セキュリティ保護されたブランチ ルータの設定例

目次

概要

このマニュアルでは、次の機能を実装してブランチ ルータをセキュリティ保護するための設定例を示します。

- **Context-Based Access Control（CBAC; コンテキストベース アクセス コントロール）**：CBAC は、ファイアウォール インターフェイスでアクセス リストに一時的な隙間を作成します。このような隙間は、指定されたトラフィックがファイアウォールを通じて内部ネットワークを出るときに作成されます。この隙間によって、通常はブロックされる戻りトラフィックや追加のデータ チャネルがファイアウォールを通じて内部ネットワークに戻ることが可能になります。ただし、こうしたトラフィックがファイアウォールを通じて戻ることができるのは、ファイアウォールから出るときに CBAC をトリガーした元のトラフィックと同じセッションにそのトラフィックが属している場合だけです。
- **Cisco IOS Intrusion Prevention System（IPS; 侵入防御システム）**：Cisco IOS IPS 機能は、既存の Cisco IOS Intrusion Detection System（IDS; 侵入検知システム）を再構成したものであり、これによりお客様は、ルータにデフォルトの組み込みシグニチャをロードするか、*attack-drop.sdf* という Signature Definition File（SDF）をロードするかを選択できます。attack-drop.sdf ファイルには、118 の高性能 IPS シグニチャが保存されており、利用可能な最新のセキュリティ脅威検知機能を提供します。

- **Cisco IOS Firewall Authentication Proxy（Cisco IOS ファイアウォール認証プロキシ）**：認証プロキシは、動的なユーザ別の認証および許可を提供し、業界標準の TACACS+ および RADIUS の認証プロトコルを使用したユーザ認証を実行します。接続に対するユーザ別の認証および許可により、ネットワーク攻撃に対する高度な防御機能が得られます。
- **Firewall Websense URL Filtering（ファイアウォール Websense URL フィルタリング）**：Firewall Websense URL Filtering 機能により、Cisco IOS ファイアウォール（別名「Cisco Secure Integrated Software」）は、Websense URL フィルタリング ソフトウェアと相互運用が可能になり、その結果、いくつかのポリシーに基づき、指定した Web サイトへのユーザ アクセスを防止できます。Cisco IOS ファイアウォールは Websense サーバと連動し、特定の URL に対する許可または拒否（ブロック）を判断します。

はじめに

表記法

表記法の詳細については、「*Conventions Used in Cisco Technical Tips*」を参照してください。

使用されるコンポーネント

このマニュアルの情報は、次のソフトウェアおよびハードウェアのバージョンに基づいています。

- Cisco 2801 ルータ
- Cisco IOS Release 12.3(8)T4
- Advanced IP Services フィーチャ セット

（注） このマニュアルの情報は、特定のラボ環境に置かれたデバイスに基づいて作成されました。このマニュアルで使用されるデバイスはすべて、初期設定（デフォルト）の状態から作業が開始されています。ネットワークが稼動中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

関連製品

この設定は、次のハードウェアにも使用できます。

- Cisco 1800 シリーズ サービス統合型ルータ（モジュラ）
- Cisco 2800 シリーズ サービス統合型ルータ
- Cisco 3800 シリーズ サービス統合型ルータ

埋め込みの Websense URL Filtering Server（UFS）を持つ Cisco Content Engine ネットワーク モジュール（NM-CE-BP）が搭載された Cisco 3800 シリーズ サービス統合型ルータにも、同様の設定を利用できます。

設定

ここでは、このマニュアルで説明する機能を設定するための情報を示します。

ヒント このマニュアルで使用されるコマンドに関する追加情報を検索するには、Command Lookup Tool を使用してください。アクセスするには、Cisco.com のアカウントが必要です。アカウントをお持ちでない場合や、ユーザ名やパスワードを忘れた場合は、ログイン ダイアログボックスで [Cancel] をクリックし、表示される説明に従ってください。

ネットワーク図

このマニュアルでは、次の図に示すネットワーク セットアップを使用します。

IP アドレス 192.168.102.119/24 の HTTP サーバはこの図に示されていません。HTTP サーバは、ネットワーク上のどの場所にも配置できます。この例では、セキュリティ保護されたブランチ ルータのファスト イーサネット 0/1 側に配置されています。

設定

このマニュアルでは、次に示す設定を使用します。

```
router# show running-config
Building configuration...
.
.
.
!---Enable the authentication, authorization, and accounting (AAA) access control model.
aaa new-model
!
!---Identify the Cisco Secure Authentication Control Server (ACS) as a member of a
!---AAA server group. In this example, the AAA server group is called “SJ.”
aaa group server tacacs+ SJ
 server 192.168.101.119
!
!---Enable AAA authentication at login and specify the authentication methods to try.
aaa authentication login default local group SJ none
```

```
!---Restrict user access to the network:
!---(a) Run authorization to determine if the user is allowed to run an EXEC shell.
!---(b) Enable authorization that applies specific security policies on a per-user basis.
!---You must use the "aaa authorization auth-proxy" command together with the
!---"ip auth-proxy <name>" command (later in this configuration). Together, these
!---commands set up the authorization policy to be retrieved by the firewall.
aaa authorization exec default group SJ none
aaa authorization auth-proxy default group SJ
!---Make sure that the same session ID is used for each AAA accounting service type
!---within a call.
aaa session-id common
.
.
.
!---Define a set of inspection rules. In this example, the set is called "myfw."
!---Include each protocol that you want the Cisco IOS firewall to inspect.
ip inspect name myfw cuseeme timeout 3600
ip inspect name myfw ftp timeout 3600
ip inspect name myfw http urlfilter timeout 3600
ip inspect name myfw rcmd timeout 3600
ip inspect name myfw realaudio timeout 3600
ip inspect name myfw smtp timeout 3600
ip inspect name myfw sqlnet timeout 3600
ip inspect name myfw streamworks timeout 3600
ip inspect name myfw tftp timeout 30
ip inspect name myfw udp timeout 15
ip inspect name myfw tcp timeout 3600
ip inspect name myfw vdolive
!
!---(Optional) Set the length of time an authentication cache entry, along with its
!---associated dynamic user access control list, is managed after a period of inactivity.
ip auth-proxy inactivity-timer 120
!---Create an authentication proxy rule; in this example it is named "aprule."
!---Set HTTP to trigger the authentication proxy.
ip auth-proxy name aprule http
!
!---Configure the Cisco IOS Intrusion Protection System (IPS) feature:
!---Specify the location from which the router loads the Signature Definition File (SDF).
!---(Optional) Specify the maximum number of event notifications that are placed
!---in the router's event queue.
!---Disable the audit of any signatures that your deployment scenario deems unnecessary.
!---Name the IPS rule, so that you can apply the rule to an interface.
!---Later in this example, this rule (named "ids-policy") is applied to FE 0/0.
ip ips sdf location tftp://192.168.1.3/attack-drop.sdf
ip ips po max-events 100
ip ips signature 1107 0 disable
ip ips signature 3301 0 disable
ip ips name ids-policy
!
!---Configure the Firewall Websense URL Filtering feature:
!---(Optional) Set the maximum number of destination IP addresses that can be cached
!---into the cache table, which consists of the most recently requested IP addresses
!---and respective authorization status for each IP address.
!---Specify domains for which the firewall should permit or deny all traffic
!---without sending lookup requests to the Firewall Websense URL filtering server (UFS).
!---Specify the IP address of the Firewall Websense UFS.
ip urlfilter cache 0
ip urlfilter exclusive-domain permit www.cisco.com
ip urlfilter server vendor websense 192.168.1.116
.
.
.
```

```
!---Configure the firewall interface that connects to the branch office PCs
!---and the Firewall Websense UFS:
!---Apply access lists and inspection rules to control access to the interface.
!---In this example, access list 116 is used to filter outbound packets, and
!---the inspection rule named "myfw" is used to filter inbound packets.
!---Enable the authentication proxy rule for dynamic, per-user authentication
!---and authorization. See the previous " ⌈aaa authorization auth-proxy default group
SJ⌋ "
!---and " ⌈ip auth-proxy name aprule http⌋ " command entries.
!---Apply the Cisco IPS rule to outbound traffic.
interface FastEthernet0/0
 ip address 192.168.1.2 255.255.255.0
 ip access-group 116 out
 ip inspect myfw in
 ip auth-proxy aprule
 ip ips ids-policy out
.
.
.
!---Configure the interface that connects to the
!---Cisco Secure Authentication Control Server (Cisco Secure ACS).
!---Apply access lists to control access to the interface.
!---In this example, access list 111 is used to filter inbound packets.
interface FastEthernet0/1
 ip address 192.168.101.2 255.255.255.0
 ip access-group 111 in
.
.
.
ip classless
!---The following command establishes a static route to the HTTP server,
!---which in this example has an IP address of 192.168.102.119.
ip route 192.168.102.0 255.255.255.0 FastEthernet0/1
!
!---Enable the HTTP server on your system.
!---Also, specify that the authentication method used for AAA login service
!---should be used for authenticating HTTP server users.
ip http server
ip http authentication aaa
no ip http secure-server
!
!---Configure the access list for the interface that connects to the
!---Cisco Secure ACS.
access-list 111 permit tcp host 192.168.101.119 eq tacacs host 192.168.101.2
access-list 111 permit udp host 192.168.101.119 eq tacacs host 192.168.101.2
access-list 111 permit icmp any any
access-list 111 deny   ip any any
!
!---Configure the access list for the firewall interface that connects to the
!---branch office PCs and the Websense URL Filtering Server (UFS).
access-list 116 permit tcp host 192.168.1.118 host 192.168.1.2 eq www
access-list 116 deny   tcp host 192.168.1.118 any
access-list 116 deny   udp host 192.168.1.118 any
access-list 116 deny   icmp host 192.168.1.118 any
access-list 116 permit tcp 192.168.1.0 0.0.0.255 any
access-list 116 permit udp 192.168.1.0 0.0.0.255 any
access-list 116 permit icmp 192.168.1.0 0.0.0.255 any
!
!
```

```
!---Specify the Cisco Secure ACS, in this case a TACACS+ server.
!---Set the authentication encryption key used for all TACACS+ communications
!---between the access server and the TACACS+ daemon. This key must match the key
!---used on the TACACS+ daemon.
tacacs-server host 192.168.101.119
tacacs-server directed-request
tacacs-server key cisco
!
.
.
.
end
```

確認

ここでは、設定が正しく機能していることを確認するために使用する情報を示します。

- 「Firewall Websense URL Filtering を確認するためのコマンド」（P.6）
- 「Cisco IOS Firewall Authentication Proxy を確認するためのコマンド」（P.7）
- 「Context-Based Access Control を確認するためのコマンド」（P.7）
- 「Cisco IOS Intrusion Prevention System を確認するためのコマンド」（P.8）

ヒント 一部の **show** コマンドは Output Interpreter Tool でサポートされています。このツールを使用すると、**show** コマンド出力の分析結果を表示できます。アクセスするには、Cisco.com のアカウントが必要です。アカウントをお持ちでない場合や、ユーザ名やパスワードを忘れた場合は、ログイン ダイアログ ボックスで [Cancel] をクリックし、表示される説明に従ってください。

Firewall Websense URL Filtering を確認するためのコマンド

- **show ip urlfilter cache**：キャッシュ テーブルにキャッシュできる最大エントリ数と、キャッシュ テーブルにキャッシュされたエントリ数および宛先 IP アドレスを表示します。

```
Router# show ip urlfilter cache

Maximum number of cache entries: 0
Number of entries cached: 0
------------------------------------------------------------
    IP address        Age          Time since last hit
                  (In seconds)      (In seconds)
------------------------------------------------------------
```

- **show ip urlfilter config**：キャッシュ サイズ、未処理の要求の最大数、および許可モードの状態を含む、設定済みのベンダー サーバを表示します。

```
Router# show ip urlfilter config
Websense URL Filtering is ENABLED

Primary Websense server configurations
======================================
Websense server IP address Or Host Name: 192.168.1.116
Websense server port: 15868
Websense retransmission time out: 6 (in seconds)
Websense number of retransmission: 2
```

```
Secondary Websense servers configurations
=========================================
Other configurations
====================
Allow Mode: OFF
System Alert: ENABLED
Audit Trail: DISABLED
Log message on Websense server: DISABLED
Maximum number of cache entries: 0
Maximum number of packet buffers: 200
Maximum outstanding requests: 1000
```

- **show ip urlfilter statistics** : Websense サーバに送信される要求、Websense サーバから受信した応答、システム内で保留中の要求、失敗した要求、ブロックされた URL の数など、URL フィルタリングの統計情報を表示します。

```
Router# show ip urlfilter statistics

URL filtering statistics
========================
Current requests count: 0
Current packet buffer count(in use): 0
Current cache entry count: 0

Maxever request count: 0
Maxever packet buffer count: 0
Maxever cache entry count: 0

Total requests sent to URL Filter Server :13
Total responses received from URL Filter Server :13
Total requests allowed: 9
Total requests blocked: 4
```

Cisco IOS Firewall Authentication Proxy を確認するためのコマンド

- **show ip auth-proxy** : 認証プロキシのエントリまたは設定を表示します。

```
Router# show ip auth-proxy cache

Authentication Proxy Cache
 Client Name admin, Client IP 192.168.1.118, Port 1902, timeout 120, Time Remaining
120, state INIT

Router# show ip auth-proxy statistics

configuration
Authentication global cache time is 120 minutes
Authentication global absolute time is 0 minutes
Authentication Proxy Watch-list is disabled

Authentication Proxy Rule Configuration
 Auth-proxy name aprule
    http list not specified auth-cache-time 120 minutes
```

Context-Based Access Control を確認するためのコマンド

- **show ip access-list** : 現在の IP アクセス リストの内容を表示します。
- **show ip inspect session** : CBAC セッションの情報を表示します。

Cisco IOS Intrusion Prevention System を確認するためのコマンド

- **show ip ips signature** : 無効にされ、削除対象としてマークされているシグニチャなど、Cisco IPS のシグニチャ情報を表示します。

```
Router# show ip ips signature

Signatures were last loaded from tftp://192.168.1.3/attack-drop.sdf

SDF release version not available

*=Marked for Deletion  Action=(A)larm,(D)rop,(R)eset   Trait=AlarmTraits
MH=MinHits             AI=AlarmInterval                CT=ChokeThreshold
TI=ThrottleInterval    AT=AlarmThrottle                FA=FlipAddr
WF=WantFrag            Ver=Signature Version

Signature Micro-Engine: SERVICE.SMTP (1 sigs)
 SigID:SubID On Action  Sev Trait     MH    AI    CT    TI AT FA WF Ver
 ----------- -- ------ ---- -----  ----- ----- ----- ----- -- -- -- ---
  3129:0      Y   ADR   MED     0      0     0     0    15 FA  N    S59

Signature Micro-Engine: SERVICE.RPC (29 sigs)
 SigID:SubID On Action  Sev Trait     MH    AI    CT    TI AT FA WF Ver
 ----------- -- ------ ---- -----  ----- ----- ----- ----- -- -- -- ---
  6100:0      Y   AD   HIGH     0      0     0   100    30 FA  N    1.0
  6100:1      Y   ADR  HIGH     0      0     0   100    30 FA  N    1.0
  6101:0      Y   AD   HIGH     0      0     0   100    30 FA  N    1.0
  6101:1      Y   ADR  HIGH     0      0     0   100    30 FA  N    1.0
  6104:0      Y   AD   HIGH     0      0     0   100    30 FA  N    2.2
  6104:1      Y   ADR  HIGH     0      0     0   100    30 FA  N    2.2
  6105:0      Y   AD   HIGH     0      0     0   100    30 FA  N    2.2
  6105:1      Y   ADR  HIGH     0      0     0   100    30 FA  N    2.2
  6188:0      Y   AD   HIGH     0      0     0   100    30 FA  N    S43
  6189:0      Y   AD   HIGH     0      0     0   100    30 FA  N    S43
  6189:1      Y   ADR  HIGH     0      0     0   100    30 FA  N    S43
  6190:0      Y   AD   HIGH     0      0     0   100    30 FA  N    2.1
  6190:1      Y   ADR  HIGH     0      0     0   100    30 FA  N    2.1
  6191:0      Y   AD   HIGH     0      0     0   100    30 FA  N    2.1
  6191:1      Y   ADR  HIGH     0      0     0   100    30 FA  N    2.1
  6192:0      Y   AD   HIGH     0      0     0   100    30 FA  N    2.1
  6192:1      Y   ADR  HIGH     0      0     0   100    30 FA  N    2.1
  6193:0      Y   AD   HIGH     0      0     0   100    30 FA  N    2.2
  6193:1      Y   ADR  HIGH     0      0     0   100    30 FA  N    2.2
  6194:0      Y   AD   HIGH     0      0     0   100    30 FA  N    2.2
  6194:1      Y   ADR  HIGH     0      0     0   100    30 FA  N    2.2
  6195:0      Y   AD   HIGH     0      0     0   100    30 FA  N    2.2
  6195:1      Y   ADR  HIGH     0      0     0   100    30 FA  N    2.2
  6196:0      Y   AD   HIGH     0      0     0   100    30 FA  N    S4
  6196:1      Y   ADR  HIGH     0      0     0   100    30 FA  N    S4
  6197:0      Y   ADR  HIGH     0      0     0   100    30 FA  N    S9
  6197:1      Y   AD   HIGH     0      0     0   100    30 FA  N    S9
  6276:0      Y   AD   HIGH     0      0     0   100    30 FA  N    S30
  6276:1      Y   ADR  HIGH     0      0     0   100    30 FA  N    S30

Signature Micro-Engine: SERVICE.HTTP (23 sigs)
 SigID:SubID On Action  Sev Trait     MH    AI    CT    TI AT FA WF Ver
 ----------- -- ------ ---- -----  ----- ----- ----- ----- -- -- -- ---
  3140:3      Y   ADR  HIGH     0      1     0     0    15 FA  N    S80
  3140:4      Y   ADR  HIGH     0      1     0     0    15 FA  N    S80
  5045:0      Y   ADR  HIGH     0      1     0     0    15 FA  N    2.2
  5047:0      Y   ADR  HIGH     0      1     0     0    15 FA  N    2.2
  5055:0      Y   AD   HIGH     0      1     0     0    15 FA  N    2.2
  5071:0      Y   ADR  HIGH     0      1     0     0    15 FA  N    2.2
```

```
 5081:0      Y   ADR   MED     0      1      0      0    15 FA  N    2.2
 5114:0      Y   ADR   MED     0      1      0      0    15 FA  N    2.2
 5114:1      Y   ADR   MED     0      1      0      0    15 FA  N    2.2
 5114:2      Y   ADR   MED     0      1      0      0    15 FA  N    2.2
 5126:0      Y   ADR   MED     0      1      0      0    15 FA  N    S5
 5159:0      Y   ADR  HIGH     0      1      0      0    15 FA  N    S7
 5184:0      Y   ADR  HIGH     0      1      0      0    15 FA  N    S12
 5188:0      Y   ADR  HIGH     0      1      0      0    15 FA  N    S12
 5188:1      Y   ADR  HIGH     0      1      0      0    15 FA  N    S12
 5188:2      Y   ADR  HIGH     0      1      0      0    15 FA  N    S12
 5188:3      Y   ADR  HIGH     0      1      0      0    15 FA  N    S12
 5245:0      Y   ADR   MED     0      1      0      0    15 FA  N    S21
 5326:0      Y   ADR  HIGH     0      1      0      0    15 FA  N    S30
 5329:0      Y   ADR  HIGH     0      1      0      0    15 FA  N    1.0
 5364:0      Y   ADR  HIGH     0      1      0      0    15 FA  N    S43
 5390:0      Y   ADR   MED     0      1      0      0    15 FA  N    S54
 5400:0      Y   ADR  HIGH     0      1      0      0    15 FA  N    S71

Signature Micro-Engine: ATOMIC.TCP (42 sigs)
 SigID:SubID On Action  Sev Trait     MH    AI    CT    TI AT FA WF Ver
 ---------- -- ------ ---- -----  ----- ----- ----- ----- -- -- -- ---
 3038:0      Y   AD   HIGH     0      0      0   100    30 FA  N  Y 2.2
 3039:0      Y   AD   HIGH     0      0      0   100    30 FA  N  Y 2.2
 3040:0      Y   AD   HIGH     0      0      0   100    30 FA  N  N 2.2
 3041:0      Y   AD   HIGH     0      0      0   100    30 FA  N  N 2.2
 3043:0      Y   AD   HIGH     0      0      0   100    30 FA  N  Y 2.2
 3300:0      Y   AD   HIGH     0      0      0   100    30 FA  N    2.1
 9200:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S40
 9201:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S40
 9202:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S40
 9203:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S40
 9204:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S40
 9205:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S40
 9206:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S40
 9207:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S40
 9208:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S40
 9209:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S40
 9210:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S40
 9211:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S40
 9212:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S40
 9213:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S40
 9214:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S40
 9215:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S40
 9216:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S40
 9217:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S40
 9218:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S40
 9223:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S40
 9224:0      Y   AD    MED     0      0      0   100    30 FA  N    S44
 9225:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S46
 9226:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S46
 9227:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S46
 9228:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S46
 9229:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S46
 9230:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S46
 9231:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S66
 9232:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S69
 9233:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S67
 9236:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S71
 9237:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S71
 9238:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S71
 9239:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S76
 9240:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S79
 9241:0      Y   AD   HIGH     0      0      0   100    30 FA  N    S82
```

```
Signature Micro-Engine: ATOMIC.IPOPTIONS (1 sigs)
 SigID:SubID On Action   Sev Trait     MH    AI    CT    TI AT FA WF Ver
 ----------- -- ------ ---- -----  ----- ----- ----- ----- -- -- -- ---
  1006:0      Y   AD   HIGH     0      0     0   100    30 FA  N    2.1

Signature Micro-Engine: ATOMIC.L3.IP (4 sigs)
 SigID:SubID On Action   Sev Trait     MH    AI    CT    TI AT FA WF Ver
 ----------- -- ------ ---- -----  ----- ----- ----- ----- -- -- -- ---
  1102:0      Y   AD   HIGH     0      0     0   100    30 FA  N    2.1
  1104:0      Y   AD   HIGH     0      0     0   100    30 FA  N    2.2
  1108:0      Y   AD   HIGH     0      0     0   100    30 GS  N    S27
  2154:0      Y   AD   HIGH     0      0     0   100    30 FA  N  Y 1.0
Total Active Signatures: 118
Total Inactive Signatures: 0
```

トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

次のマニュアルを参照してください。

- 『*Troubleshooting CBAC Configurations*』テクニカル ノート
- 『*Troubleshooting Authentication Proxy*』テクニカル ノート

トラブルシューティング コマンド

（注） **debug** コマンドを実行する前に、『*Important Information on Debug Commands*』を参照してください。

- **debug ip inspect**：Cisco IOS ファイアウォール イベントに関するメッセージを表示します。
- **debug ip urlfilter**：URL フィルタ サブシステムのデバッグ情報をイネーブルにします。

```
Router# debug ip urlfilter detailed

Urlfilter Detailed Debugs debugging is on
Router#
*Aug 26 20:11:58.538: URLF: got cache idle timer event...
*Aug 26 20:11:58.538: URLF: cache table is about to overflow, delete idle entries
*Aug 26 20:12:00.962: URLF: creating uis 0x64EF00A0, pending request 1
*Aug 26 20:12:00.962: URLF: domain name not found in the exclusive list
*Aug 26 20:12:00.962: URLF: got an cbac queue event...
*Aug 26 20:12:00.962: URLF: websns making a lookup request.
*Aug 26 20:12:00.962: URLF: socket send successful...
*Aug 26 20:12:00.962: URLF: holding pak 0x64823210 (192.168.101.119:80) ->
192.168.1.118:1087 seq 3905567052 wnd 17238
*Aug 26 20:12:00.966: URLF: got a socket read event...
*Aug 26 20:12:00.966: URLF: socket recv (header) successful.
*Aug 26 20:12:00.966: URLF: socket recv (data) successful.
*Aug 26 20:12:00.966: URLF: websns lookup code = 1
*Aug 26 20:12:00.966: URLF: websns lookup description code = 1027
*Aug 26 20:12:00.966: URLF: websns category number = 67
*Aug 26 20:12:00.966: URLF: websns cache command = 0
*Aug 26 20:12:00.966: URLF: websns cached entry type = 0
*Aug 26 20:12:00.966: URLF: Site/URL Blocked: sis 0x64A57D50, uis 0x64EF00A0
*Aug 26 20:12:00.966: URLF: Sent Deny page with FIN to client and RST to server
```

```
*Aug 26 20:12:00.966: URLF: urlf_release_http_resp_for_url_block - Discarding the pak
0x64823210 held in resp Q (count 1 : thrld 200)
*Aug 26 20:12:00.966: URLF: deleting uis 0x64EF00A0, pending requests 0
```

- **debug ip auth-proxy**：認証プロキシのアクティビティを表示します。

```
Router# debug ip auth-proxy detailed

*Aug 30 23:16:07.680: AUTH-PROXY:proto_flag=4, dstport_index=4
*Aug 30 23:16:07.680:  SYN SEQ 24350097 LEN 0
*Aug 30 23:16:07.680: dst_addr 192.168.102.119 src_addr 192.168.1.118 dst_port 80
src_port 1900
*Aug 30 23:16:07.680: AUTH-PROXY:auth_proxy_half_open_count++ 1
*Aug 30 23:16:07.684: AUTH-PROXY:proto_flag=4, dstport_index=4
*Aug 30 23:16:07.684:  ACK 2787182962 SEQ 24350098 LEN 0
*Aug 30 23:16:07.684: dst_addr 192.168.102.119 src_addr 192.168.1.118 dst_port 80
src_port 1900
*Aug 30 23:16:07.684: clientport 1900 state 0
*Aug 30 23:16:07.684: AUTH-PROXY:proto_flag=4, dstport_index=4
*Aug 30 23:16:07.684:  PSH ACK 2787182962 SEQ 24350098 LEN 282
*Aug 30 23:16:07.684: dst_addr 192.168.102.119 src_addr 192.168.1.118 dst_port 80
src_port 1900
*Aug 30 23:16:07.684: clientport 1900 state 0
*Aug 30 23:16:07.688: AUTH-PROXY:proto_flag=4, dstport_index=4
*Aug 30 23:16:07.688:  ACK 2787184131 SEQ 24350380 LEN 0
```

関連情報

- 『*Cisco IOS Security Configuration Guide*』Release 12.3
  - 「Configuring Context-Based Access Control」の章
  - 「Configuring Authentication Proxy」の章
- 『*Cisco IOS Intrusion Prevention System (IPS)*』、Cisco IOS Release 12.3(8)T フィーチャ モジュール
- 『*Firewall Websense URL Filtering*』Cisco IOS Releases 12.2(11)YU および 12.2(15)T フィーチャ モジュール
- 『*Troubleshooting CBAC Configurations*』テクニカル ノート
- 『*Troubleshooting Authentication Proxy*』テクニカル ノート
- テクニカル サポート：シスコシステムズ