Configurar a ACL (Access Control List, lista de controle de acesso) baseada em IPv4 e a entrada de controle de acesso (ACE) em um switch

Objetivo

Uma lista de controle de acesso (ACL) é uma lista de filtros de tráfego de rede e ações correlacionadas usadas para melhorar a segurança. Bloqueia ou permite que os usuários acessem recursos específicos. Uma ACL contém os hosts com permissão ou negação de acesso ao dispositivo de rede.

A ACL baseada em IPv4 é uma lista de endereços IPv4 origem que usam informações da Camada 3 para permitir ou negar acesso ao tráfego. As ACLs IPv4 restringem o tráfego relacionado ao IP com base nos filtros IP configurados. Um filtro contém as regras para corresponder a um pacote IP e, se o pacote corresponder, a regra também estipula se o pacote deve ser permitido ou negado.

Uma entrada de controle de acesso (ACE) contém os critérios reais da regra de acesso. Quando a ACE é criada, ela é aplicada a uma ACL.

Você deve usar listas de acesso para fornecer um nível básico de segurança para acessar sua rede. Se você não configurar listas de acesso em seus dispositivos de rede, todos os pacotes que passam pelo switch ou roteador poderão ser permitidos em todas as partes da rede.

Este artigo fornece instruções sobre como configurar ACL e ACE baseadas em IPv4 em seu switch gerenciado.

Dispositivos aplicáveis

- Sx350 Series
- SG350X Series
- Sx500 Series
- Sx550X Series

Versão de software

- 1.4.5.02 Sx500 Series
- 2.2.5.68 Sx350 Series, SG350X Series, Sx550X Series

Configurar ACL baseada em IPv4 e ACE

Configurar ACL baseada em IPv4

Etapa 1. Faça login no utilitário baseado na Web e vá para Controle de acesso > ACL

baseada em IPv4.



Etapa 2. Clique no botão Adicionar.

IPv4-Based ACL			
IPv4-Based ACL Table			
	ACL Name		
0 results found.			
Add Delete			
IPv4-Based ACE Table			

Etapa 3. Insira o nome da nova ACL no campo ACL Name (Nome da ACL).

O ACL Name: IPv4 ACL	(8/32 characters used)
Apply Close	

Note: Neste exemplo, a ACL IPv4 é usada.

Etapa 4. Clique em Aplicar e, em seguida, clique em Fechar.

Success. To permanently save the configuration, go to the Copy/Save Configuration page or click the Save icon.		
🗢 ACL Name:	(0/32 characters used)	
Apply Close		

Etapa 5. (Opcional) Clique em **Salvar** para salvar as configurações no arquivo de configuração de inicialização.

/IP 48-Port Gigabit PoE Stackable Managed Switch
IPv4-Based ACL
IPv4-Based ACL Table
ACL Name
IPv4 ACL
Add Delete
IPv4-Based ACE Table

Agora você deve ter configurado uma ACL baseada em IPv4 no switch.

Configurar ACE baseada em IPv4

Quando um pacote é recebido em uma porta, o switch processa o pacote através da primeira ACL. Se o pacote corresponder a um filtro ACE da primeira ACL, a ação ACE ocorrerá. Se o pacote não corresponder a nenhum dos filtros ACE, a próxima ACL será processada. Se não for encontrada nenhuma correspondência para qualquer ACE em todas as ACLs relevantes, o pacote será descartado por padrão.

Nesse cenário, uma ACE será criada para negar o tráfego enviado de um endereço IPv4 de origem definido pelo usuário para qualquer endereço de destino.

Note: Essa ação padrão pode ser evitada pela criação de uma ACE de baixa prioridade que permita todo o tráfego.

Etapa 1. No utilitário baseado na Web, vá para Controle de acesso > ACE baseada em IPv4

Access Control
MAC-Based ACL
MAC-Based ACE
IPv4-Based ACL
IPv4-Based ACE
ACL Binding (VLAN)
ACL Binding (Port)
 Quality of Service

Importante: Para utilizar plenamente os recursos e as funções disponíveis do switch, altere para o modo Avançado escolhendo **Avançado** na lista suspensa Modo de exibição no canto superior direito da página.

Display Mode:	Advanced v	Logout	About	Help
	Basic			0
	Advanced			~

Etapa 2. Escolha uma ACL na lista suspensa Nome da ACL e clique em Ir.

IPv4	Pv4-Based ACE							
IPv4	I-Based A	ACE Tab	le					
Filte	r: ACL N	lame equ	als to IPv	4 ACL 🔻	Go			
	Priority	Action	Logging	4 ACL	Source IP A	ldress	Destination I	P Address
					IP Address	Wildcard Mask	IP Address	Wildcard Mask
0 re	sults found	d.						
	Add)	dit	Delete	:			
Flag S	Set preser	nts the fla	g types in t	he following	order: Urg, A	ck, Psh, Rst, Syn,	Fin. Set is rep	presented as 1, ur
IPv4	1-Based A	CL Table						

Note: As ACEs já configuradas para a ACL serão exibidas na tabela.

Etapa 3. Clique no botão Add para adicionar uma nova regra à ACL.

Note: O campo ACL Name exibe o nome da ACL.

Etapa 4. Insira o valor de prioridade para a ACE no campo *Prioridade*. As ACEs com um valor de prioridade mais alto são processadas primeiro. O valor 1 é a prioridade mais alta. Tem um intervalo de 1 a 2147483647.

ACL Name:	IPv4 ACL
Priority:	2 (Range: 1 - 2147483647)
Action:	 Permit Deny Shutdown
Logging:	Enable
Protocol:	Any (IP) Select from list ICMP Protocol ID to match (Range: 0 - 255)

Note: Neste exemplo, 2 é usado.

I

Etapa 5. Clique no botão de opção que corresponde à ação desejada que é tomada quando um quadro atende aos critérios exigidos da ACE.

Note: Neste exemplo, Permit é escolhido.

• Permit (Permitir) — O switch encaminha pacotes que atendem aos critérios exigidos da

ACE.

- Negar O switch descarta pacotes que atendem aos critérios exigidos da ACE.
- Desligamento O switch descarta pacotes que não atendem aos critérios exigidos da ACE e desativa a porta onde os pacotes foram recebidos.

Note: As portas desativadas podem ser reativadas na página Configurações de porta.

Etapa 6. (Opcional) Marque a caixa de seleção **Habilitar** registro para habilitar o registro de fluxos de ACL que correspondem à regra de ACL.

Logging:	Enable
Time Range:	Enable
Time Range Name:	Time Range 1 🔻
Protocol:	 Any (IP) Select from list
	Protocol ID to n

Passo 7. (Opcional) Marque a caixa de seleção **Habilitar** intervalo de tempo para permitir que um intervalo de tempo seja configurado para a ACE. Os intervalos de tempo são usados para limitar o tempo durante o qual uma ECA está em vigor.

	Logging:	1	Enable	
	Time Range:		Enable	
	Time Range Name:	Tim	e Range 1 🔻 Edit	
•	Protocol:	● 4 ● 5 ● F	Any (IPv6) Select from list TCP = Protocol ID to match	(Range: 0 - 255)

Etapa 8. (Opcional) Na lista suspensa Nome do intervalo de tempo, escolha um intervalo de tempo para aplicar à ACE.

Time Range Name:	Time Range 1 🔻 Edit	
Protocol:	Any (IPv6) Select from list TCP *	
	Protocol ID to match	(Range: 0 - 255)

Note: Você pode clicar em **Editar** para navegar e criar um intervalo de tempo na página Intervalo de tempo.

Time Range Name:	Time Range 1 (12/32 characters used)
Absolute Starting Time:	Immediate Date 2010 v Jan v 01 v Time 00 v 00 v HH:MM
Absolute Ending Time:	Infinite Date 2010 • Jan • 01 • Time 00 • 00 • HH:MM
Apply Close	

Etapa 9. Escolha um tipo de protocolo na área Protocolo. A ACE será criada com base em um protocolo ou ID de protocolo específico.

Protocol:	Any (IP)	
	 Select from list ICMP 	_
	 Protocol ID to match 	(Range: 0 - 255)

As opções são:

- Any (IP) Essa opção configurará o ACE para aceitar todos os protocolos IP.
- Selecionar na lista Essa opção permitirá que você escolha um protocolo em uma lista suspensa. Se preferir esta opção, vá para a <u>Etapa 10</u>.
- ID do protocolo correspondente Essa opção permitirá que você digite uma ID do protocolo. Se preferir esta opção, vá para a <u>Etapa 11</u>.

Note: Neste exemplo, Qualquer (IP) é escolhido.

Etapa 10. (Opcional) Se você escolher Selecionar na lista na Etapa 9, escolha um protocolo na lista suspensa.

•	Protocol:	•	Any (IP) Select from list Protocol ID to r	ICMP	(Range: 0 - 255)
	Source IP Address:	•	Any User Defined	IP in IP TCP EGP	
₽	Source IP Address Value:			UDP	
₽	Source IP Wildcard Mask:			HMP RDP	atching, 1s for no matching)
	Destination IP Address:	•	Any User Defined	IDPR IPV6 IPV6:ROUT	
₽	Destination IP Address Value:			IPV6:FRAG	
₽	Destination IP Wildcard Mask:			RSVP AH	atching, 1s for no matching)
₽	Source Port:		Any Single from list Single by numb	EIGRP OSPF IPIP	(Range: 0 - 65535)

As opções são:

- ICMP Internet Control Message Protocol
- IP em IP IP no encapsulamento IP
- TCP Transmission Control Protocol
- EGP Exterior Gateway Protocol
- IGP Interior Gateway Protocol
- UDP User Datagram Protocol
- HMP Protocolo de mapeamento de host
- RDP Protocolo de Datagrama Confiável
- IDPR Roteamento de política entre domínios
- IPV6 tunelamento IPv6 sobre IPv4
- IPV6:ROUT Corresponde pacotes pertencentes à rota IPv6 sobre IPv4 através de um gateway
- IPV6:FRAG Corresponde pacotes pertencentes ao cabeçalho de fragmento IPv6 sobre IPv4
- IDRP Protocolo de roteamento entre domínios IS-IS
- RSVP Protocolo ReSerVation
- AH Cabeçalho de autenticação
- IPV6:ICMP ICMP para IPv6
- EIGRP Enhanced Interior Gateway Routing Protocol
- OSPF Open Shortest Path First
- IPIP IP no IP
- PIM Protocol Independent Multicast
- L2TP Protocolo de encapsulamento da camada 2

Etapa 11. (Opcional) Se você escolheu a ID do protocolo para corresponder na Etapa 9, insira a ID do protocolo no *ID do protocolo para corresponder ao* campo.

Protocol:

Any (IP)		
Protocol ID to n	natch 1	Range: 0 - 255)

Etapa 12. Clique no botão de opção que corresponde aos critérios desejados da ACE na área Endereço IP de origem.

Source IP Address:



As opções são:

- Qualquer Todos os endereços IPv4 de origem se aplicam à ACE.
- Definido pelo usuário Insira um endereço IP e uma máscara curinga IP a serem aplicados à ACE nos campos *Valor do endereço IP de origem* e *Máscara curinga IP de origem*. As máscaras curinga são usadas para definir um intervalo de endereços IP.

Note: Neste exemplo, Definido pelo usuário é escolhido. Se você escolheu Qualquer, vá para a <u>Etapa 15</u>.

Etapa 13. Insira o endereço IP origem no campo Source IP Address Value.

Source IP Address:	 Any User Defined 	
O Source IP Address Value:	192.168.1.1]
Source IP Wildcard Mask:		(0s for matching, 1s for no matching)

Note: Neste exemplo, 192.168.1.1 é usado.

Etapa 14. Insira a máscara curinga de origem no campo Máscara curinga de IP de origem.

Source IP Address Value:	192.168.1.1	
Source IP Wildcard Mask:	0.0.0.255	(0s for matching, 1s for no matching)

Note: Neste exemplo, 0.0.0.255 é usado.

<u>Etapa 15.</u> Clique no botão de opção que corresponde aos critérios desejados da ACE na área Endereço IP de destino.

Source IP Address:	 Any User Defined 	
Source IP Address Value:	192.168.1.1	
Source IP Wildcard Mask:	0.0.0.255	(0s for matching, 1s for no matching)
Destination IP Address:	 Any User Defined 	
举 Destination IP Address Value	:	
R Destination IP Wildcard Mask	C	(0s for matching, 1s for no matching)

As opções são:

- Qualquer Todos os endereços IPv4 destino se aplicam à ACE.
- Definido pelo usuário Insira um endereço IP e uma máscara curinga IP a serem aplicados à ACE nos campos *Valor do endereço IP de destino* e *Máscara curinga IP de destino*. As máscaras curinga são usadas para definir um intervalo de endereços IP.

Note: Neste exemplo, Qualquer é escolhido. Escolher essa opção significa que a ACE a ser criada permitirá o tráfego da ACE que vem do endereço IPv4 especificado para qualquer destino.

Etapa 16. (Opcional) Clique em um botão de opção na área Porta de origem. O valor padrão é Qualquer.

Source Port:	Any Single from list Echo	
(Single by number	(Range: 0 - 65535)
	Range -	
Destination Port:	Any	
	Single from list Echo 🔻	
	Single by number	(Range: 0 - 65535)
	Range -	

- Qualquer Corresponda a todas as portas de origem.
- Single from list Você pode escolher uma única porta de origem TCP/UDP à qual os pacotes correspondem. Esse campo ficará ativo apenas se 800/6-TCP ou 800/17-UDP forem escolhidos no menu suspenso Selecionar da lista.
- Um por número Você pode escolher uma única porta de origem TCP/UDP à qual os pacotes correspondem. Esse campo ficará ativo apenas se 800/6-TCP ou 800/17-UDP forem escolhidos no menu suspenso Selecionar da lista.
- Intervalo Você pode escolher um intervalo de portas origem TCP/UDP às quais o pacote corresponde. Há oito intervalos de porta diferentes que podem ser configurados (compartilhados entre as portas de origem e de destino). Cada um dos protocolos TCP e UDP tem oito intervalos de portas.

Etapa 17. (Opcional) Clique em um botão de opção na área Porta de destino. O valor padrão é Qualquer.

- Qualquer Corresponda a todas as portas de origem
- Single from list Você pode escolher uma única porta de origem TCP/UDP à qual os pacotes correspondem. Esse campo ficará ativo apenas se 800/6-TCP ou 800/17-UDP forem escolhidos no menu suspenso Selecionar da lista.
- Um por número Você pode escolher uma única porta de origem TCP/UDP à qual os pacotes correspondem. Esse campo ficará ativo apenas se 800/6-TCP ou 800/17-UDP forem escolhidos no menu suspenso Selecionar da lista.
- Intervalo Você pode escolher um intervalo de portas origem TCP/UDP às quais o pacote corresponde. Há oito intervalos de porta diferentes que podem ser configurados (compartilhados entre as portas de origem e de destino). Cada um dos protocolos TCP e UDP tem oito intervalos de portas.

Etapa 18. (Opcional) Na área Sinalizadores TCP, escolha um ou mais sinalizadores TCP com os quais filtrar pacotes. Os pacotes filtrados são encaminhados ou descartados. A filtragem de pacotes por flags TCP aumenta o controle de pacotes, o que aumenta a segurança da rede.

- Definir Corresponder se o sinalizador estiver definido.
- Unset Corresponde se o sinalizador não estiver definido.
- Não se importe ignore o sinalizador TCP.

Urg:	Ack:	Psh:	Rst:	Syn:	Fin:
 Set Unset Oon't care 	 ○ Set ○ Unset ⑧ Don't care 	 Set Unset Don't care 	 Set Unset Ønt care 	 Set Unset Don't care 	 Set Unset Don't care

Os flags TCP são:

- Urg Este sinalizador é usado para identificar os dados de entrada como Urgentes.
- Ack Este sinalizador é usado para confirmar o recebimento bem-sucedido de pacotes.
- Psh Esse sinalizador é usado para garantir que os dados recebam a prioridade (que merecem) e sejam processados na extremidade de envio ou recebimento.
- Rst Esse flag é usado quando um segmento chega e não se destina à conexão atual.
- Syn Este sinalizador é usado para comunicações TCP.
- Finalizar Esse sinalizador é usado quando a comunicação ou a transferência de dados é concluída.

Etapa 19. (Opcional) Clique no tipo de serviço do pacote IP na área Tipo de serviço.

Type of Service:	Any DSCP to match (Range: 0 - 63) IP Precedence to match (Range: 0 - 7)
• ICMP:	Any Select from list Echo Reply (Range: 0 - 255
ICMP Code:	Any User Defined (Range: 0 - 255)
₩ IGMP:	Any Select from list DVMRP IGMP Type to match (Range: 0 - 255
Apply	se
As opções são:	
Type of Service:	Any DSCP to match (Range: 0 - 63)

• Qualquer — Pode ser qualquer tipo de serviço para congestionamento de tráfego.

IP Precedence to match

 DSCP para corresponder — O DSCP é um mecanismo para classificar e gerenciar o tráfego de rede. Seis bits (0-63) são usados para selecionar o comportamento por salto de um pacote em cada nó.

(Range: 0 - 7)

 Precedência de IP para corresponder — a precedência de IP é um modelo de Tipo de Serviço (TOS) que a rede usa para ajudar a fornecer os compromissos de Qualidade de Serviço (QoS) apropriados. Esse modelo usa os três bits mais significativos do byte de tipo de serviço no cabeçalho IP, conforme descrito em RFC 791 e RFC 1349. A palavrachave com valor de Preferência IP é a seguinte:

- 0 — para rotina

- 1 para prioridade
- 2 para imediata
- 3 para flash
- 4 para flash-override
- 5 para críticos
- 6 para a Internet
- 7 para a rede

Etapa 20. (Opcional) Se o protocolo IP da ACL for ICMP, clique no tipo de mensagem ICMP usada para fins de filtragem. Escolha o tipo de mensagem por nome ou digite o número do tipo de mensagem:

- Qualquer Todos os tipos de mensagem são aceitos.
- Selecionar na lista Você pode escolher o tipo de mensagem por nome.
- Tipo de ICMP a corresponder O número do tipo de mensagem a ser usado para fins de filtragem. Tem um intervalo de 0 a 255.

Etapa 21. (Opcional) As mensagens ICMP podem ter um campo de código que indica como tratar a mensagem. Clique em uma das seguintes opções para configurar se deseja filtrar este código:

- Qualquer Aceite todos os códigos.
- Definido pelo usuário Você pode inserir um código ICMP para fins de filtragem. Tem um intervalo de 0 a 255.

Etapa 22. (Opcional) Se a ACL for baseada em IGMP, clique no tipo de mensagem IGMP a ser usada para fins de filtragem. Escolha o tipo de mensagem por nome ou digite o número do tipo de mensagem:

- Qualquer Todos os tipos de mensagem são aceitos.
- Selecione na lista Você pode escolher qualquer uma das opções na lista suspensa:
- DVMRP usa uma técnica de inundação de caminho reverso, enviando uma cópia de um pacote recebido através de cada interface, exceto aquela em que o pacote chegou.
- Host-Query envia periodicamente mensagens gerais de consulta de host em cada rede conectada para obter informações.
- Host-Reply responde à consulta.
- PIM O Protocol Independent Multicast (PIM) é usado entre os roteadores multicast local e remoto para direcionar o tráfego multicast do servidor multicast para muitos clientes multicast.
- Rastreamento Fornece informações sobre como ingressar e sair dos grupos de multicast IGMP.
- Tipo de IGMP a corresponder O número do tipo de mensagem a ser usado para fins de filtragem. Tem um intervalo de 0 a 255.

Etapa 23. Clique em **Aplicar** e, em seguida, clique em **Fechar**. A ACE é criada e associada ao nome da ACL.

Etapa 24. Clique em **Salvar** para salvar as configurações no arquivo de configuração de inicialização.

NP 48-Port Gigabit PoE Stackable Managed Switch									
IPv4	IPv4-Based ACE								
IPv4	IPv4-Based ACE Table								
Filte	Filter: ACL Name equals to IPv4 ACL V Go								
	Priority	Action	Logging	Time Ra	ange	Protocol	Source IP Ad	dress	
				Name	State		IP Address	Wildcard Mask	
	2	Permit	Enabled			ICMP	192.168.1.1	0.0.0.255	
Add Edit Delete									
Flag Set presents the flag types in the following order: Urg, Ack, Psh, Rst, Syn, Fin. Set is represent									

Agora, você deve ter configurado uma ACE baseada em IPv4 em seu switch.