Configurar a integração do Ative Diretory com o Firepower Appliance para a autenticação do portal cativo do Single Sign-On &

Contents

Introdução **Pré-requisitos Requisitos** Componentes Utilizados Informações de Apoio Configurar Etapa 1. Configurar o agente de usuário do Firepower para logon único Etapa 2. Integrar o Firepower Management Center (FMC) ao agente do usuário Etapa 3. Integre o Firepower ao Ative Diretory Etapa 3.1 Criar o território Etapa 3.2 Adicionar o Servidor de Diretório Etapa 3.3 Modificar a Configuração do Realm Etapa 3.4 Fazer download do banco de dados do usuário Etapa 4. Configurar a política de identidade Etapa 4.1 Portal cativo (Autenticação ativa) Etapa 4.2 Logon Único (Autenticação Passiva) Etapa 5. Configurar a Política de Controle de Acesso Etapa 6. Implantar a Política de Controle de Acesso Passo 7. Monitorar eventos do usuário e eventos de Conexões Verificar eSolucionar Problemas Verificar a conectividade entre o FMC e o agente de usuário (autenticação passiva) Verificar a conectividade entre o FMC e o Ative Diretory Verifique a conectividade entre o Firepower Sensor e o sistema final (autenticação ativa) Verificar a configuração da política e a implantação da política Analisar os registros de eventos Informações Relacionadas

Introdução

Este documento descreve a configuração da autenticação do portal cativo (Autenticação ativa) e do Logon único (Autenticação passiva).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Dispositivos Sourcefire Firepower
- Modelos de dispositivo virtual
- LDAP (Light Weight Diretory Service)
- Agente de usuário Firepower

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Firepower Management Center (FMC) versão 6.0.0 e posterior
- Sensor Firepower versão 6.0.0 e posterior

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A Autenticação do portal cativo ou a Autenticação ativa solicita uma página de login e as credenciais do usuário são necessárias para que um host obtenha acesso à Internet.

O Logon Único ou a Autenticação Passiva fornece autenticação transparente a um usuário para recursos de rede e acesso à Internet sem ocorrências de credenciais de vários usuários. A autenticação de Logon único pode ser obtida pelo agente de usuário do Firepower ou pela autenticação do navegador NTLM.

Observação: para a autenticação de portal cativo, o dispositivo deve estar no modo roteado.

Configurar

Etapa 1. Configurar o agente de usuário do Firepower para logon único

Este artigo explica como configurar o agente de usuário do Firepower em uma máquina com Windows:

Instalação e desinstalação do Sourcefire User Agent

Etapa 2. Integrar o Firepower Management Center (FMC) ao agente do usuário

Faça login no Firepower Management Center e navegue até **Sistema > Integração > Fontes de identidade.** Clique na opção **Novo agente**. Configure o endereço IP do sistema do agente de usuário e clique no botão **Add**.

Clique no botão Save para salvar as alterações.

Overview	Analysis	Policies Devices	Objects A	MP						
						Configuration	Users	Domains	Integration	Upd
Cisco CSI	Realms	Identity Sources	eStreamer	Host Input Client	Smart Software	e Satellite				
Identity S	Sources									
Service Type		None	Identity Service	s Engine User Ager	nt	New Agent				
Host Nam	e/IP User	Agent			? ×					
	Hos	st Name/IP Address 192	2.168.10.11							
				Add Cano	el					

Etapa 3. Integrar o Firepower ao Ative Diretory

Etapa 3.1 Criar o território

Faça login no FMC e navegue até **System > Integration > Realm. Clique na opção Add New Realm**.

Nome e Descrição: forneça um nome/descrição para identificar exclusivamente o território.

Tipo: AD

Domínio Primário do AD: nome de domínio do Ative Diretory

Nome de usuário do diretório: <username>

Senha do Diretório: <password>

DN base: DN de domínio ou DN de OU específico a partir do qual o sistema inicia uma pesquisa no banco de dados LDAP.

DN do grupo: DN do grupo

Atributo do Grupo: Membro

				_	Configu	ration	Users	Domains	In	tegration	Updat
Cisco CSI	Realms	Identity Sources	eStreamer	Host Input Client	Smart Software Satellite						
					Add New Realm						
Name servertest-1				Description	Name * Description Type * AD Primary Domain * Directory Username * Directory Password * Base DN * Group DN * Group Attribute * Required Field	AD serv serv dc= Mem	vertest vertest.com vertest\admi servertest,d TAC,ou = Sec nber	n Ic=com curity-Team,dc		ex: domain ex: user@e ex: ou=use ex: ou=gro	.com domain er,dc=cisc sup,dc=cis
											ОК

Este artigo ajuda a descobrir os valores DN base e DN de grupo.

Identificar Atributos de Objeto LDAP do Ative Diretory

Etapa 3.2 Adicionar o Servidor de Diretório

Clique no botão Add para navegar para a próxima etapa e, em seguida, clique na opção Add diretory.

Nome de host/Endereço IP: configure o endereço IP/nome de host do servidor do AD.

Porta: 389 (número da porta LDAP do Ative Diretory)

Encryption/SSL Certificate: (opcional) Para criptografar a conexão entre o FMC e o servidor AD , consulte o

artigo: <u>Verificação do objeto de autenticação no FireSIGHT System para autenticação do Microsoft</u> <u>AD sobre SSL/TLS</u>

Overvie	w Analysis Po	licies Devices Ot	jects AMP							
						Configuration	Users	Domains	Integration	Updat
Serve Enter a de	rtest scription Realm Configur	ation User Downloa	đ							
	Edit directory				? ×					
URL (Hos	Hostname / IP Address	192.168.10.11								none
	Port	STARTTLS O LDAA	'S 🖲 None							
	SSL Certificate		▼ Ø	Test	Cancel					

Clique no botão Test para verificar se o FMC pode se conectar ao servidor AD.

Etapa 3.3 Modificar a Configuração do Realm

Navegue para **Realm Configuration** para verificar a configuração de integração do servidor AD e você pode modificar a configuração do AD.

Etapa 3.4 Fazer download do banco de dados do usuário

Navegue até a opção Download do usuário para buscar o banco de dados do usuário no servidor do AD.

Habilite a caixa de seleção para baixar **usuários e grupos de download** e defina o intervalo de tempo sobre a frequência com que o FMC contata o AD para baixar o banco de dados do usuário.

Selecione o grupo e coloque-o na opção Include para a qual você deseja configurar a autenticação.

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

Como mostrado na imagem, habilite o estado do AD:

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

Etapa 4. Configurar a Política de Identidade

Uma política de identidade executa a autenticação do usuário. Se o usuário não autenticar, o acesso aos recursos da rede será recusado. Isso aplica o RBAC (Role-Based Access Control, controle de acesso baseado em função) à rede e aos recursos da sua empresa.

Etapa 4.1 Portal cativo (Autenticação ativa)

A Autenticação ativa solicita o nome de usuário/senha no navegador para identificar uma identidade de usuário para permitir qualquer conexão. O navegador autentica o usuário com uma página de autenticação ou autentica silenciosamente com autenticação NTLM. O NTLM usa o navegador para enviar e receber informações de autenticação. A autenticação ativa usa vários tipos para verificar a identidade do usuário. Os diferentes tipos de autenticação são:

- 1. HTTP Básico: neste método, o navegador solicita as credenciais do usuário.
- 2. NTLM: o NTLM usa credenciais da estação de trabalho Windows e negocia-o com o Ative Diretory por meio de um navegador da Web. Você precisa habilitar a autenticação NTLM no navegador. A autenticação de usuário acontece de forma transparente, sem solicitar credenciais. Ele oferece uma experiência de login único para os usuários.
- 3. **Negociação HTTP:**Nesse tipo, o sistema tenta se autenticar com NTLM. Se falhar, o sensor usará o tipo de autenticação Básica HTTP como um método alternativo e solicitará uma caixa de diálogo para as credenciais do usuário.
- 4. **Página Resposta HTTP:** Isso é semelhante ao tipo básico HTTP, no entanto, aqui o usuário é solicitado a preencher a autenticação em um formulário HTML que pode ser personalizado.

Cada navegador tem uma maneira específica de habilitar a autenticação NTLM e, portanto, segue as diretrizes do navegador para habilitar a autenticação NTLM.

Para compartilhar com segurança a credencial com o sensor roteado, você precisa instalar o certificado de servidor autoassinado ou o certificado de servidor assinado publicamente na política de identidade.

Navegue até **Policies > Access Control > Identity**. Clique no botão **Adicionar regra** e dê um nome à regra e salve-a.

Overview Analysis Policies Devices Obj	ects AMP			
Access Control + Identity Network Discovery	Application Detectors Corre	elation Actions 🔻		
Identity Policy	Domain		Status	
	New	Identity policy	? X	
	Nam	a Alexandre Alexandre	Add a new pol	icy
<	Name	e Identity_Policy		
	Desc	ription		
			Connel	
		Save	Cancer	

Navegue até a guia **Autenticação ativa** e, na opção **Certificado do servidor**, clique no **ícone** (+) e carregue o certificado e a chave privada que você gerou na etapa anterior com o openSSL.

Overview Analysis	Policies Devices Objects	AMP	
Access Control > Identit	ty Network Discovery Ap	plication Detectors Correla	ation Actions •
Identity_Policy Enter a description			
Rules Active Authentic	ation		
Server Certificate *	Self_Sign_Cert	0	
Port •	885	(885 or 1025 - 65535)	
Maximum login attempts *	3	(0 or greater. Use 0 to indicate	e unlimited login attempts)
Active Authentication Res This page will be displayed if Type.	ponse Page a user triggers an identity rule with	HTTP Response Page as the Aut	hentication
System-provided	*] 🔍	
* Required when using Activ	e Authentication		

Agora clique no botão **Add rule** e dê um nome à regra e escolha a ação como **Ative Authentication**. Defina a zona de origem/destino, a rede de origem/destino para a qual deseja habilitar a autenticação de usuário.

Selecione o **Realm**, que você configurou na etapa anterior, e o tipo de autenticação mais adequado ao seu ambiente.



Configuração do ASA para o portal cativo

Para o módulo ASA Firepower, configure esses comandos no ASA para configurar o portal cativo.

```
ASA(config)# captive-portal global port 1055
```

Certifique-se de que a porta do servidor, TCP 1055, esteja configurada na opção **port** da guia **Ative Authentication** da política de identidade.

Para verificar as regras ativas e suas contagens de ocorrências, execute o comando:

```
ASA# show asp table classify domain captive-portal
```

Observação: o comando Captive portal está disponível no ASA versão 9.5(2) e posterior.

Etapa 4.2 Logon Único (Autenticação Passiva)

Na autenticação passiva, quando um usuário de domínio faz logon e pode autenticar o AD, o agente de usuário do Firepower pesquisa os detalhes de mapeamento do IP do usuário nos logs de segurança do AD e compartilha essas informações com o Firepower Management Center (FMC). O FMC envia esses detalhes ao sensor para aplicar o controle de acesso.

Clique no botão **Add rule** e dê um nome à regra e escolha a **Action** como **Passive Authentication**. Defina a zona de origem/destino, a rede de origem/destino para a qual deseja habilitar a autenticação de usuário.

Selecione o **Realm** que você configurou na etapa anterior e o tipo de autenticação que melhor se adapta ao seu ambiente, como mostrado nesta imagem.

Aqui você pode escolher o método de retorno como Autenticação ativa se a autenticação passiva não puder identificar a identidade do usuário.

Overview Ana	ysis Policies Devices Objects AMP													
Access Control	Identity Network Discovery Application Detectors Correlation Actions •													
Identity Po	licy													
Enter a description														
	Rules Active Authentication													
Rules Active Au	thentication													
	Editing Rule - Captive_Portal													
# Name	Name Single Sign On Provide Move													
Administrator Rule	Action Descho Authentication Type: HTTP Nanctiste Evolution HTTP Nanctiste Evolution HTTP Nanctiste	0 Hear												
This category is em	Action Passive Authentication	- USCI												
Standard Rules	Zones Networks VLAN Tags Ports													
1 Captive_Portal	Realm * Servertest Y													
Root Rules	Use active authentication if passive authentication cannot identify user													
This category is em,														
	* Required Field													

Etapa 5. Configurar a Política de Controle de Acesso

Navegue até **Policies > Access Control > Create/Edit a Policy (Políticas > Controle de acesso > Criar/editar** uma política).

Clique em **Identity Policy** (**Política de identidade**) (canto superior esquerdo), escolha a Política de identidade que você configurou na etapa anterior e clique no botão **OK**, como mostrado nesta imagem.



Clique no botão **Adicionar regra** para adicionar uma nova regra. Navegue até **Usuários** e selecione os usuários para os quais a regra de controle de acesso é imposta, como mostrado nesta imagem. Clique em **OK** e clique em **Save** para salvar as alterações.

Overvie	ew Ar	naly	rsis	Po	olicie	es	Devid	es	Obj	jects	A I	MР															
Access	Contro	•	Acc	ess (Contr	ol	Netv	work	Disc	overy	A	pplic	atio	n Det	ector	s	Cor	rrelation	A	Action	is 🔻						
NGFV Enter a de	V_Po escriptio	lic	y																								
Identity Policy: Identity_Policy SSL Policy: None																											
Rules	Secu	rit ^E	Edit	ting	Rule	e - A	llow_	LAI	N_U	ser								_									_
📸 Filte	r by Dev	ric	Na	me	Allow	_LAN	_User										Ena	abled				Move					
# Na	ame	H	Ac	tion	🖌 🗸	llow							*	IPS	5: no p	oolicies	5	Variables	: n/a	File	s: no	inspe	ction	Loggi	ng: (conne	ctions: Ev
👻 Man	datory		Z	Zones	; N	letwo	orks	VL	AN T	ags	User	5	App	licat	ions	Port	s	URLs	<u>A</u> 1	ISE A	ttribu	utes					Inspecti
1 Allo	W LAN	u	Ava	ailable	e Rea	lms	¢					. /	Availa	able	Users	¢						-			Se	lected	Users (2
			9	Sear	ch by	name	e or va	lue				ון	S, S	earch	by na	me or	val	lue							4	Serv	ertest/sur
🔻 Defa	ault - NO	G F		Spec	ial Ide	entitie	:s																		14	Serv	ertest/adr
2 IPS	5_test		۳	Serv	ertest																						
Default	Action																						vdd to	Rule			
		Ш																									
		Ш																									
		Ш																									
		Ш																									
		Ш																									
		ľ																									

Etapa 6. Implantar a política de controle de acesso

Navegue até a opção **Deploy**, escolha o **Device** e clique na opção **Deploy** para enviar a alteração de configuração para o sensor. Monitore a implantação da política pela opção **Ícone do Centro de Mensagens** (ícone entre a opção Implantar e Sistema) e verifique se a política deve ser aplicada com êxito, como mostrado nesta imagem.

Sy



Etapa 7. Monitorar eventos de usuário e eventos de Conexões

As sessões de usuário ativas no momento estão disponíveis na seção Análise > Usuários > Usuários.

O monitoramento de atividade do usuário ajuda a descobrir qual usuário está associado a qual endereço IP e como o usuário é detectado pelo sistema pela autenticação ativa ou passiva. Análise > Usuários > Atividade do Usuário

User Activity

Table View of Events > Users

No Search Constraints (Edit Search)

	<u>▼ Time</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	<u>192.168.</u>
4	2015-12-10 10:47:31	<u>User Login</u>	<u>Servertest</u>	💐 <u>admin</u>	LDAP	Passive Authentication	<u>192.168.0</u>

Navegue até Analysis > Connections > Events, para monitorar o tipo de tráfego usado pelo usuário.

Ove	erviev	Analysis Polici	es Devices Obje	cts AMP										
Con	text E	xplorer Connectio	ns • Events Intru	sions • File	es 🔻 Hosts 🔻	Users • Vulnerabilities •	Correlation • Cust	om • Search						
								Bookmark This Pa						
	Connection Events (switch workflow) Connections with Application Details > Table View of Connection Events													
• Se	Search Constraints (<u>Edit Search</u>)													
Ju	imp to.													
			Last Packet ×	Action ×	Initiator IP ×	Initiator User ×	Responder IP ×	Access Control Rule ×						
4		2015-12-11 10:31:59	2015-12-11 10:34:19	Allow	192.168.20.20	Sunil (Servertest\sunil, LDAP)	74.201.154.156	Allow LAN User						
4		2015-12-11 10:31:59		Allow	192.168.20.20	📇 sunil (Servertest\sunil, LDAP)	74.201.154.156	Allow LAN User						
4		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						
4		2015-12-11 09:46:28		Allow	192.168.20.20	💐 sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User						
4		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						
4		2015-12-11 09:46:07		Allow	192.168.20.20	Sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User						
4		2015-12-11 09:45:46	2015-12-11 09:46:36	Allow	192.168.20.20	Sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User						
Last	login or	n Thursday, 2015-12-10 at	11:17:25 AM from 10.65.3	9.169 Right-clic	k for menu									

Verificar e solucionar problemas

Navegue para Analysis > Users para verificar a regra de acesso/mapeamento User-IP/tipo de autenticação/User-IP associada ao fluxo de tráfego.

Verificar a conectividade entre o FMC e o agente de usuário (autenticação passiva)

O Firepower Management Center (FMC) usa a porta TCP 3306 para receber dados do registro de atividades do usuário do agente do usuário.

Para verificar o status do serviço do FMC, use este comando no FMC.

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

Execute a captura de pacotes no FMC para verificar a conectividade com o agente de usuário.

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

Navegue até **Analysis** > **Users** > **User Activity** para verificar se o FMC recebe detalhes de login do usuário do agente do usuário.

Verificar a conectividade entre o FMC e o Ative Diretory

O FMC usa a porta TCP 389 para recuperar o banco de dados de usuários do Diretório ativo.

Execute a captura de pacotes no FMC para verificar a conectividade com o Ative Diretory.



Verifique se a credencial do usuário usada na configuração do Realm do FMC tem privilégio suficiente para buscar o banco de dados do Usuário do AD.

Verifique a configuração do realm do FMC e certifique-se de que os usuários/grupos tenham sido baixados e que o tempo limite da sessão do usuário esteja configurado corretamente.

Navegue para **Centro de mensagens > Tarefas** e certifique-se de que o **download de usuários/grupos da tarefa** seja concluído com êxito , como mostrado nesta imagem.



Verifique a conectividade entre o Firepower Sensor e o sistema final (autenticação ativa)

Para a autenticação ativa, verifique se o certificado e a porta estão configurados corretamente na política de identidade do FMC. Por padrão, o sensor Firepower ouve a autenticação ativa na porta TCP 885.

Verificar a configuração da política e a implantação da política

Verifique se os campos Realm (Território), Authentication type (Tipo de autenticação), User agent (Agente do usuário) e Action (Ação) estão configurados corretamente na Identity Policy (Política de identidade).

Verifique se a política de Identidade está associada corretamente à política de Controle de Acesso.

Navegue para **Centro de mensagens > Tarefas** e verifique se a Implantação de política foi concluída com êxito.

Analisar os registros de eventos

Os eventos Connection e User Activity podem ser usados para diagnosticar se o logon do usuário foi bemsucedido ou não. Esses eventos

O também pode verificar qual regra de Controle de Acesso é aplicada ao fluxo.

Navegue até Análise > Usuário para verificar os logs de eventos do usuário.

Navegue para Análise > Eventos de Conexão para verificar os eventos de conexão.

Informações Relacionadas

Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.