H コマンド

この章では、H で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

hardware access-list capture

すべての仮想デバイス コンテキスト（VDC）でアクセス コントロール リスト（ACL）キャプチャをイネーブルにするには、**hardware access-list capture** コマンドを使用します。ACL キャプチャをディセーブルにするには、このコマンドの **no** 形式を使用します。

hardware access-list capture

no hardware access-list capture

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.2(1)	このコマンドが追加されました。

使用上のガイドライン

M1 シリーズ モジュールのみが ACL をサポートしていません。

ACL キャプチャはハードウェアベース機能で、管理インターフェイスまたはスーパーバイザで発信される制御パケットではサポートされません。さらに、SNMP コミュニティ ACL および仮想テレタイプ（VTY）ACL などのソフトウェア ACL でもサポートされません。

ACL キャプチャをイネーブルにすると、すべての VDC の ACL ロギングと ACL ロギングのレート制限がディセーブルになります。

すべての VDC につき、システムで同時にアクティブにできる ACL キャプチャ セッションは 1 つだけです。

このコマンドには、ライセンスは必要ありません。

例

次に、すべての VDC で ACL キャプチャをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# hardware access-list capture
```

次に、すべての VDC で ACL キャプチャをディセーブルにする例を示します。

```
switch # configure terminal
switch(config)# no hardware access-list capture
```

関連コマンド

コマンド	説明
show hardware access-list status module	アクセス コントロール リスト（ACL）キャプチャ設定を表示します。

hardware access-list resource pooling

1 つまたは複数の I/O モジュールで、ACL ベースの機能によって複数の TCAM バンクを使用できるようにするには、このコマンドを使用します。ある I/O モジュールで、ACL ベースの機能によって 1 つの TCAM バンクの使用を制限するには、このコマンドの **no** 形式を使用します。

hardware access-list resource pooling module *slot-number-list*

no hardware access-list resource pooling module *slot-number-list*

構文の説明

module *slot-number-list*	I/O モジュールを指定します。*slot-number-list* 引数を使用すると、占有しているスロット番号によってモジュールを指定できます。単一の I/O モジュール、スロット番号の範囲、カンマで区切ったスロット番号と範囲を指定できます。指定できる範囲は 1 ～ 8 です

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.2(1)	**resource** キーワードと **pooling** キーワードとの間のハイフンが削除されました。
4.1(2)	このコマンドが追加されました。

使用上のガイドライン

ACL ベースの各機能では、デフォルトで、1 つの I/O モジュールで 1 つの TCAM バンクを使用できます。このデフォルト動作では、各機能が、16,000 TCAM エントリに制限されます。非常に大きなセキュリティ ACL の場合、この制限が検出される可能性があります。このコマンドを使用すると、ACL ベースの機能で、16,000 より多い TCAM エントリを使用できます。

システム全体のバンクのチェーニングをイネーブルにする場合は、このコマンドの例で説明するように、モジュール範囲コマンドを使用して、モジュールが存在しない場合でも、すべてのモジュールの範囲の設定を追加することを推奨します。

このコマンドには、ライセンスは必要ありません。

例

次の例では、スロット 1 にある I/O モジュールの TCAM バンク中で ACL プログラミングをイネーブルにする方法を示します。

```
switch# config t
switch(config)#  module 1
```

次に、スロット 5、6 を除く 10 スロット シャーシのバンクのチェーニングをイネーブルにする例を示します。

```
switch# config t
switch(config)#  module 1-4, 7-10
```

このようにして、新しいモジュールが挿入されると、そのモジュールに対してバンクのチェーニングが自動的にイネーブルになり、ユーザはコマンドの入力を行う必要がありません。

関連コマンド

コマンド	説明
hardware access-list update	スーパーバイザ モジュールが、ACL に対する変更により、I/O モジュールをアップデートする方法を設定します。
show running-config all	デフォルト設定を含む、実行コンフィギュレーションを表示します。

hardware access-list update

スーパーバイザ モジュールが、アクセス コントロール リスト（ACL）に対する変更により、I/O モジュールをアップデートする方法を設定するには、デフォルトの Virtual Device Context（VDC; 仮想デバイス コンテキスト）で **hardware access-list update** コマンドを使用します。アトミック アップデートをディセーブルにするには、このコマンドの **no** 形式を使用します。

hardware access-list update {**atomic** | **default-result permit**}

no hardware access-list update {**atomic** | **default-result permit**}

構文の説明

atomic	トラフィックを中断しないでアップデートを実行する、アトミック アップデートを指定します。Cisco Nexus 7000 シリーズ デバイスは、デフォルトで、アトミック ACL アップデートを実行します。
default-result permit	非アトミック アップデートの実行中に、アップデートした ACL が適用されるトラフィックを許可します。

デフォルト

atomic

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.1(4)	このコマンドを使用できるのは、デフォルトの VDC だけです。
4.1(2)	このコマンドは、**platform access-list update** コマンドを置き換える目的で導入されました。

使用上のガイドライン

Cisco NX-OS Release 4.1(4) およびそれ以降のリリースでは、デフォルトの VDC で **hardware access-list update** コマンドを使用でき、すべての VDC に影響が及ぼされます。

デフォルトでは、Cisco Nexus 7000 シリーズのデバイスのスーパーバイザ モジュールで、ACL の変更を I/O モジュールにアップデートする際には、Atomic ACL のアップデートを実行します。アトミック アップデートでは、アップデートされた ACL が適用されるトラフィックは中断されません。ただし、アトミック アップデートでは、ACL アップデートを受信する I/O モジュールで、影響を受ける ACL で前から存在するすべてのエントリに加え、アップデートされる各 ACL エントリを保存するために使用可能な十分なリソースが必要です。アップデートが行われた後、アップデートに使用されたリソースは解放されます。I/O モジュールに十分なリソースがない場合は、デバイスからエラー メッセージが出力され、この I/O モジュールに対する ACL のアップデートは失敗します。

I/O モジュールで、アトミック アップデートに必要なリソースが不足している場合は、**no hardware access-list update atomic** コマンドを使用して、デフォルト VDC でアトミック アップデートをディセーブルにできます。ただし、ACL をアップデートして前から存在している ACL を削除するまでの短い処理時間中、ACL が適用されるトラフィックはデフォルトでドロップされます。

非アトミック アップデートの受信中に、ACL が適用されるすべてのトラフィックを許可したい場合は、デフォルト VDC で **hardware access-list update default-result permit** コマンドを使用します。

このコマンドには、ライセンスは必要ありません。

例

（注） Cisco NX-OS Release 4.1(4) およびそれ以降のリリースでは、デフォルトの VDC でだけ、**hardware access-list update** コマンドを使用できます。現在の VDC が VDC 1（デフォルト VDC）であることを確認するには、**show vdc current-vdc** コマンドを使用します。

次に、ACL のアトミック アップデートをディセーブルにする例を示します。

```
switch# config t
switch(config)# no hardware access-list update atomic
```

次の例では、非 Atomic ACL アップデートの際に、関連するトラフィックを許可する方法を示します。

```
switch# config t
switch(config)# hardware access-list update default-result permit
```

次の例では、Atomic アップデート方式に戻る方法を示します。

```
switch# config t
switch(config)# no hardware access-list update default-result permit
switch(config)# hardware access-list update atomic
```

関連コマンド

コマンド	説明
	ACL ベースの機能で、複数の TCAM バンクを使用できます。
show running-config all	デフォルト設定を含む、実行コンフィギュレーションを表示します。

hardware rate-limiter

スーパーバイザ宛のトラフィックのレート制限をパケット/秒単位で設定するには、**hardware rate-limiter** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

hardware rate-limiter {**access-list-log** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **copy** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **f1** {**rl-1** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **rl-2** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **rl-3** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **rl-4** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **rl-5** {*packets* | **disable**} [**module** *module* [**port** *start end*]]} | **layer-2** {**l2pt** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **mcast-snooping** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **port-security** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **storm-control** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **vpc-low** {*packets* | **disable**} [**module** *module* [**port** *start end*]]} | **layer-3** {**control**{*packets* | **disable**} [**module** *module* [**port** *start end*]] | **glean** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **mtu** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **multicast** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **ttl** {*packets* | **disable**} [**module** *module* [**port** *start end*]]} | **receive** {*packets* | **disable**} [**module** *module* [**port** *start end*]]

no hardware rate-limiter {**access-list-log** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **copy** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **f1** {**rl-1** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **rl-2** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **rl-3** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **rl-4** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **rl-5** {*packets* | **disable**} [**module** *module* [**port** *start end*]]} | **layer-2** {**l2pt** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **mcast-snooping** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **port-security** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **storm-control** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **vpc-low** {*packets* | **disable**} [**module** *module* [**port** *start end*]]} | **layer-3** {**control**{*packets* | **disable**} [**module** *module* [**port** *start end*]] | **glean** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **mtu** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **multicast** {*packets* | **disable**} [**module** *module* [**port** *start end*]] | **ttl** {*packets* | **disable**} [**module** *module* [**port** *start end*]]} | **receive** {*packets* | **disable**} [**module** *module* [**port** *start end*]]

構文の説明

access-list-log	アクセス リスト ロギングのためにスーパーバイザ モジュールにコピーされるパケットを指定します。デフォルトのレートは 100 パケット/秒です。
disable	ハードウェア レート リミッタをディセーブルにします。
module *module*	（任意）モジュール番号を指定します。有効な範囲は 1 ～ 18 です。
port *start end*	（任意）ポートの開始インデックスを指定します。指定できる範囲は 1 ～ 32 です。開始ポートと終了ポートを、スペースで区切って指定します。
copy	スーパーバイザ モジュールにコピーされるデータ パケットと制御パケットを指定します。デフォルトのレートは 30000 パケット/秒です。
f1	F1 モジュールからスーパーバイザへの制御パケットを指定します。
rl-1	F1 レート リミッタ 1 を指定します。
rl-2	F1 レート リミッタ 2 を指定します。

rl-3	F1 レート リミッタ 3 を指定します。
rl-4	F1 レート リミッタ 4 を指定します。
rl-5	F1 レート リミッタ 5 を指定します。
layer-2	レイヤ 2 パケットのレート制限を指定します。
l2pt	レイヤ 2 トンネル プロトコル（L2TP）パケットを指定します。デフォルトのレートは 4096 パケット/秒です。
mcast-snooping	レイヤ 2 マルチキャストスヌーピング パケットを指定します。デフォルトのレートは 10000 パケット/秒です。
port-security	ポート セキュリティ パケットを指定します。デフォルトはディセーブルです。
storm-control	ブロードキャスト、マルチキャスト、未知のユニキャスト ストーム制御パケットを指定します。デフォルトはディセーブルです。
vpc-low	VPC low キューでのレイヤ 2 制御パケットを指定します。優先度の低い VPC ピア スイッチ間のコントロールプレーン通信を同期化し、vPC ピア スイッチの誤動作や、スイッチ間で過剰なトラフィックが発生した場合に、コントロールプレーンを保護します。デフォルトのレートは 4000 パケット/秒です。
layer-3	レイヤ 3 パケットのレート制限を指定します。
control	レイヤ 3 制御パケットを指定します。デフォルトのレートは 10000 パケット/秒です。
glean	レイヤ 3 グリーニング パケットを指定します。デフォルトのレートは 100 パケット/秒です。
mtu	レイヤ 3 MTU 障害リダイレクト パケットを指定します。デフォルトのレートは 500 パケット/秒です。
multicast	レイヤ 3 マルチキャスト パケット/秒を指定します。
ttl	レイヤ 3 TTL 障害リダイレクト パケットを指定します。デフォルトのレートは 500 パケット/秒です。
receive	スーパーバイザ モジュールにリダイレクトされるパケットを指定します。デフォルトのレートは 30000 パケット/秒です。
packets	パケット数/秒。指定できる範囲は 1 ～ 33554431 です。

デフォルト

デフォルトのレート制限は、「構文の説明」を参照してください。

F1 シリーズ モジュールのデフォルト レート制限

RL-1：毎秒 4500 パケット

RL-2：毎秒 1000 パケット

RL-3：毎秒 1000 パケット

RL-4：毎秒 100 パケット

RL-5：毎秒 1500 パケット

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.1(1)	**f1**、**rl-1**、**rl-2**、**rl-3**、**rl-4**、および **rl-5** キーワードが追加されました。 また、次のキーワードが追加されました。 **module**、**disable**、および **port**。
5.0(2)	**l2pt** キーワードが追加されました。
4.1(2)	このコマンドは、**platform rate-limit** コマンドを置き換える目的で導入されました。

使用上のガイドライン このコマンドには、ライセンスは必要ありません。

例 次に、制御パケットのレート制限を設定する例を示します。

```
switch# config t
switch(config)# hardware rate-limiter layer-3 control 20000
```

次に、制御パケットのレート制限をデフォルトの設定に戻す例を示します。

```
switch# config t
switch(config)# no hardware rate-limiter layer-3 control
```

関連コマンド

コマンド	説明
clear hardware rate-limiter	レート制限統計情報をクリアします。
show hardware rate-limiter	レート制限情報を表示します。
show running-config	実行コンフィギュレーションを表示します。

host（IPv4）

ホストまたはサブネットを IPv4 アドレス オブジェクト グループのメンバーとして指定するには、**host** コマンドを使用します。IPv4 アドレス オブジェクト グループからグループ メンバーを削除するには、このコマンドの **no** 形式を使用します。

[*sequence-number*] **host** *IPv4-address*

no {*sequence-number* | **host** *IPv4-address*}

[*sequence-number*] *IPv4-address network-wildcard*

no *IPv4-address network-wildcard*

[*sequence-number*] *IPv4-address*/*prefix-len*

no *IPv4-address*/*prefix-len*

構文の説明

sequence-number	（任意）このグループ メンバーのシーケンス番号。シーケンス番号は、オブジェクト グループ内でグループ メンバーの順序を保ちます。有効なシーケンス番号は 1 ～ 4294967295 です。シーケンス番号を指定しない場合、デバイスは最大シーケンス番号より 10 大きい番号を現在のオブジェクト グループに割り当てます。
host *IPv4-address*	グループ メンバーを単一 IPv4 アドレスで指定します。*IPv4-address* を、ドット付き 10 進表記で入力します。
IPv4-address network-wildcard	IPv4 アドレスおよびネットワーク ワイルドカード。*IPv4-address* および *network-wildcard* を、ドット付き 10 進表記で入力します。*IPv4-address* のどのビットがネットワーク部分であるかを指定するには、*network-wildcard* を次のように使用します。 `switch(config-ipaddr-ogroup)# 10.23.176.0 0.0.0.255` *network-wildcard* 値が 0.0.0.0 の場合、グループ メンバーが特定の IPv4 アドレスであることを示します。
IPv4-address/*prefix-len*	IPv4 アドレスおよび可変長サブネット マスク。*IPv4-address* を、ドット付き 10 進表記で入力します。*IPv4-address* のネットワーク部分のビット数を指定するには、*prefix-len* を次のように使用します。 `switch(config-ipaddr-ogroup)# 10.23.176.0/24` *prefix-len* 値が 32 の場合、グループ メンバーが特定の IPv4 アドレスであることを示します。

デフォルト

なし

コマンド モード

IPv4 アドレス オブジェクト グループ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

グループ メンバーとしてサブネットを指定するには、このコマンドを、次のいずれかの形式で使用します。

[*sequence-number*] *IPv4-address network-wildcard*

[*sequence-number*] *IPv4-address*/*prefix-len*

show object-group コマンドを使用すると、サブネットの指定に使用したコマンド形式に関係なく、グループ メンバーの *IP-address*/*prefix-len* 形式が表示されます。

グループ メンバーとして単一 IPv4 アドレスを指定するには、このコマンドを、次のいずれかの形式で使用します。

[*sequence-number*] **host** *IPv4-address*

[*sequence-number*] *IPv4-address* **0.0.0.0**

[*sequence-number*] *IPv4-address*/**32**

show object-group コマンドを使用すると、単一 IPv4 アドレスの指定に使用したコマンド形式に関係なく、グループ メンバーの **host** *IP-address* 形式が表示されます。

このコマンドには、ライセンスは必要ありません。

例

次に、ipv4-addr-group-13 という IPv4 アドレス オブジェクト グループに、グループ メンバーとして 2 つの特定の IPv4 アドレスと、1 つのサブネット 10.23.176.0 を設定する例を示します。

```
switch# config t
switch(config)# object-group ip address ipv4-addr-group-13
switch(config-ipaddr-ogroup)# host 10.121.57.102
switch(config-ipaddr-ogroup)# 10.121.57.234/32
switch(config-ipaddr-ogroup)# 10.23.176.0 0.0.0.255
switch(config-ipaddr-ogroup)# show object-group ipv4-addr-group-13
        10 host 10.121.57.102
        20 host 10.121.57.234
        30 10.23.176.0/24
switch(config-ipaddr-ogroup)#
```

関連コマンド

コマンド	説明
object-group ip address	IPv4 アドレス グループを設定します。
show object-group	オブジェクト グループを表示します。

host（IPv6）

ホストまたはサブネットを IPv6 アドレス オブジェクト グループのメンバーとして指定するには、**host** コマンドを使用します。IPv6 アドレス オブジェクト グループからグループ メンバーを削除するには、このコマンドの **no** 形式を使用します。

[*sequence-number*] **host** *IPv6-address*

no {*sequence-number* | **host** *IPv6-address*}

[*sequence-number*] *IPv6-address*/*network-prefix*

no *IPv6-address*/*network-prefix*

構文の説明

sequence-number	（任意）このグループ メンバーのシーケンス番号。シーケンス番号は、オブジェクト グループ内でグループ メンバーの順序を保ちます。有効なシーケンス番号は 1 ～ 4294967295 です。シーケンス番号を指定しない場合、デバイスは最大シーケンス番号より 10 大きい番号を現在のオブジェクト グループに割り当てます。
host *IPv6-address*	グループ メンバーを単一 IPv6 アドレスで指定します。*IPv6-address* を、コロンで区切った 16 進表記で入力します。
IPv6-address/*network-prefix*	IPv6 アドレスおよび可変長サブネット マスク。*IPv6-address* を、コロンで区切った 16 進表記で入力します。*IPv6-address* のネットワーク部分のビット数を指定するには、*network-prefix* を次のように使用します。 `switch(config-ipv6addr-ogroup)# 2001:db8:0:3ab7::/96` *network-prefix* 値が 128 の場合、グループ メンバーが特定の IPv6 アドレスであることを示します。

デフォルト

なし

コマンド モード

IPv6 アドレス オブジェクト グループ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

グループ メンバーとしてサブネットを指定するには、このコマンドを、次の形式で使用します。

[*sequence-number*] *IPv6-address*/*network-prefix*

グループ メンバーとして単一 IPv6 アドレスを指定するには、このコマンドを、次のいずれかの形式で使用します。

[*sequence-number*] **host** *IPv6-address*

[*sequence-number*] *IPv6-address*/**128**

show object-group コマンドを使用すると、単一 IPv6 アドレスの指定に使用したコマンド形式に関係なく、グループ メンバーの **host** *IPv6-address* 形式が表示されます。

このコマンドには、ライセンスは必要ありません。

例

次に、ipv6-addr-group-A7 という IPv6 アドレス オブジェクト グループに、グループ メンバーとして 2 つの特定の IPv6 アドレスと、1 つのサブネット 2001:db8:0:3ab7:: を設定する例を示します。

```
switch# config t
switch(config)# object-group ipv6 address ipv6-addr-group-A7
switch(config-ipv6addr-ogroup)# host 2001:db8:0:3ab0::1
switch(config-ipv6addr-ogroup)# 2001:db8:0:3ab0::2/128
switch(config-ipv6addr-ogroup)# 2001:db8:0:3ab7::/96
switch(config-ipv6addr-ogroup)# show object-group ipv6-addr-group-A7
        10 host 2001:db8:0:3ab0::1
        20 host 2001:db8:0:3ab0::2
        30 2001:db8:0:3ab7::/96
switch(config-ipv6addr-ogroup)#
```

関連コマンド

コマンド	説明
object-group ipv6 address	IPv6 アドレス グループを設定します。
show object-group	オブジェクト グループを表示します。