplegen om een probleem op te lossen.

Je kan nu proberen te pingen vanop de firewall naar 10.129.28.230 (dit kan je doen door een ssh verbinding met de firewall te maken en vervolgens het commando `ping source 10.129.22.x host 10.129.28.230` te gebruiken, uiteraard pas je de x aan zodat het adres overeenkomt met dat van e1/1). Dit zou moeten lukken, is dat niet het geval moet je de netwerkinstellingen van de firewall controleren.

Als het wel lukt, kan je een gelijkaardige test proberen vanop de client, maar die zal mislukken. Het probleem is dat we nog geen NAT-policy hebben aangemaakt. Maak dus een policy aan, noem hem “source NAT” en zorg ervoor dat die bij pakketten van clients naar untrusted een dynamische vertaling doet van IP en poort nummer. Hierbij maken alle verbindingen gebruik van het adres van e1/1.
Test de verbinding vanop de client pc, probeer zeker eens op het web te surfen. Los eventuele problemen op.

Laat controleren: toon een webpagina op de client

Extra: Vertrouwde toegang tot de webinterface (7%)

De firewall is standaard geconfigureerd om op de management interface https toegang toe te laten. Zoals je ongetwijfeld gemerkt hebt, is die verbinding niet vertrouwd. Zorg ervoor dat je vanop je laptop toegang krijgt tot de webinterface zonder beveiligingswaarschuwingen.
Voor deze opdracht zijn er drie gradaties om het op te lossen:

- de verbinding wordt vertrouwd
- je hebt gebruik gemaakt van een CA certificaat
- je krijgt toegang op naam ipv ip

Laat controleren: toon de vertrouwde toegang tot je webinterface en de trust chain

Extra: Aanmelden met certificaat bij web interface (7%)

Hoewel de firewall standaard gebruik maakt van https en paswoorden (en andere gegevens) dus versleuteld verzonden worden, blijft het gebruik van paswoorden (in het bijzonder zwakke paswoorden) een risico.
Om dit risico in te perken configureer je in deze opgave authenticatie voor een administrator account aan de hand van een certificaat.

Opgelet: Als je in de fout gaat bij een poging om dit in te stellen bestaat de kans dat je jezelf buitensluit uit de webinterface. Zolang je toegang houdt tot de cli kan je dit rechtzetten door in configure modus terug te keren naar een eerder opgeslagen configuratie. Het commando daarvoor is **load config from <naam van config>**. Voor je start met deze opgave, sla je dus best een configuratie op waarnaar je kan terugkeren.

Opmerking: Als aanmelden met certificaat aan staat, is er geen toegang meer voor docenten tot de webinterface.

Laat controleren: demonstreer het aanmelden op je firewall zonder paswoord

Extra: toegang via authentication server (7%)

Maak gebruik van de internal server om authenticatie op de firewall mogelijk te maken. De gebruiker die op die manier toegang krijgt, moet een gebruikersnaam voornaam.naam krijgen

Laat controleren: toon de authenticatie instellingen op de firewall en het aanmelden van de nieuwe admin in de logs

Applicatie filter

Het is nu de bedoeling dat je het uitgaande verkeer gaat filteren op applicaties. Na de vorige opgave heb je een regel die alle uitgaande verkeer toelaat. Deze regel moet uitgeschakeld, aangepast of verwijderd worden.
In wat volgt zal je gebruik maken van de logs om de juiste applicaties toe te laten om bepaalde webpagina's toegankelijk te maken. De logs kunnen je vertellen welke applicaties geblokkeerd worden. Belangrijk daarbij is dat de applicaties dan geblokkeerd worden door een regel die logging aan heeft staan. De standaard interzone regel blokkeert het verkeer wel, maar logt standaard niet. Je kan die aanpassen door te kiezen voor override.

Een applicatie die je zeker nog zal hebben is web-browsing, maar de andere zal je, zoals gezegd via de logging moeten ontdekken. Als je merkt dat applicaties geblokkeerd worden, zoek dan uit of ze nodig zijn om de webpagina's toegankelijk te maken. Mogelijk genereert de computer van waar je test meer verkeer dat je ook niet moet toelaten om de webpagina's toegankelijk te maken. Laat die applicaties dan ook niet toe. De bedoeling is dat je enkel de noodzakelijk applicaties bewust toelaat en al de (ook onbekende) rest blokkeert (whitelisting).

Je moet op zoek gaan naar alle applicaties die ervoor zorgen dat je toegang krijgt tot volgende webpagina's:

- http://neverssl.com
- https://www.odisee.be
- https://www.google.com

Maak zo weinig mogelijk nieuwe regels aan en benoem ze telkens als volgt: "AppFilterVoornaamNaam<nr>". Verkeer mag enkel toegelaten worden voor clients met een adres uit de interne range (172.21.x.0/24).
In deze opgave moet je geen gebruik maken van URL filtering, de opgegeven websites moeten correct weergegeven worden, een heel aantal andere websites zullen ook weergegeven worden

Bepaalde andere websites zullen niet toegankelijk zijn, als dat het gevolg is van een application block, dan moet de application block page getoond worden. Zorg ervoor dat je die te zien krijgt. Pas de standaard block pagina aan, waarbij je je eigen naam gebruikt als contact. Onder andere surfen naar volgende pagina's zou de block page moeten tonen:

- www.shutterfly.com
- www.metacafe.com

Opgelet: bij (voorlopig) gebrek aan decryptie kunnen https en hsts een heel vervelende rol spelen. Probeer zeker eens met een andere website die als aparte applicatie geklasseerd zou worden (kproxy.com, pastebin.com…) als een applicatie toch getoont wordt of de application block page er niet meteen door komt. Websites als facebook en twitter zijn om bovenvermelde reden een slechte keuze op dit moment.

Laat controleren: Toon in de logs de toegelaten toegang tot google en toon de application block page. Laat de security policy controleren (deze moet de minmale applicaties toelaten, zorg ervoor dat je van elke applicatie weet waarom je ze hebt toegelaten).

Extra: DHCP server op interne server (10%)

Bij de basisconfig werd de firewall geconfigureerd om de rol van DHCP te vervullen. Om de firewall hier niet nodeloos mee te belasten, kan die rol verhuisd worden naar de interne server. Configureer zowel de server als de firewall zodat de server via DHCP adressen uitdeelt aan de client. De interne server moet hierbij wel in een aparte zone (internal servers) ondergebracht worden.

Laat controleren: Toon op de client aan dat die zijn IP instellingen kreeg van de internal server. Toon ook de security policies en de network interfaces.

Decryption

Als je in andere delen probeerde om via HTTPS bestanden te downloaden of bepaalde applicaties of URL's te openen, dan zul je gemerkt hebben dat de firewall dit niet altijd blokkeerde of dat bijvoorbeeld de block page niet getoond werd. Als je dit nog niet vastgesteld hebt, probeer het dan eens uit, voordat je aanpassingen doet.

De reden hiervoor is dat het verkeer over een HTTPS-verbinding versleuteld verloopt en dus onleesbaar is voor alle tussenstations, ook voor de firewall. In het geval van een block page betekent het bijvoorbeeld dat ook de request niet gezien kan worden en dus ook niet beantwoord kan worden met de inhoud van de block page.

Zorg ervoor dat de firewall in staat wordt om ook versleuteld verkeer te monitoren. Dit moet transparant gebeuren voor de eindgebruiker. Dit betekent dat hij zonder waarschuwing kan surfen naar een website die een geldig certificaat aanbiedt, maar dat een website die geen vertrouwd certificaat aanbiedt, een waarschuwing blijft geven.
Als je certificaten moet aanmaken, gebruik dan je eigen naam als onderdeel voor de naam van het certificaat (eventueel aangevuld met trust of untrust).

Het is mogelijk om bepaalde categorieën niet te decrypteren. Zorg ervoor dat connecties met medische of financiële informatie niet gedecrypteerd worden.

Test een vertrouwde site uit (bijvoorbeeld google), een niet vertrouwde (bijvoorbeeld self signed via https://www.badssl.com) en een bankwebsite.
Merk op dat decryption geen verkeer blokkeert of toelaat, maar de firewall wel in staat stelt om de voorheen geconfigureerde security policies toe te passen op versleuteld verkeer.

Laat controleren: toon zelf in de logs aan dat het verkeer gedecrypteerd werd (of net niet voor de uitzonderingen). Je kan hiervoor de details van een pakket bekijken met het vergrootglas dat helemaal links bij de log entry staat of een kolom "decrypted"

toevoegen waar met een checkbox wordt aangegeven of verkeer al dan niet werd gedecrypteerd. Toon zowel voor een vetrouwde als voor een niet-vertrouwde verbinding de webpagina en de trust chain.

Extra: PKI (13%)

Zorg dat op de internal server de nodige certificaten aangemaakt kunnen worden (ook voor andere deelopgaven). Voor de certificaten werk je met een root CA en issuing CA's. Op clients installeer je een minimum aantal certificaten om vertrouwen te krijgen.
Als je het toepast op decyrption ga je uiteraard zorgen dat vertrouwen in de PKI zorgt voor vertrouwen in het trust certificaat. Je kan deze oplossing uiteraard ook gebruiken in andere situaties.

Laat controleren: toon een vertrouwde connectie en de bijhorende trust chain. Toon ook de geïnstalleerde certificaten op een client.

Extra: custom application (10%)

Heel wat websites worden door de firewall gekoppeld aan hun eigen specifieke applicatie (denk maar aan google-base). Natuurlijk zijn er nog behoorlijk wat websites die in de categorie web-browsing worden ingedeeld.
Het doel van deze opgave is om voor een website zelf een custom applicatie te maken. Je mag zelf de website kiezen (bij voorkeur één waarmee je zelf een band hebt), maar controleer of ze nog onder web-browsing valt. Gebruik in de naam van de curstom application je eigen naam.

Laat controleren: toon de identificatie van de custom application in de logs van de firewall of in de block page

Content filter

Nu is het de bedoeling dat je gaat filteren op inhoud. Controleer bij dynamic update eerst of de meest recente updates op de firewall geïnstalleerd zijn (voor application and threats, antivirus en wildfire). Controleer bij licences ook de of de PAN-DB URL filtering actief is. Na het installeren van de updates controleer je eerst of je vorige policies nog steeds werken.
Om de opgave af te werken, moet je een aantal profiles aanmaken. Gebruik steeds je eigen naam als deel van de naam van een profile.

URL-filtering

Maak een eigen URL filter aan die het verkeer zal beperken volgens onderstaande beschrijving. Gebruik URL-filter-Voornaam als naam.

Als je deze opgave oplost voordat je decryption aan de praat krijgt, let er bij het testen dan op dat je test met http-verkeer. Als je browser via hsts geleerd heeft om steeds via https te gaan, kan je de geschiedenis wissen, een “in private” of incognito venster proberen of een andere website gebruiken om te testen.
Een eerste beperking is dat je webverkeer naar websites van andere hogescholen gaat controleren. In dit geval is het de bedoeling dat

- toegang tot de website van Odisee zonder meer mogelijk moet zijn
- toegang tot andere Vlaamse hogescholen enkel mogelijk is na het ingeven van een paswoord. Test bijvoorbeeld met http://www.vives.be, http://www.ap.be, http://www.howest.be, www.kdg.be, http://www.thomasmore.be … (gebruik eventueel nog andere namen als hsts in de weg zit). Toon voor de controle ook de pagina waar je het paswoord moet intikken.
- toegang tot andere, niet-Vlaamse scholen en hogescholen mag enkel na een waarschuwing aan de gebruiker, maar de gebruiker heeft geen paswoord nodig om verder te gaan (test bijvoorbeeld met http://www.stanford.edu, http://www.ox.ac.uk/ …). Dit moet werken voor alle websites die door Palo Alto Networks als een “educational institution” worden gezien en die geen Vlaamse Hogeschool zijn.
- Blokkeer ook de toegang tot de categorie hacking. Er zijn veel andere categorieën die waarschijnlijk een stuk relevanter zijn om te blokkeren (doe dit gerust), maar deze kan je makkelijk testen zonder invloed van de centrale firewall van de school. Bijvoorbeeld http://www.2600.org/ valt in de categorie “hacking”.

URL's zullen geblokkeerd worden op basis van de categorie waar ze door Palo Alto in ondergebracht zijn. Je kan deze categorie controleren op https://urlfiltering.paloaltonetworks.com/, daar kan je ook aanpassingen vragen als je vindt dat een URL onterecht wel of niet in een bepaalde categorie is ondergebracht.

Anti-virus en -spyware
Configureer ook een antivirus profile, noem het VoornaamNaamAntivirus. Zet de actie voor alle decoders op **Alert**.

Configureer ook een anti spyware profile, noem het VoornaamNaamAntispyware. Maak twee regels aan: de eerste laat alles met **severity low** of **informational** toe, de tweede zal alles met **severity High** of **Critical** blokkeren met een **reset-both**.

Zorg ervoor dat de profiles worden toegepast en test uit door de malware testfile op eicar.org te downloaden. Dit is een bekende testfile. Het is niet abnormaal dat je een waarschuwing krijgt van de browser omdat die het ook als gevaarlijk herkent (dit betekent dat de firewall het heeft doorgelaten wat overeenkomt met de **Alert** actie).

File blocking

Zorg ervoor dat alle pdf's geblokkeerd worden (zowel upload als download), noem je profiel FileVoornaamNaam.
Maak ook een Wildfire profile aan. Wildfire is een cloud oplossing voor malware analyse. Maak een profile aan dat executable files naar de public cloud stuurt (PE staat voor portable execution).

Test beide uit door een pdf te downloaden en een zero day te genereren en downloaden op http://wildfire.paloaltonetworks.com/publicapi/test/pe (https://cutt.ly/sC1pwkH). Open het bestand niet.

Laat controleren:
Toon voor URL-filtering in de logs dat voor de verschillende categorieën de juiste actie wordt ondernomen.
Toon voor de antivirus policy in de logs aan dat er een verdacht bestand werd gedownload.
Toon in de logs de file blocking van pdf en de wildfire analyse aan. De wildfire analyse kan een tijdlang duren (10 minuten), maar met het cli-commando `debug wildfire upload-log show` kan je wel meteen nagaan of de upload naar het platform gebeurde.
Verklaar waarom deze pdf wel opent:
https://www.kbc.com/content/dam/kbccom/doc/sustainability-responsibility/PerfRep/2021/csr-vas-2021-nl.pdf (https://cutt.ly/zC1pUds).

Extra: vertrouwde override pagina (7%)

Als je decryption al hebt afgewerkt, is het testen van content filtering een stuk eenvoudiger omdat het ook werkt op HTTPS pagina's.
Bij de URL-filtering kan je er dan ook voor zorgen dat de override pagina geen beveiligingswaarschuwing op het certificaat meer geeft. Doe dit, zonder op de client extra certificaten te installeren.

Laat controleren: toon de vetrouwde override pagina en de trust chain

Extra: External Dynamic List (5%)

Om het lijstje met de Vlaamse hogescholen eenvoudig aan te kunnen passen, is het interessant om gebruik te maken van een zogenaamde External Dynamic List. Zorg ervoor dat de firewall de lijst met hogescholen gaat opzoeken op een server.

Laat controleren: toon in de config de koppeling naar de server en demonstreer het dynamisch toevoegen

Inkomende verbindingen

In dit gedeelte moet de firewall geconfigureerd worden om inkomende verbindingen toe te laten, zowel vanuit een andere interne zone als vanuit het externe netwerk. Een server in de DMZ zone wordt daardoor toegankelijk.
Geef deze server een adres in het 172.22.x.0/24 stel ook de default gateway in en stel de DNS servers in (10.129.28.232 en 10.129.28.230). Op de server moet een webserver geïnstalleerd worden en die moet toegankelijk zijn (controleer de configuratie van de server). Ping mag je altijd toelaten om te kunnen troubleshooten, maar vergeet dan niet om het op de server zelf toe te laten. Als je voor de installatie een internetverbinding nodig hebt, zal je die uiteraard ook moeten toelaten (en juist configureren) op de firewall.

Zorg er nu voor dat de server bereikbaar wordt vanuit de clients zone op zijn intern adres, laat enkel de applicaties toe die nodig zijn om te pingen en surfen naar de website.
Configureer de nodige security en NAT policies zodat deze server ook bereikbaar wordt vanop het “internet”. Bij de configuratie op de firewall maak je gebruik van adres het extra adres dat je kreeg (10.129.22.(x+1), zie overzicht).

Telkens je een policy aanmaakt gebruik je bij het geven van de naam een naam die voldoet aan volgend formaat: “FamilienaamBeschrijving” (bijvoorbeeld “Janssens Clients to DMZ”).

Zorg ervoor dat ook de interne client kan surfen naar het publieke adres van de webserver.

Laat controleren: Toon via de logs de verschillende toegangen tot de webserver aan en toon de security en NAT policies.

Extra: remote access (7%)

In de cloud opstelling zitten een aantal virtuele machines om de rol van client of server te spelen. In andere vakken werd, afhankelijk van het besturingssysteem, gebruik gemaakt van remote desktop of ssh om die virtuele machines te gebruiken. Omdat in dit geval de machines achter een firewall staan, is dit niet mogelijk zonder aanpassingen aan de firewall en lijkt de webconsole (met bepaalde nadelen) de enige optie.
In dit geval heb je echter zelf controle over de firewall en kan je die instellen om de verbindingen wel toe te laten. Afhankelijk van de oplossing die je implementeerde zou

dit erg eenvoudig kunnen lukken voor de DMZ server, maar om deze opdracht af te werken implementeer je het voor minstens twee machines.
Later in de opgave kan dit mogelijk worden door gebruik van GlobalProtect, maar dat is voor deze opgave niet de bedoeling en levert geen punten op.

Laat controleren: toon de toegang vanaf een externe client en de policies die nodig zijn om dit te laten werken.

Extra: DNS server (7%)

Zorg ervoor dat de DMZ server ook de rol gaat spelen van DNS. Dat betekent dat hij dns requests zal beantwoorden voor jouw domein (familienaam.di) en dat interne clients er gebruik van kunnen maken voor de resolving. Die moeten met andere woorden geen externe server meer kunnen aanspreken (schakel dit ook uit).
Zone delegatie wordt niet geconfigureerd, dus moet je voor het testen van de externe resolving de server rechtstreeks gebruik laten maken van je dns server.

Laat controleren: toon zowel een externe als interne client die toegang krijgt tot je DMZ server via een name based URL

Extra: DNSsec (7%)

Deze opdracht kan je enkel uitvoeren als je een DNS server hebt aangemaakt.
Zorg ervoor dat je DNS server gebruik maakt van DNSsec.

Laat controleren: toon op een client aan dat de dns records van familienaam.si

Extra: HTTPS (7%)

Configureer de webserver en firewall zodat de server toegankelijk wordt via HTTPS. Zorg ervoor dat de verbinding ook vertrouwd wordt door gebruik te maken van het vertrouwen in certificaten die je eerder installeerde. Werk ook met een redirect als een http verbinding wordt gemaakt.

Laat controleren: toon de policies op de firewall en de vertrouwde beveilgde toegang tot de website, inclusief de redirection, en de trust chain.

Extra: threat protection (10%)

Ga zelf op zoek naar een mogelijke aanval op je server die gedetecteerd kan worden door de firewall. Configureer de firewall om de aanval af te stoppen en probeer dit uit.

Laat controleren: toon de policies op de firewall en toon in de logs hoe de firewall de bedreiging afhandelde

IPsec VPN (site-to-site)

In de opstelling is een tweede firewall aanwezig. Je kan verbinding maken met de management interface van deze firewall op dezelfde manier als je dat deed bij firewall 1. Uiteraard moet je nu het IP adres gebruiken van de firewall, dat je kan aflezen in de cloud (of eventueel opzoeken via de externe console).

Configureer de tweede firewall:

- e1/1 krijgt adres het adres dat de cloud opgeeft (10.129.22.(x+2)/24)
- maak een loopback interface en geef die adres 192.168.15.23/32
- de loopback interface komt bij dezelfde virtuele router, maar in een andere zone dan e1/1
- het management profile van de loopback interface laat http en ping toe

Het is nu de bedoeling om een IPsec VPN op te zetten tussen beide firewalls. Tijdens de configuratie moet onder andere een IKE gateway ingesteld worden. Daarbij moet een crypto profile gebruikt worden met volgende instellingen: 2048 bits voor de Diffie-Hellman exchange, AES met 256 bit sleutel en SHA512 als authenticatie algoritme, noem dit profile secure-familienaam.
Tunnel interfaces die je aanmaakt moeten in een aparte zone geconfigureerd worden.

Door de tunnel moet het mogelijk worden om vanaf het interne client netwerk verbinding te maken naar de loopback interface en omgekeerd. Zorg ervoor dat de tunnel enkel verkeer tussen de juiste subnets toelaat. Beperk de applicatie om enkel ping en surfen toe te laten.
Bij de configuratie is het belangrijk te zorgen dat het verkeer dat door de tunnel moet, ook langs daar gerouteerd wordt.

Test door te pingen vanaf de interne client naar de loopback interface. Probeer ook eens te surfen naar de webinterface van de andere firewall.

Laat controleren: toon het resultaat van de ping, de bijhorende traffic logs en de configuratie van de cryptografische parameters.

Extra: VPN tussen identieke private subnets (5%)

Het zou kunnen gebeuren dat op twee fysiek verschillende locaties gebruik gemaakt wordt van hetzelfde private subnet. Als die twee locaties dan aan elkaar gekoppeld moeten worden, dan zorgt dat voor een extra uitdaging.
Maak op de tweede firewall een localhost interface aan die je een IP toekent in hetzelfde subnet als dat van de client op de eerste firewall. Configureer de firewalls nu zodat ook verbinding naar dit nieuwe subnet mogelijk wordt.

Laat controleren: toon de policies die aangemaakt werden om de connectie mogelijk te maken

Remote Access VPN (GlobalProtect)

In dit deel is het de bedoeling om een zogenaamde Remote Access VPN op te zetten. Deze verbinding moet het mogelijk maken voor thuiswerkers of werknemers op de baan om verbinding te maken met het bedrijfsnetwerk en (beveiligde) toegang te krijgen tot resources die vanaf het “untrusted” netwerk niet bereikbaar zijn. Palo Alto biedt deze mogelijkheid aan via GlobalProtect.

Als je gebruik wil maken van een eigen laptop kan je de client downloaden via de portal die je zelf moet activeren op je firewall. Je moet de client wel eerst downloaden op de firewall.

Zorg voor een GlobalProtect portal en een GlobalProtect gateway, gebruik portalNaam en gatewayNaam als naam. Beide moeten extern toegankelijk zijn. De nodige certificaten moeten afgeleid worden van eenzelfde CA certificaat. Aandachtspunt is het downloaden en activeren van de GlobalProtect client op de firewall. Als dit gebeurt is, kan je later met een https connectie op het adres van de portal de client software downloaden op de client.
Bij de configuratie van de portal wordt best gekozen voor een on-demand connectie, dit vermijdt problemen op het ogenblik dat de connectie niet meer nodig is.

Configureer de GlobalProtect Gateway waarbij een gebruiker toegang krijgt tot het lokale netwerk en zijn internetverbinding via de firewall maakt. Na connectie krijgen GlobalProtect client een adres uit deze range: 172.25.x.0/24

Configureer policies om

- remote desktop en ping toe te laten naar het internal clients netwerk. Beperk dit tot de juiste range bron en destination adressen
- internetverkeer toe te laten met url filter en applicatie filter. Zeker als je de GlobalProtect verbinding maakt vanop je laptop is het best zoveel mogelijk

verkeer toe te laten, maar zorg voor minstens één verboden applicatie, zodat de application block page kan aantonen dat het verkeer effectief door de firewall gaat. Beperk weer de source adressen tot de juiste range. Uiteraard betekent dit dat de client ook al het internetverkeer via de tunnel moeten versturen.

Voor het testen moet het GlobalProtect certificaat vertrouwd worden. Configureer de portal om het root CA waarvan het gateway certificaat werd afgeleid, door te geven aan de client. Let op: de client kan bij het maken van een connectie met de portal kiezen om het certificaat van de portal te vertrouwen. Als de client software verbinding maakt met de gateway, wordt deze keuze niet aangeboden. Let er dus ook op het certificaat van de gateway gekoppeld is aan het externe adres.
Vervolgens kan de tunnel uitgeprobeerd worden:

- controleer of je een remote desktop sessie kan opbouwen naar de interne client
- controleer of je internettoegang onderworpen is aan de policies van de firewall (laat de response pages toe op de tunnel interface).

Laat controleren: Toon de beperkingen op het Internet verkeer van de client die via GlobalProtect is verbonden en de remote desktopverbinding met de interne client

Extra: internal gateway (7%)

Zorg ervoor dat ook interne clients een globalprotect verbinding kunnen opbouwen. In dit geval is het uiteraard niet de bedoeling om een tunnel met het interne netwerk te maken, maar wel om meer controle over de client te krijgen (zo is het bijvoorbeeld mogelijk om het forward trust certificate uit te delen zodat decryption mogelijk wordt op gebruikers die met hun eigen smartphone verbinding maken met het bedrijfsnetwerk). Speciale instellingen op dat vlak zijn niet nodig, maar je moet wel de verbinding kunnen maken.

Laat controleren: Toon de geslaagde connectie vanop de interne client

Extra: allways-on VPN (7%)

In de basisopgave volstaat het om met een welbepaalde user aan te melden om de GlobalProtect verbinding te maken. Dit betekent uiteraard dat er een gebruiker nodig is, die op één of andere manier het paswoord kan doorgeven. De tunnel wordt dan ook pas ten vroegste opgebouwd als die gebruiker is aangemeld op de client.
Door gebruik te maken van certificaten kan de client zich authenticeren zonder de koppeling naar een user te moeten maken. Zodra de netwerkverbinding actief is, kan er dan ook meteen een globalprotect verbinding gemaakt worden.
Configureer de firewall en een client zodat dit ook werkt. Je mag zelf kiezen of je dat doet met een externe of interne client.

Laat controleren: toon de verschillen in configuratie op de firewall en de client

Extra: Large Scale VPN (13%)

Global protect laat ook Large Scale VPNs (LSVPN). Hierbij is het de bedoeling dat met een eenvoudige configuratie kleine remote offices (denk bijvoorbeeld aan winkelfilialen) automatisch verbinding kunnen maken met het bedrijfsnetwerk.
De meerwaarde zit in de eenvoud waarmee meerdere “satellites” kunnen toegevoegd worden. In dit geval kan enkel firewall 2 hiervoor gebruikt worden. Het doel van de opgave is om de LSVPN voor die firewall aan de praat te krijgen. De IPsec VPN wordt tijdelijk best uitgeschakeld.

Laat controleren: toon de connectie van de satellite op de portal of de gateway aan (satellite info in network - globalprotect - portal/gateway)

User-ID

De Palo Alto firewall kan op verschillende manieren detecteren welke gebruiker een bepaalde verbinding wil opzetten. Het gaat dan niet over machines, maar wel om de personen die erachter zitten. In deze opgave beperken we ons tot het aanmelden als lokale gebruiker op de firewall om dan extra toegang te krijgen.

Maak een policy aan die het mogelijk maakt voor bepaalde gebruikers om toegang te krijgen tot Facebook. Maak twee lokale gebruikers aan op de firewall en toon een webformulier om aan te melden, vooraleer door te gaan naar Facebook. De ene gebruiker heeft toegang tot Facebook, de andere niet. Maak gebruik van een captive portal.

Laat controleren: demonstreer het verbod zonder geldige login en de toegang. Als je hebt aangemeld kan je dit verifiëren via de CLI met `show user ip-user-mapping all` en je kan de authenticatie opnieuw forceren door op de firewall de koppeling IP-user te resetten: `debug user-id reset captive-portal ip-address <ip-address>`.

Extra: server als bron voor user-ID (7%)

De portal is een handige manier om zonder al te veel externe configuratie op de firewall user-id aan de praat te krijgen. Een veel frequenter voorkomende situatie is dat je de informatie over de user te pakken krijgt van één of andere server waar de gebruiker sowieso al bij moet authenticeren.
Een typisch voorbeeld zou de Domain Server kunnen zijn, maar er zijn ook alternatieven zoals radius of andere directory systemen mogelijk.

In dit deel is het de bedoeling om de koppeling te maken tussen de firewall en de informatie op zo'n server en die login informatie te gebruiken als basis voor de user-ID.
Als het authenticatiesysteem groepen ondersteund, maak je op de firewall gebruik van groepen om een security policy te implementeren (om bijvoorbeeld een bepaalde applicatie toe te laten).

Laat controleren: Toon de configuratie van de koppeling tussen firewall en server en eventuele configuratie van de server zelf (enkel het deel gerelateerd aan de communicatie met de firewall). Toon in de logs de koppeling van de users.

Voor het vak security infrastructure kan je 50$ krediet krijgen op Google cloud. Onderstaande opgaven maken gebruik van dat krediet. Let op: als je devices deployed dan is daar een kost aan verbonden, die van een aantal zaken afhangt.
Naast verwachte zaken zoals verbruikte bandbreedte en resources voor VMs spelen ook licenties een rol. Als je een windows server of firewall deployed, dan worden die verrekend naargelang ze ingeschakeld zijn. Vooral voor de Palo Alto firewall kan dit oplopen. Schakel die machines dus uit als je ze niet nodig hebt voor het configureren of testen. Als je krediet op is, vooraleer je een opgave laat controleren, zal je geen punten kunnen scoren voor die opgave.

Extra opgave: cloud server (10%)

Voor deze opgave is het de bedoeling dat je in de cloud een webserver opzet en zorgt dat die toegankelijk wordt via jouw firewall.
Voor het gemak van testen mag je de server rechtstreeks bereikbaar houden via ssh of remote desktop. Toegang tot de webserver mag in principe enkel via je firewall mogelijk zijn.
De toegang moet zowel voor een interne als een externe client in het schoolnetwerk mogelijk zijn.

Laat controleren: toon de noodzakelijk policies en configuraties op je firewall en in het cloud platform. Demonstreer de toegang.

Extra opgave: cloud firewall met server (15%)

Deploy op de cloud een Palo Alto Networks firewall. Dit kan via marketplace (zoek op palo alto networks inc) - VM series next generation firewall. Er zijn twee bundles, bundle1 kost iets minder, maar heeft beperktere licentie. Als je ook de volgende opgave wil maken met dezelfde firewall, neem je beter een bundle 2.
Deploy ook een virtuele server en configureer daarop een webserver. Bescherm toegang tot de server met de firewall. Zorg ervoor dat ook het beheer van de server afgeschermd is.

Opmerking: deze opgave gaat uit van enige ervaring met netwerken in het Google Cloud Platform. Je begint er beter niet aan als je de vorige extra opgave niet tot een goed einde hebt gebracht

Laat controleren: toon de noodzakelijk policies en configuraties op je firewall en in het cloud platform. Demonstreer de toegang.

Extra opgave: client bescherming via cloud firewall (10%)

Deploy op de cloud een Palo Alto Networks firewall. Dit kan via marketplace (zoek op palo alto networks inc) - VM series next generation firewall (bundle 2). Configureer de firewall zodanig dat je met een client op internet kan via de firewall.
Als client kan je gebruik maken van je laptop, een vm op die laptop of een vm in de private odisee cloud. Zorg voor een policy die het meeste verkeer toelaat, maar wel voor een zelfgekozen applicatie een block page toont

Laat controleren: Demonstreer de toegang aan de hand van de block page op je client en de logs op de firewall.

Extra opgave: cloud firewall VPN (10%)

Deze opgave werkt tussen twee studenten of met twee firewalls in een verschillend project. Als je geen global protect gebruikt, kan je bundle 1 gebruiken (die is iets goedkoper).
Bouw tussen de cloud firewalls een tunnel op. Je maakt daarbij een intern netwerk op de firewall toegankelijk vanaf een intern netwerk op de andere firewall. Als je nog geen intern netwerk hebt op de Google cloud firewall, dan mag gebruik gemaakt worden van een loopback interface op de firewall.

Laat controleren: Demonstreer de toegang tot de interne range van de cloud firewall. Toon ook de configuratie van de VPN tunnels op de firewalls.