& Active Directory-integratie configureren met FirePOWER-applicatie voor Single-Sign-On Captive Portal Verification

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Configureren Stap 1. De Firepower User Agent configureren voor eenmalige aanmelding Stap 2. Het Firepower Management Center (FMC) integreren met User Agent Stap 3. Integreer Firepower met Active Directory Stap 3.1 Maak het rijk Stap 3.2 Voeg de Directory Server toe Stap 3.3 Wijzig de gebiedsconfiguratie Stap 3.4 Downloaden Gebruikersdatabase Stap 4. Het identiteitsbeleid configureren Stap 4.1 Captive Portal (actieve verificatie) Stap 4.2 Enkelvoudige aanmelding (passieve verificatie) Stap 5. Het toegangscontrolebeleid configureren Stap 6. Het toegangscontrolebeleid implementeren Stap 7. Gebruikersgebeurtenissen en verbindingen bewaken Verifiëren en probleemoplossing Controleer de connectiviteit tussen VCC en User Agent (passieve verificatie) Controleer de connectiviteit tussen VCC en Active Directory Controleer de connectiviteit tussen Firepower Sensor en het eindsysteem (actieve verificatie) Controleer de beleidsconfiguratie en -implementatie De logboeken van de gebeurtenissen analyseren Gerelateerde informatie

Inleiding

In dit document wordt de configuratie beschreven van Captive Portal Authentication (Actieve verificatie) en Single-Sign-On (Passieve verificatie).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Sourcefire-apparaten voor firewalls
- Modellen voor virtuele apparaten
- Lichtgewicht Directory Service (LDAP)
- Firepower User Agent

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Firepower Management Center (FMC) versie 6.0.0 en hoger
- Firepower sensor versie 6.0.0 en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Captive Portal Verification of Active Verification vraagt om een inlogpagina en gebruikersreferenties zijn vereist voor een host om de internettoegang te krijgen.

Single-Sign-On of Passive Verification biedt een gebruiker naadloze authenticatie voor netwerkbronnen en internettoegang zonder meerdere gebruikersreferenties. De Single-Sign-on verificatie kan worden bereikt door Firepower user agent of NTLM browser authenticatie.

Opmerking: voor Captive Portal-verificatie moet het apparaat in de routeringsmodus staan.

Configureren

Stap 1. De Firepower User Agent configureren voor eenmalige aanmelding

In dit artikel wordt uitgelegd hoe u Firepower User Agent kunt configureren in een Windows-machine:

Installatie en verwijdering van Sourcefire User Agent

Stap 2. Het Firepower Management Center (FMC) integreren met User Agent

Log in bij Firepower Management Center, navigeer naar **Systeem > Integratie > Identity Sources.** Klik op de optie **New Agent**. Configureer het IP-adres van het User Agent-systeem en klik op de knop **Toevoegen**.

Klik op de knop Opslaan om de wijzigingen op te slaan.

Overview	Analysis	Policies	Devices	Objects	AMP								
								Configur	ration	Users	Domains	Integration	Upda
Cisco CSI	Realms	Identity	y Sources	eStream	er Host Inp	ut Client	Smart Soft	ware Satellite					
Identity S	Sources												
Service Type			None	Identity Ser	vices Engine	User Age	nt						
								New	Agent				
Host Name	e/IP User	Agent					? ×						
	Hos	it Name/IP Ad	idress 192.	168.10.11									
					Add	Cano	el						

Stap 3. Integreer Firepower met Active Directory

Stap 3.1 Maak het rijk

Log in bij het VCC, navigeer naar **Systeem > Integratie > Realm.** Klik op de optie **Nieuw gebied toevoegen**.

Naam & Beschrijving: Geef een naam/beschrijving om het domein uniek te identificeren.

Type: AD

AD Primary Domain: Domeinnaam van Active Directory

Gebruikersnaam: <gebruikersnaam>

Directory Wachtwoord: <password>

Base-DN: Domain of Specific OU DN waar het systeem een zoekactie start in de LDAP-database.

Groep DN: groep DN

Groepskenmerk: Member

					Cor	nfiguration	Users	Domains	Inte	gration	Update
Cisco CSI	Realms	Identity Sources	eStreamer	Host Input Client	Smart Software Sate	llite					
Name servertest-1				Description	Add New Realm Name * Description Type * AD Primary Domain * Directory Username * Directory Password * Base DN * Group DN *	AD sen dc= kn=	vertest vertest.com vertest\admi uservertest,d	n c=com :urity-Team.dc		ex: domain. ex: user@d ex: ou=use ex: ou=use	.com Iomain r,dc=cisc up,dc=cis
					Group Attribute • Required Field	Men	nber		~		ОК

Dit artikel helpt u om de waarden van de Basis DN en van de Groep DN te ontdekken.

Identificeer actieve Directory LDAP-objectkenmerken

Stap 3.2 Voeg de Directory Server toe

Klik op de knop **Toevoegen** om naar de volgende stap te gaan en klik vervolgens op de optie **Map** toevoegen.

Hostnaam/IP-adres: configureer het IP-adres/hostnaam van de AD-server.

Poort: 389 (Active Directory LDAP-poortnummer)

Versleuteling/SSL-certificaat: (optioneel) Raadpleeg voor het versleutelen van de verbinding tussen FMC-

en AD-server het volgende

artikel: <u>Verificatie van verificatieobject op FireSIGHT-systeem voor Microsoft AD-verificatie via</u> <u>SSL/TLS</u>

Overvie	w Analysis Po	licies Devices Objects	АМР						
					Configuration	Users	Domains	Integration	Updat
Serve Enter a de	rtest scription								
Directory	Realm Configur	ation User Download							
	Edit directory			? ×					
URL (Hos	Hostname / IP Address Port	192.168.10.11]						none
	Encryption SSL Certificate	STARTTLS LDAPS Non	e						
		ок	Test Ca	ancel					

Klik op de knop **Test** om te verifiëren of het VCC verbinding kan maken met de AD-server.

Stap 3.3 Wijzig de gebiedsconfiguratie

Ga naar **Realm Configuration** om de integratieconfiguratie van de AD-server te verifiëren en u kunt de AD-configuratie wijzigen.

Stap 3.4 Downloaden Gebruikersdatabase

Navigeren naar gebruiker Download optie om de gebruikersdatabase te halen van de AD server.

Schakel het aanvinkvakje in om **gebruikers en groepen downloaden** te downloaden en het tijdsinterval te definiëren over hoe vaak FMC contact opneemt met AD om gebruikersdatabase te downloaden.

Selecteer de groep en plaats deze in de optie **Opnemen** waarvoor u de verificatie wilt configureren.

Directory Realm Configuration User Download		
Download users and groups Begin automatic download at 12 AM America/New York Repe La Download Now	at Every 24 Y Hours	
Available Groups 😋	Groups to Include (1)	Groups to Ex
Search by name	Add to Include Add to Exclude	None
	Enter User Inclusion	Add Enter User Ex

Schakel de AD-status in zoals in de afbeelding:

Overview Analysis	Policies Devices	Objects AM	P				
Dashboards • Reportin	g Summary 🔻						
Cisco CSI Realms	Identity Sources	eStreamer	Host Input Client	Smart Software Sate	llite		
Name			Description	Domain	Туре	Base DN	Group DN
servertest-1				Global	AD	dc=servertest,dc=com	cn=TAC,ou=Sec

Stap 4. Het identiteitsbeleid configureren

Een identiteitsbeleid voert gebruikersverificatie uit. Als de gebruiker geen verificatie uitvoert, wordt toegang tot netwerkbronnen geweigerd. Dit dwingt Role-Based Access Control (RBAC) af op het netwerk en de resources van uw organisatie.

Stap 4.1 Captive Portal (actieve verificatie)

Actieve verificatie vraagt om gebruikersnaam/wachtwoord in de browser om een gebruikersidentiteit te identificeren om een verbinding mogelijk te maken. Browser authenticeert gebruiker met een verificatiepagina of authenticeert stilletjes met NTLM-verificatie. NTLM gebruikt de webbrowser om authenticatie-informatie te verzenden en ontvangen. Actieve verificatie maakt gebruik van verschillende typen om de identiteit van de gebruiker te verifiëren. Verschillende soorten verificatie zijn:

- 1. HTTP Basic: In deze methode vraagt de browser om gebruikersreferenties.
- 2. **NTLM:** NTLM gebruikt Windows werkstation referenties en bespreekt het met Active directory via een webbrowser. U moet de NTLM-verificatie in de browser inschakelen. Gebruikersverificatie

gebeurt transparant zonder aanwijzingen voor referenties. Het biedt een enkele aanmelding ervaring voor gebruikers.

- 3. **HTTP Onderhandelen:**In dit type, probeert het systeem te verifiëren met NTLM. Als het mislukt, dan gebruikt de sensor HTTP Basic authenticatie type als een fallback methode en vraagt een dialoogvenster voor gebruikersreferenties.
- 4. **HTTP Response page:** Dit is vergelijkbaar met HTTP basis type, maar hier wordt de gebruiker gevraagd om de authenticatie in een HTML formulier dat kan worden aangepast.

Elke browser heeft een specifieke manier om de NTLM-verificatie in te schakelen en dus houden ze zich aan de browserrichtlijnen om de NTLM-verificatie mogelijk te maken.

Om de referenties veilig te delen met de gerouteerde sensor, moet u ofwel zelf-ondertekende servercertificaat of openbaar-ondertekende servercertificaat installeren in het identiteitsbeleid.

Ga naar **Beleid > Toegangsbeheer > Identiteit**. Klik op het **beleid toevoegen** & een naam geven aan het beleid en sla het op.

Overview Analysis Policies Devices Obj	ects AMP			
Access Control > Identity Network Discovery	Application Detectors Corre	ation Actions •		
Identity Policy	Domain		Status	
	New I	dentity policy	? ×	
	Name	Identity Policy		Add a new policy
<	Descri	ption		
		Save	Cancel	

Navigeer naar het tabblad **Actieve verificatie** en klik in de optie **Servercertificaat** op het **pictogram** (+) en upload het certificaat en de privé-sleutel die u in de vorige stap met openSSL hebt gegenereerd.

Overview Analysis	Policies Devices Objects	AMP		
Access Control > Identi	ty Network Discovery App	lication Detectors Corr	elation Actions •	
Identity Policy				1
Enter a description				
Rules Active Authentic	ation			
Server Certificate *	Self Sign Cert	0		
Dort .	sen_sign_cert	-		
POIL	885	(885 or 1025 - 65535)		
Maximum login attempts *	3	(0 or greater. Use 0 to indic	ate unlimited login attempts))
Active Authentication Res	ponse Page			
This page will be displayed if Type.	a user triggers an identity rule with	HTTP Response Page as the A	Authentication	
System-provided	*	۹,		
,				
* Required when using Activ	e Authentication			

Klik nu op de knop **Regel toevoegen** en geef een naam aan de regel en kies de actie als **actieve verificatie**. Definieer de bron/doelzone, het bron/doelnetwerk waarvoor u de gebruikersverificatie wilt inschakelen.

Selecteer het **domein**, dat u in de vorige stap hebt geconfigureerd, en een verificatietype dat het beste bij uw omgeving past.

Overview Analysis Po	licies Devices Objects	АМР			
Access Control + Identity	Network Discovery Appl	ication Detectors	Correlation Actions •		
Identity_Policy Enter a description					
Rules Active Authenticatio	'n				
# Name Administrator Rules This category is empty Standard Rules	Add Rule Name Captive_Portal Action Active Authentication Zones Networks	on /LAN Tags Ports	Realm: Servertest (AD)	Inser Authentication Type:	t into Category Y Stan HTTP Negotiate Exclude HTTP User-Ag
This category is empty Root Rules	Realm *	Servertest (AD)	tion ennet identify user	¥ J	
This category is empty	Authentication Type Application Filters C Search by name Risks (Any Selected) Curve Low Curve Lo	HTTP Negotiate	Available Applications (83) Search by name ABC AdobeAIR Advanced Packaging Tool AirPlay Amazon Instant Video		Exclude HTTP User-Agen any

ASA-configuratie voor Captive Portal

Voor ASA Firepower module, configureer deze opdrachten op de ASA om het captive portal te configureren.

Zorg ervoor dat de serverpoort, TCP 1055, is geconfigureerd in de **poortoptie** van het tabblad **Actieve verificatie** Identity Policy.

Om de actieve regels en hun klaptellingen te verifiëren, voer het bevel uit:

ASA# show asp table classify domain captive-portal

Opmerking: de opdracht Captive Portal is beschikbaar in ASA versie 9.5(2) en hoger.

Stap 4.2 Enkelvoudige aanmelding (passieve verificatie)

Bij passieve authenticatie, wanneer een domeingebruiker inlogt en in staat is om de AD te authenticeren, de Firepower User Agent de User-IP-mapping details van de beveiligingslogbestanden van AD opvraagt en deze informatie deelt met Firepower Management Center (FMC). Het VCC stuurt deze gegevens naar de sensor om de toegangscontrole te handhaven.

Klik op de knop **Regel toevoegen** en geef een naam aan de regel en kies de **actie** als **passieve verificatie**. Definieer de bron/doelzone, het bron/doelnetwerk waarvoor u de gebruikersverificatie wilt inschakelen.

Selecteer het **gebied** dat u in de vorige stap hebt geconfigureerd en het verificatietype dat het best past bij uw omgeving, zoals in deze afbeelding.

Hier kunt u een terugvalmethode als **actieve verificatie** kiezen **als passieve verificatie de gebruikersidentiteit niet kan identificeren**.

Overview Ana	alysis Policies Devices Objects AMP	
Access Control	► Identity Network Discovery Application Detectors Correlation Actions ▼	
Identity Po	olicy	
Enter a description		
Rules Active A	Authentication	
	Editing Rule - Captive_Portal	
# Name	Name Circle Circ On	
Administrator Rule	Name Single_Sign_On	
This category is em	Action Passive Authentication Yes HITP Negotiate Exclude HTTP Us	sei
Standard Rules	Zones Networks VLAN Tags Ports	
1 Captive_Portal	Realm * Converteet	
Root Rules		
This category is em	Use active authentication if passive authentication cannot identify user	
	* Required Field	

Stap 5. Configureer het toegangscontrolebeleid

Navigeer naar **Beleid > Toegangsbeheer > Een** beleid **maken/bewerken**.

Klik op het **identiteitsbeleid** (linkerbovenhoek), kies het identificatiebeleid dat u in de vorige stap hebt geconfigureerd en klik op de knop **OK**, zoals in deze afbeelding.

Overview Analysis Polici	es Devices Objects	AMP		
Access Control > Access Cont	rol Network Discovery	Application Detectors	Correlation	Actions 🔻
NGFW_Policy Enter a description				
Identity Policy: None	SSL Policy: None			
Rules Security Intelligence	Identity Policy		? ×	
General Settings	Identity_Policy		▼	insport/Network Layer Preprocessor
Maximum URL characters to sto	Revert to Defaults	ок	Cancel	nore the VLAN header when tracking connec

Klik op de knop **Regel toevoegen** om een nieuwe regel toe te voegen. Navigeer naar **Gebruikers** en selecteer de gebruikers waarvoor toegangscontroleregel afdwingt, zoals in deze afbeelding. Klik op **OK** en klik op **Opslaan** om de wijzigingen op te slaan.

Overview	Anal	ysis	Po	licies	Device	es	Objects	AMF	þ											
Access Cor	ntrol 🕨	Acc	ess C	ontrol	Netw	ork [Discovery	/ App	licati	on Detect	tors	Co	rrelation	A	ctions •					
NGFW_ Enter a descr	Polic	сy																		
Identity Poli	icy: Ide	ntity	Polic	X.	SSL Poli	icy: N	lone													
Rules S	ecurit	Edi	ting	Rule -	Allow_	LAN	_User													
# Filter by	Devic	Na	ame	Allow_LA	N_User							🗸 En	abled			Mov	<u>/e</u>			
# Name		Ac	tion	🗸 Allow	(~	IPS: /	no polic	ies	Variables	: n/a	Files:	no ins	pection	Loggin	g: conn	ections: Eve
👻 Mandat	ory - I	2	Zones	Net	works	VLA	N Tags	Users	Ap	pplication	is Po	orts	URLs	🔺 I	SE Attr	ibutes	:			Inspectio
1 Allow I		Ava	ailable	e Realms	Ċ				Ava	ilable Use	ers C					_			Selecte	ed Users (2
I Allow_t	LAIN_U	9	Searc	ch by nar	ne or valu	ue			9	Search by	/ name	or va	lue						Ser	vertest/sur
👻 Default	- NGF		Spec	ial Identi	ties														Sei	rvertest/adr
2 IPS_tes	st		Serv	ertest																
Default Act	tion																Add to	Rule		

Stap 6. Implementeer het toegangscontrolebeleid

Navigeer om optie **op** te **stellen**, kies het **apparaat** en klik op de optie **op te stellen** om de configuratie te veranderen in de sensor. Controleer de implementatie van beleid vanaf de optie **Berichtencentrum** (pictogram tussen implementatie en systeemoptie) en zorg ervoor dat het beleid successol moet worden toegepast, zoals in deze afbeelding wordt getoond.

Sy



Stap 7. Controleer de gebeurtenissen van de gebruikers en van de verbindingen

Momenteel zijn actieve gebruikerssessies beschikbaar in de sectie Analyse > Gebruikers > Gebruikers.

Met de bewaking van gebruikersactiviteit kunt u uitzoeken welke gebruiker aan welk IP-adres is gekoppeld en hoe de gebruiker door het systeem wordt gedetecteerd door actieve of passieve verificatie. **Analyse > Gebruikers > Gebruikersactiviteit**

User Activity

Table View of Events > Users

No Search Constraints (Edit Search)

	<u> </u>	Event ×	<u>Realm</u> ×	<u>Username</u> ×	<u>Type</u> ×	Authentication × Type	IP Address
J.	2015-12-10 11:15:34	<u>User Login</u>	<u>Servertest</u>	<u> sunil</u>	LDAP	Active Authentication	il <u>192.168.</u>
4	2015-12-10 10:47:31	<u>User Login</u>	<u>Servertest</u>	💐 <u>admin</u>	LDAP	Passive Authentication	i92.168.0

Navigeer naar **Analyse > Verbindingen > Gebeurtenissen**, om het type verkeer te bewaken dat door de gebruiker wordt gebruikt.

Overview Analysis Policies Devices Objects AMP							
Context E	xplorer Connectio	ns • Events Intru	sions • File	es 🔻 Hosts 🔻	Users • Vulnerabilities •	Correlation Cust	tom • Search
Bookmark This F							
Connection EVENTS (switch workflow) Connections with Application Details > Table View of Connection Events							
Search Constraints (Edit Search Save Search)							
luma ta							
Jump to	• First Packet ×	Last Packet X	Action X	Initiator IP X	Initiator User X	Responder IP X	Access Control Rule X
• •	2015-12-11 10:31:59	2015-12-11 10:34:19	Allow	192.168.20.20	sunii (Servertest\sunii, LDAP)	74.201.154.156	Allow_LAN_User
1	2015-12-11 10:31:59		Allow	192.168.20.20	Sunil (Servertest\sunil, LDAP)	74.201.154.156	Allow LAN User
1	2015-12-11 09:46:28	2015-12-11 09:46:29	Allow	192.168.20.20	Sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User
+ 🗆	2015-12-11 09:46:28		Allow	192.168.20.20	📇 sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User
↓ □	2015-12-11 09:46:07	2015-12-11 09:46:58	Allow	192.168.20.20	Sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User
+ 🗆	2015-12-11 09:46:07		Allow	192.168.20.20	📇 sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User
↓ □	2015-12-11 09:45:46	2015-12-11 09:46:36	Allow	<u>192.168.20.20</u>	Sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User
Last login on Thursday, 2015-12-10 at 11:17:25 AM from 10.65.39.169 Right-click for menu							

Verifiëren en probleemoplossing

Navigeer naar **Analyse > Gebruikers** om het type Gebruikersverificatie/verificatie/Gebruiker-IP-koppeling/toegangsregel die aan de verkeersstroom is gekoppeld, te verifiëren.

Controleer de connectiviteit tussen VCC en User Agent (passieve verificatie)

Firepower Management Center (FMC) maakt gebruik van TCP-poort 3306 om loggegevens van gebruikersactiviteit te ontvangen van de User Agent.

Gebruik deze opdracht in het VCC om de status van de dienst van het VCC te verifiëren.

admin@firepower:~\$ netstat -tan | grep 3306

Voer pakketvastlegging uit op het VCC om de connectiviteit met de User Agent te verifiëren.

admin@firepower:~\$ sudo tcpdump -i eth0 -n port 3306

Ga naar **Analyse > Gebruikers > Gebruikersactiviteit** om te controleren of het VCC gebruikersaanmeldingsgegevens ontvangt van de User Agent.

Controleer de connectiviteit tussen VCC en Active Directory

FMC gebruikt TCP-poort 389 om de gebruikersdatabase op te halen uit de Actieve map.

Voer pakketvastlegging uit op het VCC om de connectiviteit met de Active Directory te verifiëren.



Zorg ervoor dat de gebruikersreferenties die worden gebruikt in de configuratie van het FMC Real voldoende rechten hebben om de AD User-database op te halen.

Controleer de configuratie van het VCC-gebied en zorg ervoor dat de gebruikers/groepen worden gedownload en de time-out van de gebruikerssessie correct wordt geconfigureerd.

Navigeer naar **Berichtencentrum > Taken** en zorg ervoor dat de taak van de **gebruikers/groepen** succesvol wordt voltooid, zoals in deze afbeelding wordt getoond.



Controleer de connectiviteit tussen Firepower Sensor en het eindsysteem (actieve verificatie)

Voor actieve verificatie, zorg ervoor dat het certificaat en de poort correct zijn geconfigureerd in FMC Identity beleid.Standaard luistert Firepower sensor op TCP poort 885 voor actieve verificatie.

Controleer de beleidsconfiguratie en -implementatie

Zorg ervoor dat de velden Realm, Verificatietype, Gebruikersagent en Actie correct zijn geconfigureerd in Identity Policy.

Zorg ervoor dat het identiteitsbeleid correct aan het toegangscontrolebeleid wordt gekoppeld.

Navigeer naar **Berichtencentrum > Taken** en zorg ervoor dat de beleidsimplementatie met succes wordt voltooid.

De logboeken van de gebeurtenissen analyseren

De verbinding en de gebeurtenissen van de Activiteit van de Gebruiker kunnen worden gebruikt om te diagnosticeren of de gebruikerslogin of niet succesvol is. Deze gebeurtenissen

U kunt ook controleren welke toegangscontroleregel op de stroom wordt toegepast.

Navigeer naar **Analyse > Gebruiker** om de logboeken met gebruikersgebeurtenissen te controleren.

Navigeer naar **Analyse > Verbindingsgebeurtenissen** om de verbindingsgebeurtenissen te controleren.

Gerelateerde informatie

• Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.